Lineární algebra

Libor Barto a Jiří Tůma

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

Toto jsou vznikající skripta k přednáškám Lineární algebra a geometrie 1 a Lineární algebra a geometrie 2. Pokud naleznete jakoukoliv chybu, dejte nám určitě vědět!

Verze z 18. října 2024

Jak používat tato skripta

Na úvod máme několik rad pro čtenáře a čtenářky těchto skript, kteří je používají pro studium předmětu Lineární algebra na Matfyzu.

- Vašim cílem není naučit se skripta nazpaměť (to by k ničemu nebylo), ale pochopit, co různé pojmy znamenají, jaké mají vlastnosti, jak je používat a jak spolu souvisí. Čím lépe budete učivu rozumět, tím méně informací si budete muset pamatovat.
- Obecné pojmy a tvrzení jdou nejlépe pochopit na příkladech, a proto tvoří velkou část skript. Nevynechávejte je, ani je neodkládejte na později.
- K pochopení jaké mají pojmy vlastnosti a jak spolu souvisí (což je náplní tvrzení) je nejprve nutné dobře chápat, co *přesně* pojmy znamenají (to říkají definice). Přesný význam lze někdy těžko odhadnout z pojmenování (např. algebraický význam pojmu těleso) a jindy může být trochu jiný, než velí vaše intuice (v tom případě se ptejte proč).
- Pro získání základního přehledu je možná dobré si nejprve studovanou část skript rychle projít. K dobrému pochopení učiva je ale potřeba studovat *aktivně*. Matematika se nedá naučit jinak, než že ji člověk dělá.
  - Mějte po ruce papír a tužku. Provádějte si výpočty (samostatným výpočtem se naučíte více než čtením ze skript), kreslete si obrázky (naučíte se více než prohlížením obrázků ve skriptech), zkuste si samostatně formulovat definice nebo tvrzení, tvořte si vlastní stručná shrnutí.
  - Snažte se skripta předbíhat. Při diskuzi speciální situace (např. řešení konkrétní soustavy rovnic) zkuste nejprve problém vyřešit sami. Zamyslete se, jak by se situace dala zobecnit (např. na řešení obecné soustavy) a jaké při tom mohou vzniknout záludnosti (např. co když je koeficient u neznámé x nula).

    Před přečtením definice nějakého pojmu se zamyslete, co by mohl znamenat (například matice v odstupňovaném tvaru). Po přečtení definice se zamyslete, zda byl váš odhad správný (případně v čem se liší a proč), jaké jsou příklady (např. několik matic v odstupňovaném tvaru) a ne-příklady (např. matice, které v odstupňovaném tvaru nejsou). Vyplatí se rovněž promyslet "degenerované" případy (např. nulová matice, matice s jedním řádkem). Pak se teprve podívejte (a zamyslete se!) na příklady ve skriptech.

    Po přečtení tvrzení se zamyslete, jak ho můžete použít a kdy ho naopak použít nelze. Také zkuste vymyslet, jak byste ho asi dokazovali. Hlavně zpočátku to asi moc nepůjde, ale když budete s důkazy aktivně zápasit, tak se vám dokazování dostane do krve mnohem rychleji, než když budete důkazy jenom pasivně číst.
  - Diskutujte učivo se spolužáky a *nebojte se zeptat* vyučujících. Pokud vám něco není jasné nebo si třeba jen nejste jistí tím, že něčemu správně rozumíte, stejný pocit má nejspíše i mnoho jiných studentů.
- Části psané

malým bezpatkovým písmem

pojednávají o aplikacích, souvislostech a doplňujících tématech. Doufáme, že pro vás budou zajímavé a objasní, proč se to či ono učíte, ale pro absolvování předmětu nejsou nezbytné. Proto jim nemusíte věnovat tolik energie jako ostatní látce.

- Je žádoucí ve skriptech vyhledávat a přeskakovat sem a tam. S vyhledáváním definic pojmů vám může pomoci *rejstřík*, který najdete na konci skript. Alternativně můžete využít fulltextové vyhledávání v prohlížeči PDF souborů.

KAPITOLA 1

Opakování

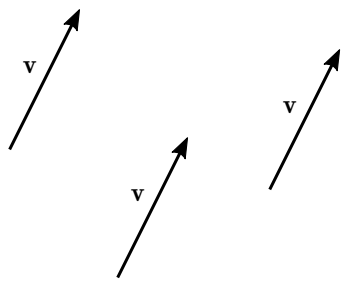
Cíl. *Zopakujeme si základy analytické geometrie v rovině a prostoru, počítání s komplexními čísly a pojem zobrazení.*

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

Zopakujeme si základy analytické geometrie, zejména rovnici přímky v rovině a roviny v prostoru a jejich parametrický tvar. V druhé části připomeneme počítání s komplexními čísly. Ukážeme si geometrickou interpretaci komplexních čísel a geometrický význam jejich součtu a součinu. Nakonec připomeneme pojem zobrazení a příslušnou základní terminologii.

1.1. Základní geometrické pojmy

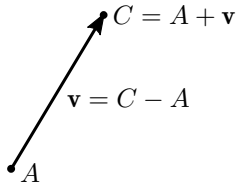
Ve fyzice je vektor veličina, která má směr a velikost. Vektory obvykle znázorňujeme geometricky jako orientované úsečky (stručněji a méně přesně říkáme také šipky). Jeden a ten samý vektor $\mathbf{v}$ můžeme znázornit různými orientovanými úsečkami, pokud mají stejný směr, délku (také se říká velikost) a orientaci. Vektory budeme označovat malými tučnými písmeny.



Obrázek 1.1. Různé šipky znázorňující stejný vektor

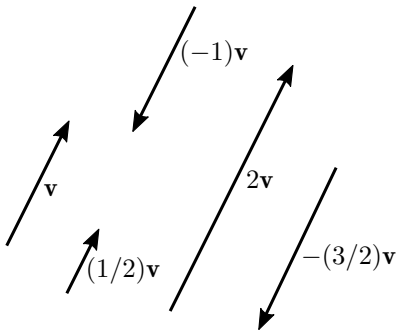
Fyzikální vektor, např. síla, může působit v nějakém bodě A. Geometricky to vyjádříme tak, že počáteční bod orientované úsečky znázorňující vektor $\mathbf{v}$ umístíme do bodu A. Tím je jednoznačně určený koncový bod této úsečky, na obrázku 1.2 je označený jako C. Říkáme také, že C je koncový bod vektoru $\mathbf{v}$ s počátečním bodem A. Stručně to zapisujeme jako $C = A + \mathbf{v}$. Orientovaná úsečka znázorňující vektor $\mathbf{v}$ je jednoznačně určená svým počátečním bodem A a koncovým bodem C, což vyjadřujeme rovností $\mathbf{v} = C - A$.

Vektory můžeme násobit reálnými čísly. Vektor $2\mathbf{v}$ má stejný směr a orientaci jako vektor $\mathbf{v}$, má ale dvojnásobnou délku. Podobně vektor $(1/2)\mathbf{v}$ má poloviční délku oproti $\mathbf{v}$, stejný směr a orientaci. Vektor $(-1)\mathbf{v}$ má stejný směr a délku jako $\mathbf{v}$, má ale opačnou orientaci. Opačný vektor k vektoru $\mathbf{v}$ také stručněji zapisujeme



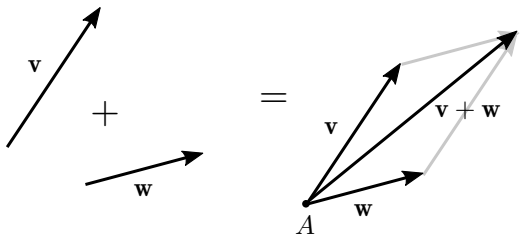
Obrázek 1.2. Počáteční a koncový bod vektoru

$-\mathbf{v}$. Násobek $0\mathbf{v}$ je *nulový vektor*. Nulový vektor jako jediný nemá jednoznačně určený směr.



Obrázek 1.3. Násobky vektoru

Vektory umíme také sčítat. Dva vektory $\mathbf{v}$ a $\mathbf{w}$ sečteme tak, že je umístíme do společného počátečního bodu A a doplníme na rovnoběžník (v případě, že je jeden z vektorů násobkem druhého, bude rovnoběžník degenerovaný). Součet $\mathbf{v} + \mathbf{w}$ je vektor s počátečním bodem A, který má směr, délku a orientaci úhlopříčky v tomto rovnoběžníku.

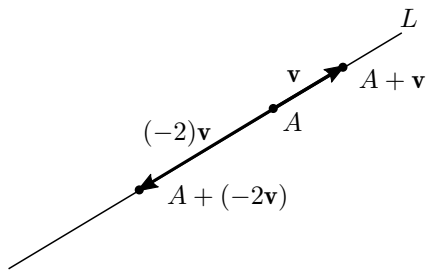


Obrázek 1.4. Součet vektorů

Přímku v rovině nebo 3D prostoru můžeme zadat mnoha různými způsoby. Jednou z možností je zadat dva různé body přímky. V dalším textu budeme často

používat zadání přímky pomocí jednoho bodu A a směrového vektoru $\mathbf{v}$. Takto zadanou přímku L pak tvoří koncové body všech násobků $t\mathbf{v}$ vektoru $\mathbf{v}$ s počátečním bodem A, tj.

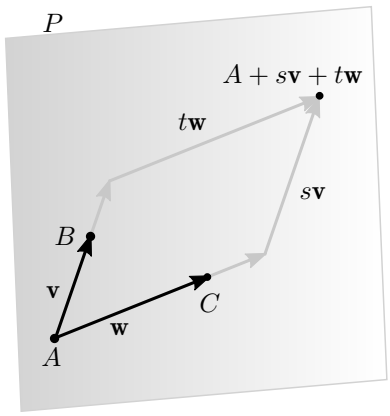
$$L = \{A + t\mathbf{v} : t \in \mathbb{R}\} \ .$$



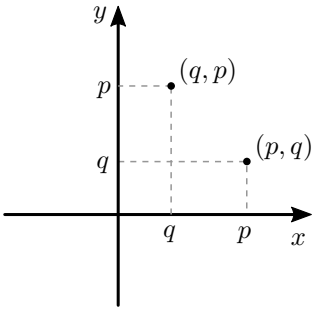
Obrázek 1.5. Přímka určená bodem a směrovým vektorem

Obvyklý způsob jak určit rovinu v 3D prostoru je zadat tři body, které neleží na jedné přímce. Jinou možností je zadat jeden bod A a dvojici vektorů $\mathbf{v}$ a $\mathbf{w}$, které nemají stejný směr (tím je vyloučena také možnost, že by jeden z těchto vektorů byl nulový). Vektor $\mathbf{v}$ s počátečním bodem A má nějaký koncový bod B a vektor $\mathbf{w}$ s tím samým počátečním bodem A má koncový bod C. Body A, B, C neleží na jedné přímce, protože vektory $\mathbf{v}$ a $\mathbf{w}$ nemají stejný směr (neboli ani jeden z nich nejde získat jako násobek druhého), a proto určují nějakou rovinu P. Leží v ní koncové body všech vektorů $s\mathbf{v} + t\mathbf{w}$ s počátečním bodem A, kde s, t jsou libovolná reálná čísla. Rovinu P tak můžeme napsat jako množinu bodů

$$P = \{A + (s\mathbf{v} + t\mathbf{w}) : s, t \in \mathbb{R}\} \ .$$



Obrázek 1.6. Rovina určená bodem a dvojicí směrových vektorů

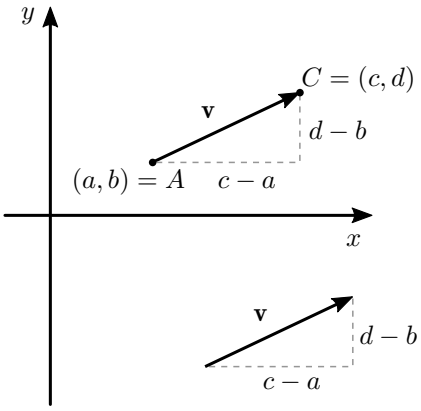


Obrázek 1.7. Souřadnice bodu v rovině

1.2. Analytická geometrie v rovině

1.2.1. 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) odpovídají různé body v rovině.

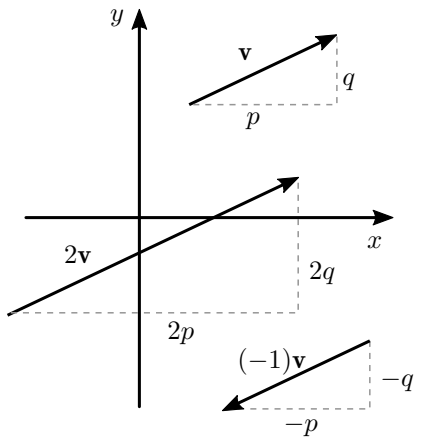
Je-li $\mathbf{v}$ vektor v rovině s počátečním bodem $A = (a, b)$ a koncovým bodem $C = (c, d)$, pak za jeho souřadnice považujeme uspořádanou dvojici $(c - a, d - b)$ reálných čísel. Souřadnice vektoru $\mathbf{v}$ nezávisí na volbě počátečního bodu a jsou definované tak, aby zachovaly rovnost $\mathbf{v} = C - A$ při přechodu k souřadnicím. Z této definice také okamžitě vyplývá, že souřadnice (c, d) koncového bodu C dostaneme jako součet souřadnic (a, b) počátečního bodu A se souřadnicemi $(c - a, d - b)$ vektoru $\mathbf{v}$. Rovnost $C = A + \mathbf{v}$ také zůstává v platnosti po přechodu od bodů a vektorů k jejich souřadnicím.



Obrázek 1.8. Souřadnice vektoru v rovině

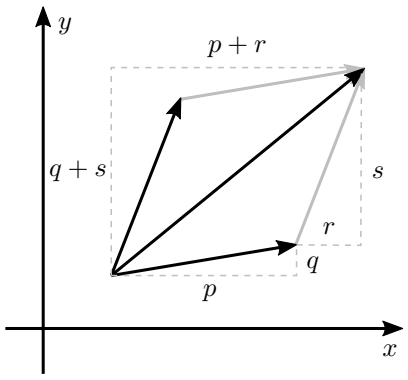
Podobně další operace s vektory mají přirozené analogie v algebraických operacích s jejich souřadnicemi. Má-li vektor $\mathbf{v}$ souřadnice (p, q), pak jeho násobek $t\mathbf{v}$ má souřadnice (tp, tq). Pokud definujeme součin čísla s uspořádanou dvojicí čísel tak, že číslem vynásobíme každou složku, dostáváme rovnost $(tp, tq) = t(p, q)$. Můžeme

tak říct, že souřadnice součinu čísla t s vektorem $\mathbf{v}$ se rovnají součinu čísla t se souřadnicemi vektoru $\mathbf{v}$.



Obrázek 1.9. Souřadnice násobku vektoru

Stejně tak souřadnice součtu dvou vektorů se rovnají součtu souřadnic těchto vektorů po složkách, zdůvodnění je na obrázku 1.10.

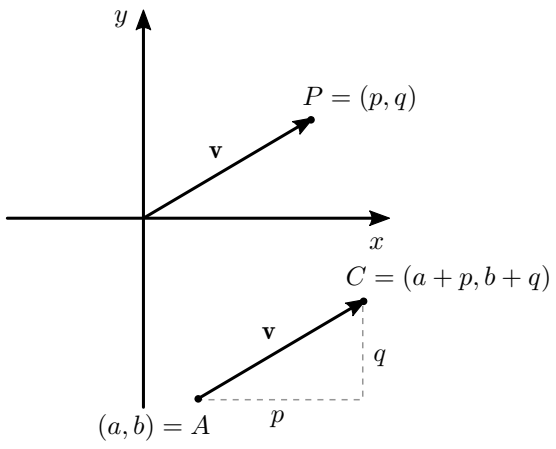


Obrázek 1.10. Souřadnice součtu vektorů

Každá uspořádaná dvojice (p, q) reálných čísel naopak určuje jednoznačně nějaký vektor $\mathbf{v}$ v rovině. Počáteční bod $A = (a, b)$ orientované úsečky znázorňující vektor $\mathbf{v}$ můžeme zvolit libovolně, koncový bod C má potom souřadnice $(a+p, b+q)$. Pokud za počáteční bod zvolíme počátek souřadnic $(0, 0)$, pak mluvíme o *polohovém vektoru* bodu (p, q).

Každé uspořádané dvojici reálných čísel (p, q) tak odpovídá buď nějaký bod $P = (p, q)$ nebo nějaký vektor $\mathbf{v} = (p, q)$ 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 $(0, 0)$.



Obrázek 1.11. Polohový vektor bodu P

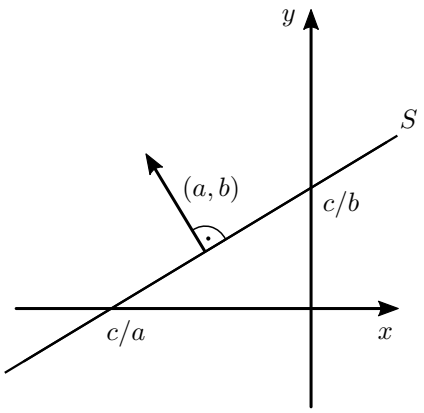
1.2.2. Rovnice přímky a parametrický tvar přímky v rovině. Každé řešení jedné lineární rovnice o dvou neznámých

$$ax + by = c$$

je nějaká uspořádaná dvojice reálných čísel (x, y). Množina S všech řešení takové rovnice je nějaká množina uspořádaných dvojic reálných čísel

$$S = \{(x, y) \in \mathbb{R}^2 : ax + by = c\} \ .$$

Tyto dvojice můžeme považovat za souřadnice bodů v rovině. Množina všech bodů v rovině, jejichž souřadnice jsou řešením uvedené rovnice, tvoří přímku (pokud je aspoň jeden z koeficientů a, b nenulový). Vektor o souřadnicích (a, b) je kolmý na přímku určenou touto rovnicí.



Obrázek 1.12. Rovnice přímky

Vlastnosti množiny všech řešení rovnice $ax + by = c$ uvedené v předchozím odstavci snadno ověříme tak, že rovnici vyřešíme. Ukážeme si to na jednoduchém příkladu.

Příklad 1.1. Najdeme všechna řešení rovnice

$$x + 2y = 3 \ .$$

Z rovnice vypočteme neznámou x,

$$x = 3 - 2y \ .$$

Odtud vidíme, že zvolíme-li jako hodnotu neznámé y libovolné reálné číslo t, můžeme pak jednoznačně vypočítat hodnotu $x = 3 - 2t$. Každé řešení rovnice tak můžeme zapsat ve tvaru uspořádané dvojice

$$(x, y) = (3 - 2t, t) \ ,$$

kde t je libovolné reálné číslo, a všechny takové dvojice rovnici řeší (ověříme dosazením), tj.

$$S = \{(3 - 2t, t) : t \in \mathbb{R}\} \ .$$

Uspořádanou dvojici $(3 - 2t, t)$ vyjádříme jako součet

$$(3 - 2t, t) = (3, 0) + (-2t, t) = (3, 0) + t(-2, 1) \ .$$

Množinu S všech řešení rovnice $x + 2y = 3$ tak můžeme rovněž zapsat jako

$$S = \{(3, 0) + t(-2, 1) : t \in \mathbb{R}\} \ .$$

Tento zápis připomíná zadání přímky pomocí bodu a směrového vektoru. Skutečně, uspořádanou dvojici $(3, 0)$ můžeme považovat za souřadnice bodu A v rovině a dvojici $(-2, 1)$ za souřadnice vektoru $\mathbf{v}$ v rovině. Množina S je potom množina souřadnic všech bodů ležících na přímce

$$L = \{A + t\mathbf{v} : t \in \mathbb{R}\} \ .$$

Zbývá ještě ověřit, že vektor $(1, 2)$ koeficientů rovnice je kolmý na přímku L. K tomu stačí ověřit, že vektor $(1, 2)$ je kolmý na směrový vektor $\mathbf{v} = (-2, 1)$ přímky L. Spočteme proto jejich skalární součin

$$1 \cdot (-2) + 2 \cdot 1 = 0$$

a rovnost 0 dokazuje, že vektory $(1, 2)$ a $\mathbf{v} = (-2, 1)$ jsou opravdu kolmé. ▲

Jakkoliv je tento příklad speciální, obsahuje všechno, co je třeba k ověření, že množinu všech řešení jakékoliv rovnice

$$ax + by = c \ ,$$

tvoří body nějaké přímky, pokud je aspoň jeden z koeficientů a, b nenulový. Můžeme bez újmy na obecnosti předpokládat, že je to koeficient u neznámé x. Pokud by tomu tak nebylo, stačí zaměnit označení neznámých (a také souřadných os). A protože množina řešení rovnice se nezmění, vynásobíme-li ji nenulovým číslem, vynásobíme ji číslem a^{-1} inverzním k a. Dostaneme tak rovnici, která má stejnou množinu řešení jako $ax + by = c$, a má navíc koeficient u neznámé x rovný 1.

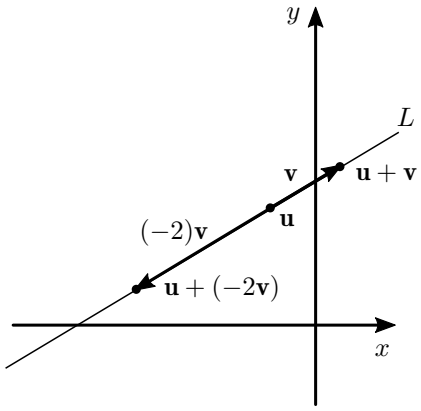
V následujících kapitolách budeme uspořádané dvojice (trojice, čtveřice, atd.) nazývat *aritmetické vektory*, abychom je odlišili od dosud používaných "geometrických"vektorů znázorňovaných orientovanými úsečkami, nebo "fyzikálních"vektorů. Každý aritmetický vektor (a, b) tak můžeme interpretovat jako souřadnice bodu nebo jako souřadnice geometrického vektoru v rovině. Rozdílnou intepretaci aritmetických vektorů pak vyjadřujeme slovně tak, že mluvíme o *bodu* (a, b) nebo o *vektoru* (a, b). Aritmetické vektory budeme označovat stejně jako geometrické vektory malými tučnými písmeny. Aritmetické vektory mají tu výhodu, že s nimi lze počítat, tj. násobit číslem nebo sčítat, pokud mají stejně složek. Bez ohledu na to, kolik těch složek je. Zatímco geometrické vektory můžeme pouze kreslit, což lze dobře v rovině, o něco hůře v 3D prostoru, a už vůbec to nejde v prostorech čtvrté nebo vyšší dimenze. Do prostorů vyšší dimenze sice nevidíme zrakem, ale můžeme do nich nahlédnout pomocí počítání s aritmetickými vektory.

Přímku v rovině zadanou nějakým bodem $A = (a, b)$ a směrovým vektorem $\mathbf{v} = (p, q)$ tak máme definovanou pomocí dvou aritmetických vektorů $\mathbf{u} = (a, b)$,

který interpretujeme jako souřadnice bodu A, a $\mathbf{v} = (p, q)$, který intepretujeme jako vektor v rovině. Přímku pak tvoří body (se souřadnicemi)

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

Tomuto vyjádření říkáme *parametrický tvar přímky* v rovině.



Obrázek 1.13. Parametrický tvar přímky

Vyřešit lineární rovnici o dvou neznámých tak znamená přejít od zadání přímky rovnicí k zadání té samé přímky v parametrickém tvaru. V praxi se často setkáváme s tím, že přímka není zadaná ani jedním z těchto způsobů. Kromě zadání pomocí dvou různých bodů můžeme přímku v rovině zadat také například tím, že je kolmá na nějaký nenulový vektor $\mathbf{v}$ a má od nějakého bodu A danou vzdálenost d, neboli že je tečnou dané kružnice o poloměru d v daném bodě. Máme-li najít souřadnice průsečíku dvou složitěji zadaných přímek, je obvyklou cestou najít napřed rovnice těchto přímek, a pak vyřešit soustavu tvořenou těmito rovnicemi.

V následujícím příkladu si ukážeme jak najít rovnici přímky definované dvojicí různých bodů.

Příklad 1.2. Najdeme rovnici a parametrický tvar přímky L, která prochází body $A = (1, 1)$ a $C = (-2, 3)$.

Snazší je vyjádřit přímku v parametrickém tvaru. Za vektor $\mathbf{u}$ zvolíme souřadnice $(1, 1)$ (polohového vektoru) bodu A. Vektorem $\mathbf{v}$ bude vektor s počátečním bodem A a koncovým bodem C, tj. $\mathbf{v} = (-2, 3) - (1, 1) = (-3, 2)$. Parametrický tvar přímky L je proto

$$\{\mathbf{u} + t\mathbf{v} : t \in \mathbb{R}\} = \{(1, 1) + t(-3, 2) : t \in \mathbb{R}\} \ .$$

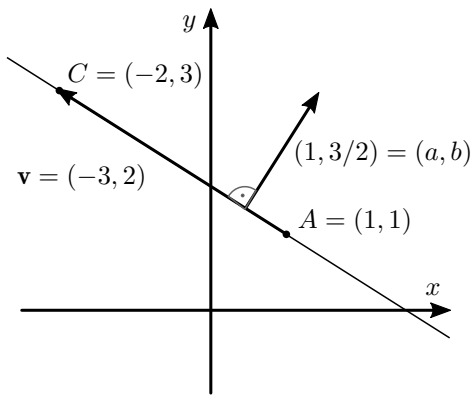
Pro nalezení rovnice $ax+by = c$ přímky L využijeme toho, že vektor koeficientů (a, b) musí být kolmý na směr přímky S, tj. na její směrový vektor $(-3, 2)$. Můžeme zvolit třeba $(a, b) = (2, 3)$ (nebo jako na obrázku vektor $(a, b) = (1, 3/2)$). Hledáme tak rovnici ve tvaru

$$2x + 3y = c \ .$$

Pravou stranu c dostaneme tak, že do rovnice dosadíme souřadnice nějakého bodu přímky L. Dosadíme souřadnice bodu $A = (1, 1)$. Dostaneme

$$2 \cdot 1 + 3 \cdot 1 = c \ ,$$

tj. $c = 5$. Přímka L tak má rovnici $2x + 3y = 5$. O správnosti se můžeme přesvědčit například dosazením souřadnic bodu C, který také musí rovnici splňovat.



Obrázek 1.14. Rovnice a parametrický tvar přímky z příkladu

Také bychom mohli hledat rovnici přímky přímo bez parametrického tvaru. V tom případě bychom vyšli z obecného tvaru rovnice přímky v rovině

$$ax + by = c \ .$$

Neznámé koeficienty a, b a pravou stranu c bychom pak našli jako nějaké řešení soustavy dvou lineárních rovnic o třech neznámých, které dostaneme dosazením souřadnic bodů A, C do této rovnice. Body na přímce leží, takže musí splňovat její rovnici. Dostaneme tak soustavu

$$\begin{aligned} a \cdot 1 + b \cdot 1 &= c \\ a \cdot (-2) + b \cdot 3 &= c \ , \end{aligned}$$

která má nekonečně mnoho řešení a můžeme zvolit kterékoliv nenulové řešení za koeficienty a, b, c v rovnici hledané přímky. To odpovída tomu, že rovnice přímky není určena jednoznačně, z jakékoliv rovnice dostaneme ty další vynásobením nenulovými čísly. ▲

Ukážeme si ještě jak najít rovnici osy úsečky. Složitější způsoby zadání přímek budeme řešit později.

Příklad 1.3. Najdeme rovnici a parametrický tvar osy L úsečky s krajními body $A = (1, -2)$ a $B = (3, 2)$.

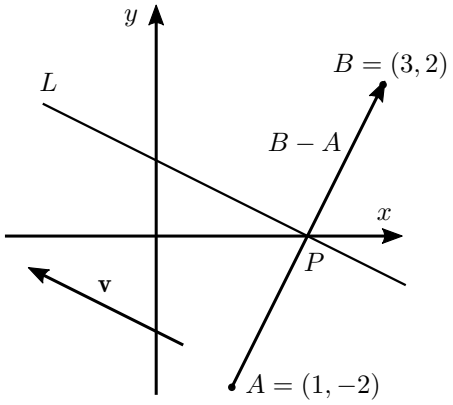
Začneme parametrickým tvarem. Známe jeden bod přímky, střed úsečky AB. Ten má souřadnice $(2, 0)$. Jde totiž o koncový bod vektoru $1/2(B - A) = (1, 2)$ s počátečním bodem $A = (1, -2)$. Směrový vektor $\mathbf{v}$ osy musí být kolmý na vektor $B - A = (2, 4)$, můžeme zvolit třeba $\mathbf{v} = (-2, 1)$. Parametrický tvar osy úsečky AB je potom

$$L = \{(2, 0) + t(-2, 1)\} \ .$$

Osa je kolmá na vektor $B - A$, jehož souřadnice jsou $(2, 4)$. Za vektor koeficientů hledané rovnice $ax + by = c$ můžeme zvolit přímo vektor $(2, 4)$, který je kolmý na osu. Rovnice osy úsečky AB pak bude $2x + 4y = c$ pro nějaké c. Přímka musí procházet středem P dané úsečky, který má souřadnice $(2, 0)$. Odtud plyne $c = 2 \cdot 2 + 4 \cdot 0 = 4$. Hledaná rovnice osy úsečky AB je tedy

$$2x + 4y = 4 \ .$$

▲

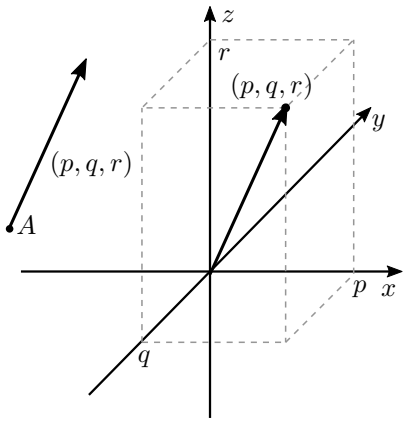


Obrázek 1.15. Rovnice osy úsečky

V kapitole o skalárním součinu si ukážeme jednoduchý způsob, jak psát přímo rovnice přímek nebo rovin kolmých na nějaký vektor.

1.3. Analytická geometrie v prostoru

1.3.1. Souřadnice v prostoru. Volba souřadného systému v prostoru umožňuje zapsat každý bod prostoru jako uspořádanou trojici (p, q, r) reálných čísel. V případě bodů v prostoru má tato trojice tři složky. Mluvíme také o třísložkovém aritmetickém vektoru.



Obrázek 1.16. Souřadnice bodu a vektoru v prostoru

Na obrázku 1.16 je také znázorněný polohový vektor bodu (p, q, r) a vektor s počátečním bodem A a souřadnicemi (p, q, r). Jakoukoliv uspořádanou trojici reálných čísel (tj. třísložkový aritmetický vektor) (p, q, r) tak můžeme geometricky intepretovat jako konkrétní bod nebo vektor v 3D 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 $(0, 0, 0)$.

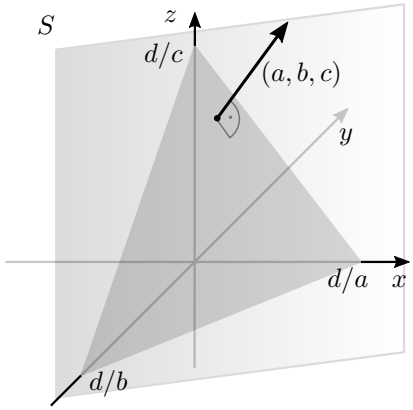
1.3.2. Rovnice roviny a parametrické vyjádření roviny v prostoru. Každé řešení jedné lineární rovnice o třech neznámých

$$ax + by + cz = d$$

je uspořádaná trojice (x, y, z) reálných čísel, která odpovídá nějakému bodu v prostoru. Množina všech řešení

$$S = \{(x, y, z) \in \mathbb{R}^3 : ax + by + cz = d\}$$

pak odpovídá nějaké rovině v prostoru, pokud je aspoň jeden z koeficientů a, b, c nenulový. Vektor koeficientů (a, b, c) je kolmý na tuto rovinu. Rovina je rovnoběžná s první souřadnou osou x právě tehdy, když je $a = 0$. Pokud je $a \neq 0$, protíná rovina S první souřadnou osu v bodě d/a. Podobně s dalšími osami. V případě $a = b = 0$ jde o rovinu rovnoběžnou s rovinou určenou prvními dvěma souřadnými osami x, y. Aritmetický vektor (a, b, c) koeficientů rovnice je nenulový a tvoří souřadnice vektoru kolmého na rovinu S.



Obrázek 1.17. Rovnice roviny v prostoru

Uvedená tvrzení si stejně jako v případě rovnice o dvou neznámých ověříme tak, že rovnici vyřešíme. Ukážeme si to opět na jednoduchém příkladu.

Příklad 1.4. Najdeme všechna řešení rovnice

$$x + 2y - 3z = 4 \ .$$

Z rovnice vypočteme x

$$x = 4 - 2y + 3z$$

a vidíme, že hodnoty neznámých y, z můžeme zvolit libovolně a že tato volba jednoznačně určí hodnotu x. Zvolíme-li $y = s$ a $z = t$, kde s, t jsou libovolná reálná čísla, pak dostaneme hodnotu $x = 4 - 2s + 3t$.

Každé řešení rovnice tak můžeme zapsat jako

$$(x, y, z) = (4 - 2s + 3t, s, t) \ .$$

Aritmetický vektor $(4 - 2s + 3t, s, t)$ upravíme do tvaru součtu

$$(4-2s+3t, s, t) = (4, 0, 0)+(-2s, s, 0)+(3t, 0, t) = (4, 0, 0)+s(-2, 1, 0)+t(3, 0, 1) \ .$$

Množinu S všech řešení rovnice $x + 2y - 3z = 4$ tak můžeme zapsat ve tvaru

$$S = \{(4, 0, 0) + s(-2, 1, 0) + t(3, 0, 1) : s, t \in \mathbb{R}\} \ .$$

Aritmetický vektor $(4, 0, 0)$ interpretujeme jako souřadnice bodu A v prostoru a aritmetické vektory $(-2, 1, 0), (3, 0, 1)$ jako souřadnice geometrických vektorů $\mathbf{v}, \mathbf{w}$ v prostoru. Množina S je tak množinou souřadnic bodů v prostoru, které leží v množině

$$P = \{A + s\mathbf{v} + t\mathbf{w}\} \ .$$

Vektory $\mathbf{v}$ a $\mathbf{w}$ mají různý směr, protože každý násobek vektoru $\mathbf{v}$ má třetí složku nulovou, zatímco $\mathbf{w}$ ji má různou od nuly. Tato množina tak tvoří množinu všech bodů nějaké roviny v prostoru – obrázek 1.6.

Pomocí skalárního součinu snadno ověříme, že vektor koeficientů $(1, 2, -3)$ je kolmý na vektory $\mathbf{v} = (-2, 1, 0)$ a $\mathbf{w} = (3, 0, 1)$ a tedy na celou rovinu P. ▲

Uvedený příklad v sobě obsahuje opět vše potřebné k tomu, abychom ověřili, že množinu všech řešení rovnice

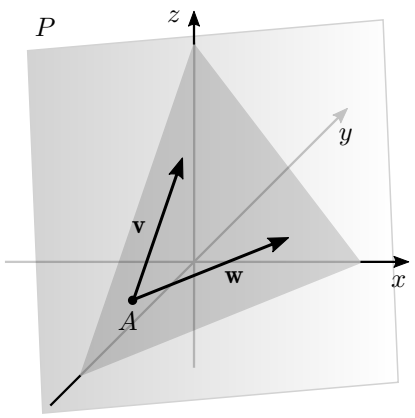
$$ax + by + cz = d$$

tvoří souřadnice bodů nějaké roviny v 3D prostoru, pokud je aspoň jeden z koeficientů a, b, c nenulový. Vždy můžeme předpokládat, že nenulový je koeficient u neznámé x a že se rovná 1.

Rovinu P v prostoru určenou nějakým jejím bodem $A = (a, b, c)$ a dvojicí vektorů $\mathbf{v} = (k, l, m), \mathbf{w} = (p, q, r)$, které nemají stejný směr, tak máme zadanou pomocí tří aritmetických vektorů $\mathbf{u} = (a, b, c), \mathbf{v}, \mathbf{w} \in \mathbb{R}^3$, a tvoří ji všechny body (se souřadnicemi)

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

Tomuto zápisu říkáme *parametrický tvar (vyjádření, zápis) roviny* v prostoru.



Obrázek 1.18. Parametrické vyjádření roviny v prostoru

Příklad 1.5. Najdeme rovnici a parametrický tvar roviny procházející body $P = (0, 2, 1)$, $Q = (1, 2, 3)$, $R = (2, 1, 0)$.

Opět je snazší vyjádřit rovinu v parametrickém tvaru. Za vektor $\mathbf{u}$ zvolíme polohový vektor bodu P, tj. $\mathbf{u} = (0, 2, 1)$. 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. $\mathbf{w} = (2, 1, 0) - (0, 2, 1) = (2, -1, -1)$. Protože vektor $\mathbf{w}$ není násobkem vektoru $\mathbf{v}$, neleží body P, Q, R na jedné přímce a rovina, kterou určují, má parametrický tvar

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

Rovnici $ax + by + cz = d$ této roviny najdeme tak, že napřed najdeme nějaký aritmetický vektor koeficientů (a, b, c), který je kolmý na vektory $\mathbf{v}$ a $\mathbf{w}$. Kdo zná vektorový součin $\mathbf{v} \times \mathbf{w}$, může jej použít, protože vektorový součin dvou vektorů je opět vektor, který je kolmý na oba činitele. Kdo si vektorový součin nepamatuje (tak jako my), může vyjít z toho, že neznámý vektor koeficientů (a, b, c) musí mít skalární součin s vektory $\mathbf{v}$ a $\mathbf{w}$ rovný 0, tj. koeficienty a, b, c musí splňovat soustavu rovnic

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

Jedním z jejích řešení je trojice $a = -2$, $b = -5$ a $c = 1$. Hledaná rovnice tak bude mít tvar $-2x - 5y + z = d$ a po dosazení souřadnic bodu P, který v rovině leží, za x, y, z najdeme $d = -9$. Jednou z rovnic dané roviny je tak

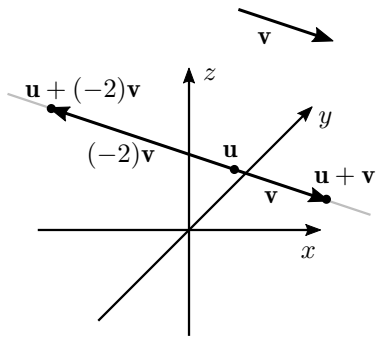
$$-2x - 5y + z = -9 \ .$$

▲

1.3.3. Soustava rovnic přímky a parametrický tvar přímky v prostoru. Parametrický tvar přímky v prostoru je formálně stejný, jako parametrický tvar přímky v rovině. Je-li přímka L zadaná nějakým svým bodem $A = (a, b, c)$ a směrovým vektorem $\mathbf{v} = (p, q, r)$, označíme $\mathbf{u}$ aritmetický vektor souřadnic (a, b, c) bodu A a dostaneme parametrický tvar této přímky

$$L = \{\mathbf{u} + t\mathbf{v} : t \in \mathbb{R}\} \ .$$

Je to množina (souřadnic) všech bodů ležících na přímce L.



Obrázek 1.19. Parametrické vyjádření přímky v prostoru

Příklad 1.6. Najdeme parametrický tvar přímky v prostoru procházející body $P = (-2, 3, 1)$ a $Q = (1, 0, 5)$.

Zvolíme $\mathbf{u} = (-2, 3, 1)$, tj. aritmetický vektor souřadnic bodu P, a za $\mathbf{v}$ souřadnice vektoru s počátečním bodem P a koncovým bodem Q, tj.

$$\mathbf{v} = (1, 0, 5) - (-2, 3, 1) = (3, -3, 4) \ .$$

Parametrické vyjádření je tedy

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

▲

PŘÍKLAD 1.7. Ukážeme, že množina všech řešení soustavy dvou lineárních rovnic

$$\begin{aligned} x + 2y - 3z &= 4 \\ 2x + 5y + z &= 1 \ , \end{aligned}$$

je přímka v prostoru a najdeme její parametrické vyjádření.

Víme už, že množina všech řešení každé z rovnic je rovina. Vektor koeficientů $(1, 2, -3)$ první rovnice není násobkem vektoru koeficientů $(2, 5, 1)$ druhé rovnice. Jednoduchý argument je třeba ten, že první a třetí složka druhého vektoru mají stejná znaménka, což platí také pro jakýkoliv jejich nenulový násobek, a neplatí pro vektor koeficientů první rovnice. Vektory koeficientů mají proto různý směr a roviny k nim kolmé jsou tedy různoběžné. Protínají se proto v přímce, která je tak množinou všech řešení naší soustavy.

Uvedený geometrický argument stačí k důkazu, že množina všech řešení soustavy je přímka. Abychom našli nějaký bod této přímky a směrový vektor, soustavu vyřešíme a najdeme tak parametrický tvar přímky všech řešení.

Od druhé rovnice odečteme dvojnásobek první rovnice a dostaneme rovnici

$$y + 7z = -7 \ ,$$

ze které vypočítáme neznámou y:

$$y = -7 - 7z \ .$$

Za hodnotu neznámé z můžeme zvolit libovolné reálné číslo t. Tato volba určí jednoznačně hodnotu $y = -7-7t$ a po dosazení do první rovnice soustavy spočteme jednoznačně hodnotu x jako

$$x = 4 - 2y + 3z = 4 - 2(-7 - 7t) + 3t = 18 + 17t \ .$$

Všechna řešení soustavy jsou tvaru

$$(x, y, z) = (18 + 17t, -7 - 7t, t) = (18, -7, 0) + t(17, -7, 1) \ .$$

Parametrický tvar přímky, která je množinou všech řešení soustavy, je

$$\{(18, -7, 0) + t(17, -7, 1) : t \in \mathbb{R}\} \ .$$

Ještě si uvědomíme, že směrový vektor přímky $(17, -7, 1)$ leží v obou rovinách určených rovnicemi soustavy a musí být tedy kolmý na oba vektory koeficientů $(1, 2, -3)$ a $(2, 5, 1)$. ▲

Neexistuje jedna lineární rovnice o třech neznámých, jejíž množina řešení by byla přímka v prostoru. To plyne samozřejmě z toho, že pokud je aspoň jeden z koeficientů rovnice nenulový, je množina všech řešení rovina v prostoru, a degenerované případy $0x + 0y + 0z = d$ nepřicházejí vůbec v úvahu (proč?).

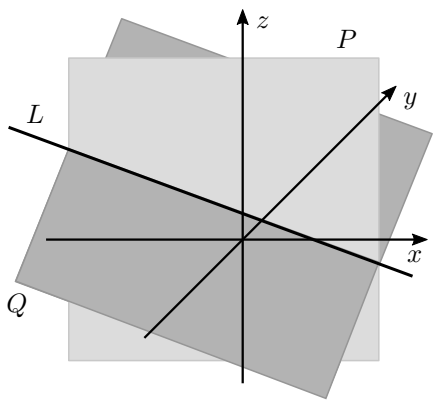
Každá přímka L v 3D-prostoru je ale průsečíkem (průnikem) nějakých dvou rovin P, Q.

Každou z obou rovin můžeme vyjádřit jako množinu všech řešení jedné lineární rovnice o třech neznámých. Jejich průnik je pak společným řešením obou rovnic, neboli řešením soustavy dvou lineárních rovnic o třech neznámých

$$\begin{aligned} ax + by + cz &= d \\ ex + fy + gz &= h \ . \end{aligned}$$

Každou přímku v prostoru tak můžeme vyjádřit jako množinu všech řešení soustavy dvou lineárních rovnic o třech neznámých.

Naopak, řešením soustavy dvou lineárních rovnic o třech neznámých je přímka, pokud soustava splňuje několik snadno ověřitelných podmínek. Především oba vektory koeficientů (a, b, c) a (e, f, g) musí být nenulové. To ještě nestačí, roviny určené



Obrázek 1.20. Průnik dvou rovin v prostoru

těmito přímkami musí být navíc různoběžné. Vektory koeficientů jsou kolmé na roviny, které definují. Roviny jsou proto různoběžné, pokud vektory (a, b, c) a (e, f, g) mají různý směr, tj. pokud ani jeden z vektorů (a, b, c) a (e, f, g) nedostaneme jako násobek druhého.

Nyní můžeme geometricky nahlédnout, jaké možnosti jsou pro množinu všech řešení libovolné soustavy lineárních rovnic o třech neznámých. Nejdříve se podíváme, obsahuje-li soustava nějaké degenerované rovnice

$$0x + 0y + 0z = d \ .$$

Pokud je v nějaké takové rovnici pravá strana $d \neq 0$, nemá tato rovnice žádné řešení a celá soustava je proto neřešitelná. Je-li $d = 0$, je naopak každý aritmetický vektor $(x, y, z) \in \mathbb{R}^3$ řešením takové rovnice a tato rovnice nijak neovlivňuje množinu všech řešení celé soustavy. Můžeme ji proto vynechat. Pokud by soustava obsahovala pouze degenerované rovnice, je množina jejích řešení buď prázdná nebo celý 3D prostor. Zbývají tak soustavy neobsahující degenerované rovnice. V takové soustavě je množina všech řešení každé rovnice nějaká rovina v 3D prostoru a řešení celé soustavy je průnikem těchto rovin, což může být buď opět rovina, nebo přímka, nebo jeden bod, nebo prázdná množina.

Podobně nahlédneme, že množina všech řešení každé soustavy lineárních rovnic o dvou neznámých je buď přímka, nebo bod, nebo prázdná množina, a nebo celá 2D rovina.

1.4. Komplexní čísla

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

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 tehdy, když se současně rovnají jejich reálné části a imaginární části, tj. právě tehdy, 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

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

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:

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

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

1.4.2. 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 1.8. 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 tehdy, 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 odvodíme 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.

1.4.3. 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):

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

1.4.4. 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 1.9. *Každý nekonstantní polynom s komplexními koeficienty má aspoň jeden komplexní kořen.*

Základní větu algebry lze formulovat také následujícím způsobem.

VĚTA 1.10. *Pro každý polynom* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *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*

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = a_n(x - z_1)(x - z_2)\cdots(x - z_n) \ .$$

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 $a_n x^n + \cdots + a_1 x + a_0 = 0$. Z porovnání stupňů polynomů na obou stranách poslední rovnosti dostaneme ihned následující důsledek.

DŮSLEDEK 1.11. *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 1.12. *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 tehdy, když je* $\overline{z}$ *(číslo komplexně sdružené k* z*) také kořen polynomu* $p(x)$.

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

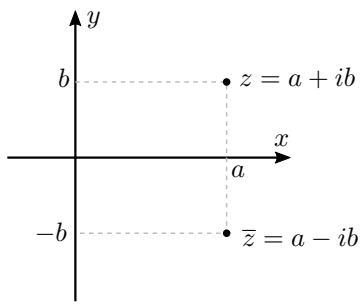
Každý koeficient a_i polynomu $p(x)$ je reálné číslo, platí proto $\overline{a_i} = a_i$. Stejně tak platí $\overline{0} = 0$. Protože předpokládáme, že z je kořen polynomu $p(x)$, platí $p(z) = 0$, a tedy také $\overline{p(z)} = \overline{0} = 0$. V následujícím výpočtu použijeme, že komplexní sdružování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

1.4.5. 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*.

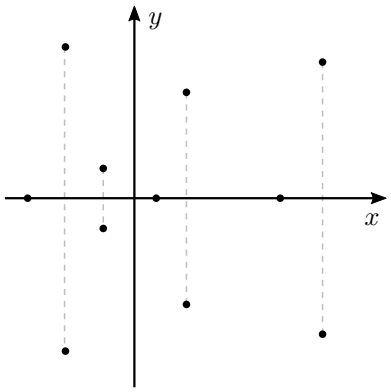


Obrázek 1.21. Geometrické znázornění komplexního čísla v rovině

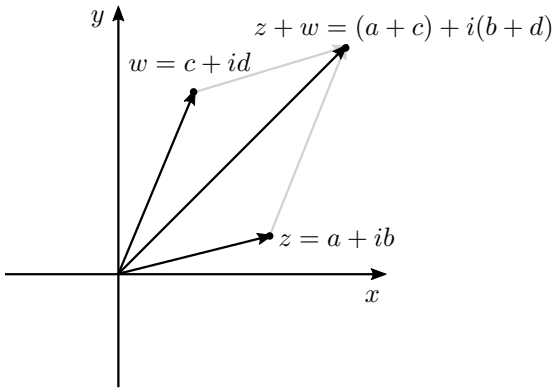
Na obrázku je kromě čísla $z = a + ib$ znázorněné také číslo komplexně sdružené k z, tj. číslo $\overline{z} = a - ib$. Geometricky je komplexně sdružené číslo $\overline{z}$ symetrické s číslem z vzhledem k reálné ose.

Obrázek 1.22 ukazuje geometrický význam věty 1.12 o komplexním sdružování kořenů polynomů s reálnými koeficienty – množina všech kořenů je symetrická vzhledem k reálné ose.

Dále si na obrázku 1.23 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.



Obrázek 1.22. Komplexní kořeny polynomu s reálnými koeficienty

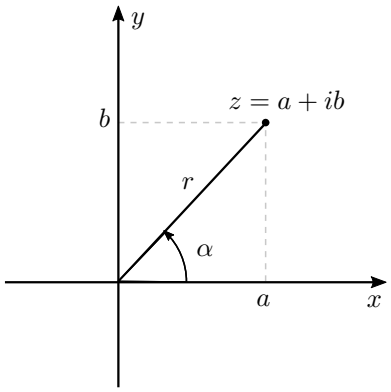


Obrázek 1.23. Součet komplexních čísel

1.4.6. Polární souřadnice v rovině. Geometrický význam násobení komplexních čísel 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 souřadnice* bodu P, viz. obrázek 1.24. Protože otočením o plný úhel 2π neboli 360 stupňů dostaneme zpět kladnou poloosu x_1, není úhel α určený jednoznačně. Různé 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.

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

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



Obrázek 1.24. Polární souřadnice bodu v rovině

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.

1.4.7. 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 1.8), že $z\,\overline{z} = a^2 + b^2$, dostáváme pro absolutní hodnotu čísla z vyjádření

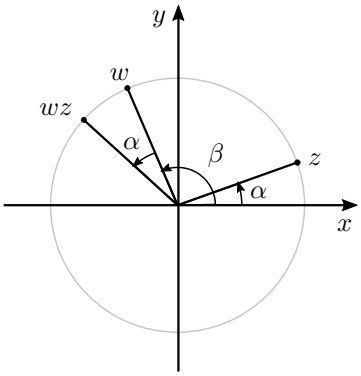
- $|z|^2 = z\,\overline{z}$.

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

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.



Obrázek 1.25. Součin komplexních jednotek

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

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

Důkaz. Pro $n = 0$ Moivreova věta zjevně platí, neboť

$$(\cos\alpha + i\sin\alpha)^0 = 1 = \cos 0 = \cos(0\alpha) + i\sin(0\alpha) \ .$$

Předpokládejme, že platí

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

pro nějaké přirozené $n \geq 0$. Z tohoto indukčního předpokladu a součtových vzorců pro *sinus* a *cosinus* pak spočítáme, že

$$\begin{aligned}
(\cos\alpha + i\sin\alpha)^{n+1} &= (\cos\alpha + i\sin\alpha)^n(\cos\alpha + i\sin\alpha) = \\
&= (\cos(n\alpha) + i\sin(n\alpha))(\cos\alpha + i\sin\alpha) = \\
&= (\cos(n\alpha)\cos\alpha - \sin(n\alpha)\sin\alpha) + i(\cos(n\alpha)\sin\alpha + \sin(n\alpha)\cos\alpha) = \\
&= \cos(n+1)\alpha + i\sin(n+1)\alpha \ ,
\end{aligned}$$

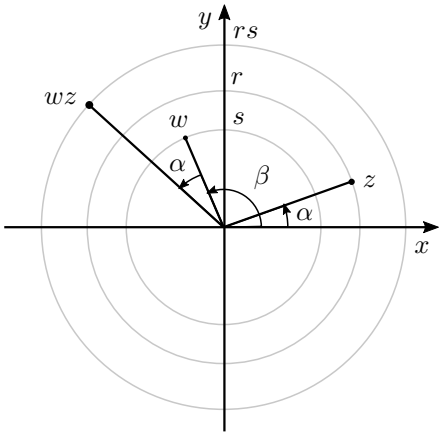
čímž je indukční krok dokázán. □

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

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

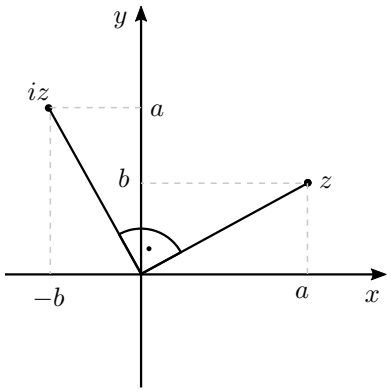
Pro absolutní hodnotu a argument součinu $w\,z$ tak platí

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



Obrázek 1.26. Součin komplexních čísel

V jednoduchém speciálním případě, kdy $w = i = \cos(\pi/2) + i\sin(\pi/2)$ dostáváme, že $|iz| = |i|\,|z| = |z|$ 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 1.27. Součin komplexního čísla s imaginární jednotkou

1.4.9. Komplexní exponenciála. *Komplexní exponenciálu* definujeme pomocí *Eulerovy formule*

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

pro každé reálné číslo α. Speciálním případem je elegantní *Eulerova identita*

$$e^{i\pi} = -1 \ .$$

Eulerovu formuli lze 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

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

Podobně jednoduše lze zapsat Moivreovu větu:

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

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

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

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

1.4.10. Trojúhelníková nerovnost. 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

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

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

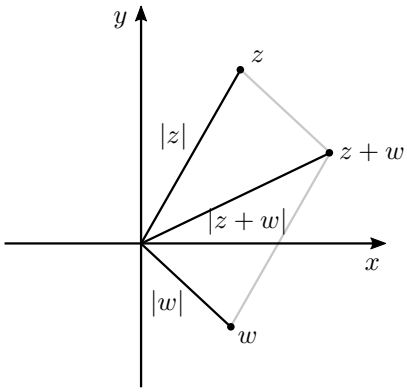
$$a \leq |a| = \sqrt{a^2} \leq \sqrt{a^2 + b^2} = |z| \quad .$$

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

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

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

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



Obrázek 1.28. Trojúhelníková nerovnost pro komplexní čísla

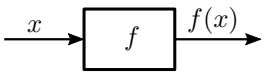
1.5. Zobrazení

Upozornění: na této části se ještě pracuje.

Velká část matematiky se zabývá zkoumáním vlastností nejrůznějších zobrazení. Obecnou formální definici přenecháme jiným textům. Neformálně, *zobrazení* (někdy se také říká *funkce*) *z množiny* X *do množiny* Y přiřazuje každému prvku $x \in X$ právě jeden prvek $y \in Y$.

Skutečnost, že f je zobrazení z množiny X do množiny Y zapisujeme $f : X \to Y$. Jednoznačně určený prvek množiny Y, který zobrazení f přiřazuje prvku $x \in X$, zapisujeme jako $f(x)$. Říkáme také, že $f(x)$ je *hodnota zobrazení* f *v bodě* x. Množina X se nazývá *definiční obor* zobrazení f, pro množinu Y zvláštní název zavádět nebudeme. Můžeme také říct, že zobrazení f *vede* z množiny X do množiny Y.

1.5.1. Příklady zobrazení. Asi nejblíže formální definici je představa zobrazení $f : X \to Y$ jako černé skříňky, která dostane na vstup nějaký prvek $x \in X$ a na výstupu nám dá odpověď v podobě hodnoty $f(x) \in Y$. Pokud bychom zkusili zadat na vstup nějaký prvek z, který neleží v množině X, skříňka nereaguje, nedá žádnou odpověď. Hodnota zobrazení f není v bodě $z \notin X$ definována. Důležité je, že pokud dáme na vstup opakovaně stejnou hodnotu $x \in X$, na výstupu se objeví vždy stejná hodnota $f(x) \in Y$.



Obrázek 1.29. Zobrazení jako černá skříňka

Vnitřek černé skříňky může být třeba elektrický obvod, do kterého po nějakých drátech přítékají (vstupují) proudy určité hodnoty a po jiných drátech z něho vytékají proudy jiných hodnot, které jsou výstupem. Nebo může vnitřek černé skříňky tvořit implementace nějakého algoritmu, který na vstupní data $x \in X$ odpoví výstupem $f(x) \in Y$.

Tento vnitřek nás ale nezajímá! Dvě zobrazení f, g z X do Y tedy považujeme za stejná, pokud pro každé $x \in X$ platí $f(x) = g(x)$. Jak se k hodnotám f a g přijde není součástí samotného objektu – zobrazení.

Zobrazení $f : X \to Y$ můžeme zadat nejrůznějšími způsoby.

Příklad 1.14. Zobrazení $f : X \to Y$ z množiny $X = \{a, b, c, d\}$ do množiny $Y = \{1, 2, 3, 4, 5\}$ můžeme zadat tak, že pro každou hodnotu $x \in \{a, b, c, d\}$ zadáme hodnotu $f(x)$:

$$\begin{aligned} f(a) &= 1\ , \\ f(b) &= 4\ , \\ f(c) &= 3\ , \\ f(d) &= 4\ . \end{aligned}$$

Jiný možný způsob zápisu je například

$$\begin{aligned} f : X &\to Y \\ a &\mapsto 1\ , \\ b &\mapsto 4\ , \\ c &\mapsto 3\ , \\ d &\mapsto 4\ . \end{aligned}$$

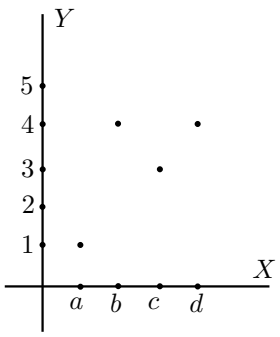
Další možností je zápis tabulkou.

x	a	b	c	d
$f(x)$	1	4	3	4

.

V uvedeném zápisu tabulkou schází informace o tom, že zobrazení f vede do množiny $\{1, 2, 3, 4, 5\}$. Tuto informaci musíme k tabulce přidat.

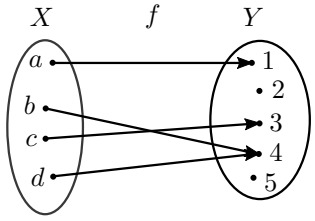
Zobrazení f můžeme popsat také pomocí grafu jako na obrázku 1.30.



Obrázek 1.30. Zápis zobrazení grafem

Nebo pomocí obrázku jako na obrázku 1.31. ▲

Příklad 1.15. Zobrazení $f : \mathbb{R} \to \mathbb{R}$ se obvykle nazývá funkce, přesněji *reálná funkce jedné reálné proměnné*. Také funkce můžeme popsat různými způsoby. Časté



Obrázek 1.31. Zápis zobrazení obrázkem

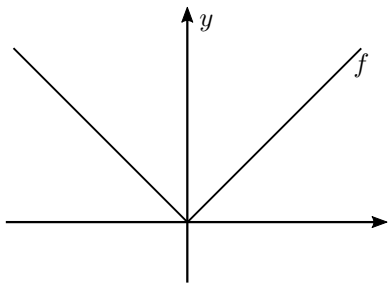
je zadání nějakou formulí (vzorcem, předpisem), např.

$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = |x| \ .$$

Nebo

$$f : \mathbb{R} \to \mathbb{R}, \quad x \mapsto \sin x \ .$$

Také funkci si lze přiblížit grafem, takový graf může ale ukázat hodnoty funkce pouze na omezeném intervalu. Např. funkce $f : \mathbb{R} \to \mathbb{R}$ definovaná na množině všech reálných čísel předpisem $f(x) = |x|$ je znázorněna grafem na obrázku 1.32.



Obrázek 1.32. Graf funkce $f(x) = |x|$.

Jedno zobrazení můžeme zadat různými předpisy. Tak např. předpisy $f(x) = |x|$ a $g(x) = \sqrt{x^2}$ definují jedno a to samé zobrazení $f = g$ na množině $\mathbb{R}$. Zobrazení a formulka definující toto zobrazení jsou dvě různé věci.

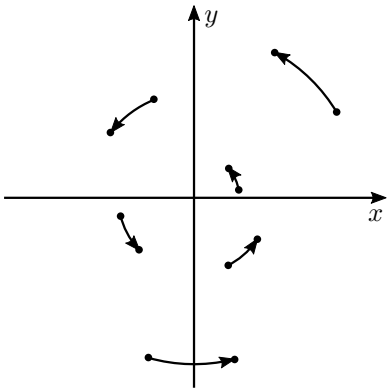
Také je důležité si uvědomit, že součástí definice konkrétního zobrazení $f : X \to Y$ není pouze vzorec pro výpočet hodnoty $f(x)$ v každém bodě $x \in X$, ale také samotný definiční obor X a množina Y. Například předpisy

$$f(x) = x + 1, \qquad g(x) = \frac{x^2 - 1}{x - 1}$$

definují jedno a to samé zobrazení s definičním oborem $\mathbb{R} \setminus \{1\}$. Pokud ale bereme předpis $f(x) = x + 1$ jako zobrazení $f : \mathbb{R} \to \mathbb{R}$, pak jde o jiné zobrazení než zobrazení $g : \mathbb{R} \setminus \{1\} \to \mathbb{R}$ definované předpisem $g(x) = (x^2 - 1)/(x - 1)$. Zobrazení f, g mají v tomto případě různé definiční obory a proto se nerovnají, přestože $f(x) = g(x)$ pro každý bod x, který leží v definičním oboru obou zobrazení. Stejně tak

zobrazení $f : \mathbb{R} \to \mathbb{R}$ definované předpisem $f(x) = x^2$ je různé od zobrazení $g : \mathbb{R} \to \mathbb{R} \setminus (-\infty, 0)$ definovaného předpisem $g(x) = x^2$, přestože obě zobrazení mají stejný definiční obor $\mathbb{R}$ a platí $f(x) = g(x)$ pro každé $x \in \mathbb{R}$. Jsou různá proto, že vedou do různých množin $\mathbb{R}$ (zobrazení f) a $\mathbb{R} \setminus (-\infty, 0)$ (zobrazení g). ▲

Příklad 1.16. Zobrazení také můžeme popsat slovně nebo geometrickou konstrukcí. Například zobrazení $f : \mathbb{R}^2 \to \mathbb{R}^2$ můžeme popsat tak, že jde o otočení kolem počátku souřadnic o úhel 30° proti směru hodinových ručiček. Na obrázku 1.33 jsou znázorněné obrazy několika bodů daným otočením.



Obrázek 1.33. Rotace kolem počátku o úhel 30°

Rotaci $f : \mathbb{R}^2 \to \mathbb{R}^2$ o úhel 30° kolem počátku proti směru hodinových ručiček můžeme také popsat pomocí předpisu

$$f((x, y)) = (x \cos 30^o - y \sin 30^o, x \sin 30^o + y \cos 30^o) \quad .$$

Graf rotace f už nakreslit nemůžeme, potřebovali bychom k tomu prostor dimenze 4. ▲

Příklad 1.17. Některá zobrazení můžeme popsat pouze formulkou. Např. zobrazení $g : \mathbb{R}^2 \to \mathbb{R}^3$ definované předpisem

$$g((x, y)) = \left(2x + \sin y + 3y^2, \cos(xy) - x, \frac{y}{x^2 + 1} - \sin(6y^3)\right)$$

nemá žádnou zjevnou geometrickou interpretaci, jeho graf také nelze nakreslit, ani nemůžeme vypsat jeho hodnoty ve všech bodech definičního oboru. ▲

Příklad 1.18. Další zobrazení můžeme zadat pouze algoritmem. Typickým příkladem jsou *kryptografické hašovací funkce*, které libovolně dlouhému vstupu x, kterým může být každá posloupnost bitů (číslic 0 a 1), přiřadí výstup $f(x)$ v délce 256 bitů. Kvalitně navržená hašovací funkce vyžaduje, aby algoritmus k danému vstupu x spočítal výstup $f(x)$ dostatečně rychle a současně nebylo možné z výstupu $f(x)$ usoudit nic o vstupu x. Mezi další požadavky patří například nemožnost najít dva různé vstupy x, y se stejným výstupem $f(x) = f(y)$. Tyto požadavky mimo jiné vylučují možnost, že by hašovací funkci f bylo možné zadat nějakou formulkou nebo vzorcem, natož grafem. ▲

Ukázali jsme si několik různých způsobů, jak popsat zobrazení $f : X \to Y$. Jsou to

- tabulkou, neboli výpisem jeho hodnot ve všech bodech definičního oboru,

- formulkou/vzorcem,
- grafem,
- slovně,
- obrázkem,
- algoritmem.

Žádný z uvedených způsobů nestačí ani k tomu, abychom mohli popsat všechna zobrazení $f : \mathbb{R} \to \mathbb{R}$. Obecnou definici zobrazení zde uvádět nebudeme. Stačí vědět, že zobrazení $f : X \to Y$ každému prvku $x \in X$ přiřazuje jednoznačně určený prvek $f(x) \in Y$. Jakým způsobem je $f(x)$ určené není podstatné.

1.5.2. Prostá zobrazení, zobrazení „na“. V této části uvedeme několik základních pojmů, které budeme v dalším textu často používat.

Definice 1.19. Zobrazení $f : X \to Y$ nazýváme

(1) *prosté*, někdy se také říká *injektivní*, jestliže pro dva různé prvky $x, y \in X$ platí $f(x) \neq f(y)$. Nebo jinak řečeno, pokud pro každé $y \in Y$ existuje nejvýše jedno $x \in X$ takové, že $f(x) = y$,
(2) *na množinu* Y, někdy se také říká *surjektivní*, pokud pro každé $y \in Y$ existuje aspoň jedno $x \in X$ takové, že $f(x) = y$,
(3) *vzájemně jednoznačné*, někdy se také říká *bijektivní*, pokud je současně prosté a na množinu Y, neboli pokud pro každé $y \in Y$ existuje právě jedno $x \in X$ takové, že $f(x) = y$.

Příklad 1.20. Zobrazení f z příkladu 1.14 není prosté, protože $f(b) = f(d)$ $(= 4)$ a platí $b \neq d$. Není ani na množinu Y, protože neexistuje žádný prvek x množiny $X = \{a, b, c, d\}$, pro který by platilo $f(x) = 2$.

Stejně tak není prosté ani zobrazení $f(x) = |x|$ z příkladu 1.15 definované jako zobrazení $f : \mathbb{R} \to \mathbb{R}$. Platí totiž např. $f(2) = f(-2) = 2$. Toto zobrazení není ani na množinu $\mathbb{R}$, protože žádné záporné reálné číslo není absolutní hodnotou nějakého reálného čísla.

Zobrazení $g : \mathbb{R} \to [0, +\infty)$ definované stejným předpisem $g(x) = |x|$ je na množinu všech nezáporných reálných čísel $[0, +\infty)$, neboť pro každé nezáporné reálné číslo a platí $g(a) = |a| = a$. ▲

Definice 1.21. *Oborem hodnot zobrazení* $f : X \to Y$ nazýváme množinu

$$\mathrm{Im}\,(f) = \{y \in Y : \text{ existuje } x \in X \text{ takové, že } f(x) = y\} \subseteq Y \ .$$

Obor hodnot můžeme alternativně také popsat jako

$$\mathrm{Im}\,(f) = \{f(x) : x \in X\}$$

Z definice ihned plyne, že zobrazení $f : X \to Y$ je na množinu Y právě když $\mathrm{Im}\,(f) = Y$.

Příklad 1.22. Obor hodnot $\mathrm{Im}\,(f)$ zobrazení $f(x) = |x|$ z příkladu 1.15 definovaného jako zobrazení $f : \mathbb{R} \to \mathbb{R}$, se rovná intervalu $[0, \infty)$ všech nezáporných reálných čísel. Pro každé nezáporné reálné číslo y totiž platí $f(y) = |y| = y$ a protože $f(x) = |x| \geq 0$ pro každé reálné číslo x, žádné záporné $y \in \mathbb{R}$ v množině $\mathrm{Im}\,(f)$ ležet nemůže. ▲

Poslední příklad ukazuje, že z každého zobrazení $f : X \to Y$ můžeme udělat zobrazení na, pokud z množiny Y vynecháme „nadbytečné“ prvky.

1.5.3. Obraz a vzor. Zabýváme-li se zobrazením $f : X \to Y$, často nás zajímají nejen obrazy jednotlivých prvků ale také celých množin.

Definice 1.23. Je-li $f : X \to Y$ zobrazení a $A \subseteq X$, pak *obrazem množiny* A *při zobrazení* f rozumíme množinu $f(A) = \{f(x) : x \in A\}$.

Obrazem množiny A je tedy podmnožina množiny Y, kterou také můžeme zapsat následujícím způsobem.

$$f(A) = \{y \in Y : \text{ existuje } x \in A \text{ takové, že } f(x) = y\}$$

Všimněte si, že $\mathrm{Im}\,(f) = f(X)$.

Podobně nás často zajímají vzory podmnožin množiny Y, tj. prvky množiny X, které se do této podmnožiny zobrazí.

Definice 1.24. Je-li $f : X \to Y$ zobrazení a $B \subseteq Y$, pak *(úplným) vzorem množiny B při zobrazení f* rozumíme množinu $f^{-1}(B) = \{x \in X : f(x) \in B\}$.

(Úplným) vzorem prvku $b \in Y$ rozumíme úplný vzor jednoprvkové množiny $\{b\}$, tj. množinu $\{x \in X : f(x) = b\}$.

Příklad 1.25. Pojem úplného vzoru si ilustrujeme na příkladu 1.14. Pro úplné vzory jednotlivých prvků množiny $\{1, 2, 3, 4, 5\}$ platí

$$\begin{aligned} f^{-1}(\{1\}) &= \{a\} \ , \\ f^{-1}(\{2\}) &= \emptyset, \\ f^{-1}(\{3\}) &= \{c\} \ , \\ f^{-1}(\{4\}) &= \{b, d\} \ , \\ f^{-1}(\{5\}) &= \emptyset. \end{aligned}$$

Dále platí např.

$$\begin{aligned} f^{-1}(\{1, 2\}) &= \{a\} \ , \\ f^{-1}(\{2, 5\}) &= \emptyset \ , \\ f^{-1}(\{3, 4, 5\}) &= \{b, c, d\} \ , \\ f^{-1}(\{1, 4\}) &= \{a, b, d\} \ . \end{aligned}$$

▲

Příklad 1.26. TODO: priklad pro nejaky geometricky zobrazeni ▲

1.5.4. Skládání zobrazení.

Definice 1.27. Jsou-li $f : X \to Y$ a $g : Y \to Z$ dvě zobrazení, pak zobrazení $h : X \to Z$, které každému $x \in X$ přiřazuje prvek $h(x) = g(f(x))$, nazýváme *složení zobrazení f a g* (v tomto pořadí), a označujeme jej $g \circ f$, nebo také gf.

Definici složení zobrazení si můžeme přiblížit graficky pomocí černých skříněk na obr.1.34. Zdůrazněme ještě jednou, že složení zobrazení f a g zapisujeme jako $g \circ f$.

Snadno ověříme, že skládání zobrazení je asociativní.

Tvrzení 1.28. *Jsou-li $f : X \to Y$, $g : Y \to Z$ a $h : Z \to W$ tři zobrazení, pak jsou obě složení $h \circ (g \circ f)$ a $(h \circ g) \circ f$ definována a platí*

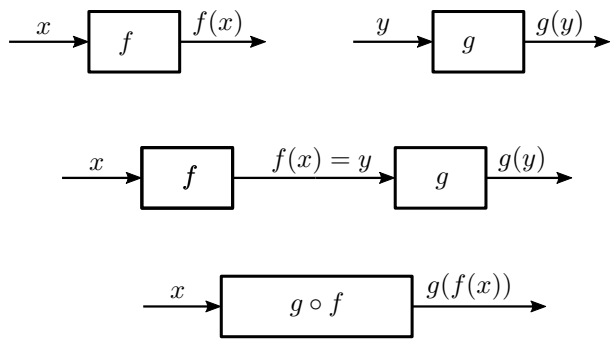
$$h \circ (g \circ f) = (h \circ g) \circ f \ .$$

Důkaz. Protože $g \circ f$ je definované jako zobrazení z množiny X do množiny Z a $h : Z \to W$, je složené zobrazení $h \circ (g \circ f) : X \to W$ definované a pro každé $x \in X$ platí

$$h \circ (g \circ f)(x) = h((g \circ f)(x)) = h(g(f(x))) \ .$$

Podobně díky tomu, že $(h \circ g) : Y \to W$ a $f : X \to Y$, je také definované složené zobrazení $(h \circ g) \circ f : X \to W$ a pro libovolné $x \in X$ platí

$$(h \circ g) \circ f(x) = (h \circ g)(f(x)) = h(g(f(x))) \ .$$



Obrázek 1.34. Skládání zobrazení pomocí černých skříněk

Obě zobrazení $h \circ (g \circ f)$ a $(h \circ g) \circ f$ vedou z množiny X do množiny W a pro každý bod x ze společného definičního oboru X platí

$$h \circ (g \circ f)(x) = (h \circ g) \circ f(x) \ ,$$

čímž je rovnost $h \circ (g \circ f) = (h \circ g) \circ f$ dokázána. □

Příklad 1.29. Definici složení dvou zobrazení si ilustrujeme na složení zobrazení $f : \{a, b, c, d\} \to \{1, 2, 3, 4, 5\}$ z příkladu 1.14 se zobrazením $g : \{1, 2, 3, 4, 5\} \to \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ definovaným tabulkou

y	1	2	3	4	5
$g(y)$	$\clubsuit$	$\diamondsuit$	$\spadesuit$	$\heartsuit$	$\clubsuit$

.

Spočítáme hodnoty složení zobrazení $g \circ f : \{a, b, c, d\} \to \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ v jednotlivých prvcích definičního oboru $\{a, b, c, d\}$:

$$\begin{aligned}
(g \circ f)(a) &= g(f(a)) = g(1) = \clubsuit \ , \\
(g \circ f)(b) &= g(f(b)) = g(4) = \heartsuit \ , \\
(g \circ f)(c) &= g(f(c)) = g(3) = \spadesuit \ , \\
(g \circ f)(d) &= g(f(d)) = g(4) = \heartsuit \ .
\end{aligned}$$

Složení $g \circ f$ můžeme rovněž zapsat tabulkou

x	a	b	c	d
$(g \circ f)(x)$	$\clubsuit$	$\heartsuit$	$\spadesuit$	$\heartsuit$

.

▲

Příklad 1.30. TODO: priklad na skladani geometrickych zobrazeni ▲

Velmi speciálním vzájemně jednoznačným zobrazením je identické zobrazení na množině X.

Definice 1.31. *Identické zobrazení na množině* X je zobrazení $\mathrm{id}_X : X \to X$, které každému prvku $x \in X$ přiřazuje ten samý prvek x, neboli

$$\mathrm{id}_X(x) = x \quad \text{pro každé} \quad x \in X.$$

Tvrzení 1.32. *Pro každé zobrazení* $f : X \to Y$ *platí*

$$\mathrm{id}_Y \circ f = f = f \circ \mathrm{id}_X \ .$$

Důkaz. Dokážeme rovnost $\mathrm{id}_Y \circ f = f$. Druhá rovnost $f = f \circ \mathrm{id}_X$ se dokáže zcela stejně.

Protože $f : X \to Y$ a $\mathrm{id}_Y : Y \to Y$, složení $\mathrm{id}_Y \circ f$ je definované a vede z množiny X do množiny Y, stejně jako zobrazení f. K důkazu rovnosti $\mathrm{id}_Y \circ f = f$ stačí ověřit, že platí $(\mathrm{id}_Y \circ f)(x) = f(x)$ pro každé $x \in X$. To je ale skoro zřejmé, neboť z definice identického zobrazení na množině Y plyne, že pro každé $x \in X$ je

$$(\mathrm{id}_Y \circ f)(x) = \mathrm{id}_Y(f(x)) = f(x) \ .$$

□

Podívejme se podrobněji, co znamená, že zobrazení $f : X \to Y$ je vzájemně jednoznačné. Definice 1.19.3 říká, že pro každé $y \in Y$ existuje jednoznačně určené $x \in X$ takové, že $f(x) = y$. Vzájemně jednoznačné zobrazení $f : X \to Y$ tak definuje jiné zobrazení $g : Y \to X$, které každému prvku $y \in Y$ přiřazuje (jednoznačně určený) prvek $g(y) = x \in X$, pro který platí $f(x) = y$.

Tvrzení 1.33. *Pro každé vzájemně jednoznačné zobrazení $f : X \to Y$ existuje (jednoznačně určené) zobrazení $g : Y \to X$ takové, že platí*

$$g \circ f = \mathrm{id}_X, \quad a \quad f \circ g = \mathrm{id}_Y \ .$$

Důkaz. Definici zobrazení $g : Y \to X$ jsme uvedli již před tvrzením. Zbývá ověřit obě rovnosti, které má g splňovat. Začneme rovností $g \circ f = \mathrm{id}_X$. Z definice g plyne, že $g \circ f : X \to X$ stejně jako $\mathrm{id}_X : X \to X$. Zvolíme libovolné $x \in X$. Potom

$$(g \circ f)(x) = g(f(x)) \ .$$

Zobrazení $f : X \to Y$ je vzájemně jednoznačné, speciálně tedy také prosté. Pokud pro nějaké $z \in X$ platí $f(z) = f(x)$, musí být $z = x$. Platí tedy $g(f(x)) = x$ pro jakékoliv $x \in X$, což dokazuje $g \circ f = \mathrm{id}_X$.

K důkazu rovnosti $f \circ g = \mathrm{id}_Y$ zvolíme libovolné $y \in Y$. Protože zobrazení f je na celou množinu Y, existuje nějaké $x \in X$, pro které platí $y = f(x)$. Protože zobrazení f je také prosté, je toto $x \in X$ určené jednoznačně, což nám dává jedinou možnost definovat $g(y) = x$. Proto platí

$$(f \circ g)(y) = f(g(y)) = f(x) = y$$

pro každé $y \in Y$. □

Definice 1.34. Jsou-li $f : X \to Y$ a $g : Y \to X$ zobrazení, pro která platí

$$g \circ f = \mathrm{id}_X, \quad \text{a} \quad f \circ g = \mathrm{id}_Y \ ,$$

pak zobrazení g nazýváme *inverzní zobrazení* k f a označujeme jej f^{-1}. Říkáme také, že zobrazení f je *invertovatelné*.

Všimněme si, že je-li g inverzní zobrazení k f, pak také f je inverzní zobrazení ke g a platí tak

$$(f^{-1})^{-1} = g^{-1} = f \ .$$

Zatím jsme si ukázali, že ke každému vzájemně jednoznačnému zobrazení $f : X \to Y$ existuje inverzní zobrazení. Ve skutečnosti existence inverzního zobrazení charakterizuje vzájemně jednoznačná zobrazení.

Tvrzení 1.35. *Inverzní zobrazení $g : Y \to X$ ke zobrazení $f : X \to Y$ existuje právě když je zobrazení f vzájemně jednoznačné.*

Důkaz. Existenci inverzního zobrazení k libovolnému vzájemně jednoznačnému zobrazení jsme ukázali už v Tvrzení 1.33. Zbývá dokázat opačnou implikaci, tj. že z existence inverzního zobrazení k $f : X \to Y$ plyne vzájemná jednoznačnost f. Předpokládejme tedy, že $g : Y \to X$ je zobrazení inverzní k $f : X \to Y$. Pro

důkaz, že f je prosté, předpokládejme, že pro dva prvky $x, y \in X$ platí $f(x) = f(y)$. Potom

$$x = \mathrm{id}_X(x) = (g \circ f)(x) = g(f(x)) = g(f(y)) = (g \circ f)(y) = \mathrm{id}_x(y) = y \ .$$

To dokazuje, že zobrazení $f : X \to Y$ je prosté.

K důkazu, že f je zobrazení na celou množinu Y, zvolme nějaké $y \in Y$. Potom platí

$$y = \mathrm{id}_Y(y) = (f \circ g)(y) = f(g(y)) \ .$$

Pro $x = g(y)$ tak platí $y = f(x)$. □

Inverzní zobrazení $g : Y \to X$ ke zobrazení $f : X \to Y$ musí splňovat obě rovnosti z definice 1.34. Pokud splňuje pouze jednu z těchto rovností, mluvíme o inverzním zobrazení zleva nebo zprava (nebo o levém nebo pravém inverzu) k zobrazení f.

Definice 1.36. Pokud pro zobrazení $f : X \to Y$ a $g : Y \to X$ platí

(1) $g \circ f = \mathrm{id}_X$, pak říkáme, že zobrazení g je *inverzní zleva* ke zobrazení f a že zobrazení f je *invertovatelné zleva.*
(2) $f \circ g = \mathrm{id}_Y$, pak říkáme, že zobrazení g je *inverzní zprava* ke zobrazení f a že zobrazení f je *invertovatelné zprava.*

Napřed si dokážeme jednoduché tvrzení, které říká, že zobrazení invertovatelné zleva i zprava už je invertovatelné.

Tvrzení 1.37. *Zobrazení $f : X \to Y$ je invertovatelné právě když je invertovatelné zleva i zprava.*

Důkaz. Přímo z definic vyplývá, že každé invertovatelné zobrazení je současně invertovatelné zleva i zprava.

Předpokládejme naopak, že zobrazení $f : X \to Y$ je současně invertovatelné zleva i zprava. Protože je invertovatelné zleva, existuje zobrazení $g : Y \to X$, pro které platí $g \circ f = \mathrm{id}_X$. Protože je invertovatelné zprava, existuje zobrazení $h : Y \to X$, pro které platí $f \circ h = \mathrm{id}_Y$. Dokážeme-li, že $g = h$, vyplyne z toho, že g je inverzní k f. Rovnost $g = h$ dokážeme následujícím výpočtem.

$$g = g \circ \mathrm{id}_Y = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_X \circ h = h \ .$$

Je důležité uvědomit si, proč každá z rovností ve výpočtu platí. Takže, první rovnost $g = g \circ \mathrm{id}_Y$ vyplývá z Tvrzení 1.32, neboť $g : Y \to X$. Druhá rovnost plyne z rovnosti $\mathrm{id}_Y = f \circ h$, neboť h je pravý inverz k f. Třetí rovnost $g \circ (f \circ h) = (g \circ f) \circ h$ je asociativita skládání zobrazení dokázaná v Tvrzení 1.28. Čtvrtá rovnost plyne z $g \circ f = \mathrm{id}_X$, neboť g je levý inverz k f. A poslední rovnost $\mathrm{id}_X \circ h = h$ plyne z Tvrzení 1.32, aplikovaného na zobrazení $h : Y \to X$. □

Z následujícího obecnějšího tvrzení vyplývá Tvrzení 1.35 charakterizující invertovatelná zobrazení. Zobrazení $f : X \to Y$ je podle definice vzájemně jednoznačné právě když je prosté a na množinu Y, což je podle následujícího tvrzení právě když je invertovatelné zleva a zprava, a to je podle právě dokázaného Tvrzení 1.37 právě když je invertovatelné. Není proto divu, že v důkazu následujícího tvrzení jsou podobné úvahy jako v důkazech Tvrzení 1.33 a 1.35. Stačí je pouze trochu jinak uspořádat a zpřesnit.

Tvrzení 1.38. *Předpokládejme, že X a Y jsou neprázdné množiny. Zobrazení $f : X \to Y$*

(1) *je prosté právě když existuje zobrazení $g : Y \to X$, které je inverzní zleva k f,*

(2) *je na množinu Y právě když existuje zobrazení $g : Y \to X$, které je inverzní zprava k f.*

Důkaz. První tvrzení se skládá ze dvou implikací. Předpokládejme napřed, že f je prosté. Hledáme zobrazení $g : Y \to X$, které je inverzní zleva k f. Jeho definici rozdělíme na dvě části. Je-li $y \in \mathrm{Im}\,(f)$, existuje podle definice $\mathrm{Im}\,(f)$ aspoň jedno $x \in X$ takové, že $f(x) = y$. Protože je f prosté, je takové x určené jednoznačně. Definujeme v tomto případě $g(y) = x$. Pokud $y \notin \mathrm{Im}\,(f)$, zvolíme za $g(y)$ libovolný prvek množiny X (která je neprázdná, takže to jde). Potom platí pro každé $x \in X$, že

$$(g \circ f)(x) = g(f(x)) = x \ ,$$

neboť $f(x) \in \mathrm{Im}\,(f)$. Tím je dokázáno, že $g \circ f = \mathrm{id}_X$, a tedy g je inverzní zleva k f.

Důkaz opačné implikace, že z existence zobrazení $g : Y \to X$ inverzního zleva k $f : X \to Y$ plyne, že f je prosté, můžeme prakticky beze změny převzít z důkazu Tvrzení 1.35. Jsou-li totiž $x, y \in X$ dva prvky takové, že $f(x) = f(y)$, pak si stačí si pouze uvědomit, že ve výpočtu

$$x = \mathrm{id}_X(x) = (g \circ f)(x) = g(f(x)) = g(f(y)) = (g \circ f)(y) = \mathrm{id}_x(y) = y$$

jsme použili pouze předpoklad, že g je inverzní zleva k f.

K důkazu druhého tvrzení můžeme také v jednom směru použít část důkazu Tvrzení 1.35. Pokud je $g : Y \to X$ zobrazení inverzní zprava k f, zvolíme libovolné $y \in Y$. Potom platí

$$y = \mathrm{id}_Y(y) = (f \circ g)(y) = f(g(y)) \ ,$$

což znamená, že pro $x = g(y)$ platí $f(x) = y$, což dokazuje, že f je na množinu Y. Při výpočtu jsme použili pouze předpoklad, že g je inverzní zprava k f.

Je-li naopak $f : X \to Y$ zobrazení na Y, existuje pro každé $y \in Y$ aspoň jeden prvek $x \in X$, pro který platí $f(x) = y$. Úplný vzor $f^{-1}(\{y\})$ je tedy vždy neprázdná množina a zvolíme za $g(y)$ libovolný prvek $x \in f^{-1}(\{y\})$. Pak platí pro každé $y \in Y$, že

$$(f \circ g)(y) = f(g(y)) = y \ ,$$

neboť jsme zvolili $g(y) \in f^{-1}(\{y\})$ a tedy platí $f(g(y)) = y$. □

Poslední odstavec důkazu předchozího tvrzení jsme použili následující krok. Pro každý prvek $y \in Y$ umíme vybrat nějaký prvek úplného vzoru $f^{-1}(\{y\}) \neq \emptyset$. K tomu, aby bylo zobrazení $g : Y \to X$ dobře definované, musíme to umět udělat pro všechna $y \in Y$ **najednou**. V případě nekonečné množiny Y je takový současný výběr prvků z podmnožin $f^{-1}(\{y\})$ pro každé $y \in Y$ možný pouze díky tzv. *axiomu výběru*. Jeho znění je následující.

Axiom výběru. Je-li $\{A_y : y \in Y\}$ soubor neprázdných podmnožin množiny X, pak existuje zobrazení $g : Y \to X$ takové, že $g(y) \in A_y$ pro každé $y \in Y$.

V případě, že Y je konečná množina, tj, když potřebujeme vybrat prvky z konečného souboru podmnožin množiny X, pak to můžeme udělat pomocí matematické indukce. Axiom výběru je nutný teprve ve chvíli, kdy je Y nekonečná množina, tj. máme-li dán nekonečný soubor podmnožin množiny X.

Axiom výběru je užitečný axiom teorie množin, bez kterého se řada oblastí matematiky neobejde. V kurzu lineární algebry axiom výběru budeme používat pouze zřídka.Ale například matematická analýza se bez axiomu výběru neobejde ani při důkazech zcela základních tvrzení.

Zakončíme jedním tvrzením, které také odlišuje konečné množiny od nekonečných.

Tvrzení 1.39. *Jsou-li X a Y dvě konečné množiny, které mají stejný počet prvků, pak zobrazení $f : X \to Y$ je prosté právě tehdy, když je na množinu Y.*

Důkaz. Je-li f prosté, má $\mathrm{Im}\,(f)$ stejný počet prvků jako X, tedy i stejný jako má Y. Protože $\mathrm{Im}\,(f) \subset Y$, musí být $\mathrm{Im}\,(f) = Y$. Není-li f prosté, má $\mathrm{Im}\,(f)$ ostře méně prvků než Y a tedy f nemůže být na množinu Y. □

Ani jedna z implikací v posledním tvrzení neplatí pro nekonečné množiny, jak ukazuje následující příklad.

Příklad 1.40. Definujeme zobrazení $f : \mathbb{N}_0 \to \mathbb{N}_0$ předpisem

$$f(n) = n + 1$$

pro každé přirozené číslo $n \in \mathbb{N}_0$ (kde $\mathbb{N}_0$ značí množinu všech přirozených čísel s nulou). Takové zobrazení není na $\mathbb{N}_0$, protože $0 \notin \mathrm{Im}\,(f)$. Je ale prosté, protože pokud pro nějaké dva prvky $m, n \in \mathbb{N}_0$ platí $f(m) = f(n)$, plyne odtud $m+1 = n+1$ a tedy $m = n$. Z toho, že f je prosté tedy neplyne, že je také na.

Zobrazení $g : \mathbb{N}_0 \to \mathbb{N}_0$ definujeme předpisem

$$g(n) = \lfloor n/2 \rfloor$$

pro každé $n \in \mathbb{N}_0$. Symbolem $\lfloor x \rfloor$ označujeme *dolní celou část* reálného čísla x, tj. největší celé číslo y menší nebo rovné x. Pro takto definované g platí $g(0) = 0 = g(1)$, takže g není prosté. Naopak pro jakékoliv přirozené číslo $k \in \mathbb{N}_0$ platí $k = g(2k)$, takže g je na množinu $\mathbb{N}_0$. Z toho, že je zobrazení g na, tak neplyne, že je prosté. ▲

KAPITOLA 2

Řešení soustav lineárních rovnic

Cíl. *Naučíme se řešit soustavy lineárních rovnic Gaussovou 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 úloh lze převést na řešení soustavy lineárních rovnic. Pro ilustraci uvedeme šest jednoduchých příkladů z různých oborů.

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

Geometricky sestrojíme střed hledané kružnice snadno. Sestrojíme osy úseček AB a BC a najdeme jejich průsečík. Chceme-li souřadnice středu vypočítat, přeložíme uvedený geometrický postup do jazyka algebry. Vše potřebné už umíme z první kapitoly, Příkladu 1.3.

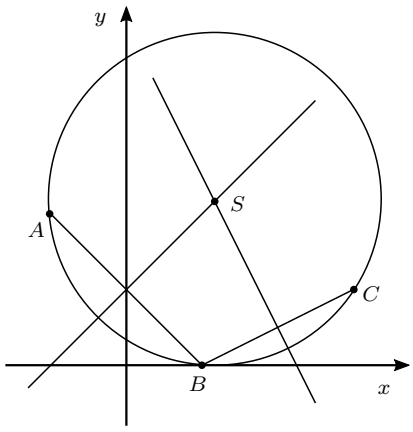
Vektor $B - A$ má souřadnice $(1, 0) - (-1, 2) = (2, -2)$, rovnice osy úsečky AB proto bude ve tvaru $2x - 2y = c$ a hodnotu c spočteme dosazením souřadnic středu úsečky AB, které jsou $(0, 1)$. Proto $c = 2 \cdot 0 - 2 \cdot 1 = -2$, takže osa AB má rovnici

$$2x - 2y = -2 \ .$$

Analogicky najdeme rovnici osy úsečky BC a dostaneme

$$2x + y = 9/2 \ .$$

Soustava těchto dvou rovnic má řešení $x = 7/6$ a $y = 13/6$.



Obrázek 2.1. Konstrukce a výpočet středu kružnice procházející třemi body

Našli jsme tak střed hledané kružnice $S = (7/6, 13/6)$. Poloměr snadno dopočítáme jako vzdálenost středu od kteréhokoliv ze tří daných bodů, vyjde $\sqrt{85/18}$.

Ve skutečnosti budou měření polohy obíhajícího objektu zatížena chybou, takže jich provedeme daleko více a vznikne soustava mnoha rovnic o dvou neznámých. Každá rovnice bude rovnicí osy nějaké dvojice naměřených poloh. Soustava zpravidla nebude mít řešení, osy se nebudou protínat v jednom bodě. Budeme hledat střed kružnice, který bude v nějakém smyslu nejlépe odpovídat naměřeným polohám. V kapitole o skalárním součinu se seznámíme s jednou metodou, pomocí které lze nějaký takový „nejlépe odpovídající bod“ najít. Bude to *metoda nejmenších čtverců*.

Otázky k samostatnému studiu 2.1. Vyřešte tuto úlohu pomocí parametrických tvarů os úseček AB, BC. Další možností jak úlohu řešit je vyjít z rovnice kružnice $(x-a)^2+(y-b)^2=r^2$ s neznámým středem (a,b) a poloměrem r. Dosadíme-li do ní postupně za x,y souřadnice bodů A,B,C, dostaneme soustavu tří kvadratických rovnic o třech neznámých a,b,r. Jak byste ji řešili? Jak soustavu upravíte, abyste dostali soustavu lineárních rovnic, kterou jsme použili my?

2.1.2. Vyčíslování chemické rovnice. Uvažujme chemickou reakci toluenu a kyseliny dusičné, při které vzniká 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.

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

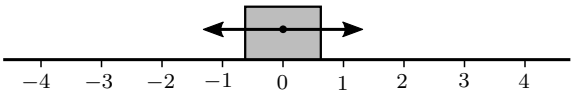
Chceme tedy najít hodnoty x,y,z,v, které splňují soustavu rovnic. To vede na rovnice

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

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*. Množina všech řešení takových soustav je důležitá pro obor nazývaný *lineární optimalizace* nebo také *lineární programování*. V takových úlohách se hledá maximum nebo minimum 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.

2.1.3. Řízení pohybu tělesa po přímce. Objekt jednotkové hmotnosti se pohybuje bez tření po přímce, na počátku je v poloze 0 a má nulovou rychlost. Po dobu osmi 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 $j = 1,2,\ldots,8$. Kladná síla působí zleva doprava, se záporným znaménkem působí opačným směrem. Chceme dosáhnout toho, aby se po osmi vteřinách poloha objektu rovnala 4 a jeho rychlost byla 0. Jde o velmi jednoduchý příklad úlohy *teorie řízení*.



Obrázek 2.2. Pohyb tělesa po přímce

Podle Newtonova zákona síla x_1 způsobí zrychlení tělesa $a_1 = x_1/m$, kde m je hmotnost tělesa, a protože předpokládáme $m = 1$, platí $a_1 = x_1$. Během jedné vteřiny tím změní rychlost tělesa o $v_1 = a_1 \cdot 1 = x_1$. Během druhé vteřiny se rychlost změní o x_2. Je-li směr působení síly x_2 opačný než u síly x_1, těleso se přibrzdí nebo dokonce změní směr pohybu, v případě souhlasně orientovaných sil se jeho rychlost zvýší. Po osmi vteřinách bude mít těleso rychlost

$$x_1 + x_2 + \cdots + x_8 \ .$$

Poloha tělesa po jedné vteřině bude $(1/2)v_1 \cdot 1^2 = (1/2)x_1$. Během druhé vteřiny rychlost v_1 přidá vzdálenost $v_1 \cdot 1 = x_1$. Síla x_2 působící během druhé vteřiny dále změní polohu tělesa o $(1/2)v_2 \cdot 1^2 = (1/2)x_2$. Jeho poloha po dvou vteřinách bude

$$\frac{1}{2}x_1 + \left(x_1 + \frac{1}{2}x_2\right) = \frac{3}{2}x_1 + \frac{1}{2}x_2 \ .$$

Má-li síla x_2 opačné znaménko než síla x_1, bude po dvou vteřinách vzdálenost tělesa od počátku menší, než by byla bez aplikace síly x_2.

Na konci druhé vteřiny tak bude mít těleso rychlost $x_1 + x_2$, která jej během třetí vteřiny posune dále o vzdálenost $x_1 + x_2$. Působení síly x_3 k ní přidá/ubere (v závislosti na znaménku x_3) ještě vzdálenost $(1/2)x_3$, takže po třech vteřinách bude těleso v poloze

$$\left(\frac{3}{2}x_1 + \frac{1}{2}x_2\right) + \left(x_1 + x_2 + \frac{1}{2}x_3\right) = \frac{5}{2}x_1 + \frac{3}{2}x_2 + \frac{1}{2}x_3 \ .$$

Po osmi vteřinách tedy bude poloha tělesa

$$\frac{15}{2}x_1 + \frac{13}{2}x_2 + \frac{11}{2}x_3 + \cdots + \frac{3}{2}x_7 + \frac{1}{2}x_8 \ .$$

Vidíme, že konečná poloha tělesa závisí nejvíce na síle aplikované v první vteřině a nejméně na síle použité v poslední osmé vteřině. Zatímco konečná rychlost je ovlivněná všemi silami stejně.

Řešení naší úlohy tak spočívá v řešení soustavy rovnic

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 &= 0 \\ \frac{15}{2}x_1 + \frac{13}{2}x_2 + \frac{11}{2}x_3 + \frac{9}{2}x_4 + \frac{7}{2}x_5 + \frac{5}{2}x_6 + \frac{3}{2}x_7 + \frac{1}{2}x_8 &= 4 \ , \end{aligned}$$

kterým získáme všechny možnosti pro vektor sil $(x_1, x_2, \ldots, x_8)$, které přemístí těleso během osmi vteřin z klidové polohy v počátku do klidové polohy v bodě 4.

Soustava má mnoho neznámých, málo rovnic a mnoho řešení. V této kapitole se naučíme uspokojivě popsat všechna řešení. V pozdějších kapitolách uvidíme, že množina všech řešení má dimenzi 6. V nematematických oborech se často říká, že úloha má 6 stupňů volnosti.

V praxi nám většinou půjde o to vybrat v nějakém smyslu nejvýhodnější řešení. Třeba chceme minimalizovat množství energie, kterou je třeba na přemístění tělesa vynaložit. Z fyziky víme, že působením síly x_j, která změní rychlost tělesa o $v_j = x_j$, vynaložíme energii $(1/2)mv_j^2 = (1/2)x_j^2$. Celková energie, kterou vynaložíme, zvolíme-li řešení $(x_1, x_2, \ldots, x_8)$, se tak rovná

$$E(x_1, x_2, \ldots, x_8) = \frac{1}{2}(x_1^2 + x_2^2 + \cdots + x_7^2 + x_8^2) \ .$$

Hledáme tedy to řešení, které minimalizuje funkci E na množině všech řešení. Další možná omezení jsou dána třeba maximální silou, kterou můžeme aplikovat, takže uvažujeme pouze ta řešení soustavy, pro která platí $-C \leq x_j \leq C$ pro nějakou konstantu $C > 0$ a každé x_j.

Stejně jako v úlohách lineárního programování minimalizujeme hodnotu nějaké funkce, v tomto případě kvadratické, na množině splňující soustavu lineárních rovnic a nerovností. Takovým úlohám se říká úlohy *kvadratické optimalizace* nebo *kvadratického programování*.

2.1.4. Navigace v rovině pomocí vzdálených majáků. Bezedným zdrojem soustav lineárních rovnic je tzv. *linearizace*. Linearizace spočívá v tom, že v úloze, kterou chceme řešit, složitější křivky nebo plochy nahradíme přímkami nebo rovinami. Často nahrazujeme křivku tečnou v daném bodě křivky, plochu tečnou rovinou v daném bodě plochy, možností je mnohem více. Jako příklad linearizace uvedeme navigaci v rovině pomocí vzdálených majáků. Jde o velmi zjednodušenou verzi GPS.

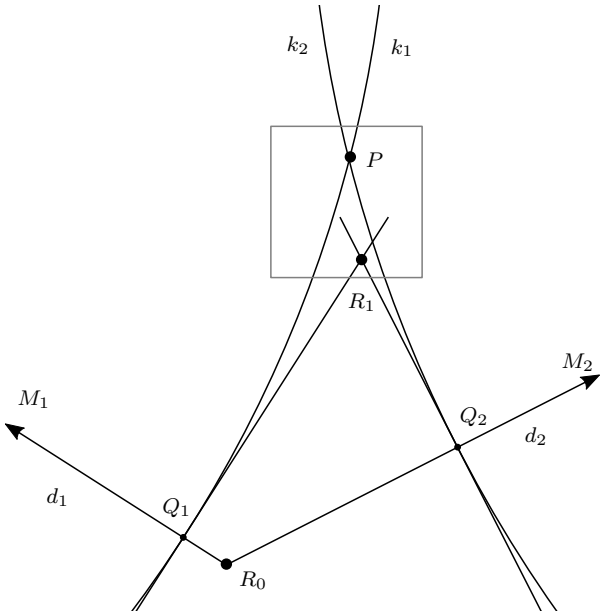
Navigační přístroj se nachází v rovině v nějakém bodě P s neznámými souřadnicemi (p, q). Umí ale získat vzdálenosti od majáků M_1 a M_2, které mají známé souřadnice (a_1, b_1) a (a_2, b_2). Vzdálenost od majáku M_1 je d_1, od majáku M_2 je d_2.

Souřadnice bodu P pak lze získat jako souřadnice průsečíku kružnice k_1 se středem M_1 a poloměrem d_1 s kružnicí k_2, která má střed v bodě M_2 a poloměr d_2. Čili jako řešení soustavy dvou kvadratických rovnic

$$\begin{aligned} (x - a_1)^2 + (y - b_1)^2 &= d_1^2 \\ (x - a_2)^2 + (y - b_2)^2 &= d_2^2 \ . \end{aligned}$$

Na rozdíl od hledání středu kružnice procházející třemi danými body nelze poslední soustavu převést na nějakou soustavu lineárních rovnic se stejným řešením. Příčina je v tom, že uvedená soustava dvou kvadratických rovnic může mít také dvě řešení, zatímco řešitelná soustava lineárních rovnic o dvou neznámých má buď jedno nebo nekonečně mnoho řešení.

Linearizace úlohy je znázorněna na obrázku 2.3. Navigace si zvolí jako počáteční odhad polohy nějaký bod R_0 se souřadnicemi (r_0, s_0). Pak spočítá vektory $M_1 - R_0$ a $M_2 - R_0$. Jednoduše lze najít rovnici tečny ke kružnici k_1 v bodě Q_1, který leží na spojnici bodů M_1 a R_0 (tj. ve vzdálenosti



OBRÁZEK 2.3. Navigace pomocí vzdálených majáků

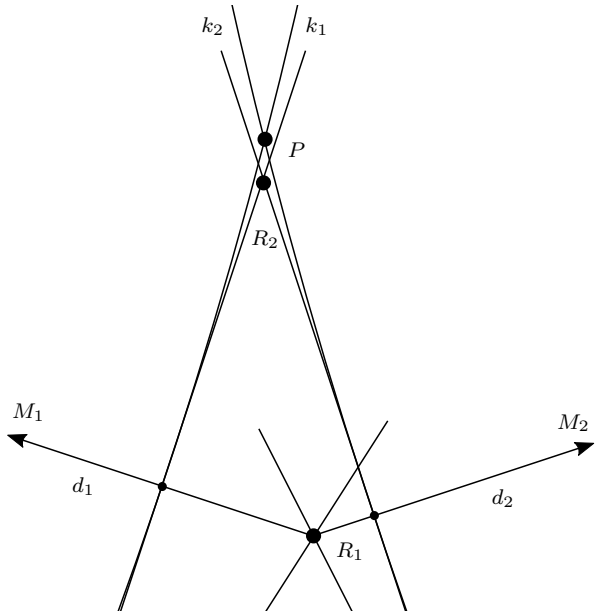
d_1 od majáku M_1). To už umíme, stačí modifikovat postup z příkladu 1.3. Později se v kapitole o skalárním součinu naučíme mnohem jednodušší způsob. Analogicky lze napsat rovnici tečny ke kružnici k_2 v průsečíku Q_2 spojnice bodů M_2 a R_0, který je ve vzdálenosti d_2 od majáku M_2. Nahrazením kružnic k_1 a k_2 tečnami v bodech Q_1 a Q_2 jsme úlohu *linearizovali*. Souřadnice průsečíku tečen už najdeme jako řešení soustavy dvou lineárních rovnic o dvou neznámých. Průsečík R_1 obou tečen zjevně není bodem P, ale je mu blíže, než původní odhad R_0, pokud je počáteční odhad R_0 zvolen blíže k bodu P než k druhému průsečíku obou kružnic.

Celý postup pak opakujeme s tím, že původní odhad polohy R_0 nahradíme vypočítaným bodem R_1. Na obrázku 2.4 je znázorněna druhá iterace hledání polohy ve zvětšeném výřezu z obrázku 2.3. Dostaneme tak souřadnice bodu R_2, který je ještě blíže ke skutečné poloze P. Celý výpočet opakujeme tak dlouho, dokud není rozdíl mezi dvěma po sobě vypočítanými body R_i dostatečně malý. Co je dostatečně malé, závisí na tom, jak přesně se při výpočtech chceme přiblížit skutečné poloze P.

Reálná situace je mnohem složitější. I v rovině můžeme použít více než dva majáky. V tom případě dostaneme aspoň tři tečny, které se nebudou protínat v jednom bodě, nejen kvůli nepřesnostem měření, soustava tří lineárních rovnic o dvou neznámých bude neřešitelná. V tom případě musíme použít metodu nejmenších čtverců, abychom získali bod R_1, který bude nejlépe odpovídat naměřeným vzdálenostem od tří nebo více majáků.

Reálná GPS pracuje v 3D prostoru s družicemi na oběžné dráze místo majáků. Každá družice vysílá každou tisícinu vteřiny informaci o své poloze v daném okamžiku. Navigační přístroj vidí v každém okamžiku aspoň čtyři družice, obvykle ale šest nebo sedm. Vzdálenosti od družic přístroj získá na základě toho, jak dlouho signál z družice letí. K tomu potřebuje napřed synchronizovat svůj čas s časem na družicích. Signál navíc prochází různými vrstvami atmosféry různou rychlostí, což je třeba také vzít v úvahu. Linearizace spočívá v náhradě koulí se středy v místech výskytu družic tečnými rovinami a výpočtem společného bodu těchto rovin coby řešení soustavy lineárních rovnic. Jako počáteční odhad polohy přijímač volí střed Země.

Uvedený příklad dobře ilustruje obvyklou metodu řešení praktických úloh. Absolutně přesné řešení sice existuje (v našem případě je to reálná poloha navigačního přístroje), ale nelze je vypočítat, protože výpočty závisí na měřených parametrech, jejichž hodnoty jsou zatížené chybami, tolerancí přístrojů, atmosférickými vlivy, erupcemi na Slunci, apod. Místo hledání přesného řešení se snažíme postupně se k němu přibližovat opakovaným použitím nějakého výpočetního postupu, v našem případě to bylo postupné řešení různých soustav lineárních rovnic o dvou neznámých, jejichž konkrétní podoba závisí na měřeních a předchozích výpočtech. Pokud umíme nějak dokázat, že přibližná řešení získaná v jednotlivých iteracích konvergují k absolutně přesnému řešení, můžeme se k němu přiblížit s libovolnou přesností, záleží pouze na tom, kolikrát postup opakujeme.

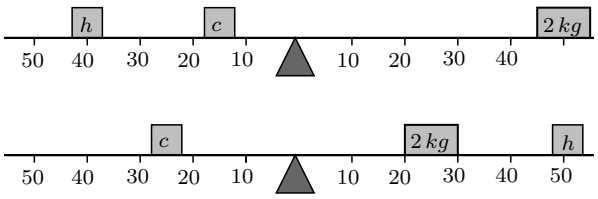


Obrázek 2.4. Navigace, druhá iterace

Otázky k samostatnému studiu 2.2. Na čem záleží rychlost konvergence postupně počítaným poloh ke skutečné poloze navigačního přístroje? Skutečná poloha navigace je v jednom ze dvou průsečíků kružnic se středem v majácích a poloměrem daným naměřenou vzdáleností navigace od majáku. Ke kterému z obou možných průsečíků se postupně přibližujeme pomocí výpočtů přibližných poloh?

2.1.5. Neznámá závaží. Dalším zdrojem úloh vedoucích na soustavy lineárních rovnic je studium rovnovážných fyzikálních systémů, které se nevyvíjejí v čase, jsou ustálené. Zde si ukážeme jeden příklad z mechaniky a v další úloze příklad z elektřiny.

Máme tři závaží. První váží $2kg$, ale hmotnost dalších dvou neznáme (představte si vesmírné objekty, jejichž vzdálenosti lze přímo určit, ale hmotnosti nikoliv). Podařilo se nám ale najít dvě rovnovážné polohy, viz obrázek.



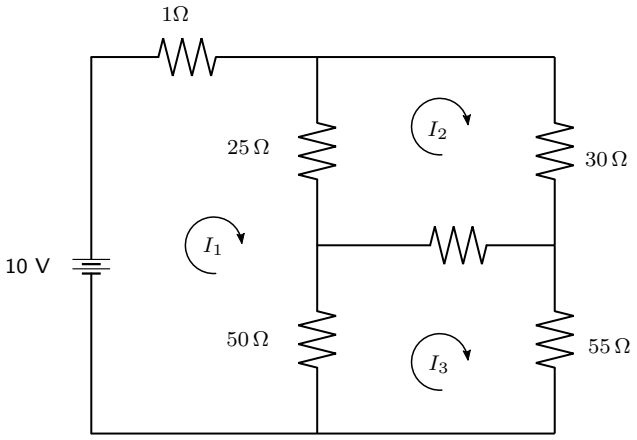
Obrázek 2.5. Neznámá závaží na páce

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.

Q_0



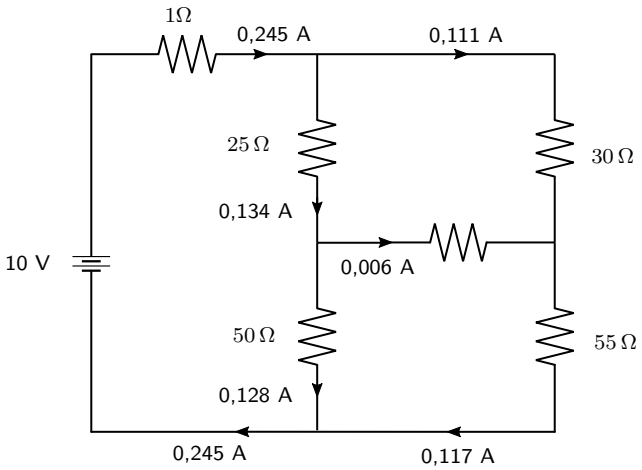
Obrázek 2.6. Elektrický obvod

2.1.6. Elektrické obvody. U elektrického obvodu na obrázku 2.6 chceme určit proudy protékající jednotlivými větvemi.

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. 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. 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.



Obrázek 2.7. Vypočítané proudy ve větvích obvodu

Výsledek na obrázku 2.7 je v souladu s dalším Kirchhoffovým zákonem, který říká, že součet velikostí proudů přitékajících do nějakého uzlu se rovná součtu proudů z tohoto uzlu odtékajících.

2.2. Soustavy lineárních rovnic a aritmetické vektory

2.2.1. Soustavy lineárních rovnic.

DEFINICE 2.3. *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 $x_1, x_2, \ldots, x_n$.

Reálná čísla $x_1, \ldots, x_n$ jsou *řešením* dané soustavy, pokud splňují zároveň všechny rovnice.

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

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} .$$

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.

Jak je vidět z definice, 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 2.5. 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 2.6.

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

▲

Pokud interpretujeme 2-složkové aritmetické vektory jako souřadnice geometrických vektorů v rovině, pak součet aritmetických vektorů odpovídá součtu geometrických vektorů, ukázali jsme si to na obrázku 1.10 v úvodní kapitole. Podobně součin čísla t s 2-složkovým aritmetickým vektorem $\mathbf{u}$ odpovídá t-násobku geometrického vektoru v rovině – obrázek 1.9. Stejný vztah mají operace s 3-složkovými aritmetickými vektory a odpovídající operace s vektory v prostoru, pouze obrázky by byly méně přehledné.

2.3. Ekvivalentní a elementární úpravy

Soustavy lineárních rovnic lze řešit tak, že postupně eliminujeme neznámé. Používáme k tomu úpravy, které nemění množinu všech řešení soustavy. Takovým úpravám říkáme *ekvivalentní úpravy.*

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

Eliminaci neznámé si nejprve ukážeme na příkladu dvou lineárních rovnic o dvou neznámých.

PŘÍKLAD 2.8. 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. Provedené úpravy jsou vratné v tom smyslu, že ze vzniklé soustavy rovnic lze odvodit původní soustavu. Proto mají obě soustavy stejnou množinu všech řešení a provedená úprava je tedy ekvivalentní.

Stejné úpravy soustavy můžeme dosáhnout mnohem rychleji tak, že připočteme (-3)-násobek první rovnice k druhé a první rovnici necháme beze změny. Vyjadřování a dosazování proto nebudeme nadále při eliminaci používat.

Vzniklou soustavu můžeme jednoduše dořešit. Z druhé rovnice vypočteme $x_2 = 1$ a dosadíme do první rovnice (znovu eliminace, tentokrát neznámé x_2). Dostaneme

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

Původní soustava má právě jedno řešení, a to $(1, 1)^T$. Jinými slovy, množina všech řešení soustavy je

$$\left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\} \ .$$

▲

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

DEFINICE 2.9. *Elementární úpravy* soustavy lineárních rovnic jsou

(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 2.10. *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 $(x_1, x_2, \ldots, x_n)^T$ 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. □

2.3.1. Soustava s jedním řešením. Jako další příklad vyřešíme následující soustavu tří lineárních rovnic o třech neznámých x_1, x_2, x_3 pomocí elementárních úprav.

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

Budeme postupně eliminovat neznámé tak, abychom převedli soustavu do tvaru, ze kterého se řešení snadno dopočítá. Tvar, o který se snažíme, je tzv. *odstupňovaný tvar*. Poněkud nepřesně řečeno odstupňovaný tvar znamená, že v každé rovnici je na začátku více nulových koeficientů než v rovnici předcházející.

Nejprve eliminujeme neznámou x_1, tj. docílíme toho, že ve všech rovnicích kromě první bude nulový koeficient u 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

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

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*.

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

Definice 2.11. *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 2.12. *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.

2.3.3. 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 (vynechání této rovnice není elementární úpravou, ale je zřejmě úpravou ekvivalentní). 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 $(-4, 1, 0)^T$.

2.3.4. Více parametrů. Podíváme se na soustavu s více parametry, ze které již snad bude vidět obecný postup. Soustava bude mít pět neznámých x_1, 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. Gaussova eliminační metoda

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*. Použití elementárních řádkových úprav je mnohem širší než na pouhé řešení soustav lineárních rovnic. S jejich pomocí zjistíme základní vlastnosti jakékoliv matice. Definujeme je proto obecně pro jakoukoliv matici.

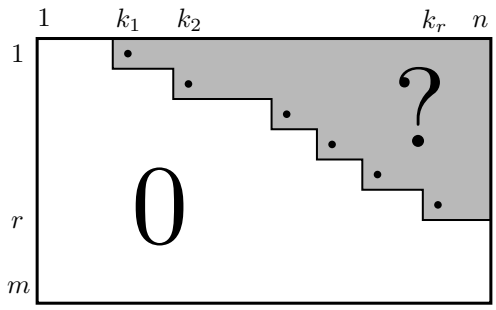
Definice 2.13. *Elementárními řádkovými úpravami* matice rozumíme následující tři typy úprav:

(i) prohození dvou řádků matice,

(ii) vynásobení jednoho z řádků matice nenulovým číslem,
(iii) přičtení libovolného 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. Matice $C = (c_{ij})_{m\times n}$ je v *odstupňovaném* tvaru, pokud v každém nenulovém řádku matice C kromě prvního je na počátku (tj. zleva) více nul, než na počátku řádku nad ním. Z této definice 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 2.8. Matice v řádkově odstupňovaném tvaru

Symbolicky můžeme definovat matici v řádkově odstupňovaném tvaru následovně.

Definice 2.14. 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 $k_1 < k_2 < \dots < k_r$, kde k_i je index sloupce, ve kterém je první nenulové číslo v i-tém řádku (tedy platí $c_{i1} = c_{i2} = \dots = c_{i,k_i-1} = 0$ a $c_{i,k_i} \neq 0$; ještě jinak, $k_i = \min\{l : c_{il} \neq 0\}$).

Prvkům c_{i,k_i}, $i = 1, 2, \dots, r$, 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 2.15. Matice

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

jsou v odstupňovaném tvaru. Matice

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

v odstupňovaném tvaru nejsou. ▲

Gaussova eliminace 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.

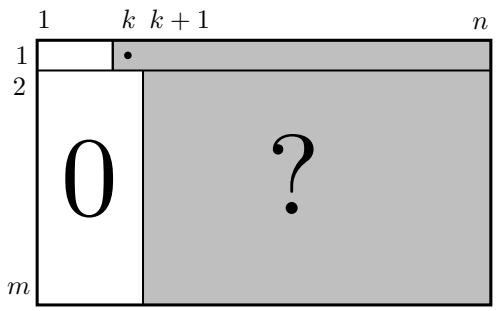
Náš popis Gaussovy eliminace není jednoznačný algoritmus, protože nepředepisujeme, který řádek prohodíme s prvním řádkem v kroku 2. Různé implementace Gaussovy eliminace to řeší různým způsobem, což je důvod, proč žádný konkrétní způsob nepředepisujeme. Více o tom v části 2.6 o numerické stabilitě.

VĚTA 2.16. *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. Pro $m = 1$ Gaussova eliminace nic nedělá a matice je vždy v odstupňovaném tvaru, takže tvrzení platí.

Předpokládejme, 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 2.9. 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 2.17. Nechť A je matice a C matice v odstupňovaném tvaru, kterou dostaneme z matice A Gaussovou eliminací. Nechť $r, k_1, k_2, \ldots, k_r$ jsou čísla z definice 2.14 pro matici C (!). Číslo r, tj. počet nenulových řádků v matici C, se nazývá *hodnost matice* A a značí se $r(A)$ nebo $\operatorname{rank}(A)$. Sloupce v matici A s indexy $k_1, k_2, \ldots, k_r$ nazýváme *bázové sloupce* matice A.

Přímo z definice hodnosti matice snadno ověříme následující tvrzení.

Pozorování 2.18. *Pro hodnost* $\operatorname{rank}(A)$ *matice* A *typu* $m \times n$ *platí nerovnosti*

$$\operatorname{rank}(A) \leq m, n \ .$$

Důkaz. Gaussova eliminace nemění počet řádků v matici, takže počet nenulových řádků v jakékoliv matici C, kterou dostaneme z matice A, je nejvýše rovný počtu všech řádků v matici A. Elementární řádkové úpravy zachovávají typ matice.

Dále v každém nenulovém řádku jakékoliv matice v odstupňovaném tvaru je první nenulový prvek pivot a různé pivoty leží v různých sloupcích, takže počet nenulových řádků v jakékoliv matici C v odstupňovaném tvaru, kterou dostaneme z matice A posloupností elementárních řádkových úprav, se rovná počtu pivotů v matici C a ten je menší nebo rovný počtu sloupců v matici C, tj. také v matici 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, ze které také můžeme určit bázové sloupce. Je-li sloupec pravých stran bázový, je poslední nenulový řádek matice $(C \,|\, \mathbf{d})$ tvaru $(0\ 0\ \ldots\ 0 \,|\, d_r)$, 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 nejsou bázové, tj.

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

Množina P může být i prázdná, pokud je každý sloupec s výjimkou sloupce pravých stran bázový. Proměnným x_p, $p \in P$, říkáme volné proměnné (nebo též parametry). Ostatní proměnné, tj. proměnné $x_{k_1}, x_{k_2}, \ldots, x_{k_r}$ jsou bázové 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 2.19. *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 $x_{k_1}, x_{k_2}, \ldots, x_{k_r} \in \mathbb{R}$ taková, že aritmetický vektor $(x_1, x_2, \ldots, x_n)^T$ je řešením soustavy $(A \,|\, \mathbf{b})$.*

Nakonec podobně jako v částech 2.3.3 a 2.3.4 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. Nebylo by těžké nahlédnout, že řešení lze skutečně zapsat v tomto tvaru, ale důkaz odložíme na dobu, kdy budeme mít vhodné pojmy a aparát.

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

Věta 2.20. *Množina všech řešení řešitelné soustavy $(A \,|\, \mathbf{b})$ o n neznámých je rovná množině*

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

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

Připomeňme ještě geometrický význam: S je nějaký "rovný útvar" (bod, přímka, rovina, ...), $\mathbf{u}$ je jeden z bodů v S a $\mathbf{v}_p$, $p \in P$ jsou směrové vektory.

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 $0x_1 + 0x_2 + \cdots + 0x_n = d \neq 0$, skončíme s tím, že soustava je neřešitelná.
3. Je-li řešitelná, 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 $(A \,|\, \mathbf{b})$ Gaussovou eliminací. Již dříve jsme definovali, že toto číslo se rovná hodnosti $\operatorname{rank}(A \,|\, \mathbf{b})$ 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.

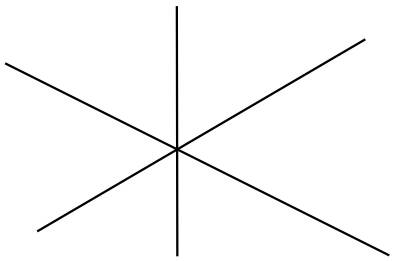
- Jak rozumět geometrii soustav lineárních rovnic?
- Co se může přihodit, budeme-li soustavy lineárních rovnic řešit na počítači?
- Jak dlouho to bude trvat?

2.5. Geometrie soustav lineárních rovnic

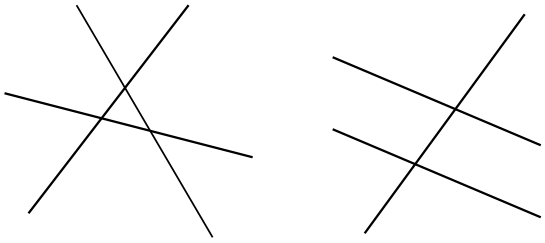
2.5.1. Řádkový pohled na soustavy lineárních rovnic. V první opakovací kapitole jsme si ukázali, že v případě soustavy lineárních rovnic o dvou neznámých x_1, x_2 určuje každá rovnice nějakou přímku v rovině, pokud je aspoň jeden z koeficientů u x_1 a x_2 nenulový. Množina všech řešení je potom průnikem 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.
- 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.



Obrázek 2.10. Geometrie jednoznačně řešitelné soustavy o dvou neznámých



Obrázek 2.11. Geometrické důvody neřešitelnosti soustavy o dvou neznámých

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

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

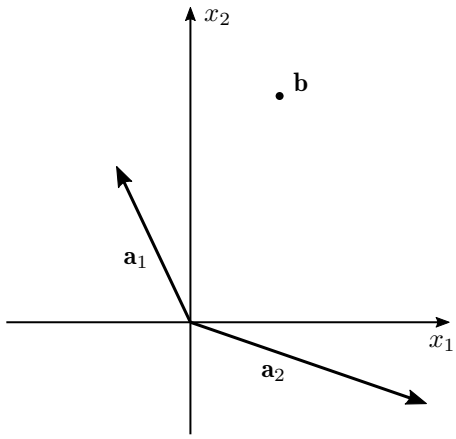
Všimněme si, že v prvním sloupci matice soustavy jsou koeficienty u proměnné x_1 a ve druhém sloupci jsou koeficienty u proměnné x_2. Těmto vektorům říkáme *sloupcové vektory* matice soustavy. Levou stranu poslední rovnosti můžeme pomocí sloupcových vektorů přepsat ve tvaru

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

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.



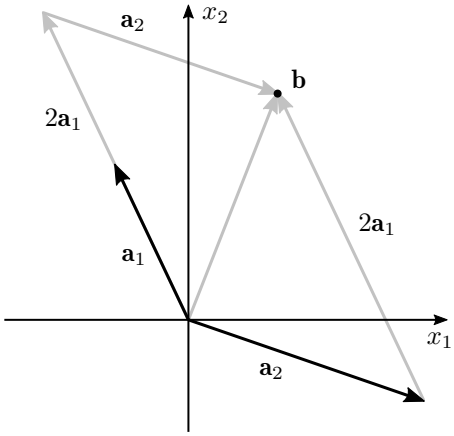
Obrázek 2.12. Sloupcové zadání soustavy o dvou neznámých

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 $(2, 1)^T$.



Obrázek 2.13. Geometrické řešení soustavy o dvou neznámých sloupcově

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. Z geometrického náhledu vidíme (i když to ještě neumíme efektivně dokázat), že vhodnou volbou násobků vektorů $\mathbf{a}_1 = (-1, 2)^T$ a $\mathbf{a}_2 = (3, -1)^T$ se můžeme trefit do jakéhokoliv bodu roviny a navíc právě jedním způsobem. Tento poznatek můžeme zformulovat také tak, že soustava

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

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 $\mathbf{a}_1 = (1, 2, 3)^T$ 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 $(0,0,0)^T$). 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, které je navíc určené jednoznačně. Soustava je tedy řešitelná právě tehdy, 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 2.21. 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 tehdy, 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 tehdy, 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, že 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 (všechny příklady v části o numerické stabilitě jsme převzali z učebnice Carl D. Meyer, *Matrix Analysis and Applied Linear Algebra*, SIAM 2000)

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

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 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.

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 průsečík 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 získané měřením, takže jsou zatížené chybou. Je proto zapotřebí změnit matematický model, který vedl k soustavě, navrhnout jiný experiment, apod., abychom se vyhnuli špatně podmíněným soustavám.

Nicméně numerická stabilita a špatná podmíněnost spolu těsně souvisí – numerickým řešením soustavy lineárních rovnic můžeme z dobře podmíněné soustavy vytvořit soustavu špatně podmíněnou a zaokrouhlování vedoucí k nepatrné změně koeficientů pak vede k naprosto jinému řešení.

Přesvědčit se o tom můžeme hned u prvního příkladu v části 2.6.1 o numerické stabilitě. V soustavě s maticí

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

svírají přímky určené jednotlivými rovnicemi úhel přibližně $\pi/4$, tj. 45°, což je docela dobrá podmíněnost. Po prvním kroku Gaussovy eliminace jsme dostali soustavu

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

ve které rovnice určují skoro rovnoběžné přímky. Drobná změna koeficientů a pravé strany v důsledku zaokrouhlování pak způsobila velkou změnu v řešení.

Při použití částečné pivotace jsme z původní soustavy dostali soustavu

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

a přímky definované rovnicemi soustavy stále svíraly úhel skoro $\pi/4$. Proto se řešení soustavy vlivem zaokrouhlování změnilo nepatrně.

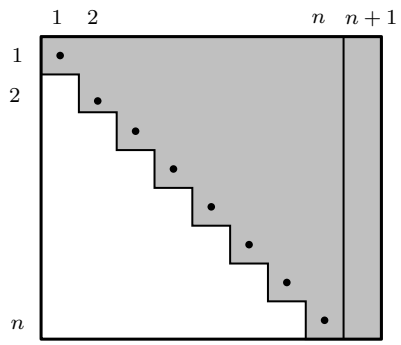
Z těchto úvah plyne zásadní poučení – numericky stabilní metody řešení soustav lineárních rovnic by neměly měnit úhly mezi přímkami (obecně nadrovinami) definovanými jednotlivými rovnicemi soustavy, méně formálně řečeno by neměly zhoršovat podmíněnost soustavy. V kapitole o skalárním součinu si ukážeme, jak toho dosáhnout. Tak jako ve všem, ani numerická stabilita není zadarmo, numericky stabilní algoritmy pro řešení soustav lineárních rovnic jsou pomalejší než Gaussova eliminace.

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 parametr, neboli že každá proměnná je bázová. Po Gaussově eliminaci jsou proto pivoty na místech s indexy 11, 22, 33, ..., nn. Ve skutečnosti toto je případ, který vyžaduje nejvíce aritmetických operací.



OBRÁZEK 2.14. Rozšířená matice soustavy po Gaussově eliminaci

Zvlášť spočteme počet aritmetických operací nutných pro Gaussovu eliminaci a zvlášť pro zpětnou substituci. 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_1 rovné 0.

Nakonec spočteme $n-1$ součtů $-(a_{21}/a_{11})a_{1i} + a_{2i}$ pro $i = 2, 3, \ldots, n$. 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 pod a_{11}, 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

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

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 následujícího tvrzení.

TVRZENÍ 2.22. *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

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

TVRZENÍ 2.23. *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 dvěma 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

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

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

(3) Vystačíme s ekvivalentními 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

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

(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:

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

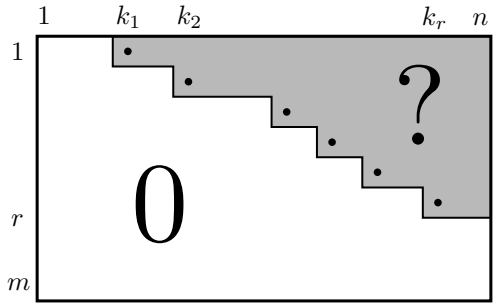
(8) Přidáme-li k matici soustavy *vektor pravých stran* $(b_1, b_2, \ldots, b_m)^T$, dostaneme *rozšířenou matici soustavy*

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

(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



Obrázek 2.15. Matice v řádkově odstupňovaném tvaru

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) Gaussovou 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 tvaru 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 Gaussovou 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 $x_{k_r}, x_{k_{r-1}}, \ldots, x_1$ 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 $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ aritmetické vektory nad $\mathbb{R}$ s m složkami a $a_1, a_2, \ldots, a_n$ reálná čísla, pak *lineární kombinací vektorů* $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ *s koeficienty* $a_1, a_2, \ldots, a_n$ nazýváme vektor

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

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

KAPITOLA 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 (tj. s reálnými koeficienty). 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 binární operaci $+$ s těmito vlastnostmi, pak můžeme na řešení rovnic typu $x + a = b$ (nebo $a + x = b$) použít zcela stejný postup. Binární operací 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

$$1 \cdot a = a \cdot 1 = a \ .$$

(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 dvěma 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 (5).

(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 $r \in \{0, 1, 2, \ldots, n-1\}$ 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

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

Zbytek při dělení číslem n je vždy v množině $\{0, 1, \ldots, n-1\}$. 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 $s = b \bmod n$. 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 označení 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 součin 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 těles 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. Jako první krok důkazu ukážeme, 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

$$\frac{a+b}{1+1}$$

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 v podstatě (až na přeznačení prvků) 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 $i \to j \to k \to i$:

$$\begin{tikzcd} & i \arrow[dr] & \\ k \arrow[ur] & & j \arrow[ll] \end{tikzcd}$$

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

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

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. Důležitými příklady takových zobrazení jsou rotace o nějaký úhel α kolem nějaké osy. V kapitole o unitární diagonalizaci si ukážeme, že složení dvou rotací kolem různých os je opět rotace kolem nějaké osy. Najít osu a úhel složené rotace ale 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, ze 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 $a, b \in T$, $b \neq 0$ 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, ...navzájem různá.

9. Nechť **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 dvěma binárními operacemi** $+$ a $\cdot$ na T splňující následující podmínky

(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 $a, b, c \in T$ platí $a \cdot (b + c) = a \cdot b + a \cdot c$.

(nT) T má aspoň dva prvky.

Uvedeným 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 $\mathbb{Q}$, $\mathbb{R}$ 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 $\mathbb{Z}_n = \{0, 1, \ldots, n - 1\}$.

(6) Analogicky definujeme *součin modulo* n jako zbytek při dělení běžného součinu ab číslem n.

(7) Pro každé prvočíslo p je množina $\mathbb{Z}_p$ všech „zbytků“ modulo p spolu s operacemi sčítání a násobení modulo p 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 odvozené vlastnosti.
(2) Umět počítat v tělesech $\mathbb{Z}_p$ a umět řešit soustavy lineárních rovnic nad tělesy $\mathbb{Z}_p$.
(3) Vědět, co je charakteristika tělesa.

KAPITOLA 4

Matice

Cíl. *Definujeme základní operace s maticemi a jejich vlastnosti. Jednoduché jsou operace sčítání matic, součin čísla s maticí a transponování matice. Složitější a zajímavější operací je součin matic. Ukážeme, jak matici interpretovat jako geometrické zobrazení a odhalíme geometrický význam násobení matic jako skládání zobrazení. Dále několika způsoby charakterizujeme matice, které jdou invertovat, a naučíme se inverzní matice počítat. Nakonec využijeme poznatky k dalšímu studiu soustav lineárních rovnic.*

Matice pro nás zatím byly pouze pomůckou k přehlednému zápisu soustav lineárních rovnic. Mnohá další data mají přirozenou maticovou strukturu nebo jdou do matice uspořádat. Uvedeme několik příkladů.

Příklad 4.1. 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 4.2. Nějaká velká korporace vyrábí řadu produktů. K jejich výrobě potřebuje mnoho vstupů (materiál, součástky, pracovní síly, energie, voda, atd.). Informaci o tom, kolik jednotek vstupů do výroby je potřeba na výrobu kterého produktu lze zaznamenat do matice $A = (a_{ij})$, kde a_{ij} je počet jednotek vstupu j potřebných k výrobě jednoho produktu i. V i-tém řádku matice A jsou tak počty jednotek jednotlivých vstupů potřebných k výrobě i-tého produktu. ▲

Příklad 4.3. Digitální fotoaparát zaznamenává pro každý pixel jeho barvu. Barva se skládá ze tří základních složek - R,G,B. Intenzitu každé ze tří základních 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 4.4. 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*. Jako konkrétní příklad si představte mapu leteckých spojení: vrcholy jsou letiště a dvě letiště u, v jsou spojeny hranou, pokud existuje přímé letecké spojení z u do v.

Graf lze zapsat pomocí *matice sousednosti*. Je to čtvercová matice řádu $|V|$, prvky a sloupce budeme indexovat prvky množiny V. Prvek na místě (u, v) je

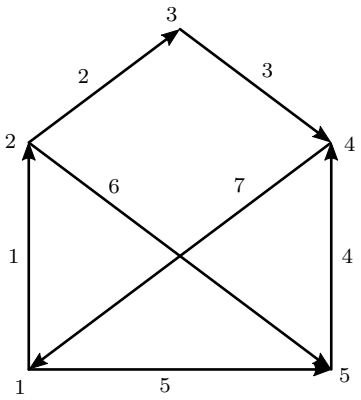
$$a_{uv} = \begin{cases} 1 & \text{pokud } (u,v) \in E, \\ 0 & \text{pokud } (u,v) \notin E. \end{cases}$$

Graf na obrázku 4.1 popíšeme maticí řádu 5:

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

▲

Příklad 4.5. Jiný typ matice grafu (V, E) je *matice incidence*. Je to obdélníková matice typu $|E| \times |V|$, jejíž řádky odpovídají hranám grafu a sloupce jeho vrcholům. Prvky matice se rovnají 0, 1 nebo -1. V řádku určeném hranou (u, v) je



OBRÁZEK 4.1. Příklad grafu

- 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 4.1 tak můžeme zapsat také následující maticí typu 7×5.

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

Tento způsob zápisu grafu je vhodný například ke zkoumání toků v sítích. ▲

PŘÍKLAD 4.6. Do matice můžeme také zapsat koeficienty kvadratického polynomu (lépe kvadratické formy)

$$x_1^2 + 4x_1x_2 + x_1x_3 + 2x_2^2 + 6x_2x_3 + 3x_2x_4 + 3x_3^2 + 2x_3x_4 + 4x_4^2 \ .$$

Jde o kvadratický polynom, protože v každém členu je součin nějakých dvou proměnných (mohou být i stejné) s nějakým koeficientem. Koeficienty zapíšeme do čtvercové matice $A = (a_{ij})$ řádu 4 (tj. řád je počet proměnných) tak, že na hlavní diagonálu zapíšeme koeficienty u druhých mocnin jednotlivých proměnných a mimo hlavní diagonálu na místo (i, j) zapíšeme jednu polovinu koeficientu u součinu x_ix_j. To znamená, že prvky na místech (i, j) a (j, i) se rovnají. Např. na místech $(1, 2)$ a $(2, 1)$ je číslo 2, neboť je to polovina koeficientu v členu $4x_1x_2$.

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

▲

4.1. Matice, jednoduché operace, typy matic

Začneme definicí matice a speciálních typů matic. Nová definice rozšiřuje stávající definice 2.4 a 2.11 tím, že prvky mohou být z libovolného pevně zvoleného tělesa.

DEFINICE 4.7. 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.

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 $i \in \{1, 2, \ldots, m\}$ a každé $j \in \{1, 2, \ldots, n\}$ platí $a_{ij} = b_{ij}$. Ověřit rovnost mezi dvěma maticemi tak znamená ověřit mn rovností mezi jejich prvky na stejných místech.

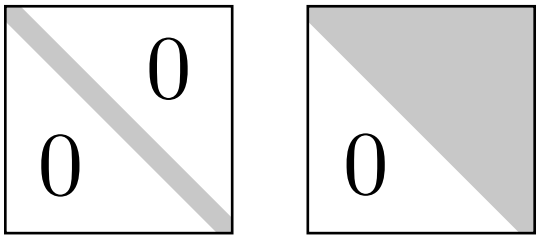
V dalším textu budeme používat následující speciální typy čtvercových matic.

Definice 4.8. Čtvercovou matici $A = (a_{ij})$ nazýváme

- *horní trojúhelníková*, pokud $a_{ij} = 0$ kdykoliv $i > j$,
- *dolní trojúhelníková*, pokud $a_{ij} = 0$ kdykoliv $i < j$,
- *diagonální*, pokud $a_{ij} = 0$ kdykoliv $i \neq j$,
- *jednotková*, pokud je diagonální a navíc $a_{ii} = 1$ pro každé i,
- *permutační*, má-li v každém řádku a každém sloupci právě jeden prvek 1 a ostatní 0,
- *symetrická*, pokud $a_{ij} = a_{ji}$ pro každé dva indexy i, j.

(Ve všech případech se rozumí, že daná podmínka je splněná pro všechny přípustné hodnoty i, j, tedy přirozená čísla mezi 1 a řádem matice.)

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



Obrázek 4.2. Diagonální a horní trojúhelníková matice

Jednotkovou matici řádu n (nad tělesem $\mathbf{T}$) budeme značit I_n:

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

Těleso, ve kterém počítáme, musí být zřejmé z kontextu. Prvky jednotkové matice také zapisujeme pomocí symbolu δ_{ij}, tzn. *Kroneckerovo delta*. Ten se rovná 1, pokud $i = j$, a 0 jinak. Pak můžeme napsat $I_n = (\delta_{ij})_{n \times n}$.

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

Definice 4.9. 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.

Příklad 4.10. 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 4.11. *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. □

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

Definice 4.12. Je-li $A = (a_{ij})$ matice typu $m \times n$ nad tělesem $\mathbf{T}$ a $t \in T$, 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 4.13. 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 4.14. *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. □

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

Definice 4.15. *Transponovaná matice* k matici $A = (a_{ij})_{m\times n}$ je matice $A^T = (b_{ij})_{n\times m}$, kde $b_{ij} = a_{ji}$ pro libovolné indexy $i \in \{1, 2, \dots, n\}$ a $j \in \{1, 2, \dots, m\}$.

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

Přímo z definic symetrické matice a transponované matice plyne, že čtvercová matice A je symetrická právě když $A^T = A$.

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 4.16. *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

Složitější a zajímavější operací s maticemi je jejich součin. Využijeme jej mimo jiné na maticový popis soustav lineárních rovnic a eliminačního procesu. Součin také umožňuje matematicky formulovat řadu situací a úloh. Několik z nich se naučíme řešit už v této kapitole, například se naučíme skládat některé typy geometrických zobrazení.

Pro součin 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

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

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.

Řádkový zápis matice je při tomto značení

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

kde $\tilde{\mathbf{a}}_i^T = (a_{i1}, a_{i2}, \ldots, a_{in})$ 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 4.17. Je-li $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ matice typu $m \times n$ nad tělesem $\mathbf{T}$ a $\mathbf{b} = (b_1, b_2, \ldots, b_n)^T$ (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 $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$ s koeficienty $b_1, b_2, \ldots, b_n$. Výsledkem je m-složkový vektor nad $\mathbf{T}$.

Příklad 4.18. 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 $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T \in \mathbf{T}^n$ 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.

Násobení matice vektorem má přirozenou interpretaci pro většinu příkladů z úvodu kapitoly. Podíváme se na příklad 4.2 o matici vstupů do výroby.

PŘÍKLAD 4.19. Matice $A = (a_{ij})$ zaznamenává vstupní materiálové jednotky náklady na produkty, řádky odpovídají produktům a sloupce vstupům. Prvek a_{ij} je roven počtu jednotek vstupu j potřebných k výrobě jednoho produktu i.

Označíme $\mathbf{x}$ vektor jednotkových 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 jednoho i-tého produktu. V tomto smyslu vektor $A\mathbf{x}$ popisuje výrobní ceny. ▲

4.2.2. Součin dvou matic.

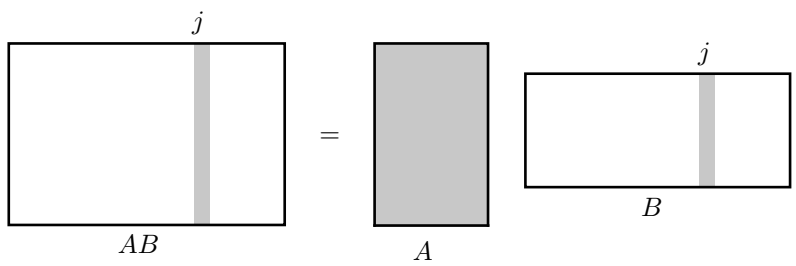
DEFINICE 4.20. Je-li A matice typu $m \times n$ a $B = (\mathbf{b}_1|\mathbf{b}_2|\cdots|\mathbf{b}_p)$ matice typu $n \times p$, obě nad stejným tělesem $\mathbf{T}$, pak *součinem matic* A a B rozumíme matici

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

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 4.3. 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 4.21. 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 výpočtu součinu dvou matic je někdy výhodnější použít následující tvrzení, které říká jak přímo spočítat jednotlivé prvky v součinu matic.

Tvrzení 4.22. *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*

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

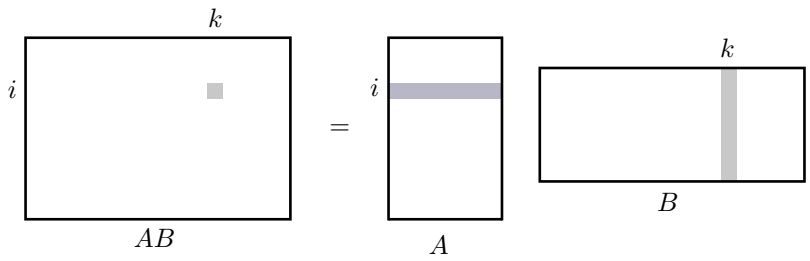
Důkaz. Prvek na místě (i,k) v součinu AB leží v k-tém sloupci, který se rovná $A\mathbf{b}_k$. Protože

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

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 4.4. Prvky v součinu 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 4.23. Počítáme opět nad $\mathbb{R}$.

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

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

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

▲

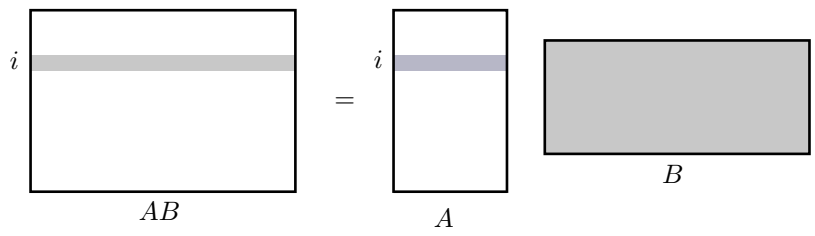
Víme už, jak vypadají sloupce a jednotlivé prvky v součinu AB. V následujícím tvrzení popíšeme jak v součinu AB vypadají řádky.

Tvrzení 4.24. *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. Tvzení lze dokázat podobně jako předchozí (cvičení), nebo můžeme využít transponování (viz příklad 4.34). □

Na obrázku 4.5 vidíme grafické znázornění řádků v součinu AB. Každý řádek v součinu matic je nějakou lineární kombinací řádků pravého činitele.



Obrázek 4.5. Řádky v součinu matic

Příklad 4.25. Podívejme se ještě jednou na součin v příkladu 4.23.

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

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. ▲

Dohromady zatím máme tři pohledy na součin matic: sloupcový (definice 4.20), po prvcích (tvrzení 4.22) a řádkový (tvrzení 4.24). Další, geometrický význam, bude vysvětlen v 4.3.3.

4.2.3. Vlastnosti součinu. Začneme varováním:

násobení matic není komutativní.

Jsou pro to dokonce tři různé důvody. Může být definován pouze jeden ze součinů AB a BA (například když A má typ 2×2 a B má typ 2×3). Pokud jsou definovány oba, mohou mít různý typ (příklad 4.26). A pokud mají stejný typ, může platit $AB \neq BA$ (příklad 4.27).

Příklad 4.26. Nad tělesem $\mathbb{R}$ máme

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

▲

Příklad 4.27. Opět počítáme s reálnými maticemi.

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

zatímco

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

▲

Některé jiné vlastnosti počítání v tělesech se ale na počítání s maticemi přenáší.

Tvrzení 4.28. *Pro libovolnou matice A typu $m \times n$ platí $I_m A = A = A I_n$.*

Důkaz. První rovnost plyne z řádkového pohledu na maticové násobení: i-tý řádek matice $I_m A$ je roven i-tému řádku matice A. Analogicky, druhá rovnost plyne ze sloupcového pohledu. □

Tvrzení 4.29. *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 4.22 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

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

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. Tento krok je založený na definici příslušných operací s maticemi a vlastnostech počítání v tělese.

Důležitou asociativitu násobení matic dokážeme v následujícím tvrzení.

Tvrzení 4.30. *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 $i \in \{1, 2, \dots, m\}$ a $l \in \{1, 2, \dots, q\}$ 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 $(BC)D = B(CD)$. □

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

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

Výsledek totiž nezávisí na uzávorkování. Mocnění matic hraje důležitou roli v aplikacích, jako ukázku uvedeme v části 4.2.6 dva příklady. Při této definici kladných

mocnin čtvercové matice platí pro každou matici A a každá dvě kladná celá čísla k, l rovnost

$$A^{k+l} = A^k A^l \ .$$

Jak rychle spočítat libovolnou kladnou mocninu čtvercové matice se naučíme v kapitole o vlastních číslech.

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

Tvrzení 4.31. *Pro libovolné matice A typu $m \times n$ a B typu $n \times p$, a každý prvek s tělesa $\mathbf{T}$ platí*

- $s(AB) = (sA)B = A(sB)$,
- $(AB)^T = B^T A^T$,
- *matice AA^T a $A^T A$ symetrické.*

Vlastnosti transponování lze často využít k důkazu nějakého tvrzení pro sloupce, známe-li již příslušné tvrzení pro řádky.

V následujícím příkladu využijeme řadu vlastností operací s maticemi.

Příklad 4.32. Víme už, že čtvercová matice $A = (a_{ij})$ řádu n je symetrická právě když platí $A^T = A$. Pomocí vlastností z tvrzení 4.31 a tvrzení 4.16 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 druhou vlastnost z tvrzení 4.31, když jsme například nepsali závorky ve výrazu $2AA^T$. ▲

Při řešení předchozího příkladu jsme použili speciální případ následujícího tvrzení, které si snadno dokážete sami.

Tvrzení 4.33. *Pro každou matici A typu $m \times n$ jsou matice AA^T a $A^T A$ symetrické.*

Vlastnosti transponování lze často využít k důkazu nějakého tvrzení pro sloupce, známe-li již příslušné tvrzení pro řádky. Jako ukázku dokážeme tvrzení 4.24.

Příklad 4.34. Máme matice A typu $m \times n$ a B typu $n \times p$. Chceme dokázat, že se i-tý řádek v součinu AB rovná

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

Podle definice transponované matice se i-tý řádek v matici AB rovná i-tému sloupci transponované matice $(AB)^T$. Z třetí rovnosti v předchozím tvrzení 4.31 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. platí

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

Přechodem k transponovaným maticím na obou stranách poslední rovnosti a s využitím vlastností transponování z tvrzení 4.16 dostaneme rovnost

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

▲

Z uvedených vlastností součinu snadno vyplývají další vlastnosti, jako například

$$A(B-C) = AB - AC, \quad A(-B) = -AB,$$

kdykoliv má jedna strana smysl. Důkazy přenecháme jako cvičení.

Následující tvrzení ukazuje, že součin dvou matic jednoho ze speciálních typů z definice 4.8 je opět matice téhož typu.

Tvrzení 4.35. *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 4.22. 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 4.20 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 4.22. 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). □

4.2.4. Elementární matice. Tvrzení 4.24 o řádkovém pohledu na násobení matic vede k následujícímu maticovému popisu elementárních řádkových úprav.

TVRZENÍ 4.36. *Nechť C je matice typu $m \times n$ nad tělesem $\mathbf{T}$, $i, j \in \{1, 2, \dots, m\}$, $i \neq j$, a $0 \neq t \in T$.*

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

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

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

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

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

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

DŮKAZ. Tvrzení plyne z tvrzení 4.24. □

Maticím E z předchozího tvrzení říkáme *elementární matice*. Elegatně je můžeme definovat následujícím způsobem.

DEFINICE 4.37. *Elementární matice* je čtvercová matice, která vznikne z jednotkové matice jednou elementární řádkovou úpravou.

Elementární řádkovou úpravu nějaké matice C lze tedy chápat tak, že matici C násobíme zleva vhodnou elementární maticí. To nám dává elegantní a účinný formalizmus pro řádkové úpravy. Elementární matice využijeme například při výpočtu inverzních matic a při dalším zkoumání průběhu Gaussovy eliminace.

4.2.5. Dyadický rozvoj součinu matic. Ukážeme si ještě jeden pohled na součin matic, tzv. *dyadický rozvoj* součinu matic. Začneme jednoduchým tvrzením charakterizujícím matice hodnosti 1.

TVRZENÍ 4.38. *Jsou-li* $\mathbf{a} = (a_1, a_2, \ldots, a_m)^T \in \mathbf{T}^m$ *a* $\mathbf{b} = (b_1, b_2, \ldots, b_n)^T \in \mathbf{T}^n$ *libovolné dva nenulové vektory, pak matice* $\mathbf{a}\mathbf{b}^T$ *typu* $m \times n$ *má hodnost 1. Naopak, každou matici* C *typu* $m \times n$*, která má hodnost 1, lze vyjádřit ve tvaru* $C = \mathbf{a}\mathbf{b}^T$ *pro vhodné vektory* $\mathbf{a} \in \mathbf{T}^m$ *a* $\mathbf{b} \in \mathbf{T}^n$.

DŮKAZ. Podle tvrzení 4.24 o řádcích v součinu dvou matic se i-tý řádek v součinu $\mathbf{a}\mathbf{b}^T$ rovná a_i-násobku řádkového vektoru $\mathbf{b}^T = (b_1, b_2, \ldots, b_n) \neq \mathbf{o}_n$, takže

$$\mathbf{a}\mathbf{b}^T = \begin{pmatrix} a_1\mathbf{b}^T \\ a_2\mathbf{b}^T \\ \vdots \\ a_m\mathbf{b}^T \end{pmatrix} .$$

Při Gaussově eliminaci matice $\mathbf{a}\mathbf{b}^T$ najdeme nějaký nenulový řádek, tj. nějaké i takové, že $a_i \neq 0$. Prohodíme první a i-tý řádek, je-li $i > 1$. Nyní pro každé $k > 1$ odečteme $(a_k a_i^{-1})$-násobek prvního řádku $a_i\mathbf{b}^T$ od k-tého řádku $a_k\mathbf{b}^T$. Tím vynulujeme celý k-tý řádek. Po prvním cyklu Gaussovy eliminace zůstane jediný nenulový řádek, takže tím Gaussova eliminace končí a $\operatorname{rank}(\mathbf{a}\mathbf{b}^T) = 1$.

Má-li naopak matice C hodnost 1, skončí Gaussova eliminace po prvním cyklu. V něm, je-li to třeba, prohodíme první řádek s nějakým řádkem pod ním. Pak odečítáme vhodné násobky prvního řádku od řádků pod ním. Pro jednoduchost předpokládejme, že první řádek matice C není třeba prohazovat s nějakým řádkem pod ním. Položíme $\mathbf{b} = \tilde{\mathbf{c}}_1$, tj. $\mathbf{b}^T$ se rovná prvnímu řádku matice C. Protože Gaussova eliminace skončí po prvním cyklu, všechny řádky pod prvním řádkem tím vynulujeme. Pro každé $i = 2, \ldots, m$ je proto i-tý řádek matice C nějakým a_i-násobkem prvního řádku $\tilde{\mathbf{c}}_1^T = \mathbf{b}^T$. Položíme $\mathbf{a} = (a_1 = 1, a_2, \ldots, a_m)$. Pak $\mathbf{a}\mathbf{b}^T = C$.

V případě, že první cyklus Gaussovy eliminace vyžaduje prohození prvního a i-tého řádku, jsou všechny řádky matice C násobky i-tého řádku. Zbytek důkazu v tomto případě ponecháme jako cvičení. □

DEFINICE 4.39. *Dyadickým rozvojem* nějaké matice C typu $m \times n$ nad $\mathbf{T}$ nazýváme její vyjádření jako součtu matic hodnosti 1, tj. vyjádření ve tvaru

$$C = \sum_{i=1}^{k} \mathbf{a}_i \mathbf{b}_i^T ,$$

kde $\mathbf{a}_i \in \mathbf{T}^m$ a $\mathbf{b}_i \in \mathbf{T}^n$ jsou nenulové vektory pro všechna $i = 1, 2, \ldots, k$.

Součin dvou matic má velmi jednoduchý dyadický rozvoj.

TVRZENÍ 4.40. *Jsou-li* $A = (a_{ij})$ *matice typu* $m \times n$ *a* $B = (b_{jk})$ *matice typu* $n \times p$*, obě nad tělesem* $\mathbf{T}$*, pak platí*

$$AB = \sum_{j=1}^{n} \mathbf{a}_j \tilde{\mathbf{b}}_j^T .$$

DŮKAZ. Podle tvrzení 4.22 o prvcích v součinu matic dostáváme, že prvek na místě (i, k) v součinu $\mathbf{a}_j\tilde{\mathbf{b}}_j^T$ se rovná $a_{ij}b_{jk}$. Prvek na místě (i, k) v sumě na pravé straně dokazované rovnosti se tak rovná

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

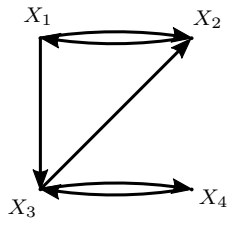
což je podle téhož tvrzení 4.22 prvek na místě (i, k) v součinu matic AB. Protože to platí pro každé $i = 1, 2, \ldots, m$ a $k = 1, 2, \ldots, p$, je tím rovnost dokázána. □

Každý sčítanec v rozvoji součinu AB z předchozího tvrzení má buď hodnost 1 podle tvrzení 4.38 charakterizujícího matice s hodností 1 a nebo jsou to nulové matice (pokud je aspoň jeden z vektorů $\mathbf{a}_j, \tilde{\mathbf{b}}_j$ nulový).

V kapitole o ortogonální diagonalizaci si ukážeme speciální dyadický rozvoj libovolné matice, tzv. singulární rozklad, který má rozsáhlé využití ve všech možných oblastech matematiky a jejich aplikacích.

4.2.6. Tři aplikace. Ukážeme dvě úlohy, které vedou na výpočet mocniny matice.

Příklad 4.41 (Počet cest). Na obrázku 4.6 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.



Obrázek 4.6. Letecká spojení

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 spojení do X_j, a $a_{ij} = 0$ v opačném případě. (Je to matice sousednosti grafu, viz příklad 4.4.)

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

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

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

▲

Příklad 4.42 (Rekurentní rovnice). Asi jste se již setkali s Fibonacciho posloupností definovanou předpisem

$$a_0 = 0,\ a_1 = 1, \quad a_{i+2} = a_{i+1} + a_i \text{ pro každé } i = 0, 1, 2 \ldots$$

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

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = C \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}, \begin{pmatrix} a_2 \\ a_3 \end{pmatrix} = C \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = C \left(C \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \right) = C^2 \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} ,$$

a indukcí podle i dostaneme

$$\begin{pmatrix} a_{i+1} \\ a_{i+2} \end{pmatrix} = C^i \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = C^i \begin{pmatrix} 0 \\ 1 \end{pmatrix} \ .$$

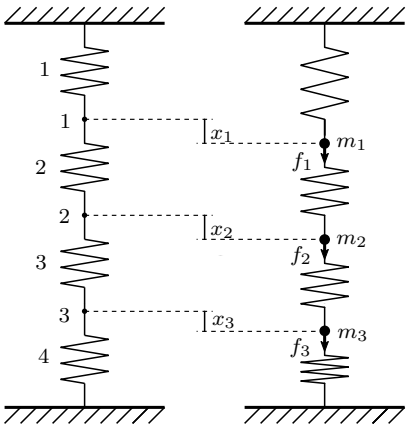
Podstatným způsobem zde využíváme asociativitu násobení matic. K výpočtu i-tého členu Fibonacciho posloupnosti tedy stačí umět mocnit matice. To se naučíme v kapitole o vlastních číslech a vektorech. Vyjde možná překvapivý vzorec

$$a_i = \frac{\varphi^i}{\sqrt{5}} - \frac{(1-\varphi)^i}{\sqrt{5}} \ ,$$

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

Poslední příklad ukazuje využití maticového násobení k matematickému popisu fyzikální úlohy.

Příklad 4.43. Na obrázku 4.7 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 $x_0 = x_4 = 0$.



Obrázek 4.7. Zavěšené pružiny

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

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, tentokrát 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

$$A^T C A \mathbf{x} = \mathbf{f},$$

což je soustava lineárních rovnic s maticí $A^T C A$ a pravou stranou $\mathbf{f}$. Z té 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.

4.2.7. 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 4.22. 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 $m_1, \ldots, m_r$, $n_1, \ldots, n_s$ a $p_1, \ldots, p_t$ 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_r 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}.

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

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

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

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

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

$$C = AB = \begin{array}{c} \\ m_1 \\ m_2 \\ \vdots \\ m_r \end{array} \begin{array}{c} \begin{array}{cccc} p_1 & p_2 & & p_t \end{array} \\ \left(\begin{array}{c|c|c|c} C_{11} & C_{12} & \vdots\vdots\vdots & C_{1t} \\ \hline C_{21} & C_{22} & \ldots & C_{2t} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline C_{r1} & C_{r2} & \ldots & C_{rt} \end{array}\right) \end{array} ,$$

kde pro každé $i \in \{1, 2, \ldots, r\}$ a $k \in \{1, 2, \ldots, t\}$ 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 4.44. 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. Matice jako zobrazení

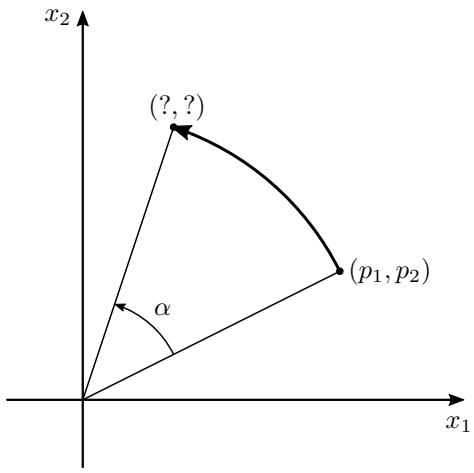
Každá matice A typu $m \times n$ nad tělesem $\mathbf{T}$ přirozeným způsobem určuje zobrazení $T^n \to T^m$, které budeme označovat f_A. Tato geometrická představa matic se od teď bude prolínat celým výkladem. Zobrazení f_A určené maticí A je popsáno v definici 4.47. Nejprve se ale podíváme na několik příkladů, jak pomocí matic algebraicky popsat některá jednoduchá geometrická zobrazení v rovině.

4.3.1. Zobrazení v rovině. Začneme otočením kolem počátku souřadnic o úhel α v kladném směru, tj. proti směru hodinových ručiček.

Příklad 4.45. Rovinu otočíme kolem počátku souřadnic o úhel α. Kam se pootočí bod se souřadnicemi $(p_1, p_2)^T$, tj. jaké budou jeho souřadnice po otočení?

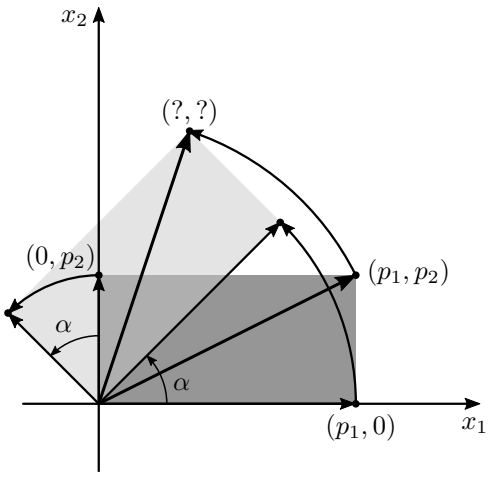
Spočítat souřadnice bodu, do kterého se pootočí bod $(p_1, p_2)^T$, přímo pomocí euklidovské geometrie je dost pracné. Ukážeme si algebraické řešení, na kterém lze vidět základní rysy lineárně algebraického uvažování. Místo toho, abychom počítali ihned souřadnice bodu, do kterého se pootočí bod $(p_1, p_2)^T$, se napřed zamyslíme nad tím, můžeme-li úlohu snadno vyřešit pro nějaké jiné body. A pokud to pro nějaké jiné body umíme, jak této znalosti můžeme využít pro výpočet souřadnic bodu, do kterého se pootočí bod $(p_1, p_2)^T$? Na obrázku 4.9 vidíme obdélník, jehož vrcholy jsou body $(0, 0)^T, (p_1, 0)^T, (0, p_2)^T, (p_1, p_2)^T$. Tento obdélník se pootočením o úhel α kolem počátku souřadnic zobrazí do druhého obdélníku na obrázku.

Nyní přichází to hlavní. Polohový vektor bodu $(p_1, p_2)^T$ je součtem polohových vektorů bodů $(p_1, 0)^T$ a $(0, p_2)^T$. Pomocí obrázku 4.9 nahlédneme, že tato vlastnost se otočením zachová – polohový vektor bodu $(?, ?)^T$, do kterého se pootočí bod



Obrázek 4.8. Rotace v rovině kolem počátku o úhel α

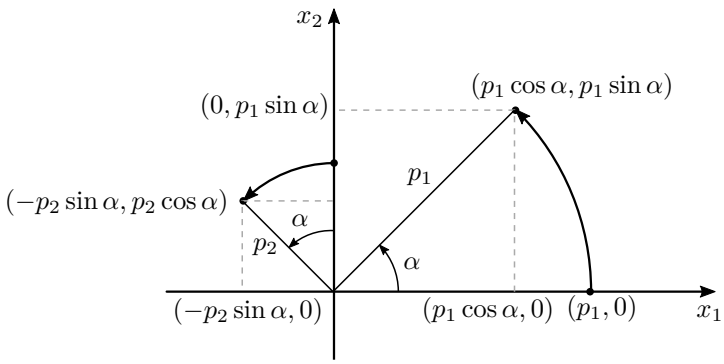
$(p_1, p_2)^T$, je součtem polohových vektorů bodů, do kterých se pootočí body $(p_1, 0)^T$ a $(0, p_2)^T$.



Obrázek 4.9. Rotace obdélníku v rovině kolem počátku o úhel α

Snadno spočítáme, že bod na první souřadné ose se souřadnicemi $(p_1, 0)^T$ se pootočí do bodu $(p_1 \cos\alpha, p_1 \sin\alpha)^T$. A podobně bod na druhé souřadné ose se souřadnicemi $(0, p_2)$ se pootočí do bodu o souřadnicích $(-p_2 \sin\alpha, p_2 \cos\alpha)^T$, viz obrázek 4.10.

Tím pádem také víme, že souřadnice polohového vektoru bodu $(?, ?)^T$ jsou součtem aritmetických vektorů $(p_1 \cos\alpha, p_1 \sin\alpha)^T$ a $(-p_2 \sin\alpha, p_2 \cos\alpha)^T$.



Obrázek 4.10. Výpočet souřadnic obrazů bodů na souřadných osách

Bod se souřadnicemi $(p_1, p_2)^T$ se tedy pootočí do bodu se souřadnicemi

$$\begin{pmatrix} ? \\ ? \end{pmatrix} = \begin{pmatrix} p_1 \cos\alpha \\ p_1 \sin\alpha \end{pmatrix} + \begin{pmatrix} -p_2 \sin\alpha \\ p_2 \cos\alpha \end{pmatrix} = p_1 \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} + p_2 \begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix}$$
$$= \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} .$$

▲

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 4.46. Osová symetrie vzhledem k první souřadné ose v rovině zobrazuje každý bod se souřadnicemi $(p_1, p_2)^T$ do bodu se souřadnicemi

$$\begin{pmatrix} p_1 \\ -p_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} .$$

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). ▲

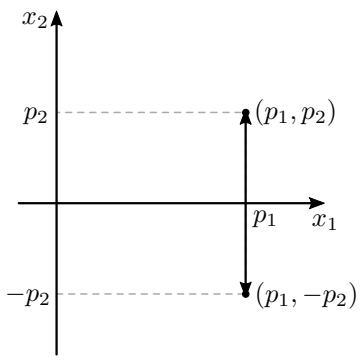
V obou příkladech jsme ze znalosti hodnot zobrazení (rotace nebo symetrie) v těchto dvou bodech mohli odvodit hodnotu zobrazení v každém dalším bodě roviny.

4.3.2. Zobrazení určené maticí. Pro každou matici A typu $m \times n$ nad tělesem $\mathbf{T}$ a každý n-složkový aritmetický vektor $\mathbf{x} \in T^n$ je součin $A\mathbf{x}$ prvkem T^m. Matice A tak určuje zobrazení z T^n do T^m ve smyslu následující **zásadní** definice.

Definice 4.47. Je-li A matice typu $m \times n$ nad tělesem $\mathbf{T}$, pak definujeme *zobrazení $f_A : T^n \to T^m$ určené maticí A* předpisem

$$f_A(\mathbf{x}) = A\mathbf{x}$$

pro každý aritmetický vektor $\mathbf{x} \in T^n$.



Obrázek 4.11. Symetrie v rovině vzhledem k první souřadné ose

Je-li

$$A = (a_{ij})_{m\times n} = (\mathbf{a}_1|\mathbf{a}_2|\dots|\mathbf{a}_n)$$

a přepíšeme-li výraz $A\mathbf{x}$ pomocí sloupcové definice součinu matic, dostáváme

$$f_A\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = x_1\mathbf{a}_1 + x_2\mathbf{a}_2 + \dots + x_n\mathbf{a}_n \ .$$

Obrazem vektoru $\mathbf{x}$ při zobrazení f_A je tedy lineární kombinace sloupcových vektorů matice A s koeficienty rovnými složkám vektoru $\mathbf{x}$.

Pokud přepíšeme výraz $A\mathbf{x}$ pomocí „prvkové“ definice součinu matic, dostaneme

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

Každá složka obrazu vektoru $\mathbf{x}$ je tedy tvaru $c_1x_1 + \dots + c_nx_n$ pro nějaké prvky $c_i \in T$.

Příklad 4.48. V příkladu 4.45 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

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

Obrazem vektoru $\mathbf{x} = (x_1, x_2)^T$ je vektor

$$f_A(\mathbf{x}) = A\mathbf{x} = x_1\begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} + x_2\begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix} = \begin{pmatrix} x_1\cos\alpha - x_2\sin\alpha \\ x_1\sin\alpha + x_2\cos\alpha \end{pmatrix}$$

▲

Příklad 4.49. Osová symetrie v rovině vzhledem k první souřadné ose je podle příkladu 4.46 zobrazení určené maticí

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

▲

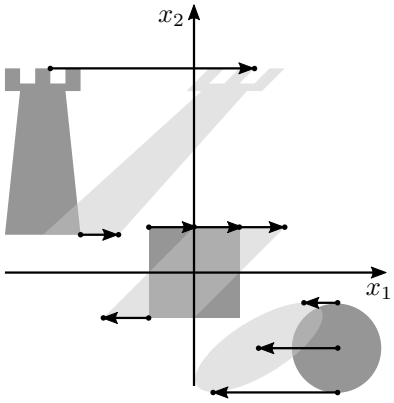
Příklad 4.50. Matice

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

určuje zobrazení $f_A : \mathbb{R}^2 \to \mathbb{R}^2$ v rovině, kterému se říká *zkosení*. Na obrázku 4.12 vidíme, jak zkosení zobrazí některé objekty v rovině. Z formulky

$$A\mathbf{x} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ x_2 \end{pmatrix}$$

ihned vidíme, že druhé souřadnice bodů se zkosením zachovávají, čili každý bod přímky rovnoběžné s první souřadnou osou se posouvá do nějakého bodu téže přímky. Velikost a směr posunutí závisí na první souřadnici zobrazovaného bodu.



Obrázek 4.12. Jak se zobrazují objekty v rovině zkosením

▲

Příklad 4.51. Jaké zobrazení určuje diagonální matice

$$A = \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix} \ ?$$

Z formulky

$$A\mathbf{x} = \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} (1/2)x_1 \\ 2x_2 \end{pmatrix}$$

ihned vidíme, že první souřadnice se zmenší na polovinu a druhá se zdvojnásobí. Na obrázku 4.13 opět vidíme, jak se zobrazí několik objektů v rovině zobrazením $f_A : \mathbb{R}^2 \to \mathbb{R}^2$.

▲

Příklad 4.52. Zobrazení $f_A : \mathbb{R}^2 \to \mathbb{R}^3$ určené maticí

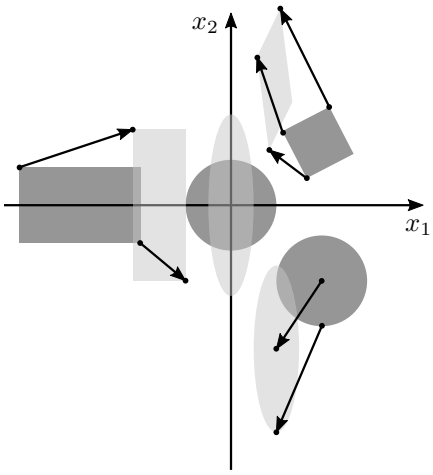
$$A = \begin{pmatrix} 5 & 1 \\ 2 & 3 \\ 1 & -1 \end{pmatrix} = (\mathbf{a}_1 | \mathbf{a}_2)$$

zobrazuje každý bod $(p_1, p_2)^T$ v rovině do bodu v 3-dimenzionálním prostoru se souřadnicemi

$$f_A((p_1, p_2)^T) = p_1\mathbf{a}_1 + p_2\mathbf{a}_2 \ ,$$

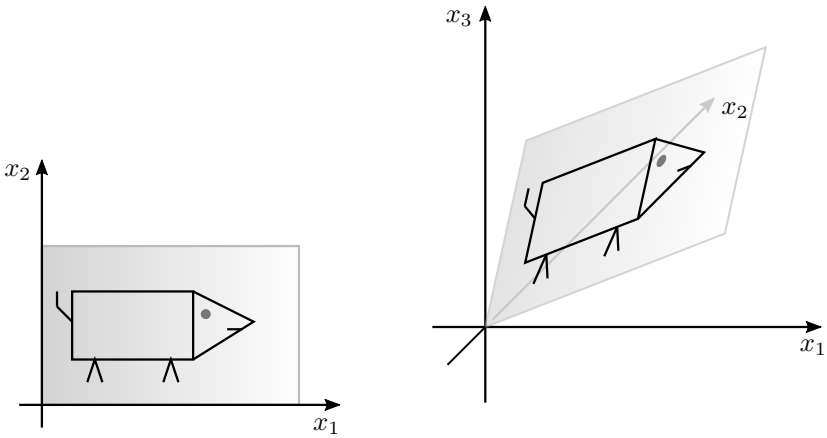
který leží v rovině s parametrickým vyjádřením $\{x_1\mathbf{a}_1 + x_2\mathbf{a}_2 : x_1, x_2 \in \mathbb{R}\}$.

Na obrázku 4.14 vidíme několik bodů v rovině $\mathbb{R}^2$ a jejich obrazy v prostoru $\mathbb{R}^3$. Na rozdíl od reálných funkcí jedné reálné proměnné si pro zobrazení f_A určené



Obrázek 4.13. Jak se zobrazují objekty v rovině diagonální maticí

maticí A nemůžeme nakreslit graf, ze kterého bychom viděli hodnotu zobrazení v každém bodě definičního oboru.

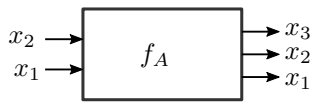


Obrázek 4.14. Zobrazení určené reálnou maticí typu 3×2

▲

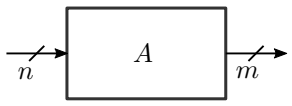
Pro zobrazení $f_A : T^n \to T^m$ určené maticí A typu $m \times n$ nad tělesem $\mathbf{T}$ máme pouze předpis, jak pro daný vektor $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$ spočítat hodnotu zobrazení f_A v bodě $\mathbf{x}$: $f_A(\mathbf{x}) = A\mathbf{x}$.

Důležité je ale také umět si představit zobrazení $f_A : T^n \to T^m$ 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 jiné proudy). Pokud si žádný obvod neumíme představit, můžeme zobrazení f_A považovat za „černou skříňku“. Na obrázku 4.15 je „černá skříňka“ reprezentující zobrazení z příkladu 4.52.



Obrázek 4.15. Zobrazení určené reálnou maticí typu 3×2

Zobrazení $f_A : T^n \to T^m$ určené obecnou maticí A typu $m \times n$ si pak můžeme představit jako na obrázku 4.16.



Obrázek 4.16. Zobrazení určené reálnou maticí typu $m \times n$

Zobrazení–černé skříňce můžeme klást dotazy typu *jaká je tvoje hodnota v prvku* $\mathbf{x} \in T^n$? Je-li $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ matice typu $m \times n$ nad tělesem $\mathbf{T}$ a $\mathbf{e}_1 = (1, 0, \ldots, 0)^T \in T^n$, 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 T^n.

Definice 4.53. Je-li $\mathbf{T}$ nějaké těleso a $n \in \mathbb{N}$, pak pro každé $j = 1, 2, \ldots, n$ označíme $\mathbf{e}_j = (0, \ldots, 0, 1, 0, \ldots, 0)^T \in T^n$ 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 4.54. *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 sloupce a proto se rovnají.

Opačná implikace je triviální. □

Při odvození matice určující otočení v rovině kolem počátku souřadnic o úhel α v příkladu 4.45 jsme využili jednu vlastnost rotace, a sice to, že rotace zobrazí součet dvou vektorů do součtu jejich obrazů. Další důležitou vlastností rotace kolem počátku je to, že zobrazí s-násobek nějakého vektoru do s-násobku obrazu tohoto vektoru. Tyto dvě vlastnosti má zobrazení určené jakoukoliv maticí.

Tvrzení 4.55. *Je-li A matice typu $m \times n$ nad tělesem $\mathbf{T}$, pak pro každé dva aritmetické vektory $\mathbf{x}, \mathbf{y} \in T^n$ a každý prvek $s \in T$ 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 4.31 dostáváme

- $f_A(s\mathbf{x}) = A(s\mathbf{x}) = s(A\mathbf{x}) = s\, f_A(\mathbf{x})$.

Podobně z definice 4.47 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: zachovávají násobení skalárem a zachovávají sčítání. Takovým zobrazením budeme v kapitole 6 říkat lineární. Uvidíme, že zobrazení $f : T^n \to T^m$ je rovno f_A pro nějakou matici A právě když f je lineární.

4.3.3. Součin matic a skládání zobrazení. Z definice 4.47 ihned dostaneme následující tvrzení.

Tvrzení 4.56. *Jsou-li A matice typu $m \times n$ a B matice typu $n \times p$ nad stejným tělesem $\mathbf{T}$, pak zobrazení $f_A : T^n \to T^m$ a $f_B : T^p \to T^n$ můžeme složit v pořadí $f_A f_B$ a pro složené zobrazení $f_A f_B : T^p \to T^m$ platí*

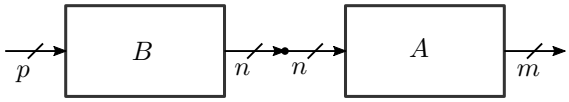
$$f_A f_B = f_{AB} \ .$$

Důkaz. Plyne ihned z asociativity násobení matic. Pro každý vektor $\mathbf{x} \in T^p$ platí

$$f_A f_B(\mathbf{x}) = f_A(f_B(\mathbf{x})) = f_A(B\mathbf{x}) = A(B\mathbf{x}) = (AB)\mathbf{x} = f_{AB}(\mathbf{x}) \ .$$

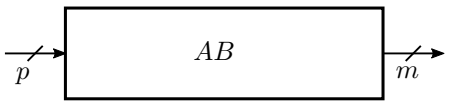
□

Graficky můžeme složené zobrazení $f_A f_B$ znázornit jako na obrázku 4.17.



Obrázek 4.17. Diagram pro složení $f_A f_B$ zobrazení určených maticemi

Tvrzení 4.56 říká, že tento diagram můžeme nahradit jednodušším diagramem na obrázku 4.18.



Obrázek 4.18. Zobrazení f_{AB} určené součinem matic

Ukážeme si ještě několik příkladů, jejichž řešení je založené na tvrzení 4.56. Jako první dokážeme součtové vzorce pro funkce *sinus* a *cosinus*.

PŘÍKLAD 4.57. Otočíme-li rovinu kolem počátku souřadnic o úhel β v kladném směru, je tato rotace podle příkladu 4.45 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 4.54, 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

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

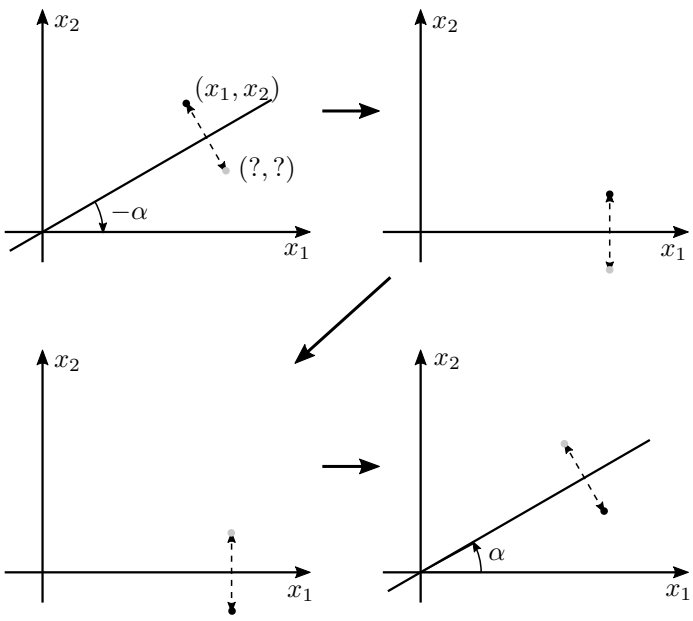
pro libovolné dva úhly α, β. ▲

PŘÍKLAD 4.58. Odvodíme matici určující symetrii 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 danou osu symetrie otočíme do směru první souřadné osy po směru hodinových ručiček, tj. o úhel $-\alpha$. Poté použijeme symetrii vzhledem k první souřadné ose a nakonec vše otočíme o úhel α zpět.

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



Obrázek 4.19. Rozklad symetrie vzhledem k obecné přímce

se souřadnicemi

$$\begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix} \begin{pmatrix} 2 \\ 3 \end{pmatrix}$$
$$= \begin{pmatrix} 2\cos 2\alpha + 3\sin 2\alpha \\ 2\sin 2\alpha - 3\cos 2\alpha \end{pmatrix} .$$

▲

Příklad 4.59. 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

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ -\sin\alpha & -\cos\alpha \end{pmatrix}$$
$$= \begin{pmatrix} \cos(-\alpha) & \sin(-\alpha) \\ \sin(-\alpha) & -\cos(-\alpha) \end{pmatrix} .$$

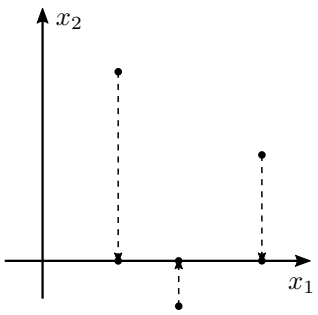
Na základě předchozího příkladu 4.58 tak můžeme odpovědět, že složené zobrazení je symetrie vzhledem k ose, kterou dostaneme z první souřadné osy otočením o úhel $\alpha/2$ v záporném směru, tj. po směru hodinových ručiček. ▲

Příklad 4.60. 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.

Odtud snadno dostaneme matici, která projekci na první souřadnou osu určuje. Platí totiž

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

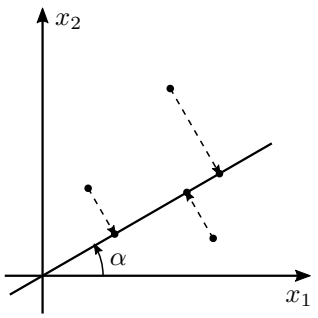
pro každý bod $(x_1, x_2)^T \in \mathbb{R}^2$. ▲



Obrázek 4.20. Projekce na první souřadnou osu

Příklad 4.61. Podobně jako v příkladu 4.58 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

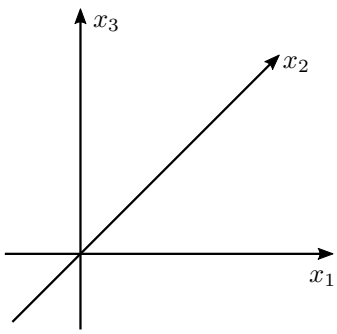
$$\begin{aligned}
&\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{pmatrix} \\
&= \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos\alpha & \sin\alpha \\ 0 & 0 \end{pmatrix} \\
&= \begin{pmatrix} \cos^2\alpha & \sin\alpha\cos\alpha \\ \sin\alpha\cos\alpha & \sin^2\alpha \end{pmatrix} .
\end{aligned}$$



Obrázek 4.21. Projekce na obecnou přímku procházející počátkem

▲

Příklad 4.62. 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 $\pi/2$ v kladném směru s rotací kolem třetí souřadné osy o úhel $\pi/2$ v kladném směru.



Obrázek 4.22. Kladně orientovaný souřadný systém v prostoru

Matici B rotace kolem osy x_1 o úhel $\pi/2$ v kladném směru 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 $\pi/2$ v kladném směru:

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

Složením je zobrazení $f_A f_B = f_{AB}$ určené součinem matic

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

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. Na první pohled ale není vidět, že jde o rotaci o úhel $2\pi/3$ v kladném směru, jak jsme zjistili výpočtem pomocí kvaternionů. Nicméně, pokud opakujeme zobrazení f_{AB} třikrát, dostaneme zobrazení určené maticí

$$(AB)^3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3 .$$

To znamená, že opakujeme-li rotaci f_{AB} třikrát, dostaneme identické zobrazení na prostoru $\mathbb{R}^3$, což je totéž, jako rotace o úhel 2π. Odtud plyne, že zobrazení f_{AB} rotuje prostor $\mathbb{R}^3$ o třetinu úhlu 2π, tj. o úhel $2\pi/3$. Nevíme pouze, jestli v kladném směru nebo v záporném směru. V kapitole o vlastních číslech si ukážeme další metodu, kterou lze spočítat osu a úhel rotace bez použití kvaternionů. ▲

PŘÍKLAD 4.63. Jednotková matice I_n řádu n nad tělesem $\mathbf{T}$ určuje zobrazení $f_{I_n} : T^n \to T^n$. Pro libovolný vektor $\mathbf{x} \in T^n$ platí

$$f_{I_n}(\mathbf{x}) = I_n\mathbf{x} = \mathbf{x} \ ,$$

jednotková matice I_n tedy určuje identické zobrazení na množině T^n všech n-složkových aritmetických vektorů nad tělesem $\mathbf{T}$. ▲

Identické zobrazení na množině T^n budeme v dalším textu označovat id_{T^n}.

4.3.4. Duální zobrazení. Matice A typu $m \times n$ nad $\mathbf{T}$ určuje zobrazení $f_A : T^n \to T^m$. Obrazem aritmetického vektoru $\mathbf{x} \in T^n$ je $A\mathbf{x}$, což můžeme poněkud nepřesně vyjádřit slovy „f_A je násobení zleva maticí A“. V řadě situací má význam i tzv. duální zobrazení $f_{A^T} : T^m \to T^n$ určené transponovanou maticí A^T. Protože pro libovolný aritmetický vektor $\mathbf{y} \in T^m$ platí

$$A^T\mathbf{y} = (\mathbf{y}^T A)^T \ ,$$

obrazem řádkového vektoru $\mathbf{y}^T$ je řádkový vektor $\mathbf{y}^T A$. V tomto smyslu „f_{A^T} je násobení zprava maticí A“.

Význam obou zobrazení f_A i f_{A^T} si ukážeme na matici vstupů do výroby z příkladů 4.2 a 4.19.

PŘÍKLAD 4.64. Matice $A = (a_{ij})$ typu $m \times n$ nad $\mathbb{R}$ zaznamenává vstupní náklady na produkty, řádky odpovídají produktům a sloupce vstupům. Prvek a_{ij} je roven počtu jednotek vstupu j potřebných k výrobě produktu i.

Jak jsme nahlédli v příkladu 4.19, je-li $\mathbf{x} \in \mathbb{R}^n$ vektor jednotkových cen vstupů, pak $A\mathbf{x}$ je vektor výrobních cen. Takže

$$f_A : \begin{array}{ccc} \mathbb{R}^n & \to & \mathbb{R}^m \\ \text{jednotkové ceny vstupů} & \mapsto & \text{výrobní ceny produktů} \end{array} .$$

Podobně se nahlédne, že je-li $\mathbf{y} \in \mathbb{R}^m$ počet výrobků, které chceme vyrobit, pak $A^T\mathbf{y}$ udává potřebný počet jednotek vstupu – i-tá složka je počet jednotek vstupu i potřebných k výrobě daného počtu výrobků. Schematicky

$$f_{A^T} : \begin{array}{ccc} \mathbb{R}^m & \to & \mathbb{R}^n \\ \text{počet výrobků} & \mapsto & \text{počet jednotek vstupů} \end{array} .$$

Na okraj ještě poznamenejme, že nás v této situaci bude asi nejvíce zajímat zobrazení $g : \mathbb{R}^m \times \mathbb{R}^n \to \mathbb{R}$ definované $g(\mathbf{y}, \mathbf{x}) = \mathbf{y}^T A\mathbf{x}$, které v sobě v nějakém smyslu ukrývá obě zobrazení f_A i f_{A^T}.

$$g : \begin{array}{ccc} \mathbb{R}^m \times \mathbb{R}^n & \to & \mathbb{R} \\ \text{(počet výrobků, jednotkové ceny vstupů)} & \mapsto & \text{cena} \end{array} .$$

▲

4.4. Inverzní matice

V další části této kapitoly se budeme zabývat otázkou, kdy k matici existuje inverzní matice. Protože násobení matic není komutativní, musíme inverzní matice definovat opatrněji než inverzní prvky v tělesech.

4.4.1. Algebraický pohled. Začneme algebraickou definicí.

DEFINICE 4.65. Je-li A matice typu $m \times n$ nad tělesem $\mathbf{T}$, pak matici X nad $\mathbf{T}$ nazýváme *inverzní zprava k matici* A, pokud platí $AX = I_m$, matice A se v tom případě nazývá *invertovatelná zprava*.

Matice Y nad $\mathbf{T}$ se nazývá *inverzní zleva k matici* A, pokud platí $YA = I_n$, matice A se v tom případě nazývá *invertovatelná zleva*.

Je-li A čtvercová matice řádu n nad $\mathbf{T}$, pak matici X nad $\mathbf{T}$ nazýváme *inverzní k matici* A, pokud $AX = XA = I_n$, matice A se v tom případě nazývá *invertovatelná matice*. Je-li A invertovatelná matice, pak matici inverzní k A označujeme A^{-1}.

Aby měly všechny součiny v definici smysl, matice X inverzní zprava k matici A typu $m \times n$ musí mít typ $n \times m$, matice Y inverzní zleva k A musí mít typ $n \times m$ a inverzní matice ke čtvercové matici řádu n musí být opět čtvercová řádu n.

Poslední část definice 4.65 říká, že invertovatelná čtvercová matice je současně invertovatelná zprava i zleva. Následující jednoduché pozorování říká opak, tj. že čtvercová matice invertovatelná zleva i zprava je už invertovatelná a inverzní matice je určená jednoznačně.

POZOROVÁNÍ 4.66. *Je-li čtvercová matice A řádu n nad $\mathbf{T}$ invertovatelná zprava i zleva, pak je invertovatelná a každá matice X inverzní zprava k A se rovná každé matici Y inverzní zleva k matici A. Inverzní matice k A je proto určená jednoznačně, pokud existuje.*

DŮKAZ. Protože X je inverzní zprava k A, musí platit $AX = I_n$. Stejně tak pro matici Y inverzní zleva k A platí $YA = I_n$. Nyní stačí využít asociativitu násobení matic:

$$X = I_n X = (YA)X = Y(AX) = Y I_n = Y \ .$$

Platí tedy $AX = I_n = Y A = XA$, což dokazuje, že X je inverzní k A a všechny inverzní matice k A se rovnají. □

4.4.2. Hledání matice inverzní zprava. Začneme příkladem.

PŘÍKLAD 4.67. Zkusíme najít matici X inverzní zprava k matici

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 9 & 8 \end{pmatrix} \ .$$

Z definice 4.65 různých typů invertovatelnosti víme, že matice X musí být typu 3×2, tedy $X = (\mathbf{x}_1|\mathbf{x}_2)$. Pro X musí platit $AX = A(\mathbf{x}_1|\mathbf{x}_2) = (A\mathbf{x}_1|A\mathbf{x}_2) = I_2 = (\mathbf{e}_1|\mathbf{e}_2)$. Takže potřebujeme vyřešit soustavy $A\mathbf{x}_1 = \mathbf{e}_1$ a $A\mathbf{x}_2 = \mathbf{e}_2$, tj. soustavy

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 9 & 8 \end{pmatrix} \begin{pmatrix} x_{11} \\ x_{21} \\ x_{31} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ \begin{pmatrix} 1 & 2 & 3 \\ 4 & 9 & 8 \end{pmatrix} \begin{pmatrix} x_{12} \\ x_{22} \\ x_{32} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \ .$$

Tak je vyřešíme

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 4 & 9 & 8 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & 1 & -4 & -4 \end{array}\right), \ \mathbf{x}_1 = \begin{pmatrix} x_{11} \\ x_{21} \\ x_{31} \end{pmatrix} = \begin{pmatrix} 9 - 11t \\ -4 + 4t \\ t \end{pmatrix} \ ,$$

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 0 \\ 4 & 9 & 8 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 3 & 0 \\ 0 & 1 & -4 & 1 \end{array}\right), \ \mathbf{x}_2 = \begin{pmatrix} x_{12} \\ x_{22} \\ x_{32} \end{pmatrix} = \begin{pmatrix} -2 - 11s \\ 1 + 4s \\ s \end{pmatrix} \ .$$

Pro libovolné hodnoty parametrů $s, t \in \mathbf{T}$ je matice

$$X = (\mathbf{x}_1|\mathbf{x}_2) = \begin{pmatrix} 9 - 11t & -2 - 11s \\ -4 + 4t & 1 + 4s \\ t & s \end{pmatrix}$$

inverzní zprava k matici

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 9 & 8 \end{pmatrix} \ .$$

▲

Obě soustavy $A\mathbf{x}_1 = \mathbf{e}_1$ a $A\mathbf{x}_2 = \mathbf{e}_2$ z předchozího příkladu mají stejnou matici A a mohli jsme je tedy řešit stejnými řádkovými úpravami. Můžeme je proto řešit současně tak, že pravé strany napíšeme vedle matice soustavy všechny najednou a upravíme celou matici do odstupňovaného tvaru. Dopočtení zpětnou substitucí pak

proběhne zvlášť pro každou pravou stranu. V našem případě by úprava vypadala následovně.

$$\left(\begin{array}{ccc|cc} 1 & 2 & 3 & 1 & 0 \\ 4 & 9 & 8 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|cc} 1 & 2 & 3 & 1 & 0 \\ 0 & 1 & -4 & -4 & 1 \end{array}\right) .$$

Geometricky si matici A představujeme jako zobrazení f_A určené maticí A. Různé typy invertovatelnosti matice A odpovídají různým vlastnostem zobrazení f_A.

TVRZENÍ 4.68. *Pro matici A typu $m \times n$ nad tělesem $\mathbf{T}$ jsou následující podmínky ekvivalentní:*

(1) *matice A je invertovatelná zprava,*
(2) *zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^m$ je na (celý prostor) $\mathbf{T}^m$ (jinými slovy, soustava $A\mathbf{x} = \mathbf{b}$ má pro každou pravou stranu $\mathbf{b} \in \mathbf{T}^m$ vždy aspoň jedno řešení),*
(3) *matice v odstupňovaném tvaru, kterou dostaneme z A Gaussovou eliminací, má všechny řádky nenulové,*
(4) *pro hodnost matice A platí* $\operatorname{rank}(A) = m$.

DŮKAZ. (1) $\Rightarrow$ (2) Zvolíme libovolné $\mathbf{b} \in \mathbf{T}^m$. Potřebujeme najít aspoň jedno $\mathbf{x} \in \mathbf{T}^n$, pro které platí $A\mathbf{x} = \mathbf{b}$. Protože předpokládáme, že A je invertovatelná zprava, existuje matice X typu $n \times m$ nad $\mathbf{T}$, pro kterou platí $AX = I_m$. Položíme $\mathbf{x} = X\mathbf{b}$. Potom platí

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

(2) $\Rightarrow$ (3) Označíme C matici v odstupňovaném tvaru, kterou dostaneme z A Gaussovou eliminací, což je nějaká posloupnost elementárních řádkových úprav. Dále budeme pokračovat sporem. Pokud by matice C měla aspoň jeden nulový řádek, byla by soustava $C\mathbf{x} = \mathbf{e}_m$ neřešitelná. Protože jsou všechny elementární řádkové úpravy vratné, mohli bychom celou Gaussovu eliminaci provést pozpátku na neřešitelnou soustavu $C\mathbf{x} = \mathbf{e}_m$ a dostat z ní jinou neřešitelnou soustavu $A\mathbf{x} = \mathbf{b}$ s maticí soustavy A a nějakou pravou stranou $\mathbf{b} \in \mathbf{T}^m$, což je spor s podmínkou (2).

(3) $\Rightarrow$ (1) Protože v matici C není žádný nulový řádek, soustava $A\mathbf{x} = \mathbf{b}$ má řešení pro jakoukoliv pravou stranu $\mathbf{b} \in \mathbf{T}^m$. Speciálně má řešení soustava $A\mathbf{x} = \mathbf{e}_j$ pro každý prvek $\mathbf{e}_j$ kanonické báze prostoru $\mathbf{T}^m$. Zvolíme pro každé $j = 1, 2, \ldots, m$ libovolné řešení $\mathbf{x}_j$ soustavy $A\mathbf{x} = \mathbf{e}_j$ a tato řešení uspořádáme do matice $X = (\mathbf{x}_1|\mathbf{x}_2|\cdots|\mathbf{x}_m)$. Pak platí

$$AX = A(\mathbf{x}_1|\mathbf{x}_2|\cdots|\mathbf{x}_m) = (A\mathbf{x}_1|A\mathbf{x}_2|\cdots|A\mathbf{x}_m) = (\mathbf{e}_1|\mathbf{e}_2|\cdots|\mathbf{e}_m) = I_m \ .$$

(3) $\Leftrightarrow$ (4) plyne přímo z Definice 2.17 – hodnost matice. □

Z Pozorování 2.18 víme, že pro jakoukoliv matici A typu $m \times n$ platí $\operatorname{rank}(A) \leq n$. Z bodu (4) pak plyne, že je-li matice A typu $m \times n$ invertovatelná zprava, platí $m = \operatorname{rank}(A) \leq n$. Můžeme proto hned usoudit, že například k matici

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

matice inverzní zprava neexistuje.

Podmínka (3) navíc uvádí jednoduchý test, jak zjistit, kdy matice inverzní zprava k dané matici A existuje – po Gaussově eliminaci matice A jsou všechny řádky nenulové. A důkaz implikace (3) $\Rightarrow$ (1) dává návod, jak najít matici inverzní zprava k A v případě, že matice A podmínku (3) splňuje.

Z příkladu 4.67 také hned vidíme, že pokud matice inverzní zprava k matici A typu $m \times n$ existuje, tj. platí-li $\operatorname{rank}(A) = m$, a současně matice A není čtvercová,

tj. $m < n$, aspoň jeden sloupec matice A není bázový. Každá soustava $A\mathbf{x}_j = \mathbf{e}_j$ tak má více než jedno řešení a matice inverzní zprava k A není určená jednoznačně.

Jiná situace nastává pokud je A čtvercová matice, tj. $m = n$. V tom případě je v matici C, kterou dostaneme z A Gaussovou eliminací, $m = n$ pivotů. Což znamená, že v každém sloupci C je jeden pivot, neboli každý sloupec matice C je bázový, žádná neznámá v soustavě $A\mathbf{x} = \mathbf{e}_j$ není volná a soustava má proto jednoznačné řešení $\mathbf{x}_j$. Matice inverzní zprava k matici A je určená jednoznačně. V tom případě můžeme náš výpočet modifikovat tak, abychom se úplně vyhnuli zpětné substituci. Ukážeme si to opět na příkladu.

Příklad 4.69. Najdeme matici inverzní zprava k reálné matici

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

K matici A připíšeme všechny sloupce jednotkové matice I_2 a provedeme Gaussovu eliminaci na celou matici:

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

Nyní nenavážeme zpětnou substitucí pro jednotlivé soustavy, ale budeme pokračovat dalšími elementárními řádkovými úpravami, kterými matici A převedeme do jednotkové matice:

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

Soustavu s jednotkovou maticí je velmi snadné vyřešit – řešením je přímo pravá strana. Dostáváme tedy $\mathbf{x}_1 = (3, -2/3)^T$ a $\mathbf{x}_2 = (-1, 1/3)^T$. Jednoznačně určená matice inverzní zprava k A se tedy rovná matici

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

▲

Postup řešení příkladu snadno zobecníme na libovolnou čtvercovou matici A řádu n. Pokud po Gaussově eliminaci použité na matici A dostaneme matici, ve které je aspoň jeden řádek nulový, matice A nesplňuje podmínku (3) z Tvrzení 4.68 a matice inverzní zprava k matici A neexistuje. Pokud jsou po Gaussově eliminaci všechny řádky nenulové, je v každém řádku právě jeden pivot, všechny sloupce jsou proto bázové (neboť matice A je čtvercová), pro odstupňovaný tvar proto platí $k_1 = 1$, $k_2 = 2, \ldots, k_n = n$. Matice v řádkově odstupňovaném tvaru je proto horní trojúhelníková a všechny prvky na hlavní diagonále jsou nenulové. Pak pomocí přičítání vhodných násobků jednotlivých řádků k řádkům nad nimi vynulujeme všechny prvky nad hlavní diagonálou a nakonec pomocí násobení řádků nenulovými čísly změníme všechny prvky na hlavní diagonále na 1. Dostaneme tak matici $(I_n|X)$ a matice X je inverzní zprava k matici A. Stručně řečeno, řádkovými úpravami převedeme matici $(A|I_n)$ do tvaru $(I_n|X)$ a vpravo přečteme matici X inverzní zprava k matici A.

4.4.3. Hledání matice inverzní zleva. V příkladu 4.69 jsme spočítali, že k matici

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

je inverzní zprava matice

$$X = \begin{pmatrix} 3 & -1 \\ -2/3 & 1/3 \end{pmatrix} ,$$

tj. platí $AX = I_2$.

Vynásobíme-li obě matice v opačném pořadí, dostaneme také $XA = I_2$. Matice X je tedy rovněž inverzní zleva k matici A. To není žádná náhoda, platí to pro jakoukoliv čtvercovou matici A.

Pokud se nám čtvercovou matici A řádu n podaří převést pomocí elementárních řádkových úprav do jednotkové matice I_n, podíváme se na celý postup pomocí elementárních matic. V tvrzení 4.36 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

$$A \sim E_1 A \sim E_2(E_1 A) \sim \cdots \quad ,$$

kde $E_1, E_2, \ldots$ jsou elementární matice příslušných elementárních řádkových úprav.

Vezmeme-li v úvahu asociativitu násobení matic, můžeme celý postup zapsat ve tvaru

$$A \sim E_1 A \sim E_2 E_1 A \sim \cdots \sim E_k \cdots E_2 E_1 A = I_n \quad .$$

To znamená, že součin elementárních matic $E_k \cdots E_2 E_1$ je matice inverzní zleva k matici A. Zbývá pouze nějak se dopracovat k součinu $E_k \cdots E_2 E_1$ v průběhu elementárních úprav vedoucích od matice A k jednotkové matici I_n. K tomu stačí si uvědomit, že

$$E_k \cdots E_2 E_1 = E_k \cdots E_2 E_1 I_n \quad ,$$

což znamená, že součin $E_k \cdots E_2 E_1$ dostaneme provedením téže posloupnosti elementárních úprav na jednotkovou matici I_n. Provádíme tedy řádkové úpravy současně na obě matice neboli na matici $(A|I_n)$. Podle pravidla o násobení po blocích dostaneme

$$\begin{aligned}(A \mid I_n) \sim (E_1 A \mid E_1 I_n) = (E_1 A \mid E_1) \sim (E_2 E_1 A \mid E_2 E_1) \sim \cdots \sim \\ \sim (E_k \cdots E_2 E_1 A \mid E_k \cdots E_2 E_1) = (I_n \mid E_k \cdots E_2 E_1) \quad .\end{aligned}$$

V pravém bloku tak dostaneme matici $E_k \ldots E_2 E_1$ inverzní zleva k matici A. Jeden a ten samý postup proto v případě čtvercové matice A vede současně k nalezení matice inverzní zprava a matice inverzní zleva.

Nepatrně složitější je hledání matice inverzní zleva k matici, která není čtvercová. Ukážeme si to na následujícím příkladu.

Příklad 4.70. Spočítáme matici inverzní zleva k matici

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

Zkusíme matici A převést elementárními řádkovými úpravami do tvaru

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} I_2 \\ O_{1\times 2} \end{pmatrix} \quad .$$

Stejně jako při výpočtu matice inverzní zleva ke čtvercové matici si k matici A připíšeme ještě jednotkovou matici I_3 a řádkové úpravy děláme na celou matici $(A \mid I_3)$:

$$\left(\begin{array}{cc|ccc} 1 & 2 & 1 & 0 & 0 \\ 3 & 4 & 0 & 1 & 0 \\ 5 & 6 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|ccc} 1 & 2 & 1 & 0 & 0 \\ 0 & -2 & -3 & 1 & 0 \\ 0 & -4 & -5 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|ccc} 1 & 2 & 1 & 0 & 0 \\ 0 & -2 & -3 & 1 & 0 \\ 0 & 0 & 1 & -2 & 1 \end{array}\right)$$

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

Zjistili jsme tak, že platí

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

Z levého činitele vynecháme spodní řádek, dostaneme matici

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

pro kterou platí $YA = I_2$, takže Y je inverzní zleva k A. ▲

Geometrický význam invertovatelnosti zleva je součástí následujícícho tvrzení.

Tvrzení 4.71. *Pro matici A typu $m \times n$ nad $\mathbf{T}$ jsou následující podmínky ekvivalentní:*

(1) *matice A je invertovatelná zleva,*
(2) *zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^m$ určené maticí A je prosté (jinými slovy soustava $A\mathbf{x} = \mathbf{b}$ má nejvýše jedno řešení pro jakoukoliv pravou stranu $\mathbf{b} \in \mathbf{T}^m$),*
(3) *soustava $A\mathbf{x} = \mathbf{o}$ má právě jedno řešení $\mathbf{x} = \mathbf{o}$,*
(4) *matice C, kterou dostaneme z matice A Gaussovou eliminací, má všechny sloupce bázové,*
(5) *platí* $\operatorname{rank}(A) = n$.

Důkaz. (1) $\Rightarrow$ (2). Zvolíme dva vektory $\mathbf{x}, \mathbf{y} \in \mathbf{T}^n$, pro které platí $f_A(\mathbf{x}) = f_A(\mathbf{y})$. Podle definice zobrazení f_A to znamená $A\mathbf{x} = A\mathbf{y}$. Poslední rovnost (sloupcových vektorů) vynásobíme zleva nějakou maticí Y, která je inverzní zleva k matici A. Dostaneme

$$YA\mathbf{x} = YA\mathbf{y} \ .$$

Protože $YA = I_n$, plyne odtud $\mathbf{x} = \mathbf{y}$.

(2) $\Rightarrow$ (3). Podle (2) má soustava $A\mathbf{x} = \mathbf{o}$ nejvýše jedno řešení. Jedním řešením je $\mathbf{x} = \mathbf{o}$, takže to je jediné řešení soustavy $A\mathbf{x} = \mathbf{o}$.

(3) $\Rightarrow$ (4). Tuto implikaci dokážeme sporem. Předpokládejme, že v matici C je aspoň jeden sloupec nebázový. Soustava $A\mathbf{x} = \mathbf{o}$ má stejnou množinu řešení jako soustava $C\mathbf{x} = \mathbf{o}$ s maticí v odstupňovaném tvaru. Protože předpokládáme, že C má aspoň jeden sloupec nebázový, množina všech řešení soustavy $C\mathbf{x} = \mathbf{o}$ má aspoň jeden volný parametr a tedy aspoň dva prvky. To je spor s předpokladem, že soustava $A\mathbf{x} = \mathbf{o}$ má pouze jedno řešení.

(4) $\Rightarrow$ (1). Důkaz této implikace bude současně obecným návodem, jak matici inverzní zleva k matici A najít v případě, že existuje. Gaussova eliminace převede matici A do matice v odstupňovaném tvaru C, ve které jsou všechny sloupce bázové. Pro indexy bázových sloupců matice v odstupňovaném tvaru (Definice 2.14) tak platí $k_1 = 1, k_2 = 2, \ldots, k_n = n$. První až n-tý řádek matice C jsou proto nenulové a všechny další jsou nulové. (Cestou jsme v této chvíli už také dokázali (4) $\Rightarrow$ (5).) Matice C se tak skládá ze dvou bloků

$$C = \begin{pmatrix} D_{n\times n} \\ O_{(m-n)\times n} \end{pmatrix} ,$$

kde D je horní trojúhelníková matice řádu n s nenulovými prvky na hlavní diagonále a $O_{(m-n)\times n}$ je nulová matice typu $(m-n) \times n$. Stejně jako při hledání matice inverzní zprava budeme ještě pokračovat a dalšími elementárními řádkovými úpravami vynulujeme všechny prvky nad hlavní diagonálou matice D a všechny prvky na hlavní diagonále upravíme na 1. Protože používáme pouze elementární řádkové

úpravy a každou takovou úpravu můžeme zapsat jako násobení nějakou elementární maticí zleva, existují elementární matice $E_1, E_2, \ldots, E_k$ řádu m, pro které platí

$$E_k \cdots E_2 E_1 A = \begin{pmatrix} I_n \\ O_{(m-n)\times n} \end{pmatrix} .$$

Čtvercovou matici $E = E_k \cdots E_2 E_1$ řádu m také rozdělíme do dvou bloků – bloku Y typu $n \times m$ tvořeného prvními n řádky a spodního bloku Z typu $(m-n) \times m$ tvořeného zbývajícími řádky, neboli

$$E = \begin{pmatrix} Y \\ Z \end{pmatrix} .$$

Součin na levé straně rovnosti

$$EA = \begin{pmatrix} I_n \\ O_{(m-n)\times n} \end{pmatrix}$$

spočítáme po blocích:

$$EA = \begin{pmatrix} Y \\ Z \end{pmatrix} A = \begin{pmatrix} YA \\ ZA \end{pmatrix} = \begin{pmatrix} I_n \\ O_{(m-n)\times n} \end{pmatrix} ,$$

takže $YA = I_n$ a matice Y je inverzní zleva k matici A.

(4) $\Rightarrow$ (5) jsme dokázali už v průběhu důkazu (4) $\Rightarrow$ (1).

(5) $\Rightarrow$ (4). Rovnost $\operatorname{rank}(A) = n$ znamená, že v matici v odstupňovaném tvaru C, kterou dostaneme z A Gaussovou eliminací, je prvních n řádků nenulových a zbylé nulové. V každém nenulovém řádku C leží právě jeden pivot a těchto n pivotů musí ležet v různých sloupcích matice C, což znamená, že všechny sloupce matice C, a tedy i matice A jsou bázové. □

Při řešení příkladu 4.70 jsme se nezabývali otázkou jednoznačnosti matice Y inverzní zleva k matici A.

Otázky k samostatnému studiu 4.72. Je-li A matice z příkladu 4.70, najděte libovolná dvě řešení $\mathbf{u}, \mathbf{v}$ homogenní soustavy $A^T\mathbf{x} = \mathbf{o}$. Tato řešení si napište jako řádky v matici

$$D = \begin{pmatrix} \mathbf{u}^T \\ \mathbf{v}^T \end{pmatrix}$$

a ověřte, že také matice $Y + D$ je také inverzní zleva k matici A.

4.4.4. Regulární matice. V této části se budeme zabývat otázkou, které matice jsou současně invertovatelné zleva i zprava. Začneme jednoduchým pozorováním.

Pozorování 4.73. *Je-li matice A typu $m \times n$ nad $\mathbf{T}$ invertovatelná zleva i zprava, pak je čtvercová, tj. $m = n$.*

Důkaz. Z předpokladu, že A je invertovatelná zprava, plyne podle podmínky (4) z tvrzení 4.68 rovnost $\operatorname{rank}(A) = m$. Podmínka (5) z tvrzení 4.71 říká, že pro matici A invertovatelnou zleva platí $\operatorname{rank}(A) = n$. Takže $m = n$ a matice A je čtvercová. □

V případě oboustranné invertovatelnosti tak stačí zkoumat pouze čtvercové matice. Dalším bezprostředním důsledkem Tvrzení 4.68 a 4.71 je následující tvrzení.

Tvrzení 4.74. *Následující vlastnosti čtvercové matice A řádu n jsou ekvivalentní:*

(1) *matice A je invertovatelná zprava,*
(2) *matice A je invertovatelná zleva,*
(3) *matice A je invertovatelná.*

Důkaz. (1) $\Rightarrow$ (2). Je-li matice A řádu n invertovatelná zprava, pak podle podmínky (3) z tvrzení 4.68 jsou v matici C, kterou dostaneme Gaussovou eliminací z matice A, všechny řádky nenulové. V každém řádku C je proto právě jeden pivot, tyto pivoty leží v různých sloupcích matice C, a protože těchto sloupců je přesně n, každý sloupec matice C je bázový a podle podmínky (4) z tvrzení 4.71 je matice A invertovatelná zleva.

(2) $\Rightarrow$ (1). Opačnou implikaci můžeme dokázat stejným způsobem a nebo můžeme využít transponování matic. Je-li A invertovatelná zleva, existuje matice Y řádu n, pro kterou platí $YA = I_n$. Transponováním dostaneme rovnost $(YA)^T = I_n^T$, což po úpravě znamená $A^T Y^T = I_n$. Čtvercová matice A^T je tedy invertovatelná zprava a podle již dokázané implikace (1) $\Rightarrow$ (2) je také invertovatelná zleva, existuje proto matice Z řádu n, pro kterou platí $ZA^T = I_n$. Dalším transponováním dostaneme rovnost $(ZA^T)^T = I_n^T = I_n$. A protože $(ZA^T)^T = (A^T)^T Z^T = AZ^T$, je matice Z^T inverzní zprava k matici A.

(2) $\Rightarrow$ (3). Víme už, že čtvercová matice invertovatelná zleva je také invertovatelná zprava. Podle pozorování 4.66 je proto invertovatelná.

(3) $\Rightarrow$ (1) je triviální. □

Jakákoliv čtvercová matice A invertovatelná z jedné strany je tak invertovatelná z obou stran a existuje k ní jednoznačně určená inverzní matice A^{-1}.

Geometricky si matici A představujeme jako zobrazení f_A určené maticí A. V případě čtvercové matice řádu n jde o zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^n$. Matice A je invertovatelná zleva právě když je zobrazení f_A prosté podle podmínky (2) z tvrzení 4.71. Je invertovatelná zprava právě když je zobrazení f_A na (celý prostor) $\mathbf{T}^n$, podle podmínky (2) z tvrzení 4.68. Pro invertovatelnou matici A řádu n je proto zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^n$ prosté i na $\mathbf{T}^n$. Takovému zobrazení říkáme *vzájemně jednoznačné zobrazení* nebo také *bijekce*. Tyto úvahy vedou k následující definici.

Definice 4.75. Čtvercová matice A nad tělesem $\mathbf{T}$ řádu n se nazývá *regulární*, pokud je zobrazení $f_A : T^n \to T^n$ určené maticí A vzájemně jednoznačné (tj. bijekce).

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

Úvahy před definicí dokazují že každá invertovatelná matice je regulární. Ve skutečnosti jsou oba pojmy ekvivalentní.

Tvrzení 4.76. *Matice A je regulární právě když je invertovatelná.*

Důkaz. Je-li matice A regulární, je zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^n$ vzájemně jednoznačné, tj. prosté a na (celý prostor) $\mathbf{T}^n$. Podle tvrzení 4.71 je matice A invertovatelná zleva, podle Tvrzení 4.68 je invertovatelná zprava a podle Tvrzení 4.74 je invertovatelná. □

Ke každému vzájemně jednoznačnému zobrazení existuje jednoznačně určené inverzní zobrazení. Je-li A regulární matice řádu n, je zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^n$ vzájemně jednoznačné. Asi nikoho nepřekvapí, že inverzní zobrazení k f_A je určené maticí inverzní k A.

Tvrzení 4.77. *Je-li A regulární (což je podle Tvrzení 4.76 totéž, co invertovatelná) matice a X je inverzní matice k A, pak je f_X inverzní zobrazení k f_A.*

Důkaz. Je-li A invertovatelná, existuje matice X, pro kterou platí $AX = XA = I_n$. Podle Tvrzení 4.56 platí pro zobrazení $f_A : T^n \to T^n$ a $f_X : T^n \to T^n$ rovnosti

$$f_A f_X = f_{I_n} = \mathrm{id}_{T^n}, \quad f_X f_A = f_{I_n} = \mathrm{id}_{T^n} \quad .$$

Použili jsme fakt, že zobrazení f_{I_n} je identické zobrazení na množině T^n, viz příklad 4.63. Zobrazení f_X určené maticí X je tedy inverzní k f_A. □

Regularitu matice A také můžeme přeložit do řešitelnosti soustav lineárních rovnic s maticí A.

POZOROVÁNÍ 4.78. *Matice A je regulární právě když soustava $A\mathbf{x} = \mathbf{b}$ má právě jedno řešení pro každou pravou stranu $\mathbf{b}$.*

Víme-li, jaké zobrazení f_A matice A určuje, můžeme v některých případech ihned napsat matici inverzní k A.

PŘÍKLAD 4.79. 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 $AX = XA = I_2$. Takže $X = A^{-1}$. ▲

PŘÍKLAD 4.80. 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. ▲

PŘÍKLAD 4.81. 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 $CX \neq I_2$. K matici C tak neexistuje matice inverzní zprava, proto nemůže být invertovatelná. ▲

4.4.5. Charakterizace regulárních matic. V případě čtvercových matic je invertovatelnost zleva totéž, co invertovatelnost zprava, a v obou případech je to totéž, co existence inverzní matice. Všechny podmínky z Tvrzení 4.68 a Tvrzení 4.71 jsou proto navzájem ekvivalentní a také ekvivalentní s invertovatelností matice A. A protože invertovatelnost matice A je ekvivalentní regularitě této matice, můžeme všechny dosavadní poznatky o regulárních maticích shrnout do následující věty.

VĚTA 4.82. *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 T^n (jinými slovy, soustava $A\mathbf{x} = \mathbf{b}$ má pro každou pravou stranu $\mathbf{b} \in T^n$ alespoň jedno řešení),*
(3) *zobrazení f_A je prosté (jinými slovy, soustava $A\mathbf{x} = \mathbf{b}$ má pro každou pravou stranu $\mathbf{b} \in T^n$ nejvýše jedno řešení),*

(4) *soustava* $A\mathbf{x} = \mathbf{o}$ *má jediné řešení* $\mathbf{x} = \mathbf{o}$,

(5) *Gaussova eliminace převede matici* A *do horního trojúhelníkového tvaru s nenulovými prvky na 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) $\operatorname{rank}(A) = n$.

Důkaz. Ekvivalenci (1) a (7) jsme dokázali v tvrzení 4.76. Ekvivalenci (7), (8) a (9) jsme dokázali v tvrzení 4.74. Ekvivalenci (8) a (2) jsme dokázali v tvrzení 4.68, ekvivalenci (3), (4), (9) a (10) jsme dokázali v tvrzení 4.71. V případě čtvercové matice A je podmínka (5) ekvivaletní tomu, že Gaussova eliminace převede matici A do matice, která má všechny sloupce bázové, což je ekvivalentní s podmínkou (9) podle tvrzení 4.71.

(5) $\Rightarrow$ (6). To, jak lze z horní trojúhelníkové matice s nenulovými prvky na hlavní diagonále po Gaussově eliminaci (kdy používáme elementární řádkové úpravy) dostat jednotkovou matici pomocí dalších řádkových úprav, jsme si ukázali v odstavci následujícím po příkladu 4.69. Matici A převedeme do horní trojúhelníkové matice s nenulovými prvky na hlavní diagonále a pak doeliminujeme postupně prvky nad hlavní diagonálou ve druhém sloupci, třetím sloupci, atd. Získáme diagonální matici a stačí vynásobit řádky vhodnými prvky tělesa.

(6) $\Rightarrow$ (9). Také toto by už mělo být zřejmé. Posloupnost elementárních řádkových úprav vedoucí z matice A na jednotkovou matici I_n znamená existenci elementárních matic $E_1, E_2, \ldots, E_k$ takových, že

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

takže matice $Y = E_k \cdots E_2 E_1$ je inverzní zleva k matici A. □

Najít inverzní matici k regulární matici je také snadné. Stačí najít matici inverzní zprava a to už umíme. Ukážeme si ještě pár příkladů.

Příklad 4.83. 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 4.84. 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) $\Leftrightarrow$ (5) z věty 4.82. 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 4.85. 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 4.24. 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 4.86. Pokud A je regulární matice, pak každá soustava rovnic $A\mathbf{x} = \mathbf{b}$ má podle definice regulární matice právě jedno řešení. Jak jsme již viděli v důkazu věty 4.82, 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 4.83.

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 jednoduše zapsat/vyjádřit 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 4.87. *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 4.82. □

4.4.6. Regularita a maticové operace.

Tvrzení 4.88. *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 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 $(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}B = I$. □

Geometrickou interpretaci bodů (1), (3), (4) si rozmyslete jako cvičení.

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 4.82.

Tvrzení 4.89. *Čtvercová matice A je regulární právě tehdy, když jde napsat jako součin elementárních matic.*

Důkaz. Každá elementární matice je regulární podle tvrzení 4.87, 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 4.82). Elementární řádkové úpravy se dají napsat jako násobení zleva elementární maticí, takže existují elementární matice E_1, E_2, ..., 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 4.87), 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 4.87). □

Příklad 4.90. 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 elegantně popsat, 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 $E_1, \ldots, E_k$, které popisují provedené úpravy, platí

$$B = E_k \cdots E_2 E_1 A \ .$$

Podle tvrzení 4.89 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 $E_1, \ldots, E_k$. Z toho vyplývá, že B lze z A získat posloupností elementárních úprav. Dokázali jsme následující tvrzení.

TVRZENÍ 4.91. *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 $B = RA$.*

4.5. Soustavy lineárních rovnic podruhé

Matice poskytují efektivní formalismus ke studiu soustav lineárních rovnic. Již samotná formulace problému je nyní velice elegantní: pro danou matici A typu $m \times n$ nad $\mathbf{T}$ a daný aritmetický vektor $\mathbf{b} \in T^m$ hledáme všechny $\mathbf{x} \in T^n$, pro které platí

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

4.5.1. Tvar řešení. V kapitole 2 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

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

kde

- P je množina indexů volných proměnných,
- $\mathbf{u}$, $\mathbf{v}_p$, $p \in P$, jsou „vhodné“ n-složkové aritmetické vektory nad $\mathbf{T}$.

Navíc víme, že různé volby parametrů $t_p \in T$ dávají různá řešení. (Vlastně jsme vše probírali jen pro $\mathbf{T} = \mathbb{R}$, ale postup nad obecným tělesem je stejný.)

Aritmetické vektory $\mathbf{u}$ a $\mathbf{v}_p$, $p \in P$ jsme získali užitím zpětné substituce a algebraických úprav. Jde spočítat tyto vektory přímo? Co se stane, když změníme pouze pravou stranu soustavy? Nyní máme nástroje na takové otázky snadno odpovědět.

Z tvaru řešení vidíme, že zvolíme-li hodnoty parametrů $t_p = 0$ pro každé $p \in P$, dostaneme řešení $\mathbf{x} = \mathbf{u}$. Vektor $\mathbf{u}$ tedy můžeme spočítat z odstupňovaného tvaru tím, že zvolíme volné proměnné rovné 0 a dopočteme řešení soustavy. Zvolíme-li jeden z parametrů $t_p = 1$ a ostatní parametry rovné 0, dostaneme jiné řešení $\mathbf{x} = \mathbf{u} + \mathbf{v}_p$. Z následujícího pozorování vyplývá, že vektor $\mathbf{v}_p = (\mathbf{u} + \mathbf{v}_p) - \mathbf{u}$ je řešením soustavy se stejnou maticí a nulovou pravou stranou, tzv. příslušné homogenní soustavy.

POZOROVÁNÍ 4.92. *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

$$A(\mathbf{w} - \mathbf{u}) = A\mathbf{w} - A\mathbf{u} = \mathbf{b} - \mathbf{b} = \mathbf{o} \ .$$

Aritmetický vektor $\mathbf{w} - \mathbf{u}$ je proto řešením soustavy $A\mathbf{x} = \mathbf{o}$. □

DEFINICE 4.93. Soustava $A\mathbf{x} = \mathbf{o}$ se nazývá *homogenní soustava lineárních rovnic* (příslušná k soustavě $A\mathbf{x} = \mathbf{b}$).

Vektor $\mathbf{v}_p$, $p \in P$ lze tedy získat tak, že zvolíme $x_p = 1$, ostatní volné proměnné zvolíme rovné 0 a dopočteme řešení **příslušné homogenní soustavy**. Tato pozorování nám dávají odpověď i na druhou otázku – směrové vektory $\mathbf{v}_p$ na pravé straně vůbec nezáleží. Geometricky, změníme-li pravou stranu, řešením bude útvar rovnoběžný k původnímu.

PŘÍKLAD 4.94. Vrátíme se k soustavě k příkladu z oddílu 2.3.4. Po eliminaci jsme získali ekvivalentní soustavu s rozšířenou maticí

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

Soustava má řešení, bázové proměnné jsou x_1 a x_3, volné proměnné jsou x_2, x_4 a x_5. Množina všech řešení proto bude tvaru

$$\{\mathbf{u} + t_2\mathbf{v}_2 + t_4\mathbf{v}_4 + t_5\mathbf{v}_5 : t_2, t_4, t_5 \in \mathbb{R}\},$$

Na rozdíl od předchozího postupu, určíme nyní aritmetické vektory $\mathbf{u}$, $\mathbf{v}_2$, $\mathbf{v}_4$ a $\mathbf{v}_5$ rychleji. Zvolíme $x_2 = x_4 = x_5 = 0$ a dopočteme řešení soustavy zpětnou substitucí. Při počítání na papíře to většinou půjde zpaměti. Následující schéma znázorňuje volbu parametrů a postupný výpočet proměnných x_3 a x_1.

$$(?, 0, ?, 0, 0)^T \quad (?, 0, -3, 0, 0)^T \quad (-1, 0, -3, 0, 0)^T = \mathbf{u}$$

Vektor $\mathbf{v}_2$ určíme volbou $x_2 = 1, x_4 = x_5 = 0$ a dopočtením řešení **příslušné homogenní soustavy**.

$$(?, 1, ?, 0, 0)^T \quad (?, 1, 0, 0, 0)^T \quad (-2, 1, 0, 0, 0)^T = \mathbf{v}_2$$

Podobně spočítáme $\mathbf{v}_4$ a $\mathbf{v}_5$.

$$(?, 0, ?, 1, 0)^T \quad (?, 0, 0, 1, 0)^T \quad (-3, 0, 0, 1, 0)^T = \mathbf{v}_4$$
$$(?, 0, ?, 0, 1)^T \quad (?, 0, -2, 0, 1)^T \quad (-2, 0, -2, 0, 1)^T = \mathbf{v}_5$$

Množina řešení je tedy

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

▲

Všimněte si rovněž, že

$$\left\{ \sum_{p \in P} t_p \mathbf{v}_p : \ t_p \in T \ \text{ pro každé } \ p \in P \right\}$$

je množina všech řešení příslušné homogenní soustavy. 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 4.95. 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 $\operatorname{Ker} A$.

Nabízejí se další otázky. Je důležité zvolit při výpočtu $\mathbf{u}$ všechny volné proměnné rovny 0, nebo můžeme volit libovolně? Věta 4.97 na tuto otázku odpovídá. Podobná otázka se nabízí pro výpočet vektorů $\mathbf{v}_p$, tu ale budeme umět uspokojivě zodpovědět až v kapitole o vektorových prostorech.

K důkazu slíbené věty učiníme ještě jedno jednoduché pozorování.

POZOROVÁNÍ 4.96. *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.

VĚTA 4.97. *Je-li* $\mathbf{u}$ *jakékoliv řešení soustavy lineárních rovnic* $A\mathbf{x} = \mathbf{b}$ *nad tělesem* $\mathbf{T}$ *(tzv.* partikulární řešení*), 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 4.92 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 4.96. □

Ve formulaci věty je zároveň vysvětlen význam výrazů typu $\mathbf{u} + \operatorname{Ker} A$, kdy „sčítáme“ vektor s množinou vektorů. Toto značení budeme příležitostně používat.

4.5.2. LU–rozklad. Začneme podrobným rozborem jednoho příkladu.

PŘÍKLAD 4.98. Máme vyřešit reálnou soustavu

$$\left(\begin{array}{ccc|c} 2 & 2 & 2 & 1 \\ 4 & 7 & 7 & 2 \\ 6 & 18 & 22 & 7 \end{array}\right) \ .$$

Gaussovou 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 nejspíš 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

$$\begin{aligned} R = E_3 E_2 E_1 &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 5 & -4 & 1 \end{pmatrix} \ . \end{aligned}$$

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 bodu (6) tvrzení 4.35.

Řešíme-li další soustavu $(A|\mathbf{b})$ se stejnou maticí soustavy A Gaussovou 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

$$U\mathbf{x} = R\mathbf{b}$$

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 prvním cyklu Gaussovy eliminace. 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. o druhém cyklu Gaussovy eliminace.

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). Toto není náhoda, ale obecné zdůvodnění vynecháme (zkuste to!).

Díky tomu, že matici R^{-1} známe hned po prvním řešení soustavy $A\mathbf{x} = \mathbf{b}$ Gaussovou eliminací, v tomto kontextu je matice R^{-1} 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*. Vyjádření matice A jako součinu $A = LU$ je záznamem o celém průběhu Gaussovy eliminace matice A. Matice L říká, jaké elementární řádkové úpravy třetího typu jsme použili, matice U je horní trojúhelníková matice, kterou jsme dostali po Gaussově eliminaci použité na matici A. Důležité také je, že jsme během Gaussovy eliminace nikde nemuseli použít 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 řešení soustavy $A\mathbf{x} = \mathbf{b}$ z předchozího příkladu byl založen na rozkladu matice A ve tvaru součinu $A = LU$, kde L je dolní trojúhelníková matice s jednotkami na hlavní diagonále a U je horní trojúhelníková matice s nenulovými prvky na hlavní diagonále. Takový rozklad matice A se nazývá *LU–rozklad*.

LU–rozklad regulární matice A nemusí existovat. Pokud totiž $A = LU$ je LU–rozklad matice A, pak se první řádky matic A a U shodují, jak si snadno ověříte řádkovým pohledem na násobení. Speciálně $a_{11} = u_{11} \neq 0$, takže matice

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

je příkladem regulární matice, pro kterou LU–rozklad neexistuje. Pokud je ale A regulární matice, u které při Gaussově eliminaci nemusíme prohazovat řádky, pak LU–rozklad existuje a je dokonce jednoznačný, jak ukážeme ve větě 4.101. Matice U je výsledkem Gaussovy eliminace, při které používáme pouze třetí krok. Matice L má na místě (i, j) pod hlavní diagonálou prvek opačný k číslu, kterým jsme násobili j-tý řádek při eliminaci prvku na místě (i, j) (ale tento přesný popis matice L nebudeme ve větě 4.101 dokazovat).

Příklad 4.99. Spočítáme LU–rozklad reálné matice

$$A = \begin{pmatrix} 2 & 1 & 1 \\ 4 & -6 & 0 \\ -2 & 7 & 2 \end{pmatrix} .$$

Gaussovou eliminací matici A upravíme do odstupňovaného tvaru.

$$A = \begin{pmatrix} 2 & 1 & 1 \\ 4 & -6 & 0 \\ -2 & 7 & 2 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & 1 \\ 0 & -8 & -2 \\ 0 & 8 & 3 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & 1 \\ 0 & -8 & -2 \\ 0 & 0 & 1 \end{pmatrix} = U .$$

V první úpravě jsme (-2)-násobek prvního řádku přičetli k druhému a 1-násobek prvního řádku přičetli k třetímu. Ve druhé úpravě jsme 1-násobek druhého řádku přičetli k třetímu. Získáváme LU–rozklad

$$\begin{pmatrix} 2 & 1 & 1 \\ 4 & -6 & 0 \\ -2 & 7 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 & 1 \\ 0 & -8 & -2 \\ 0 & 0 & 1 \end{pmatrix} .$$

▲

Myšlenka důkazu existence LU–rozkladu je vysvětlena v příkladu 4.98. Nalezneme nejprve matici R takovou, že $RA = U$ a R je dolní trojúhelníková s jednotkami na hlavní diagonále, a pak položíme $L = R^{-1}$. To, že matice L má také požadované vlastnosti, vyplývá z následujícího tvrzení.

Tvrzení 4.100. *Nechť R je dolní (horní) trojúhelníková matice řádu n s nenulovými všemi prvky na hlavní diagonále. Pak R je regulární a 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. Je-li R dolní trojúhelníková s nenulovými prvky na hlavní diagonále, pak R^T je regulární podle bodu (5) z věty 4.82. Tím pádem je i R^{-1} regulární podle tvrzení 4.88.

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 pod 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 bodu (5) tvrzení 4.35.

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 bodu (6) tvrzení 4.35.

Případy, kdy je matice R horní trojúhelníková plynou pomocí transponování z právě dokázaných vlastností inverze dolních trojúhelníkových matic. □

Dokázané tvrzení se nám bude hodit i k důkazu jednoznačnosti LU–rozkladu.

VĚTA 4.101 (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. Nejprve dokážeme existenci. Za daných předpokladů na matici A můžeme přičítáním vhodných násobků řádků k řádkům pod ním postupně převést matici A na horní trojúhelníkovou matici U s nenulovými prvky na hlavní diagonále. Všem řádkovým úpravám odpovídají dolní trojúhelníkové matice $E_1, E_2, \ldots, E_k$ s jednotkami na hlavní diagonále, platí proto $E_k \cdots E_2 E_1 A = U$ a matice $R = E_k \cdots E_2 E_1$ je dolní trojúhelníková s jednotkami na hlavní diagonále podle bodu (6) tvrzení 4.35. Podle tvrzení 4.100 inverzní matice R^{-1} existuje a je také dolní trojúhelníková s jednotkami na hlavní diagonále. Protože $RA = U$, platí $A = R^{-1}U$, takže stačí položit $L = R^{-1}$.

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 podle tvrzení 4.100 a tvrzení 4.35. 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 $U_1 = U_2$. □

Jak jsme ukázali dříve, LU-rozklad regulární matice $A = LU$ řádu n lze využít 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.

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. 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.

6. 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.

7. Dokažte přímo tvrzení 4.24.

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 4.14.

12. Dokažte druhou distributivitu z tvrzení 4.29.

13. Dokažte vztahy $A(B-C) = AB - AC$ a $A(-B) = -AB$, má-li jedna strana smysl.

14. Dokažte tvrzení 4.31.

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

16. Dokažte vzorec pro blokové násobení matic.

17. Najděte A^n pro matici z příkladu 4.44.

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 4.85 alternativními postupy navržené v tomto příkladu.

20. Ke každé elementární matici najděte příslušnou matici inverzní, viz tvrzení 4.87.

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 4.82.

23. Dokažte přímo implikaci (9) $\Rightarrow$ (3) z věty 4.82.

24. Dokažte tvrzení 4.88 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) U libovolné matice $A = (a_{ij})$ říkáme, že prvky a_{ii} tvoří *hlavní diagonálu.*

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

(6) 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 $i < j$.

(7) 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 $0_{m \times n} = (0)_{m \times n}$.

(8) 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) $A + B = B + A$.

(9) 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 $t \cdot A = tA = (ta_{ij})_{m \times n}$.

(10) 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) $s(A + B) = sA + sB$.

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

(12) 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) $(sA)^T = s\,A^T$.

(13) Matici $A = (a_{ij})_{m\times n}$ nad tělesem $\mathbf{T}$ můžeme také zapsat po sloupcích. *Sloupcový zápis* matice A je

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

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

(14) Sloupcový zápis matice A^T je

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

kde pro každé $i = 1, 2, \dots, m$ vektor $\tilde{\mathbf{a}}_i = (a_{i1}, a_{i2}, \dots, a_{in})^T$ 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.

(15) 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

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

(16) 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.*

(17) 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 $m \times p$.

(18) 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*“.

(19) 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. $\tilde{\mathbf{a}}_i^T B$.

(20) **Násobení matic není komutativní**.

(21) 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) $I_m A = A = A I_n$,
 (b) $B(CD) = (BC)D$,
 (c) $(A + B)C = AC + BC$,
 (d) $C(D + E) = CD + CE$,
 (e) $(BC)^T = C^T B^T$,
 (f) $s(BC) = (sB)C = B(sC)$.

(22) Pro libovolné čtvercové 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.

(23) *Elementární matice* řádu m je libovolná matice, kterou dostaneme z identické matice I_m jednou elementární řádkovou úpravou.

(24) 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.

(25) 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.

(26) 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 $\mathbf{x} \in \mathbf{T}^n$.

(27) Rotace kolem počátku souřadnic v rovině o úhel α proti směru hodinových ručiček je určená maticí

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

(28) Symetrie v rovině vzhledem k první souřadné ose je určená maticí

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

(29) 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 $\mathbf{T}^n$.

(30) Pro každou matici $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ a každé $j = 1, 2, \ldots, n$ platí rovnost $f_A(\mathbf{e}_j) = \mathbf{a}_j$. Matice A určující zobrazení f_A je určená jenoznačně.

(31) 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
- $f_A(s\mathbf{x}) = A(s\mathbf{x}) = s\,A\mathbf{x} = s\,f_A(\mathbf{x})$,
- $f_A(\mathbf{x} + \mathbf{y}) = A(\mathbf{x} + \mathbf{y}) = A\mathbf{x} + A\mathbf{y} = f_A(\mathbf{x}) + f_A(\mathbf{y})$.

(32) 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 $\mathbf{x} \in \mathbf{T}^{\mathbf{p}}$ platí $f_A f_B(\mathbf{x}) = f_A(B\mathbf{x}) = A(B\mathbf{x}) = (AB)\mathbf{x} = f_{AB}(\mathbf{x})$.

(33) Symetrie v rovině vzhledem k přímce, kterou dostaneme z první souřadné osy otočením kolem počátku o úhel α v kladném směru, je určená maticí

$$\begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix} .$$

(34) Ortogonální projekce v rovině na první souřadnou osu je určená maticí

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

(35) Jednotková matice I_n nad tělesem $\mathbf{T}$ určuje identické zobrazení na množině $\mathbf{T}^n$.

(36) 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}.

(37) 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*.

(38) **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.

(39) Speciálně, čtvercová matice A je invertovatelná právě když je regulární.

(40) 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}.

(41) 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.

(42) Každá elementární matice je regulární, navíc inverzní matice k elementární matici je opět elementární matice.

(43) 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 $(AB)^{-1} = B^{-1}A^{-1}$.

(44) 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 $B = RA$.

(45) 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 $\mathbf{T}^m$.

(46) 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.

(47) Soustava $A\mathbf{x} = \mathbf{o}$ s nulovou pravou stranou se nazývá *homogenní soustava lineárních rovnic*.

(48) 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 $\operatorname{Ker} A$.

(49) 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

$$\{\mathbf{u} + \mathbf{v} : \mathbf{v} \in \operatorname{Ker} A\} \;=\; \mathbf{u} + \operatorname{Ker} A \;.$$

Vektor $\mathbf{u}$ spočítáme z odstupňovaného tvaru tím, že zvolíme volné proměnné rovné 0 a dopočteme řešení soustavy. Vektor $\mathbf{v}_p$, $p \in P$ spočítáme tak, že zvolíme $x_p = 1$, ostatní volné proměnné zvolíme rovné 0 a dopočteme řešení **příslušné homogenní soustavy**.

(50) 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.

(51) **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.

(52) 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 Gaussovou eliminací matice A.

(53) 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.

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) Speciální typy matic, jejich součiny a inverzní matice k nim.
(4) Zobrazení určené maticí a jeho vlastnosti.
(5) Matice jednoduchých geometrických zobrazení.
(6) Matice složeného zobrazení $f_A f_B$.
(7) Regulární matice a různé podmínky ekvivalentní s regularitou.
(8) Metoda výpočtu inverzní matice.
(9) Vztah invertování a ostatních operací.
(10) Kdy lze jednu matici dostat z druhé posloupností elementárních řádkových úprav.
(11) Homogenní soustava rovnic a jádro matice.
(12) Vyjádření množiny všech řešení soustavy $A\mathbf{x} = \mathbf{b}$ ve tvaru $\{\mathbf{u} + \operatorname{Ker} A\}$.

KAPITOLA 5

Vektorové prostory

Cíl. *Podobně jako jsme běžné vlastnosti počítání s reálnými čísly zobecnili do pojmu tělesa, zobecníme vlastnosti počítání s aritmetickými vektory do pojmu vektorového prostoru. Ukážeme si některé základní vlastnosti vektorových prostorů. Budeme zkoumat důležité pojmy jako podprostor, lineární obal, množina generátorů, lineární závislost a nezávislost, báze a dimenze. Motivací je porozumět geometrickým vztahům mezi vektory a podprostory (rovné útvary procházející počátkem) například v rovině a v prostoru. To nám také umožní lépe porozumět řešení soustav lineárních rovnic.*

5.1. Definice, příklady a základní vlastnosti

V kapitole o tělesech jsme 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 vektorového prostoru nad tělesem $\mathbf{T}$. Prvky vektorového prostoru mohou být nejen aritmetické vektory, ale například také nekonečné posloupnosti čísel, reálné funkce reálné proměnné, matice, polynomy, apod.

Pojem vektorového 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 1.4 nebo 1.3. 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 vektorového prostoru přenášet úvahy o vektorech na funkce na základě analogie.

Vektorový prostor nad $\mathbb{R}$ tvoří množina (jejíž prvky nazýváme vektory), operace sčítání vektorů a operace násobení vektoru reálným číslem. Tyto ingredience musí splňovat sadu axiomů, které jsou ve shodě s představou vektoru jako „šipky“ v rovině nebo prostoru a operací prováděných podle obrázků 1.4 a 1.3. Obecněji definujeme vektorový prostor nad tělesem $\mathbf{T}$, kde místo násobení vektoru reálným číslem máme operace násobení vektoru prvkem T.

Definice 5.1. Nechť $\mathbf{T}$ je těleso. *Vektorovým prostorem* $\mathbf{V}$ *nad tělesem* $\mathbf{T}$ rozumíme množinu V spolu s binární operací $+$ na V (tj. $+$ je zobrazení z $V \times V$ do V) a operací $\cdot$ násobení 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 vektorových prostorů budeme prvkům T někdy říkat *skaláry* a prvkům V *vektory* (nebo prostě prvky V). **Výrazy skalár a vektor nemají samostatný smysl**, používáme je jen když je z kontextu zřejmé, které těleso a vektorový prostor máme na mysli.

„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 $\mathbf{o}$ ve vektorovém prostoru $\mathbf{V}$. Abychom je odlišili i jazykově, budeme v případě $0 \in T$ mluvit o *nulovém skaláru* a v případě $\mathbf{o} \in V$ o *nulovém vektoru*. 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.

Zopakujme, že základním příkladem vektorového prostoru nad $\mathbb{R}$ je množina všech „fyzikálních“ vektorů (šipek) v ideální rovině s běžnými operacemi definovanými podle obrázků 1.4 a 1.3. Podobně, množina šipek v ideálním prostoru tvoří vektorový prostor nad $\mathbb{R}$. Abychom v těchto vektorových prostorech mohli efektivně počítat, zavádíme soustavu souřadnic a místo s vektory počítáme s jejich souřadnicemi. Tím převádíme výpočty v těchto ideálních prostorech na výpočty v tzv. aritmetických vektorových prostorech.

5.1.1. Aritmetické vektorové prostory. Základním příkladem vektorového prostoru, který je vhodný k počítání, 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 $\cdot$ (definovanými jako v definici 2.5). Označujeme jej $\mathbf{T}^n$.

To, že aritmetický vektorový prostor $\mathbf{T}^n$ je skutečně vektorovým prostorem, jsme dokázali obecně pro matice v tvrzení 4.11 a tvrzení 4.14.

Aritmetické vektorové prostory jsou velmi konkrétní, zároveň ale v jistém smyslu „jediné“, příklady vektorových prostorů konečné dimenze (pojem konečné dimenze

přesně definujeme později, zatím chápejte intuitivně). Uvidíme, že v každém vektorovém 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 vektorový 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 vektorového 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 vektorových 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.

5.1.2. Další příklady. Uvedeme několik dalších příkladů vektorových prostorů.

Příklad 5.3. Množina V všech trojic $(x_1, x_2, x_3)^T \in \mathbb{R}^3$, které splňují rovnici $2x_1 + 3x_2 + 4x_3 = 0$, spolu s běžnými operacemi tvoří vektorový prostor nad $\mathbb{R}$ (obecněji $\operatorname{Ker} A$ pro libovolnou matici A nad $\mathbf{T}$ tvoří s běžnými operacemi vektorový prostor nad $\mathbf{T}$, viz tvrzení 5.14).

K ověření, že tomu tak skutečně je, je potřeba si nejprve uvědomit, že operace jsou dobře definovány, tedy součet dvou vektorů ve V je opět vektor ve V a skalární násobek vektoru ve V je opět vektor ve V. Dále je třeba ověřit všechny axiomy. V tvrzení 5.14 vše dokážeme obecněji.

Uvědomte si, že tento prostor **není** aritmetickým prostorem $\mathbb{R}^3$, protože V není tvořeno všemi trojsložkovými reálnými aritmetickými vektory, jen některými. Jde o tzv. podprostor aritmetického vektorového prostoru $\mathbb{R}^3$. Podprostory se budeme zabývat v oddílu 5.2.

Také si všimněte, že kdybychom místo $2x_1 + 3x_2 + 4x_3 = 0$ uvažovali rovnici $2x_1 + 3x_2 + 4x_3 = 10$, vektorový prostor bychom (s běžnými operacemi) nedostali. Operace nejsou dobře definovány, protože například trojice $(5, 0, 0)^T$ rovnici splňuje, kdežto $0 \cdot (5, 0, 0)^T = (0, 0, 0)^T$ nikoliv. ▲

Příklad 5.4. Množina všech polynomů stupně nejvýše 173 s reálnými koeficienty (nebo jiného daného maximálního stupně, s koeficienty v jiném tělese) s běžnými operacemi sčítání polynomů a násobení polynomu reálným číslem. Tento vektorový prostor je „v podstatě“ 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 5.5. Množina všech matic typu 7×15 nad tělesem $\mathbb{Z}_3$ s běžnými operacemi sčítání a násobení skalárem je vektorový prostor nad $\mathbb{Z}_3$ (obecněji množina matic daného typu nad jiným tělesem). Vzhledem k operacím $+$ a $\cdot$ se tato množina chová stejně jako množina uspořádaných 105-tic, takže tento vektorový prostor je „v podstatě“ aritmetický vektorový prostor $\mathbb{Z}_3^{105}$. To, že množina matic daného typu nad daným tělesem je vektorový prostor jsme dokázali v tvrzení 4.11 a tvrzení 4.14. 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. ▲

Vektorový 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 vektorových prostorů.

Příklad 5.6. 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 vektorový prostor nad $\mathbb{Z}_2$. Jako cvičení dokažte, že toto je skutečně vektorový prostor, a vysvětlete proč je tento prostor „v podstatě“ $\mathbb{Z}_2^{11}$. ▲

Příklad 5.7. 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 5.8. Těleso $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ s běžnými operacemi sčítání a násobení racionálním číslem je vektorový prostor nad $\mathbb{Q}$. Skutečně, číslo $a + b\sqrt{2}$ lze chápat jako dvojici $(a, b)^T \in \mathbb{Q}^2$. Není ale na první pohled patrné, že každá dvojice odpovídá právě jednomu prvku tělesa $\mathbb{Q}(\sqrt{2})$, důkaz je přenechán jako cvičení. ▲

Vlastnosti podobných vektorových prostorů, jako například dimenze, jsou důležité například v již zmíněných problémech kvadratury kruhu, trisekce úhlu, zdvojení krychle a „neřešitelnosti“ rovnic pátého stupně.

Příklad 5.9. Množina všech reálných posloupností tvoří spolu s přirozenými operacemi sčítání posloupností a násobení posloupnosti reálným číslem po jednotlivých složkách (podobně jako pro aritmetické vektory) vektorový prostor nad $\mathbb{R}$. Značíme jej $\mathbb{R}^\omega$. (Znak ω chápejte nyní jen jako symbol. Je to značení prvního „nekonečného čísla“.) Podobně bychom mohli uvažovat například množinu všech posloupností konvergentních k 0.

Příklad 5.10. Množina všech funkcí z $\mathbb{R}$ do $\mathbb{R}$ tvoří spolu s přirozenými operacemi sčítání funkcí a násobení funkce reálným číslem vektorový prostor nad $\mathbb{R}$. Podobnými příklady jsou množina všech spojitých funkcí na $\mathbb{R}$, množina diferencovatelných funkcí, množina polynomiálních funkcí, nebo třeba množina spojitých funkcí na intervalu $[0, 1]$. ▲

Prostory posloupností a funkcí jsou důležité příklady vektorových prostorů nekonečné dimenze, kterými se budete v dalším studiu zabývat hlavně v jiných předmětech, například ve funkcionální analýze. Zde se soustředíme hlavně na vektorové prostory konečné dimenze.

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

Tvrzení 5.11. *V každém vektorovém 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 vektor* $\mathbf{v} \in V$*,*
(4) $a\mathbf{o} = \mathbf{o}$ *pro libovolný skalár* $a \in T$*,*
(5) *je-li* $a\mathbf{v} = \mathbf{o}$*, pak buď* $a = 0$ *nebo* $\mathbf{v} = \mathbf{o}$*,*

(6) $-\mathbf{v} = (-1)\mathbf{v}$ *pro libovolný vektor* $\mathbf{v} \in V$*, speciálně* $-(-\mathbf{v}) = \mathbf{v}$.

Axiomy vektorového prostoru 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

V příkladu 5.3 jsme viděli, že z vektorových prostorů můžeme konstruovat další vektorové prostory tím, že vybereme jen některé vektory a operace sčítání a násobení skalárem zúžíme. Říkáme, že nový prostor je podprostorem původního:

Definice 5.12. Je-li $\mathbf{V}$ vektorový prostor nad $\mathbf{T}$, pak vektorový 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 $\mathbf{V}$. V této situaci budeme také psát $U \leq \mathbf{V}$.

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 5.13. *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 vektorový prostor.

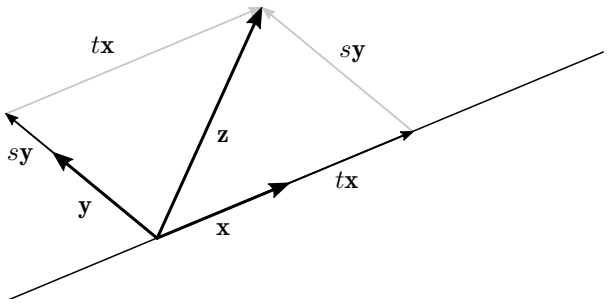
Předpokládejme, že U je neprázdná množina uzavřená na sčítání a násobení skalárem. Pak opačný prvek k $\mathbf{u} \in U$ je v U, protože $-\mathbf{u}$ lze napsat jako $(-1) \cdot \mathbf{u}$. Rovněž nulový prvek vektorového prostoru $\mathbf{V}$ je prvkem U, protože U je neprázdná a platí $0 \cdot \mathbf{u}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

Množina $\{\mathbf{o}\}$ tvořená pouze nulovým vektorem $\mathbf{o}$ je vždy podprostorem $\mathbf{V}$, rovněž celý prostor 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: $\{t\mathbf{x} : t \in \mathbb{R}\} \subseteq U$. Snadno ověříme, že pro libovolný vektor $\mathbf{o} \neq \mathbf{x} \in \mathbb{R}^2$ je množina $\{t\mathbf{x} : t \in \mathbb{R}\}$ uzavřená na sčítání a násobení skalárem a tedy podprostor $\mathbb{R}^2$. Pokud uspořádané dvojice interpretujeme jako souřadnice vektorů v rovině, jsou to všechny vektory, které mají stejný směr jako $\mathbf{x}$ (včetně nulového vektoru). Pokud je interpretujeme jako souřadnice bodů v rovině, je to přímka procházející počátkem a bodem $\mathbf{x}$.

Jestliže 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 $\mathbf{z} \in \mathbb{R}^2$ 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.



Obrázek 5.1. Podprostor $\mathbb{R}^2$ obsahující přímku $\{t\mathbf{x} : t \in \mathbb{R}\}$ a vektor $\mathbf{y}$ mimo ni

Ukázali jsme, že kromě triviálních podprostorů $\{\mathbf{o}\}$ a $\mathbb{R}^2$ jsou jedinými podprostory $\mathbb{R}^2$ množiny tvaru $\{t\mathbf{x} : t \in \mathbb{R}\}$. Při intepretaci 2-složkových reálných aritmetických vektorů jako bodů v rovině jsou tedy podprostory $\mathbb{R}^2$ počátek souřadnic $\{\mathbf{o}\}$, přímky procházející počátkem, a celá rovina $\mathbb{R}^2$.

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 $\mathbf{y}$, 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 $\mathbf{o} \neq \mathbf{x} \in T^2$.

S podprostory $\mathbf{T}^n$ jsme se již setkali v předchozí kapitole při řešení homogenních soustav lineárních rovnic. Zde je třeba si připomenout definici 4.95 jádra matice A jako množinu všech řešení homogenní soustavy $A\mathbf{x} = \mathbf{o}$.

Tvrzení 5.14. *Pro libovolnou matici A typu $m \times n$ nad $\mathbf{T}$ platí, že* $\operatorname{Ker} A$ *je podprostor $\mathbf{T}^n$, neboli* $\operatorname{Ker} A \leq \mathbf{T}^n$.

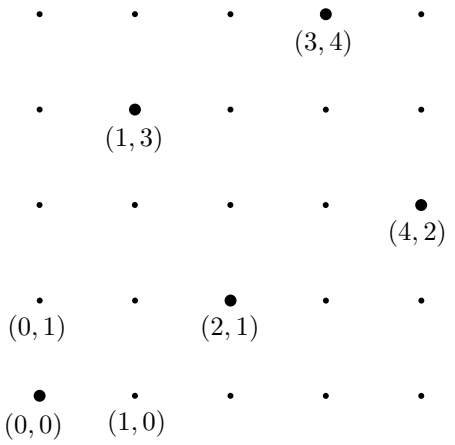
Důkaz. Podle tvrzení 5.13 stačí ověřit, že množina $\operatorname{Ker} A$ je neprázdná a uzavřená na sčítání a násobení skalárem.

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 $\operatorname{Ker} A$ úplným vzorem nulového vektoru při zobrazení f_A. Úplný vzor nenulového vektoru $\mathbf{b} \in \mathbf{T}^m$ (neboli množina všech řešení soustavy $A\mathbf{x} = \mathbf{b}$) **není** podprostor $\mathbf{T}^n$. Tato množina je sice „rovný útvar“, ale neobsahuje nulový prvek $\mathbf{o} \in \mathbf{T}^n$. Takovým množinám budeme později říkat afinní podprostory $\mathbf{T}^n$.



Obrázek 5.2. Přímka $\{t(2,1)^T : t \in \mathbb{Z}_5\}$ v prostoru $\mathbb{Z}_5^2$

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 vektorového prostoru $\mathbf{T}^n$.

5.2.3. Další příklady podprostorů.

Příklad 5.15. Množina všech čtvercových matic řádu 4 nad tělesem $\mathbb{Z}_5$ takových, že součet prvků na hlavní diagonále je roven nule, je podprostor vektorového prostoru $\mathbb{Z}_5^{4\times 4}$. Je totiž neprázdná (obsahuje například nulovou matici) a je uzavřená na sčítání a násobení skalárem, jak se snadno ověří. ▲

Příklad 5.16. Množina všech polynomů p stupně nejvýše 173 s reálnými koeficienty, pro které platí $p(5) = 0$, je podprostorem vektorového prostoru (z příkladu 5.4) všech reálných polynomů stupně nejvýše 173. ▲

Příklad 5.17. Množina reálných čísel je podprostorem prostoru komplexních čísel, kde obě tělesa reálných a komplexních čísel chápeme jako vektorové prostory nad $\mathbb{Q}$. ▲

Příklad 5.18. Množina spojitých funkcí z $\mathbb{R}$ do $\mathbb{R}$ je podprostorem vektorového prostoru všech funkcí z $\mathbb{R}$ do $\mathbb{R}$, protože množina spojitých funkcí je neprázdná a uzavřená na operace sčítání a násobení reálným číslem. Podobně, množina diferencovatelných funkcí z $\mathbb{R}$ do $\mathbb{R}$ je podprostorem vektorového prostoru spojitých funkcí. ▲

5.2.4. Lineární kombinace. Už mnohokrát jsme se setkali s výrazy typu $r\mathbf{u} + s\mathbf{v} + t\mathbf{w}$, kde $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w}$ jsou nějaké reálné aritmetické vektory a $r, s, t \in \mathbb{R}$. Takovým výrazům říkáme lineární kombinace vektorů $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w}$. Lineární kombinace můžeme definovat v každém vektorovém prostoru.

Definice 5.19. Jsou-li $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ prvky vektorového prostoru $\mathbf{V}$ nad $\mathbf{T}$ a $t_1, t_2, \ldots, t_k \in \mathbf{T}$ skaláry, tj. prvky tělesa $\mathbf{T}$, pak vektor

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

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 vektorů prostoru $\mathbf{V}$. Součet nekonečně mnoha vektorů ve vektorovém prostoru není obecně definován.

5.2.5. Lineární obal. Lineární kombinace se vyskytují v popisu podprostorů, například pro aritmetické vektory $\mathbf{x} = (1,1,1)^T$ a $\mathbf{y} = (1,2,3)^T \in \mathbb{R}^3$ je $\{s\mathbf{x} + t\mathbf{y} : s,t \in \mathbb{R}\}$ množina všech lineárních kombinací vektorů $\mathbf{x}, \mathbf{y}$ – rovina v $\mathbb{R}^3$. Obecně definujeme *lineární obal množiny* X jako množinu všech lineárních kombinací prvků X. Tato množina tvoří vždy podprostor (viz tvrzení 5.24).

Definice 5.20. Nechť $\mathbf{V}$ je vektorový prostor nad $\mathbf{T}$ a $X \subseteq V$. Pak *lineárním obalem množiny* X rozumíme množinu $\mathrm{LO}\, X$ všech lineárních kombinací prvků X, tj. množinu

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

Geometricky, lineární obal je „rovný útvar procházející počátkem“ obsahující dané vektory. Poznamenejme, že množina X může být i nekonečná. Definici můžeme trochu zjednodušit pro konečné množiny vektorů.

Pozorování 5.21. *Jsou-li* $\mathbf{v}_1, \ldots, \mathbf{v}_l$ *prvky vektorového prostoru* $\mathbf{V}$ *nad tělesem* $\mathbf{T}$*, pak*

$$\mathrm{LO}\,\{\mathbf{v}_1, \ldots, \mathbf{v}_l\} = \{t_1\mathbf{v}_1 + \cdots + t_l\mathbf{v}_l : t_1, \ldots, t_l \in T\}\ .$$

Důkaz. Inkluze „$\supseteq$“ plyne triviálně z definice lineárního obalu.

Naopak, je-li $\mathbf{u} \in \mathrm{LO}\,\{\mathbf{v}_1, \ldots, \mathbf{v}_l\}$, pak $\mathbf{u} = s_1\mathbf{u}_1 + \cdots + s_k\mathbf{u}_k$, kde každý z vektorů $\mathbf{u}_i$ leží v množině $\{\mathbf{v}_1, \ldots, \mathbf{v}_l\}$. V součtu $s_1\mathbf{u}_1 + \cdots + s_k\mathbf{u}_k$ seskupíme sčítance podle vektorů $\mathbf{v}_1, \ldots, \mathbf{v}_l$ 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 $\mathbf{u} = t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_l\mathbf{v}_l$. ▲

Příklad 5.22. $\mathrm{LO}\,\emptyset = \{\mathbf{o}\}$ – lineární obal prázdné množiny je triviální prostor tvořený nulovým vektorem. ▲

Příklad 5.23. V prostoru $\mathbb{R}^3$ máme

$$\mathrm{LO}\left\{\begin{pmatrix}1\\2\\3\end{pmatrix}, \begin{pmatrix}4\\5\\6\end{pmatrix}, \begin{pmatrix}9\\12\\15\end{pmatrix}\right\} = \mathrm{LO}\left\{\begin{pmatrix}1\\2\\3\end{pmatrix}, \begin{pmatrix}4\\5\\6\end{pmatrix}\right\} =$$

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

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 kombinaci 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.

Někdy říkáme „lineární obal vektorů …“, místo formálně přesného „lineární obal množiny vektorů $\{\dots\}$“. ▲

TVRZENÍ 5.24. *Pro libovolný vektorový prostor* $\mathbf{V}$ *nad* $\mathbf{T}$ *a libovolnou* $X \subseteq V$ *je* $\mathrm{LO}\, X$ *podprostorem* $\mathbf{V}$.

DŮKAZ. Je třeba ověřit, že $\mathrm{LO}\, X$ je neprázdná množina uzavřená na sčítání a násobení libovolným $r \in T$.

Předně $\mathrm{LO}\, X$ 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 $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k \in X$ 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 $\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_l \in X$ s koeficienty t_1, t_2, …, $t_l \in T$ 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 $\mathbf{v}_1, \dots, \mathbf{v}_k, \mathbf{w}_1, \dots, \mathbf{w}_l \in X$ 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 $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k \in X$ s koeficienty $s_1, s_2, \dots, s_k$ 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. ▲

5.2.6. Množina generátorů. 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 $\mathrm{LO}\, X$ je „nejmenší“ podprostor, který obsahuje X. Slovo nejmenší je zde třeba chápat vzhledem k inkluzi, tj. tak, že jakýkoliv podprostor obsahující X obsahuje $\mathrm{LO}\, X$. Proto se rovněž hovoří o podprostoru generovaném X.

DEFINICE 5.25. Je-li $\mathbf{V}$ vektorový prostor nad $\mathbf{T}$ a $X \subseteq V$. Pokud $\mathrm{LO}\, X = V$, 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 5.26.

- 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 $\mathbf{V} = \mathrm{LO}\left\{(1,2,3)^T\right\}$ 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 5.27. 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 5.28. Uvažujme prostor $\mathbb{R}^\omega$ všech nekonečných posloupností reálných čísel. Množina

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

negeneruje prostor $\mathbb{R}^\omega$, protože $\mathrm{LO}\,X$ obsahuje pouze posloupnosti s konečně mnoha nenulovými prvky. Negeneruje ani podprostor posloupností reálných čísel konvergujících k 0 ▲

5.2.7. Opět soustavy lineárních rovnic. Uvažujme matici A typu $m \times n$ nad tělesem $\mathbf{T}$ a aritmetický vektor $\mathbf{b} \in T^m$. Množinu řešení řešitelné soustavy rovnic $A\mathbf{x} = \mathbf{b}$ jsme dosud zapisovali ve tvaru

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

kde $\mathbf{u}$ a $\mathbf{v}_p$ jsou vhodné aritmetické vektory z $\mathbf{T}^n$. Již také víme, že

$$\left\{ \sum_{p \in P} t_p \mathbf{v}_p : \ t_p \in T \ \text{ pro každé } \ p \in P \right\}$$

je množina všech řešení příslušné homogenní soustavy rovnic $A\mathbf{x} = \mathbf{o}$ – jádro matice A.

Zavedené pojmy umožňují kompaktnější zápis a formulace. Jádro matice A je podprostor $\mathbb{R}^n$ rovný

$$\mathrm{LO}\,\{\mathbf{v}_p : p \in P\},$$

jinými slovy, $\{\mathbf{v}_p : p \in P\}$ je množina generátorů jádra matice A. Množinu všech řešení pak můžeme zapsat

$$\mathbf{u} + \mathrm{LO}\,\{\mathbf{v}_p : p \in P\}.$$

Připomeňme, že tato množina je podprostorem $\mathbb{R}^n$ právě tehdy, když $\mathbf{b} = \mathbf{o}$.

Příklad 5.29. Množina řešení soustavy z příkladu 2.3.4 je

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

$$\begin{pmatrix} -1 \\ 0 \\ -3 \\ 0 \\ 0 \end{pmatrix} + \mathrm{LO} \left\{ \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -3 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ 0 \\ -2 \\ 0 \\ 1 \end{pmatrix} \right\}.$$

Množina řešení příslušné homogenní soustavy je podprostor $\mathbb{R}^5$ generovaný vektory $(-2,1,0,0,0)^T$, $(-3,0,0,1,0)^T$, $(-2,0,-2,0,1)^T$. ▲

5.2.8. 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 5.30. 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 $\operatorname{Im} A$.

$$\operatorname{Im} A = \operatorname{LO}\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\} \leq \mathbf{T}^m$$

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

$$\operatorname{Im} A^T = \operatorname{LO}\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m\} \leq \mathbf{T}^n$$

Příklad 5.31. Pro reálnou matici

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

je

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

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

▲

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 obor hodnot zobrazení f_A.

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

Oboru hodnot se někdy také říká obraz (anglicky image), proto značení $\operatorname{Im} A$.

Příklad 5.32. Pro matici A z předchozího příkladu nejprve ověříme, že $(0,1)^T \in \operatorname{Im} A$ a $(1,0)^T \in \operatorname{Im} A$ a vyjádříme tyto vektory jako lineární kombinaci sloupců.

Protože máme dvě soustavy rovnic se stejnou maticí, můžeme je řešit najednou.

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

Vidíme, že obě soustavy mají řešení, tedy dané vektory do sloupcového prostoru matice A patří.

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

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

Ukázali jsme, 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 5.26 víme, že $\operatorname{LO}\left\{(1,0)^T, (0,1)^T\right\} = \mathbb{R}^2$.

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. ▲

5.2.9. Prostory určené maticí a elementární úpravy. K matici A typu $m \times n$ nad $\mathbf{T}$ máme přiřazeny čtyři základní podprostory aritmetických prostorů:

- $\operatorname{Im} A \leq \mathbf{T}^m$ – sloupcový prostor matice A, neboli lineární obal sloupcových vektorů, neboli obor hodnot zobrazení f_A.
- $\operatorname{Im} A^T \leq \mathbf{T}^n$ – řádkový prostor matice A, neboli sloupcový prostor matice A^T, neboli lineární obal řádkových vektorů (psaných do sloupců), neboli obor hodnot zobrazení f_{A^T}.
- $\operatorname{Ker} A \leq \mathbf{T}^n$ – jádro matice A, neboli množina všech řešení soustavy $A\mathbf{x} = \mathbf{o}$, neboli množina všech vektorů, jejichž obrazem při zobrazení f_A je nulový vektor.
- $\operatorname{Ker} A^T \leq \mathbf{T}^m$ – jádro matice A^T, neboli množina všech řešení soustavy $A^T\mathbf{x} = \mathbf{o}$, neboli množina všech vektorů, jejichž obrazem při zobrazení f_{A^T} je nulový vektor.

Jak se tyto prostory mění při elementárních řádkových (sloupcových) úpravách?

Již v kapitole o řešení soustav lineárních rovnic jsme si všimli, že elementární řádkové úpravy nemění množinu všech řešení soustavy lineárních rovnic. Když toto tvrzení napíšeme maticově pro homogenní soustavy, máme $\operatorname{Ker}(EA) = \operatorname{Ker} A$ pro každou elementární matici E (správného typu nad správným tělesem). Protože každá regulární matice R je součinem elementárních matic $R = E_1E_2\dots E_k$, máme obecněji

$$\operatorname{Ker}(RA) = \operatorname{Ker}(E_1E_2\dots E_kA) = \operatorname{Ker}(E_2\dots E_kA) = \dots = \operatorname{Ker} A \ .$$

Toto tvrzení dokážeme níže trochu rychleji. Všimněte si, že elementární sloupcové úpravy podprostor $\operatorname{Ker} A$ obecně mění.

Dalším 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 maticí R obecně mění $\operatorname{Im} A$ tak, že sloupcový prostor vzniklé matice je lineární obal R-násobků původních sloupců.

Tvrzení 5.33. *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*

$$\operatorname{Im}(RA) = \operatorname{LO}\{R\mathbf{a}_1, R\mathbf{a}_2, \dots, R\mathbf{a}_n\}, \quad \operatorname{Ker}(RA) = \operatorname{Ker} A, \quad \operatorname{Im}(RA)^T = \operatorname{Im} A^T \ .$$

Důkaz. První část je důsledkem definice součinu matic 4.20.

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 4.88.1. 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 v matici RA je každý řádek lineární kombinací řádků matice A podle tvrzení 4.24. 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 $\operatorname{Im}(A^T) = \operatorname{Im}(R^{-1}RA)^T \subseteq \operatorname{Im}(RA)^T$. ▲

Zformulujte si podobné tvrzení pro sloupce, tj. pro násobení regulární maticí zprava. Máme 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 $\operatorname{Im}(A^T)^T = \operatorname{Im}(R^T A^T)^T$, což po úpravě za použití rovností $(A^T)^T = A$ a $(R^T A^T)^T = AR$ dokazuje rovnost $\operatorname{Im} A = \operatorname{Im}(AR)$.

Důsledek 5.34. *Elementární řádkové úpravy matice A (obecněji násobení regulární maticí zleva) nemění* $\operatorname{Ker} A$ *a* $\operatorname{Im} A^T$. *Elementární sloupcové úpravy nemění* $\operatorname{Ker} A^T$ *a* $\operatorname{Im} A$.

Rovněž se zamyslete, jak se sloupcovými úpravami mění $\operatorname{Ker} A$.

5.3. Lineární závislost a nezávislost

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 5.23. Důvod je ten, že třetí vektor $(9,12,15)^T$ lze napsat jako lineární kombinaci zbývajících dvou vektorů. Množinám prvků libovolného vektorového prostoru, ve kterých žádný z prvků není lineární kombinací ostatních, říkáme *lineárně nezávislé*. Z formulačních důvodů definujeme lineární (ne)závislost pro posloupnosti prvků vektorového prostoru, nikoliv pro množiny.

Definice 5.35. Nechť $\mathbf{V}$ je vektorový 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 $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_{i-1}$, $\mathbf{v}_{i+1}$, …, $\mathbf{v}_k$.

V opačném případě říkáme, že posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ 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 $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ je lineárně závislá, pokud existuje $i \in \{1, 2, \ldots, k\}$ tak, že

$$\mathbf{v}_i \in \operatorname{LO}\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_k\} \quad ,$$

ekvivalentně

$$\operatorname{LO}\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\} = \operatorname{LO}\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_k\} \quad .$$

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

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

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

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

Posloupnost vektorů $(\mathbf{u}, \mathbf{v}, \mathbf{u}+\mathbf{v})$ v libovolném vektorovém prostoru je vždy lineárně závislá.

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

Posloupnost čísel $(1, \sqrt{2})$ je lineárně nezávislá ve vektorovém prostoru $\mathbb{R}$ nad tělesem $\mathbb{Q}$, protože $\sqrt{2}$ je iracionální číslo. Stejná posloupnost je lineárně závislá ve vektorovém prostoru $\mathbb{R}$ nad tělesem $\mathbb{R}$, protože např. $\sqrt{2}$ je $\sqrt{2}$-násobkem vektoru 1. Protože je druhý vektorový prostor nad tělesem reálných čísel, můžeme použít číslo $\sqrt{2} \in \mathbb{R}$ jako koeficient lineární kombinace. ▲

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.
- Můžeme povolit i prázdnou posloupnost vektorů, tedy případ $k = 0$ v definici 5.35. Tato posloupnost je lineárně nezávislá.
- 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 $\mathbf{v}_1$, …, $\mathbf{v}_k$ 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 5.37. *Nechť $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ je posloupnost prvků vektorového 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

$$\mathbf{v}_i = -a_i^{-1}a_1\mathbf{v}_1 - \ldots - a_i^{-1}a_{i-1}\mathbf{v}_{i-1} \ ,$$

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 vektorového 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).

Připomeňme, že vektory $\mathbf{v}_1, \ldots, \mathbf{v}_k$ generují vektorový prostor $\mathbf{V}$, pokud se každý vektor dá napsat jako lineární kombinace těchto vektorů alespoň jedním způsobem. Srovnejte tuto skutečnost s bodem (4).

Příklad 5.38. Zjistíme, zda je posloupnost aritmetických vektorů

$$((1,1,1,1)^T, (1,2,1,1)^T, (0,1,0,1)^T)$$

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 všechny 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 5.39. *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 $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$, pak podle definice 4.17 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 4.95 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 5.37 ekvivalentní lineární nezávislosti posloupnosti sloupcových vektorů matice A. ▲

PŘÍKLAD 5.40. 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.

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 bázové proměnné zpětnou substitucí. ▲

Na tomto místě si znovu uvědomme, že aritmetické vektorové prostory tvoří jen jeden z mnoha možných typů vektorových prostorů. (I když jsme v úvodu tvrdili, že jsou „v podstatě jediné“. Uvozovky jsou zde podstatné, na přesný význam si musíme ještě chvíli počkat.) Častá chybná odpověď studentů na otázku, jak určit, zda je daná posloupnost lineárně závislá, je typu „Napíšeme si vektory 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 $\cos(2x), \sin x + e^x, x^3$ vektorového prostoru spojitých reálných funkcí jedné reálné proměnné?

5.3.1. 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 při hledání báze řádkového prostoru.

Rovnou si také všimneme, že řádkové úpravy nemění ani lineární (ne)závislost sloupců. Tvrzení nejprve formulujeme pro sloupce. Řádkovou verzi dostaneme transponováním.

TVRZENÍ 5.41. *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 nad $\mathbf{T}$ a Q je regulární matice řádu n nad $\mathbf{T}$. Pak platí*

(1) *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*,*
(2) *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*.*

Důkaz. Použijeme pozorování formulované jako tvrzení 5.39, 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 $(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n)$ 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 $(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n)$ 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 4.82, 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 5.33. 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 5.42. *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 matice. Protože posloupnost řádkových vektorů matice A se rovná posloupnosti sloupcových vektorů transponované matice A^T, plynou řádkové verze z právě dokázaných sloupcových verzí. ▲

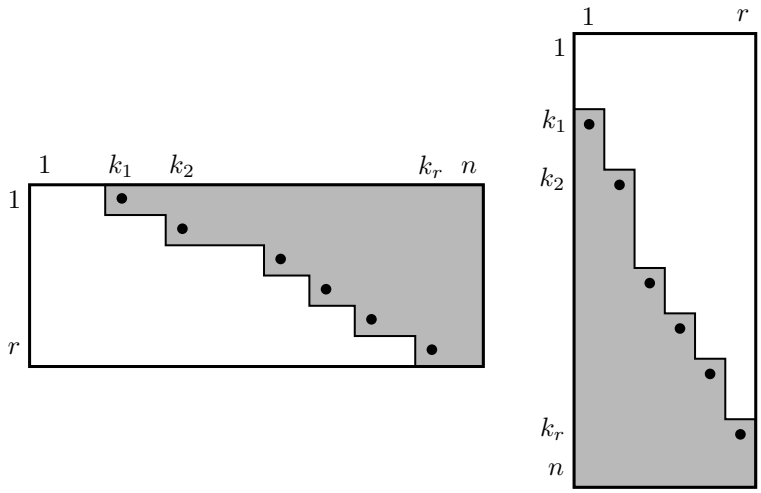
Zbývá nahlédnout, kdy je lineárně nezávislá posloupnost řádkových vektorů matice v řádkově odstupňovaném tvaru. Z předchozího tvrzení a tvrzení 5.39 vidíme, kdy je posloupnost sloupcových vektorů matice v odstupňovaném tvaru lineárně nezávislá. Je to právě tehdy, když příslušná homogenní soustava nemá žádné volné proměnné.

Je zřejmé, že je-li v matici nulový řádek, pak je posloupnost jejích řádkových vektorů lineárně závislá.

TVRZENÍ 5.43. *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 5.39). 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.



OBRÁZEK 5.3. Matice A a matice A^T

▲

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 $(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_p)$ je lineárně nezávislá.

PŘÍKLAD 5.44. Chceme zjistit, je-li posloupnost aritmetických vektorů

$$((1, 37, 3, 45, 1)^T, (0, -e, 1, \pi^e, 4)^T, (0, -12, 0, 33, 2)^T)$$

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 posloupnosti nám stačilo vybrat pouze první, třetí a pátou složku těchto vektorů. ▲

Příklad 5.45. Podíváme se znovu na příklad 5.38, 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 5.42 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 5.46. 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

Dostali jsme se ke stěžejnímu pojmu *báze* vektorového prostoru. Jako u lineární nezávislosti množin se budeme zabývat především konečnými bázemi a obecnou definici odložíme na později.

Definice 5.47. Posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ prvků vektorového prostoru $\mathbf{V}$ nad $\mathbf{T}$ se nazývá *báze*, pokud je lineárně nezávislá a $\mathrm{LO}\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\} = \mathbf{V}$.

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 5.37 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 5.48. *Posloupnost prvků* $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ *tvoří bázi vektorového prostoru* $\mathbf{V}$ *právě tehdy, když lze každý prvek* $\mathbf{b} \in V$ *vyjádřit právě jedním způsobem jako lineární kombinaci prvků* $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_n$.

Pozorování 5.49. *Posloupnost prvků* $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ *tvoří bázi vektorového prostoru* $\mathbf{T}^n$ *právě tehdy, když je matice* $(\mathbf{v}_1|\mathbf{v}_2|\ldots|\mathbf{v}_n)$ *regulární.*

Důkaz. Podle věty 4.82 (podmínky 2 a 3) je matice $(\mathbf{v}_1|\mathbf{v}_2|\ldots|\mathbf{v}_n)$ regulární právě tehdy, když má soustava $A\mathbf{x} = \mathbf{b}$ právě jedno řešení pro každý vektor pravých stran $\mathbf{b}$. ▲

Tedy například posloupnost sloupců (řádků) horní trojúhelníkové matice s nenulovými prvky na diagonále tvoří bázi.

Příklad 5.50. 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 5.43, a generuje $\mathbf{T}^n$, protože každý vektor $(x_1, \ldots, x_n)^T$ 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 $(x_1, x_2, \ldots, x_n)^T \in \mathbf{T}^n$ lze jednoznačně vyjádřit jako právě uvedenou lineární kombinaci ▲

Báze z posledního příkladu jsou význačné báze aritmetických prostorů, proto mají svoje pojmenování a značení.

Definice 5.51. *Kanonická báze* (též *standardní báze*) v aritmetickém prostoru $\mathbf{T}^n$ je posloupnost

$$(\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n) = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \right) .$$

Příklad 5.52.

- Jednočlenná posloupnost $((3,3,3)^T)$ je báze prostoru $\mathrm{LO}\left\{(1,1,1)^T\right\} \leq \mathbb{R}^3$.
- 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

$$\mathbf{V} = \mathrm{LO}\left\{(1,2,3)^T, (9,12,15)^T, (4,5,6)^T\right\} \leq \mathbb{R}^3 \ ,$$

  protože je lineárně závislá podle příkladu 5.36. 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 5.32. Posloupnost $((1,2,3)^T,\ (4,5,6)^T)$ je bází $\mathbf{V}$, protože generuje $\mathbf{V}$ (viz opět 5.36) a je lineárně nezávislá, jak se snadno přesvědčíme.

▲

Příklad 5.53. Najdeme nějakou bázi prostoru

$$\mathbf{V} = \mathrm{LO}\left\{ \begin{pmatrix} 2 \\ 1 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 5 \\ 0 \end{pmatrix}, \begin{pmatrix} 6 \\ 3 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 6 \\ 6 \end{pmatrix}, \begin{pmatrix} 3 \\ 5 \\ 2 \\ 3 \end{pmatrix} \right\} \leq \mathbb{Z}_7^4 \ .$$

Využijeme toho, že řádkové úpravy matice nemění lineární obal řádků (viz důsledek 5.34). Vektory tedy napíšeme do řádků a převedeme řádkovými úpravami na odstupňovaný tvar. Nenulové řádky generují stejný prostor a navíc jsou podle tvrzení 5.43 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 5.54. Uvažujme prostor $\mathbf{V}$ nekonečných posloupností $\mathbf{a} = (a_0,\ a_1,\ a_2, \dots)$ splňujících rovnost $a_{n+2} = a_n + a_{n+1}$ pro každé $n \geq 0$, s běžnými operacemi sčítání a násobení skalárem. Prostor $\mathbf{V}$ je podprostorem $\mathbb{R}^\omega$ mezi jehož prvky patří také Fibonacciho posloupnost, viz příklad 5.28.

Teď nás osvítí záblesk geniality a zkusíme najít v prostoru $\mathbf{V}$ nějakou nenulovou geometrickou posloupnost $\mathbf{q} = (q^0, q^1, q^2, q^3, \dots)$ pro vhodné $q \in \mathbb{R}$. Geometrická posloupnost leží v prostoru $\mathbf{V}$ právě když platí $q^{n+2} = q^n + q^{n+1}$ pro každé $n \geq 2$, 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

$$\mathbf{p}_1 = (1, \varphi, \varphi^2, \varphi^3, \dots), \quad \mathbf{p}_2 = (1, (1-\varphi), (1-\varphi)^2, (1-\varphi)^3, \dots) \ ,$$

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

Ukážeme, že uspořádaná dvojice posloupností $(\mathbf{p}_1, \mathbf{p}_2)$ je báze ve $\mathbf{V}$. Použijeme podmínku 3. z tvrzení 5.37. Platí-li pro nějaká dvě čísla $s, t \in \mathbb{R}$ rovnost

$$s\mathbf{p}_1 + t\mathbf{p}_2 = (0, 0, 0, \dots) \ ,$$

porovnáme první dva prvky v posloupnostech na obou stranách. Musí platit rovnosti

$$\begin{aligned} s\,1 + t\,1 &= 0 \\ s\varphi + t(1-\varphi) &= 0 \ . \end{aligned}$$

Čísla s, t jsou tedy řešením homogenní soustavy lineárních rovnic s maticí

$$\begin{pmatrix} 1 & 1 \\ \varphi & 1-\varphi \end{pmatrix} \sim \begin{pmatrix} 1 & 1 \\ 0 & 1-2\varphi \end{pmatrix} \sim \begin{pmatrix} 1 & 1 \\ 0 & -\sqrt{5} \end{pmatrix} \ .$$

Matice soustavy je regulární a jediným řešením soustavy jsou proto čísla $s = t = 0$. Podle tvrzení 5.37 je posloupnost $(\mathbf{p}_1, \mathbf{p}_2)$ lineárně nezávislá ve $\mathbf{V}$.

Dokážeme, že také LO $\{\mathbf{p}_1, \mathbf{p}_2\} = \mathbf{V}$. Je-li $\mathbf{a} = (a_0, a_1, a_2, \dots) \in \mathbf{V}$, pak soustava

$$\begin{aligned} s\,1 + t\,1 &= a_0 \\ s\varphi + t(1-\varphi) &= a_1 \end{aligned}$$

má regulární matici a tudíž právě jedno řešení $(s, t)^T$. Protože je posloupnost $\mathbf{a}$ určená stejně jako každý jiný prvek prostoru $\mathbf{V}$ prvními dvěma prvky, musí platit rovnost $s\mathbf{p}_1 + t\mathbf{p}_2 = \mathbf{a}$.

Pro vyjádření Fibonacciho posloupnosti $\mathbf{a} = (0, 1, 1, 2, \dots) \in \mathbf{V}$ jako lineární kombinaci posloupností $\mathbf{p}_1$ a $\mathbf{p}_2$ stačí najít koeficienty s, t jako řešení soustavy

$$\begin{aligned} s\,1 + t\,1 &= 0 \\ s\varphi + t(1-\varphi) &= 1 \ . \end{aligned}$$

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 4.42.

Jak tento vzorec nalézt bez záblesku geniality je vysvětleno v kapitole o vlastních číslech. ▲

5.4.1. Steinitzova věta o výměně a důsledky, dimenze. Z vizuální představy prostorů $\mathbb{R}^2$ je patrné, že všechny báze $\mathbb{R}^2$ 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 vektorový prostor má bázi a všechny báze mají stejný počet prvků. Tomuto počtu říkáme dimenze. Tyto zásadní skutečnosti v této části dokážeme pro konečně generované prostory.

Definice 5.55. Vektorový prostor se nazývá *konečně generovaný*, pokud má nějakou konečnou množinu generátorů.

Jedna možnost, jak se můžeme pokusit hledat bázi vektorového prostoru, je vzít nějakou posloupnost generátorů a vynechávat 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 5.56. *Minimální posloupnost generátorů* $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ *vektorového prostoru* $\mathbf{V}$ *je báze* $\mathbf{V}$.

Důkaz. Podle poznámek za definicí 5.35 je posloupnost lineárně závislá právě tehdy, když

$$\mathrm{LO}\,\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\} = \mathrm{LO}\,\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n\}$$

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 5.57. *Z každé konečné množiny generátorů vektorového 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 5.58. *Každý konečně generovaný vektorový prostor má bázi.*

Příklad 5.59. Podíváme se znovu na příklad prostoru $\mathbf{V} = \mathrm{LO}\,X \leq \mathbb{R}^3$, 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 5.36). 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 5.56, 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 5.60 (Steinitzova věta o výměně). *Nechť $N = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ je lineárně nezávislá posloupnost prvků vektorového prostoru $\mathbf{V}$ nad $\mathbf{T}$. Nechť G je konečná množina generátorů prostoru $\mathbf{V}$, označme $l = |G|$. Pak*

(1) *$l \geq k$,*
(2) *existují vektory $\mathbf{w}_1, \ldots, \mathbf{w}_{l-k} \in G$ takové, že množina*

$$\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k, \mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_{l-k}\}$$

generuje $\mathbf{V}$.

Důkaz. Dokážeme indukcí podle k. Pro $k = 0$ vybereme celou množinu G.

V indukčním kroku aplikujme indukční předpoklad na lineárně nezávislou posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{k-1})$. Pak $l \geq k-1$ a existují vektory $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_{l-k+1} \in G$ takové, že množina

$$M = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{k-1}, \mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_{l-k+1})$$

generuje $\mathbf{V}$. Zbývá do M umístit prvek $\mathbf{v}_k$ výměnou za některý z prvků $\mathbf{w}_1, \ldots, \mathbf{w}_{l-k+1}$. Protože M generuje $\mathbf{V}$, prvek $\mathbf{v}_k$ lze napsat jako lineární kombinace prvků z M:

$$\mathbf{v}_k = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_{k-1}\mathbf{v}_{k-1} + b_1\mathbf{w}_1 + b_2\mathbf{w}_2 + \cdots + b_{l-k+1}\mathbf{w}_{l-k+1}.$$

Posloupnost N je lineárně nezávislá, proto $\mathbf{v}_k$ není lineární kombinací vektorů $\mathbf{v}_1, \ldots, \mathbf{v}_{k-1}$. Z toho plyne $l \geq k$ a navíc alespoň jeden z prvků $b_1, \ldots, b_{l-k+1}$ je nenulový, označme jej b_s. Ukážeme, že

$$M' = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k, \mathbf{w}_1, \ldots, \mathbf{w}_{s-1}, \mathbf{w}_{s+1}, \ldots, \mathbf{w}_{l-k+1}\}$$

generuje $\mathbf{V}$. Prvek $\mathbf{w}_s$ je lineární kombinací prvků M' (z rovnosti výše vyjádříme $b_s\mathbf{w}_s$ a vynásobíme b_s^{-1}), takže $V = \mathrm{LO}\{M\} \subseteq \mathrm{LO}\{M'\}$, a tedy $\mathrm{LO}\{M'\} = V$. ▲

Nejdůležitější důsledek Steinitzovy věty je, že všechny báze obsahují stejný počet prvků. To umožňuje dát přesný význam slovu dimenze.

Důsledek 5.61. *Každé dvě báze konečně generovaného vektorového prostoru mají stejný počet prvků.*

Důkaz. Předpokládejme, že $B = (\mathbf{v}_1, \ldots, \mathbf{v}_k)$ a $C = (\mathbf{w}_1, \ldots, \mathbf{w}_l)$ jsou dvě báze vektorového prostoru $\mathbf{V}$. Protože posloupnost B je lineárně nezávislá a posloupnost C generuje $\mathbf{V}$, platí podle Steinitzovy věty $k \leq l$. Z téže věty plyne také $l \leq k$, protože C je lineárně nezávislá a B generuje $\mathbf{V}$. Dohromady dostáváme $k = l$. ▲

Definice 5.62. *Dimenzí* konečně generovaného vektorového prostoru $\mathbf{V}$ nad $\mathbf{T}$ rozumíme počet prvků jeho libovolné báze. Dimenzi prostoru $\mathbf{V}$ značíme $\dim(\mathbf{V})$.

Příklad 5.63. 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 $\mathrm{LO}\left\{(1,1,1)^T\right\} \leq \mathbb{R}^3$ má dimenzi 1, protože $((1,1,1)^T)$ je jeho bází. To odpovídá geometrické představě, že daný prostor je přímkou.

Dimenze prostoru

$$\mathbf{V} = \mathrm{LO}\left\{\begin{pmatrix}2\\1\\3\\0\end{pmatrix}, \begin{pmatrix}1\\4\\5\\0\end{pmatrix}, \begin{pmatrix}6\\3\\1\\1\end{pmatrix}, \begin{pmatrix}1\\4\\6\\6\end{pmatrix}, \begin{pmatrix}3\\5\\2\\3\end{pmatrix}\right\} \leq \mathbb{Z}_7^4$$

je 3, protože v příkladu 5.53 jsme nalezli tříprvkovou bázi.

Zdůvodnění následujících tvrzení přenecháme do cvičení.

- Dimenze prostoru všech matic nad $\mathbf{T}$ typu $m \times n$ je mn.
- Dimenze prostoru reálných polynomů stupně nejvýše n je $n + 1$.
- Dimenze prostoru $\mathbb{C}$ jako vektorového prostoru nad $\mathbb{R}$ je 2.

▲

V důsledku 5.57 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 5.64. *Nechť G je konečná množina generátorů vektorového 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 5.57 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 5.57 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 5.65. *Maximální lineárně nezávislá posloupnost v konečně generovaném prostoru je bází.*

Obecněji, maximální lineárně nezávislá posloupnost prvků konečné množiny generátorů je bází.

Příklad 5.66. V příkladu 5.53 jsme hledali nějakou bázi prostoru

$$\mathbf{V} = \mathrm{LO}\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5\} = \mathrm{LO}\left\{\begin{pmatrix}2\\1\\3\\0\end{pmatrix}, \begin{pmatrix}1\\4\\5\\0\end{pmatrix}, \begin{pmatrix}6\\3\\1\\1\end{pmatrix}, \begin{pmatrix}1\\4\\6\\6\end{pmatrix}, \begin{pmatrix}3\\5\\2\\3\end{pmatrix}\right\} \leq \mathbb{Z}_7^4 \ .$$

Teď z vektorů $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_5$ bázi $\mathbf{V}$ vybereme. Z důsledku 5.57 plyne, že to jde. Předchozí důsledek 5.64 nám dává návod, jak to jde udělat. Stačí totiž vzít libovolnou maximální lineárně nezávislou podmnožinu $\{\mathbf{v}_1, \ldots, \mathbf{v}_5\}$ a uspořádat libovolně do posloupnosti. 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 5.67. *V každém vektorovém 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 5.68. V příkladu 5.40 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 5.69. *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 $\mathbf{W}$, existuje prvek $\mathbf{w}_2 \in W$ takový, že $\mathbf{w}_2 \notin \mathrm{LO}\{\mathbf{w}_1\}$, 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 tvrzení 5.37 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 5.58. 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 5.70. Podle tvrzení mají podprostory $\mathbb{R}^3$ dimenzi 0 (triviální podprostor $\{\mathbf{o}\}$), 1 (podprostory tvaru $\mathrm{LO}\{\mathbf{u}\}$, kde $\mathbf{u}$ je nenulový vektor, tedy přímky procházející počátkem), 2 (podprostory tvaru $\mathrm{LO}\{\mathbf{u}, \mathbf{v}\}$, 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. ▲

5.4.2. Báze jako souřadnicový systém. Vraťme se teď k pozorování 5.48, které říká, že máme-li bázi $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ prostoru $\mathbf{V}$, pak každý vektor $\mathbf{v} \in V$ lze jednoznačným způsobem vyjádřit jako lineární kombinaci vektorů $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Koeficientům této lineární kombinace říkáme souřadnice $\mathbf{v}$ vzhledem k B.

DEFINICE 5.71. Nechť $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ je báze vektorového prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ a $\mathbf{w} \in V$. *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.

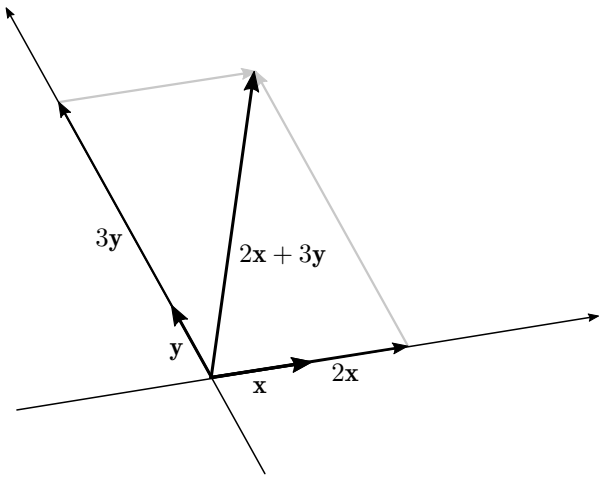
$$[\mathbf{w}]_B = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \ .$$

PŘÍKLAD 5.72. 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 $\mathbf{u}, \mathbf{v}$“.

▲

Souřadnice závisí na pořadí prvků v bázi. Z tohoto důvodu jsme bázi definovali jako posloupnost prvků vektorového 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.



Obrázek 5.4. Lineární kombinace $2\mathbf{x} + 3\mathbf{y}$ (k příkladu 5.72)

Příklad 5.73. V příkladu 5.50 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 $\mathbf{V} = \mathrm{LO}\left\{(1,2,3)^T, (4,5,6)^T\right\} \leq \mathbb{R}^3$ je posloupnost $B = ((1,2,3)^T, (4,5,6)^T)$ (viz příklad 5.52). 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 5.74. 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 **??**.

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 vektorového prostoru a jejich souřadnicemi ve zvolené bázi je ještě těsnější, zachovává totiž operace vektorového 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 5.75. *Nechť $B = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ je báze vektorového prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$, nechť $\mathbf{u}, \mathbf{w} \in V$ a $t \in T$. Pak platí*

(1) $[\mathbf{u} + \mathbf{w}]_B = [\mathbf{u}]_B + [\mathbf{w}]_B$ *a*
(2) $[t\mathbf{u}]_B = t[\mathbf{u}]_B$

Na levých stranách vystupují operace v prostoru $\mathbf{V}$, na pravých stranách jsou operace v $\mathbf{T}^n$.

Důkaz. Je-li $[\mathbf{u}]_B = (a_1, a_2, \dots, a_n)^T$ a $[\mathbf{w}]_B = (b_1, b_2, \dots, b_n)^T$, pak podle definice souřadnic platí

$$\mathbf{u} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n, \quad \mathbf{w} = b_1\mathbf{v}_1 + b_2\mathbf{v}_2 + \cdots + b_n\mathbf{v}_n \ .$$

Sečtením a úpravou získáme

$$\mathbf{u} + \mathbf{w} = (a_1 + b_1)\mathbf{v}_1 + (a_2 + b_2)\mathbf{v}_2 + \cdots + (a_n + b_n)\mathbf{v}_n \ ,$$

což podle definice znamená $[\mathbf{u}+\mathbf{w}]_B = (a_1+b_1, a_2+b_2, \dots, a_n+b_n)^T = [\mathbf{u}]_B + [\mathbf{v}]_B$.

Druhá část tvrzení je rovněž snadné cvičení. ▲

Příklad 5.76. V prostoru $\mathbf{V} = \mathrm{LO}\{(1,2,3),(4,5,6)\} \leq \mathbb{R}^3$ uvažujme bázi $B = ((1,2,3)^T, (4,5,6)^T)$ a vektory $\mathbf{u}, \mathbf{w}$ se souřadnicemi $(1,2)^T$, $(3,-1)^T$ vzhledem k B:

$$\mathbf{u} = \begin{pmatrix} 9 \\ 12 \\ 15 \end{pmatrix}, [\mathbf{u}]_B = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \quad \mathbf{w} = \begin{pmatrix} -1 \\ 1 \\ 3 \end{pmatrix}, [\mathbf{w}]_B = \begin{pmatrix} 3 \\ -1 \end{pmatrix} .$$

Součtem $\mathbf{u}$ a $\mathbf{w}$ je vektor $(8,13,18)^T$, jeho souřadnice vzhledem k B jsou $(1,2)^T + (3,-1)^T = (4,1)^T$. Skutečně, $4 \cdot (1,2,3)^T + 1 \cdot (4,5,6)^T = (8,13,18)^T$. ▲

Teď již vidíme přesný význam hesla „všechny konečně generované vektorové prostory jsou v podstatě $\mathbf{T}^n$“. Zvolíme-li v prostoru bázi B, můžeme místo původních 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 5.77. *Nechť B je báze vektorového prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ dimenze n. Pak platí*

(1) *posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k)$ je lineárně nezávislá ve $\mathbf{V}$ právě tehdy, když je posloupnost $([\mathbf{v}_1]_B, [\mathbf{v}_2]_B, \dots, [\mathbf{v}_k]_B)$ lineárně nezávislá v $\mathbf{T}^n$;*
(2) *množina X generuje $\mathbf{V}$ právě tehdy, když $[X]_B$ generuje $\mathbf{T}^n$;*
(3) *posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k)$ je báze $\mathbf{V}$ právě tehdy, když je posloupnost $([\mathbf{v}_1]_B, [\mathbf{v}_2]_B, \dots, [\mathbf{v}_k]_B)$ báze $\mathbf{T}^n$.*

5.4.3. 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 vektorového prostoru.

Definice 5.78. Nechť $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ a C jsou báze vektorového 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 5.79. *Nechť $\mathbf{V}$ je vektorový prostor 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 $\mathbf{x} = a_1\mathbf{v}_1 + \dots + a_n\mathbf{v}_n$. Podle tvrzení 5.75 platí

$$\begin{aligned}[\mathbf{x}]_C &= [a_1\mathbf{v}_1 + \dots + a_n\mathbf{v}_n]_C = [a_1\mathbf{v}_1]_C + \dots + [a_n\mathbf{v}_n]_C \\ &= a_1[\mathbf{v}_1]_C + \dots + a_n[\mathbf{v}_n]_C = ([\mathbf{v}_1]_C|\dots|[\mathbf{v}_n]_C)(a_1, \dots, a_n)^T \\ &= [\mathrm{id}]_C^B[\mathbf{x}]_B \ .\end{aligned}$$

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 5.80. 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 5.81. Najdeme matici přechodu od báze B k bázi C prostoru $\mathbf{V} \leq \mathbb{R}^3$, kde

$$\mathbf{V} = \mathrm{LO}\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\}, \ B = \left(\begin{pmatrix} 2 \\ 4 \\ 4 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix} \right), \ C = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right) \ .$$

(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. Hodnost matice

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 $\mathrm{Im}\, A \leq \mathbf{T}^m$. 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 5.86). Výsledek samozřejmě formulujeme v jazyku matic.

Definice 5.82. 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

$$\mathbf{a}_i \notin \mathrm{LO}\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{i-1}\} \ .$$

Pojmenování ospravedlňuje skutečnost, že bázové sloupce tvoří bázi sloupcového prostoru matice. To si rozmyslete jako cvičení.

Pozorování 5.83. *Pro libovolnou matici A tvoří bázové sloupce bázi sloupcového prostoru. Speciálně, dimenze* $\mathrm{Im}\, A$ *je rovna počtu bázových sloupců.*

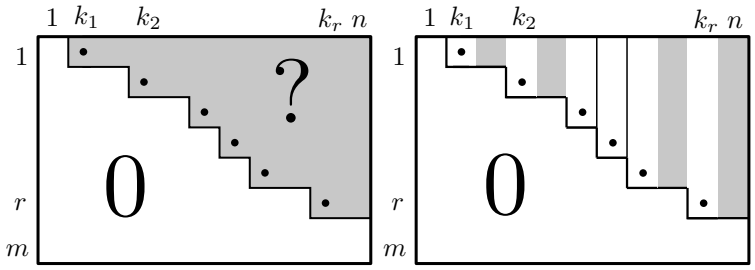
Příklad 5.84. V matici

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

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 5.85. *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 čísla z definice 2.14 odstupňovaného tvaru.*



Obrázek 5.5. Matice v odstupňovaném tvaru

Důkaz. Označme $A = (\mathbf{a}_1 | \ldots | \mathbf{a}_n)$. Pro libovolné $i = 1, 2, \ldots, r$ je sloupec k_i bázový, protože vektor $\mathbf{a}_{k_i}$ má i-tou složkou nenulovou, kdežto předchozí sloupcové vektory mají tuto složku nulovou. Vektor $\mathbf{a}_{k_i}$ tedy nemůže být lineární kombinací předchozích sloupcových vektorů.

Zbývá ukázat, že ostatní sloupce bázové nejsou. To je jistě pravda pro sloupce $1, 2, \ldots, k_1 - 1$, které jsou celé nulové. Uvažujme sloupec $l > k_1$ různý od k_2, k_3, ... Chceme ukázat, že $\mathbf{a}_l$ je lineární kombinací předchozích sloupcových vektorů, jinými slovy (opět sloupcový pohled!), že soustava lineárních rovnic $(\mathbf{a}_1 | \mathbf{a}_2 | \ldots | \mathbf{a}_{l-1})\mathbf{x} = \mathbf{a}_l$ má řešení. To je ale pravda, protože rozšířená matice této soustavy je v odstupňovaném tvaru a splňuje nutnou a postačující podmínku pro řešitelnost takové soustavy – neobsahuje řádek tvaru $(00 \cdots 0 | c)$, kde $c \neq 0$. ▲

Tvrzení 5.86. *Nechť A je matice nad tělesem $\mathbf{T}$ typu $m \times n$ a R je regulární matice řádu m. Pak pro libovolné $i \in \{1, 2, \ldots, n\}$ platí, že i-tý sloupec matice A je bázový právě tehdy, když je bázový i-tý sloupec matice RA.*

Důkaz. Tvrzení je důsledkem definice a pozorování, že matice A má stejné lineární závislosti mezi sloupci jako matice RA (toho jsme si všimli v poznámce za tvrzením 5.41). Obšírněji, i-tý sloupec matice $A = (\mathbf{a}_1 | \ldots | \mathbf{a}_n)$ není bázový právě tehdy, když je lineární kombinací předchozích sloupců, tj. $\mathbf{a}_i = t_1\mathbf{a}_1 + \cdots + t_{i-1}\mathbf{a}_{i-1}$ pro nějaké prvky $t_1, \ldots, t_{i-1} \in T$. Upravený vztah $-t_1\mathbf{a}_1 - \ldots - t_{i-1}\mathbf{a}_{i-1} + \mathbf{a}_i = \mathbf{o}$ lze maticově zapsat $A(-t_1, \ldots, -t_{i-1}, 1, 0, \ldots, 0)^T = \mathbf{o}$. Vynásobením maticí R zleva dostáváme $RA(-t_1, \ldots, -t_{i-1}, 1, 0, 0, \ldots, 0)^T = \mathbf{o}$, z čehož plyne, že i-tý sloupec matice RA je lineární kombinací předchozích.

Druhá implikace se dokáže podobně, například vynásobením poslední rovnosti zleva maticí R^{-1}.) ▲

Příklad 5.87. 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 5.88. *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 5.83), tyto dimenze jsou stejné (viz tvrzení 5.86) a rovnají se počtu nenulových řádků matice RA (viz tvrzení 5.85).

Dimenze řádkového prostoru matice RA je také rovna počtu nenulových řádků, protože nenulové řádky tvoří lineárně nezávislou posloupnost (viz tvrzení 5.43), která zřejmě generuje řádkový prostor. Ale násobení regulární maticí zleva nemění lineární obal řádků (viz tvrzení 5.33), speciálně, dimenze řádkového prostoru matice RA je stejná jako dimenze řádkového prostoru matice A. ▲

Definice 5.89. *Hodností* matice A rozumíme dimenzi řádkového (sloupcového) prostoru matice A. Značíme $\operatorname{rank}(A)$.

Shrneme některé důležité triviální důsledky do pozorování.

Pozorování 5.90. *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 5.91. V závislosti na $a, b \in \mathbb{Z}_3$ určíme dimenzi prostoru

$$\mathbf{V}_{a,b} = \mathrm{LO}\left\{ \begin{pmatrix} a \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ b \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} \right\} \leq \mathbb{Z}_3^3 \ ,$$

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 třeba 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 jsme 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 oboru hodnot příslušného zobrazení f_A. Máme-li ještě matici B, aby byl definován součin AB, pak hodnost AB je rovná dimenzi oboru hodnot zobrazení f_{AB}. Ale obor hodnot zobrazení $f_{AB} = f_A \circ f_B$ je podprostorem oboru hodnot zobrazení f_A, takže hodnost AB je menší nebo rovna hodnosti A. Tuto nerovnost a obdobnou nerovnost pro násobení zleva dokážeme algebraicky.

Tvrzení 5.92. *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. Podle sloupcové definice součinu je každý sloupec matice AB lineární kombinací sloupců matice A. Z toho plyne $\operatorname{Im}(AB) \leq \operatorname{Im}(A)$, takže $\operatorname{rank}(AB) \leq \operatorname{rank}(A)$ podle tvrzení 5.69 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 5.93. *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 4.82. 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 5.69 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 5.94. *Nechť A je čtvercová matice nad $\mathbf{T}$ řádu n. Následující tvrzení jsou ekvivalentní.*

(1) *A je regulární.*
(2) $\operatorname{rank}(A) = n$.
(3) *Posloupnost sloupců (řádků) matice A je lineárně nezávislá.*
(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 5.67.

PŘÍKLAD 5.95. 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 $b_{kk} = 1$ a $b_{kl} = 0$ 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 5.92 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 $r \geq 1$ 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 5.97 ukážeme, že v tomto případě tvoří matici C nenulové řádky tzv. redukovaného odstupňovaného tvaru matice A.

DEFINICE 5.96. 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 Gaussovou eliminací převedeme do odstupňovaného tvaru.
(2) Vynásobíme nenulové řádky tak, aby byl každý pivot roven 1.
(3) Postupně (nejlépe od konce) vynulujeme zbylé prvky v každém bázovém sloupci.

Tomuto procesu se říká Gaussova-Jordanova eliminace. Vzniklé matici říkáme *redukovaný odstupňovaný tvar* matice A.

Přejdeme ke slíbenému tvrzení o skeletním rozkladu pomocí redukovaného odstupňovaného tvaru.

TVRZENÍ 5.97. *Libovolná matice A typu $m \times n$ nad $\mathbf{T}$ s hodností $r \geq 1$ 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 2.14, $B = (\mathbf{a}_{k_1} | \dots | \mathbf{a}_{k_r})$ a navíc platí $\mathbf{d}_{k_i} = \mathbf{e}_i$ pro každé $1 \le i \le r$, tedy také $\mathbf{c}_{k_i} = \mathbf{e}_i$ (v tomto výrazu má $\mathbf{e}_i$ jiný počet složek než v přechozím).

Vztah $A = BC$ plyne z toho, že A a RA mají stejné lineární závislosti mezi sloupci. Důkaz provedeme podrobněji.

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 $j \ge k_i$. 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

$$B\mathbf{c}_j = B(t_1, \dots, t_i, 0, \dots, 0)^T = t_1 \mathbf{a}_{k_1} + \dots + t_i \mathbf{a}_{k_i} = \mathbf{a}_j \ .$$

▲

Jako cvičení dokažte, že redukovaný odstupňovaný tvar je 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. Opět lze argumentovat lineárními závislostmi mezi sloupci.

5.5.4. Ještě jednou soustavy rovnic, dimenze jádra a obrazu. Nyní si zopakujeme různé pohledy na řešení soustav lineárních rovnic a formulujeme již známé skutečnosti o existenci a tvaru řešení pomocí pojmů zavedených v této kapitole.

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 $(A|\mathbf{b})$, určuje jednu „nadrovinu“).
(2) Hledání koeficientů lineárních kombinací sloupců matice A, jejímž výsledkem je $\mathbf{b}$.
(3) Určování úplného vzoru vektoru $\mathbf{b}$ při zobrazení f_A.

Pomocí pojmu hodnost můžeme formulovat kritérium řešitelnosti.

Věta 5.98 (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 $\operatorname{Im} A \le \operatorname{Im}(A \mid \mathbf{b})$, vidíme, že podprostory jsou rovny právě tehdy, když se rovnají jejich dimenze (viz tvrzení 5.69). ▲

Prakticky, hodnosti vidíme z odstupňovaného tvaru 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 $(0, 0, \dots, 0, a)$, $a \ne 0$ v odstupňovaném tvaru).

Tvar řešení je určený řešením příslušné homogenní soustavy: je-li $\mathbf{u}$ libovolné řešení, pak množina všech řešení dané soustavy je podle věty 4.97 rovná

$$\mathbf{u} + \operatorname{Ker} A \ .$$

Řešením je tedy vždy posunutí podprostoru $\operatorname{Ker} A$ o nějaký vektor.

Jádro matice A jsme nejprve popisovali ve tvaru

$$\left\{ \sum_{p \in P} t_p \mathbf{v}_p : \ t_p \in T \ \text{ pro každé } \ p \in P \right\}$$

a nyní píšeme stručněji

$$\mathrm{LO}\,\{\mathbf{v}_p : p \in P\} \quad ,$$

kde P jsou indexy nebázových sloupců – volných proměnných. Ze způsobu nalezení vektorů $\mathbf{v}_p$ (připomenutého v důkazu následující věty) se snadno ukáže, že tyto vektory tvoří bázi prostoru $\operatorname{Ker} A$. Protože počet volných proměnných je $n - \operatorname{rank}(A)$, dostáváme:

Věta 5.99 (Věta o dimenzi jádra a obrazu). *Pro libovolnou matici A nad $\mathbf{T}$ typu $m \times n$ platí*

$$\dim(\operatorname{Ker} A) + \dim(\operatorname{Im} A) = n \quad (= \dim(\operatorname{Ker} A) + \operatorname{rank}(A) \ ) \ .$$

Důkaz. Nechť $r = \operatorname{rank}(A)$ a označme $P = \{j_1, \dots, j_{n-r}\}$, $j_1 < j_2 < \dots < j_{n-r}$ nebázové sloupce matice A (příslušné proměnné nazýváme volné). Připomeňme, že každý prvek $\mathbf{x} = (x_1, \dots, x_n)^T \in \operatorname{Ker} A$ (neboli každé řešení homogenní soustavy $A\mathbf{x} = \mathbf{o}$) je jednoznačně určen vektorem $(x_{j_1}, x_{j_2}, \dots, x_{j_{n-r}})^T \in T^{n-r}$ a naopak, libovolný vektor v T^{n-r} určuje jedno řešení. Toto jsme nahlédli v pozorování 2.19 použitím odstupňovaného tvaru, můžeme to ale dokázat přímo z definice bázových sloupců (viz cvičení).

Zvolíme libovolnou bázi $U = (\mathbf{u}_{j_1}, \dots, \mathbf{u}_{j_{n-r}})$ prostoru $\mathbf{T}^{n-r}$ a najdeme (jednoznačně určené) vektory $\mathbf{v}_p \in \operatorname{Ker} A$ tak, že pro každé $p \in P$ a $k \in \{1, \dots, n-r\}$ je j_k-tá složka vektoru $\mathbf{v}_p$ rovná k-té složce vektoru $\mathbf{u}_p$. Podle připomenutí z předchozího odstavce je $(\mathbf{v}_{j_1}, \dots, \mathbf{v}_{j_{n-r}})$ báze prostoru $\operatorname{Ker} A$: je lineárně nezávislá (protože U je lineárně nezávislá) a generuje $\operatorname{Ker} A$ (protože U generuje $\mathbf{T}^{n-r}$). Poznamenejme, že v diskuzi v oddílu 4.5.1 jsme při výpočtu $\mathbf{v}_p$ volili vždy jednu volnou proměnnou rovnou 1 a zbylé rovné 0. Za U jsme tedy volili kanonickou bázi prostoru $\mathbf{T}^{n-r}$.

V prostoru $\operatorname{Ker} A$ jsme nalezli $(n-r)$–prvkovou bázi, máme tedy

$$\dim(\operatorname{Ker} A) + \dim(\operatorname{Im} A) = (n-r) + r = n \ .$$

▲

Důkaz věty zároveň odpovídá na poslední otázku, která v oddílu 4.5.1 zůstala otevřená: je nutné při výpočtu vektorů $\mathbf{v}_p$ volit za volné proměnné prvky kanonické báze $\mathbf{T}^{n-r}$? Odpověď je ne, můžeme zvolit prvky libovolné báze $\mathbf{T}^{n-r}$.

Příklad 5.100. Vrátíme se k soustavě z oddílu 2.3.4 a příkladu 4.94.

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

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 4.94 jsme zvolili nulový vektor a dostali jsme vektor $(-1, 0, -3, 0, 0)^T$. Bázi $\operatorname{Ker} A$ získáme dopočítáním z nějaké báze U prostoru $\mathbb{R}^3$. V 4.94 jsme volili kanonickou bázi $\mathbb{R}^3$ 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

$$\begin{pmatrix} -1 \\ 0 \\ -3 \\ 0 \\ 0 \end{pmatrix} + \mathrm{LO}\left\{ \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -3 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ 0 \\ -2 \\ 0 \\ 1 \end{pmatrix} \right\} .$$

Jiné partikulární řešení je například $(-8,1,-5,1,1)^T)$ získáné volbou jedniček za parametry. Jinou bázi $\operatorname{Ker} A$ můžeme dostat například volbou následující báze prostoru $\mathbb{R}^3$.

$$U = ((1,1,1)^T, (0,1,1)^T, (0,0,2)^T)$$

Dopočtením prvků v posloupnosti

$$((?,1,?,1,1)^T, (?,0,?,1,1)^T, (?,0,?,0,2)^T)$$

získáme následující bázi prostoru $\operatorname{Ker} A$.

$$((-7,1,-2,1,1)^T, (-5,0,-2,1,1)^T, (-4,0,-4,0,2)^T) \ .$$

Množina všech řešení dané soustavy je tedy také rovná

$$\begin{pmatrix} -8 \\ 1 \\ -5 \\ 1 \\ 1 \end{pmatrix} + \mathrm{LO}\left\{ \begin{pmatrix} -7 \\ 1 \\ -2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} -5 \\ 0 \\ -2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} -4 \\ 0 \\ -4 \\ 0 \\ 2 \end{pmatrix} \right\} .$$

▲

Věta o dimenzi jádra a obrazu a věta 5.88 o rovnosti dimenzí sloupcového a řádkového prostoru ukazují, že dimenze čtyř základních prostorů určených maticí (prostorů $\operatorname{Im} A$, $\operatorname{Im} A^T$, $\operatorname{Ker} A$, $\operatorname{Ker} A^T$) jsou dohromady těsně svázány. Každá z těchto dimenzí určuje zbývající tři.

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 4.14), 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 5.101. *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 5.13). 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 součtem.

Definice 5.102. 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.

$$\sum_{i\in I} V_i = \mathrm{LO} \bigcup_{i\in I} V_i \ .$$

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 5.103 (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 5.69). 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 5.58). 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 5.64). 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 (viz cvičení 23). Zbývá ukázat, že E je lineárně nezávislá. Předpokládejme, že

$$\sum_{i=1}^{k} a_i \mathbf{w}_i + \sum_{i=1}^{l} b_i \mathbf{u}_i + \sum_{i=1}^{m} c_i \mathbf{v}_i = \mathbf{o} \ .$$

Chceme dokázat, že všechny koeficienty jsou nutně nulové. Vztah drobně upravíme.

$$\sum_{i=1}^{l} b_i \mathbf{u}_i = -\sum_{i=1}^{m} c_i \mathbf{v}_i - \sum_{i=1}^{k} a_i \mathbf{w}_i$$

Vektor $\mathbf{u} = \sum_{i=1}^{l} b_i \mathbf{u}_i$ leží v prostoru $\mathbf{U}$ a také leží, podle odvozeného vztahu, v lineárním obalu vektorů $\mathbf{v}_1, \ldots, \mathbf{v}_m, \mathbf{w}_1, \ldots, \mathbf{w}_k$, čili v prostoru $\mathbf{V}$. Vektor $\mathbf{u}$ tedy leží v průniku $\mathbf{U} \cap \mathbf{V}$ a proto jej lze vyjádřit jako lineární kombinaci vektorů $\mathbf{w}_1, \ldots, \mathbf{w}_k$ báze B.

$$\mathbf{u} = \sum_{i=1}^{k} d_i \mathbf{w}_i$$

Z toho získáme následující vyjádření $\mathbf{o}$ jako lineární kombinaci prvků C:

$$\mathbf{o} = \sum_{i=1}^{k} d_i \mathbf{w}_i - \sum_{i=1}^{l} b_i \mathbf{u}_i \ ,$$

takže $b_1 = b_2 = \cdots = b_l = d_1 = d_2 = \cdots = d_k = 0$, protože C je lineárně nezávislá..

Podobně bychom dokázali, že koeficienty c_1, c_2, ..., c_m jsou rovněž všechny nulové. Nyní ale $a_1 = a_2 = \cdots = a_k = 0$, protože B je lineárně nezávislá. ▲

Věta se geometricky dobře představí, když si ze vztahu vyjádříme dimenzi součtu podprostorů jako součet dimenzí jednotlivých prostorů minus dimenze společné části (průniku). Věta se může hodit třeba při určování dimenze průniku, protože dimenze prostorů a jejich součtu nebývá problém spočítat.

Příklad 5.104. Určíme dimenzi průniku podprostorů $\mathbf{U}, \mathbf{V} \leq \mathbb{Z}_5^4$.

$$U = \mathrm{LO}\left\{\begin{pmatrix}2\\1\\0\\3\end{pmatrix}, \begin{pmatrix}3\\4\\2\\1\end{pmatrix}, \begin{pmatrix}3\\4\\3\\3\end{pmatrix}\right\}, \quad V = \mathrm{LO}\left\{\begin{pmatrix}2\\3\\4\\1\end{pmatrix}, \begin{pmatrix}4\\4\\0\\1\end{pmatrix}\right\}$$

Dimenze $\mathbf{U}$ a $\mathbf{V}$ 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 5.105. 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 5.69 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 5.106. 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 5.107. *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 $\mathbf{V} = \mathbf{V}_1 \oplus \mathbf{V}_2 \oplus \cdots \oplus \mathbf{V}_k$. Pak $\mathbf{V}$ je součtem podprostorů $\mathbf{V}_1$, $\mathbf{V}_2$, ..., $\mathbf{V}_k$, takže každý vektor $\mathbf{v} \in V$ lze zapsat ve tvaru $\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2 + \cdots + \mathbf{v}_k$, kde $\mathbf{v}_i \in \mathbf{V}_i$ 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 $\mathbf{v}_i - \mathbf{v}'_i = \mathbf{o}$, čili $\mathbf{v}_i = \mathbf{v}'_i$.

Předpokládejme naopak, že platí podmínka (2). Pak z existence vyjádření každého vektoru jako součtu vektorů z $V_1, \ldots, V_k$ plyne $\mathbf{V} = \mathbf{V}_1 + \mathbf{V}_2 + \cdots + \mathbf{V}_k$.

Zbývá tedy dokázat, že $\mathbf{V}_i \cap (\mathbf{V}_1 + \mathbf{V}_2 + \cdots + \mathbf{V}_{i-1} + \mathbf{V}_{i+1} + \mathbf{V}_{i+2} + \cdots + \mathbf{V}_k) = \{\mathbf{o}\}$ pro libovolné $i \in \{1, 2, \ldots, k\}$. Pro spor předpokládejme, že pro nějaké i existuje nenulový vektor $\mathbf{u}$ v průniku $\mathbf{V}_i$ a $\sum_{j \neq i} \mathbf{V}_j$. Ze druhé podmínky dostaneme, že existují vektory $\mathbf{v}_1 \in V_1$, $\mathbf{v}_2 \in V_2$, ..., $\mathbf{v}_{i-1} \in V_{i-1}$, $\mathbf{v}_{i+1} \in V_{i+1}$,..., $\mathbf{v}_k \in V_k$ takové, že platí

$$\mathbf{u} = \mathbf{v}_1 + \mathbf{v}_2 + \cdots + \mathbf{v}_{i-1} + \mathbf{v}_{i+1} + \cdots + \mathbf{v}_k$$

Vektoru $\mathbf{u}$ má tedy dvě vyjádření pomocí součtu vektorů z prostorů $V_1, \ldots, V_k$:

$$\begin{array}{lllllllllllllllll}
\mathbf{u} & = \mathbf{v}_1 & + & \mathbf{v}_2 & + & \cdots & + & \mathbf{v}_{i-1} & + & \mathbf{o} & + & \mathbf{v}_{i+1} & + & \cdots & + & \mathbf{v}_k \\
\mathbf{u} & = \mathbf{o} & + & \mathbf{o} & + & \cdots & + & \mathbf{o} & + & \mathbf{u} & + & \mathbf{o} & + & \cdots & + & \mathbf{o}.
\end{array}$$

Protože $\mathbf{u} \neq \mathbf{o}$, jsou tato dvě vyjádření různá, což je spor s jednoznačností z (2). ▲

Direktní součet lze chápat jako rozklad podprostoru na vzájemně nezávislé části. Všimněte si, že $\mathbf{V}$ je direktním součtem jednodimenzionálních podprostorů $\mathbf{V} = \mathrm{LO}\{\mathbf{v}_1\} \oplus \mathrm{LO}\{\mathbf{v}_2\} \oplus \cdots \oplus \mathrm{LO}\{\mathbf{v}_k\}$ 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 5.35 a 5.47). 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 5.37 charakterizující lineární nezávislost.
- Pozorování 5.48, 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 5.75 o souřadnicích a operacích i obdoba pozorování 5.77 o zachovávání důležitých vlastností jako lineární nezávislost platí.
- Minimální soubor generátorů je vždy báze (obdoba tvrzení 5.56). Obdoba důsledku 5.57, 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 5.58).
- Všechny báze mají stejnou mohutnost (obdoba důsledku 5.61), takže má smysl zavést dimenzi jako mohutnost libovolné báze. Rovněž platí obdoba důsledku 5.64, že libovolný lineárně nezávislý soubor lze doplnit do báze vektory z libovolné množiny generátorů. Z toho plyne obdoba důsledku 5.65, že maximální lineárně nezávislý soubor je báze.
- Obdoba tvrzení 5.69 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 $0, 1, \dots, 9$. 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

$$G = 00,\ C = 01,\ T = 10,\ A = 11.$$

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 5.108. *Binární blokový kód* délky n je libovolná podmnožina C aritmetického vektorového prostoru $\mathbb{Z}_2^n$. Prvkům C říkáme *slova* nebo také *bloky* kódu C. *Zprávou* v kódu C potom rozumíme posloupnost slov kódu C.

Tak například, je-li $C = \{000, 001, 010, 001, 110, 111\}$ kód délky 3, pak posloupnost

$$000\ 111\ 110\ 010\ 001$$

je zpráva v tomto kódu. Mezery mezi jednotlivými slovy kódu děláme pro pohodlí. Také vynecháváme závorky při zápisu vektorů a čárky mezi jejich složkami, jak je v teroii kódování běžné. Stejná délka jednotlivých bloků v binárním kódu umožňuje jednoznačně interpretovat tutéž zprávu zapsanou bez mezer

$$000111110010001.$$

Zprávu zapsanou v jakékoliv abecedě s konečným počtem symbolů můžeme jednoznačně zakódovat pomocí bloků binárního kódu vhodné délky n. Stačí pouze, aby bylo číslo 2^n aspoň tak velké jako počet znaků v původní abecedě.

V této "digitalizované"podobě můžeme zprávu přenést nějakým *komunikačním kanálem*. Pokud je kanál bez jakéhokoliv šumu, neni žádné nebezpečí, že přijímající strana přijme zprávu v jiné podobě, než v jaké byla vyslána. Takové kanály ale v reálném světě neexistují, vždy je nenulová pravděpodobnost, že některá z cifer 0 nebo 1 se během přenosu změní na opačnou. Pro kanály se šumem nejsou blokové kódy typu $C = \mathbb{Z}_2^n$ vhodné. Skutečnost, že každý blok z n cifer 0 nebo 1 je kódovým slovem, znamená že přijímající strana nemá možnost poznat, že během přenosu zprávy byl nějaký blok pozměněn. Každý přijatý blok mohl být také vyslán.

Řešením je nepoužívat jako kódová slova všechny bloky dané délky n, ale pouze některé. Pokud jsou kódová slova dobře vybrána, může přijímající strana poznat, že během přenosu bloku zprávy došlo k nějaké chybě díky tomu, že přijme posloupnost délky n, která není kódovým slovem. Takový blok vysílající strana nemohla vyslat. Daní, kterou je nutné za to zaplatit, je snížení *rychlosti přenosu informace*, množství informace, kterou kanálem přeneseme za jednotku času. Do kódu vnášíme *nadbytečnost*, cizím slovem *redundanci* - pro přenášení informace používáme více symbolů, než kolik je potřeba. nadbytečnost ale umožňuje odhalovat a opravovat chyby při přenosu dat.

Nejjednodušší způsob jak bojovat se šumem, je vyslat každý blok dvakrát po sobě. Příkladem takového *opakovacího kódu* je následující kód délky 4:

$$C = \{0000, 0101, 1010, 1111\}.$$

Každé slovo má dvě části. První dva symboly jsou *informační symboly*, zbylé dva jsou *kontrolní symboly*. Kontrolní symboly nenesou žádnou informaci, pouze opakují předchozí dva symboly. Z každých čtyř symbolů vyslaného slova pouze první dva nesou informaci. Rychlost přenosu informace pomocí takového kódu je poloviční oproti rychlosti přenosu informace kódem $D = \{00, 01, 10, 11\}$.

Narozdíl od kódu D ale kód C umožňuje přijímající straně poznat, pokud během přenosu slova došlo k jedné chybě. První a druhá polovina přijatého čtyřprvkového bloku se v takovém případě liší. Říkáme, že kód C *odhalí jednu chybu*.

V opakovacím kódu můžeme počáteční informační část opakovat vícekrát. Kód

$$\{000, 111\} \subseteq \mathbb{Z}_2^3$$

obsahuje pouze dva bloky, v každém z nich se první symbol opakuje třikrát. Je to příklad *3-opakovacího kódu*. Jiným příkladem 3-opakovacího kódu je

$$\{000000, 010101, 101010, 111111\} \subseteq \mathbb{Z}_2^6,$$

ve kterém opakujeme třikrát vždy první dva informační symboly. Rychlost přenosu informace kterýmkoliv z těchto dvou kódů je $1/3$. V každém bloku je pouze jedna třetina symbolů informačních, zbylé dvě třetiny jsou kontrolní.

Každý 3-opakovací kód odhalí jednu chybu – změníme-li v libovolném bloku jeden symbol, dostaneme slovo, které do kódu nepatří. Oproti prostému opakovacímu kódu ale dokáže navíc *lokalizovat (opravit) jednu chybu*. Ukážeme si to na příkladu, kdy vyslaný blok 010101 přijme přijímající strana jako 010001. Graficky to znázorníme takto:

$$010101 \longrightarrow 010001.$$

Rozdělíme-li libovolné slovo 3-opakovacího kódu na tři stejně dlouhé úseky, jsou tyto úseky stejné. Tak jsou kódová slova definována. Pokud tomu tak u přijatého slova není, došlo během přenosu informace k nějaké chybě. Pokud došlo k jedné chybě, dva z těchto úseků zůstanou stejné, třetí (ten, ve kterém se chyba vyskytla) se od nich liší. Předpokládáme, že vysláno bylo to kódové slovo, ve kterém se všechny tři úseky rovnají těm dvěma stejným přijatým. Je to jediná možnost, jak z přijatého slova dostat kódové slovo změnou jediného symbolu. V našem případě změníme čtvrtý přijatý symbol z 0 na 1 a dostaneme kódové slovo. Jakékoliv jiné kódové slovo dostaneme z přijatého pomocí změny aspoň dvou symbolů. Například tak, že obě přijaté 1 změníme na 0.

Pokud předpokládáme, že pravděpodobnost změny symbolu vlivem šumu je $p < 1/2$, a tedy pravděpodobnost, že symbol byl přijatý správně (tj. tak jak byl vyslán) je $1 - p > 1/2 > p$, pak v případě přijetí nekódového slova je nejpravděpodobnější, že bylo vysláno to slovo, které se od přijatého liší v co nejméně symbolech.

5.8.2. Hammingova vzdálenost. Pro teorii samoopravných kódů je následující definice klíčová.

Definice 5.109. 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 5.110. 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 5.111.

- 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 5.112. *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 5.113. 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 5.114. *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 5.115. 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 5.116. 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 5.117. *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 5.114 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 5.118. Kontrolní matice A kódu C z Příkladu 5.115 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 5.119. 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 5.120. *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 5.121. 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 5.122. 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 $\mathbf{a}_j = (s_1 s_2 s_3)^T$. 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

$$A(\mathbf{y}^T + \mathbf{e}_j^T) = A\mathbf{y}^T + A\mathbf{e}_j^T = (s_1 s_2 s_3)^T + \mathbf{a}_j = (s_1 s_2 s_3)^T + (s_1 s_2 s_3)^T = \mathbf{o}^T.$$

Slovo $\mathbf{y} + \mathbf{e}_j$ tak patří do kódu H_3 a má Hammingovu vzdálenost 1 od přijatého slova $\mathbf{y}$. Je to tedy to slovo, které bylo vysláno a při přenosu byl poškozen j-tý symbol. ▲

Příklad 5.123. 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 5.124. *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 5.125. *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 $\{1, 2, 3, \ldots, n\}$ (nebo jiné dané množiny X) spolu s operací symetrické diference, tj. $A + B = (A \setminus B) \cup (B \setminus A)$, je vektorový prostor nad $\mathbb{Z}_2$. (Násobení skalárem je jednoznačně dané axiomy.) Dokažte a vysvětlete, proč je tento prostor „v podstatě“ $\mathbb{Z}_2^n$.

5. Dokažte tvrzení 5.11 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. Zjistěte lineární obal množiny X z příkladu 5.28 a dokažte, že množina Y tvoří podprostor.

9. Dokažte, že posloupnost vektorů $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ ve vektorovém prostoru $\mathbf{V}$ nad $\mathbf{T}$ je lineárně nezávislá právě tehdy, když žádný z vektorů není v lineárním obalu předchozích (tj. pro každé i platí $\mathbf{v}_i \notin \mathrm{LO}\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{i-1}\}$).

10. Dokažte, že sloupce matice v řádkově odstupňovaném tvaru jsou lineárně nezávislé právě tehdy, když příslušná homogenní soustava nemá žádné volné proměnné.

11. Dokončete příklad 5.54 o Fibonacciho posloupnostech.

12. Dokažte, že sloupce (řádky) čtvercové matice A nad $\mathbf{T}$ řádu n tvoří bázi $\mathbf{T}^n$ právě tehdy, když A je regulární.

13. Dokažte:

- Dimenze prostoru všech matic nad $\mathbf{T}$ typu $m \times n$ je mn.
- Dimenze prostoru reálných polynomů stupně nejvýše n je $n+1$.
- Dimenze prostoru $\mathbb{C}$ jako vektorového prostoru nad $\mathbb{R}$ je 2.

14. 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 $a_1 = 3$, $a_2 = 7$.

15. Dokažte, že z každé množiny generátorů konečně generovaného prostoru lze vybrat bázi.

16. Dokažte, že důsledek 5.64 platí bez předpokladu konečnosti G. Předpoklad tedy změníme na „G je množina generátorů konečně generovaného prostoru $\mathbf{V}$“.

17. Spočítejte počet všech různých bází $\mathbf{V}$ vybraných z vektorů $\mathbf{v}_1, \dots, \mathbf{v}_5$ z příkladu 5.66.

18. Dokažte druhou část tvrzení 5.75.

19. Dokažte, že bázové sloupce tvoří bázi sloupcového prostoru matice.

20. 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 $(x_1, x_2, \dots, x_n)$.

21. Buď A matice typu $n \times m$ nad T. Buďte B a C dvě matice v redukovaném odstupňovaném tvaru vzniklé z A posloupností elementárních úprav. Dokažte, že pak $B = C$.

22. Dokažte, že pro libovolné tři podprostory $\mathbf{V}_1, \mathbf{V}_2, \mathbf{V}_3$ prostoru $\mathbf{V}$ platí

$$(V_1 + V_2) + V_3 = V_1 + (V_2 + V_3) \ .$$

23. Buďte $\mathbf{V}_1$ a $\mathbf{V}_2$ podprostory vektorového prostoru $\mathbf{V}$ nad nějakým tělesem T. Buďte G_1 a G_2 množiny generátorů $\mathbf{V}_1$ respektive $\mathbf{V}_2$. Dokažte, že pak $G_1 \cup G_2$ je množina generátorů prostoru $V_1 + V_2$.

24. Dokažte, že

$$V_1 + V_2 + \dots + V_k = \{v_1 + v_2 + \dots + v_k : v_1 \in V_1, v_2 \in V_2, \dots, v_k \in V_k\} \ .$$

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 5.125.

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 *vektorovým prostorem* $\mathbf{V}$ *nad tělesem* $\mathbf{T}$ rozumíme množinu V spolu s binární operací $+$ na V (tj. $+$ je zobrazení z $V \times V$ do V) a operací $\cdot$ násobení 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 2.5), označujeme jej $\mathbf{T}^n$.

(3) Další příklady vektorových 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 vektorovém 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 $\mathbf{V}$ vektorový prostor nad $\mathbf{T}$, pak vektorový 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 $\mathbf{U} \leq \mathbf{V}$.

(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 $\operatorname{Ker} A \leq \mathbf{T}^n$.

(9) Jsou-li $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ prvky vektorového 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.

(10) Nechť $\mathbf{V}$ je vektorový prostor nad $\mathbf{T}$ a $X \subseteq V$. Pak *lineárním obalem množiny* X rozumíme množinu $\mathrm{LO}\, X$ všech lineárních kombinací prvků X, tj. množinu

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

(11) Pro libovolný vektorový prostor $\mathbf{V}$ nad $\mathbf{T}$ a libovolnou $X \subseteq V$ je $\mathrm{LO}\, X$ podprostorem $\mathbf{V}$.

(12) Je-li $\mathbf{V}$ vektorový prostor nad $\mathbf{T}$ a $X \subseteq U \leq \mathbf{V}$, pak $\mathrm{LO}\, X \subseteq \mathbf{U}$. Lineární obal $\mathrm{LO}\, X$ je proto nejmenší podprostor $\mathbf{V}$ obsahující množinu X.

(13) Jsou-li X, Y dvě podmnožiny vektorového prostoru $\mathbf{V}$ nad $\mathbf{T}$, pak platí

$$\mathrm{LO}\, X \subseteq \mathrm{LO}\, Y \quad \text{právě když pro každé} \quad x \in X \quad \text{platí} \quad x \in \mathrm{LO}\, Y \ .$$

(14) Je-li $\mathbf{V}$ vektorový prostor nad $\mathbf{T}$ a $X \subseteq V$. Pokud $\mathrm{LO}\, X = V$, 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 vektorového prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$, pak

$$\mathrm{LO}\, \{\mathbf{v}_1, \ldots, \mathbf{v}_l\} = \{t_1\mathbf{v}_1 + \cdots + t_l\mathbf{v}_l : t_1, \ldots, t_l \in T\} \ .$$

(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 $\mathrm{Im}\, A$.

$$\mathrm{Im}\, A = \mathrm{LO}\, \{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\} \leq \mathbf{T}^m$$

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

$$\mathrm{Im}\, A^T = \mathrm{LO}\, \{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m\} \leq \mathbf{T}^n$$

(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

$$\mathrm{Im}\,(RA) = \mathrm{LO}\, \{R\mathbf{a}_1, \ldots, R\mathbf{a}_n\}\,,\ \mathrm{Ker}\, A = \mathrm{Ker}\,(RA),\ \mathrm{Im}\, A^T = \mathrm{Im}\,(RA)^T.$$

(18) Elementární řádkové úpravy nemění $\mathrm{Ker}\, A$ a $\mathrm{Im}\, A^T$. Elementární sloupcové úpravy nemění $\mathrm{Ker}\, A^T$ a $\mathrm{Im}\, A$.

(19) Nechť $\mathbf{V}$ je vektorový 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 $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_{i-1}$, $\mathbf{v}_{i+1}$, ..., $\mathbf{v}_k$.

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 vektorového 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 $\mathrm{Ker}\, A = \{\mathbf{o}\}$, 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 vektorového prostoru $\mathbf{V}$ nad $\mathbf{T}$ se nazývá *báze*, pokud je lineárně nezávislá a LO $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\} = \mathbf{V}$.

(26) Posloupnost prvků $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ tvoří bázi vektorového 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) Vektorový prostor se nazývá *konečně generovaný*, pokud má nějakou konečnou množinu generátorů.

(30) Minimální posloupnost generátorů $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ vektorového prostoru $\mathbf{V}$ je báze $\mathbf{V}$.

(31) Z každé konečné množiny generátorů vektorového prostoru lze vybrat bázi.

(32) Každý konečně generovaný vektorový 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 vektorového 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 vektorového prostoru mají stejný počet prvků.

(35) *Dimenzí* konečně generovaného vektorového 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 vektorového 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 vektorovém 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 $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ je báze vektorového 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.

$$[\mathbf{w}]_B = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \ .$$

(41) Nechť $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ 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 vektorového prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ dimenze n. Pak platí
(a) posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ je lineárně nezávislá ve $\mathbf{V}$ právě tehdy, když je posloupnost $([\mathbf{v}_1]_B, [\mathbf{v}_2]_B, \ldots, [\mathbf{v}_k]_B)$ lineárně nezávislá v $\mathbf{T}^n$;
(b) množina X generuje $\mathbf{V}$ právě tehdy, když $[X]_B$ generuje $\mathbf{T}^n$;
(c) posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ je báze $\mathbf{V}$ právě tehdy, když je posloupnost $([\mathbf{v}_1]_B, [\mathbf{v}_2]_B, \ldots, [\mathbf{v}_k]_B)$ báze $\mathbf{T}^n$.

(43) Nechť $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ a C jsou báze vektorového 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 vektorový 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

$$\mathbf{a}_i \notin \mathrm{LO}\,\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{i-1}\} \ .$$

(46) Pro libovolnou matici A tvoří bázové sloupce bázi sloupcového prostoru. Speciálně, dimenze $\mathrm{Im}\,A$ 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, ..., k_r, kde $r, k_1, \ldots, k_r$ jsou parametry z definice 2.14 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 $\dim(\mathrm{Im}\,A) = \dim(\mathrm{Im}\,A^T)$.

(50) *Hodností* matice A rozumíme dimenzi řádkového (sloupcového) prostoru matice A. Značíme $\mathrm{rank}(A)$.

(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

$$\operatorname{rank}(AB) \leq \operatorname{rank}(A), \quad \operatorname{rank}(AB) \leq \operatorname{rank}(B) \ .$$

(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.
- A je regulární.
- $\operatorname{rank}(A) = n$.
- Sloupce (řádky) matice A jsou lineárně nezávislé.
- Sloupce (řádky) matice A generují $\mathbf{T}^n$.
- 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 Gaussovou 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

$$\dim(\operatorname{Ker} A) + \dim(\operatorname{Im} A) = n \ .$$

(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.

$$\sum_{i \in I} V_i = \mathrm{LO}\left\{\bigcup_{i \in I} V_i\right\} \ .$$

Součet podprostorů $V_1, V_2, \ldots, V_k$ také značíme $V_1 + V_2 + \cdots + V_k$.

(63) Pro podprostory $\mathbf{U}$, $\mathbf{W}$ vektorového 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 z páté kapitoly nezbytné pro průběžné sledování přednášek s pochopením

(1) Definice vektorového prostoru nad tělesem $\mathbf{T}$ a jednoduché vlastnosti počítání v něm, příklady vektorových prostorů.
(2) Pojem podprostoru vektorového prostoru a ekvivalentní definnice pomocí uzavřenosti na operace.
(3) Definice lineární kombinace prvků, lineárního obalu množiny prvků, množiny generátorů, a konečně generovaného vektorového prostoru.
(4) Lineární obal $\mathrm{LO}\, X$ množiny $X \subseteq \mathbf{V}$ je nejmenší podprostor $\mathbf{V}$ obsahující X.
(5) Lineární závislost a nezávislost konečné posloupnosti prvků vektorového prostoru, různé ekvivalentní definice.
(6) Báze konečně generovaného vektorového 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 vektorového 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 vektorového 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.

KAPITOLA 6

Lineární zobrazení

Cíl. *Dosud jsme zobecnili počítání s reálnými čísly na počítání v tělese a počítání s aritmetickými vektory na počítání ve vektorovém 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 oboru hodnot 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 vektorovými prostory (nejen aritmetickými vektorovými).

Definice 6.1. Nechť $\mathbf{V}, \mathbf{W}$ jsou vektorové prostory nad stejným tělesem $\mathbf{T}$. Zobrazení $f : V \to W$ nazýváme *lineární zobrazení* (nebo *homomorfismus*) z $\mathbf{V}$ do $\mathbf{W}$, pokud

(1) $f(\mathbf{u} + \mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v})$ pro libovolné $\mathbf{u}, \mathbf{v} \in V$ a
(2) $f(t\mathbf{u}) = tf(\mathbf{u})$ pro libovolné $\mathbf{u} \in V$ a $t \in T$.

Skutečnost, že f je lineární zobrazení z $\mathbf{V}$ do $\mathbf{W}$ zapisujeme $f : \mathbf{V} \to \mathbf{W}$.

Vlevo v rovnostech vystupují operace v prostoru $\mathbf{V}$ a vpravo operace v prostoru $\mathbf{W}$. Zdůrazněme, že prostory $\mathbf{V}$ a $\mathbf{W}$ musí být nad stejným tělesem. Všimněte si rovněž, že každé lineární zobrazení zobrazuje nulový prvek ve $\mathbf{V}$ na nulový prvek v $\mathbf{W}$.

Pro libovolnou matici A nad $\mathbf{T}$ typu $m \times n$ je zobrazení $f_A : T^n \to T^m$ lineární, protože

$$f_A(\mathbf{u}+\mathbf{v}) = A(\mathbf{u}+\mathbf{v}) = A\mathbf{u} + A\mathbf{v} = f_A(\mathbf{u}) + f_A(\mathbf{v})$$

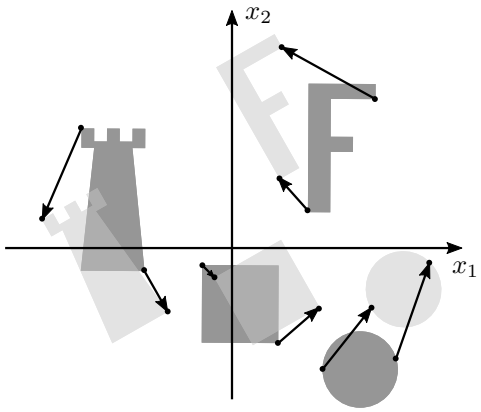
a

$$f_A(t\mathbf{u}) = A(t\mathbf{u}) = t(A\mathbf{u}) = tf_A(\mathbf{u}) \ .$$

To nám dává řadu příkladů lineárních zobrazení mezi aritmetickými vektorovými prostory (a jak jsme zmínili 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) kolem počátku o daný úhel – obrázek 6.1.

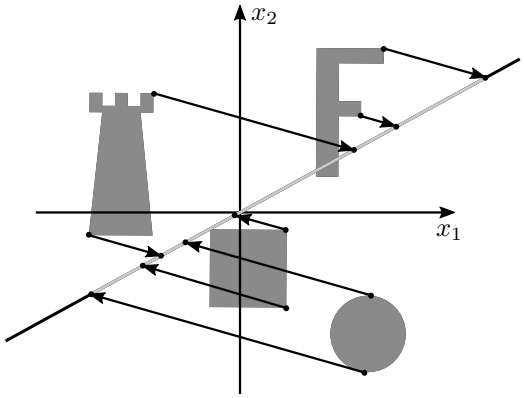


Obrázek 6.1. Rotace v rovině kolem počátku souřadnic

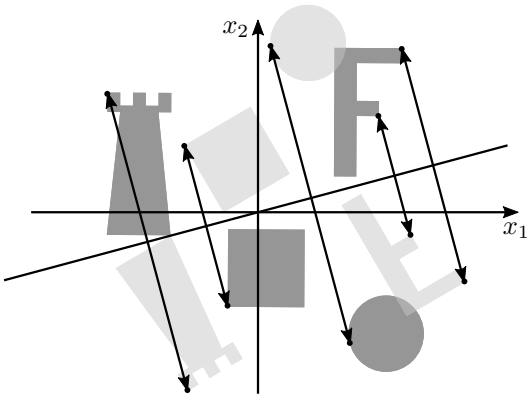
  - Zkosení – obrázek 4.12.
  - Projekce na přímku procházející počátkem – obrázek 6.2.
  - Osová souměrnost podle přímky procházející počátkem – obrázek 6.3.
  - Stejnolehlost se středem v počátku (zvětšení) – obrázek 6.4
- Lineární zobrazení z $\mathbb{R}^3$ do $\mathbb{R}^3$ jsou například rotace, zrcadlení 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 $\mathbb{R}^2$ do $\mathbb{R}$ je zobrazení d udávající orientovanou vzdálenost (polohového vektoru) bodu od zvolené přímky l procházející počátkem. Orientovaná vzdálenost je vzdálenost (polohového



Obrázek 6.2. Projekce na přímku procházející počátkem



Obrázek 6.3. Osová souměrnost podle přímky procházející počátkem

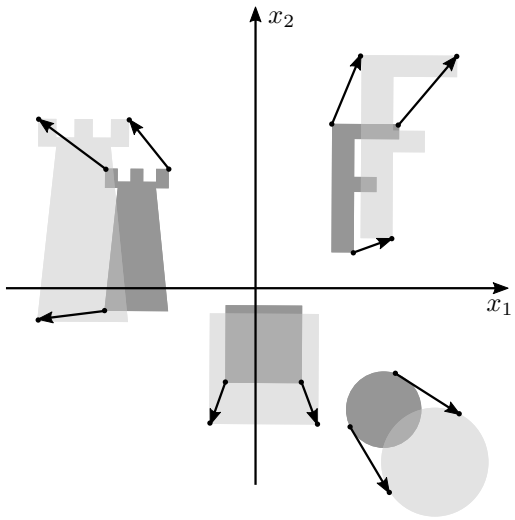
vektoru) bodu od přímky l spolu se znaménkem $+/-$ v závislosti na tom, ve které polorovině určené přímkou l daný bod leží. V jedné polorovině je znaménko $+$, v opačné polorovině je znaménko $-$.

- Podobně je příkladem lineárního zobrazení z $\mathbb{R}^3$ do $\mathbb{R}$ zobrazení d udávající orientovanou vzdálenost od zvolené roviny p procházející počátkem.

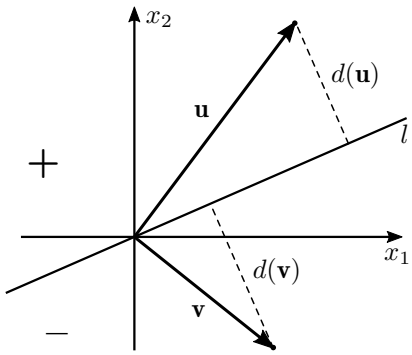
▲

Ještě než popíšeme, jak vypadají lineární zobrazení obecně, podíváme se na další příklady.

Příklad 6.3.

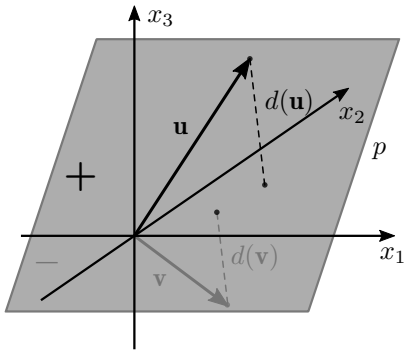


Obrázek 6.4. Stejnolehlost se středem v počátku



Obrázek 6.5. Lineární zobrazení z $\mathbb{R}^2$ do $\mathbb{R}$: orientovaná vzdálenost od přímky procházející počátkem

- Identické zobrazení $\mathrm{id}_{\mathbf{V}}$ na libovolném vektorovém prostoru $\mathbf{V}$ je lineární zobrazení $\mathbf{V} \to \mathbf{V}$.
- Tzv. *nulové zobrazení* 0 z $\mathbf{V}$ do $\mathbf{W}$ přiřazující všem vektorům ve $\mathbf{V}$ nulový vektor ve $\mathbf{W}$ je lineární.
- Nechť $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ je báze vektorového prostoru $\mathbf{V}$. Zobrazení f z V do T^n definované $f(\mathbf{v}) = [\mathbf{v}]_B$ je lineární zobrazení $\mathbf{V} \to \mathbf{T}^n$ podle tvrzení 5.75 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.



Obrázek 6.6. Lineární zobrazení z $\mathbb{R}^3$ do $\mathbb{R}$: orientovaná vzdálenost od roviny procházející počátkem

- 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 $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n \in V$, a skaláry $t_1, t_2, \ldots, t_k \in T$ 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* $\mathbf{W}$ *vektorové 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* $i \in \{1, 2, \ldots, n\}$.

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, $[\mathbf{x}]_B = (t_1, t_2, \ldots, t_n)$) 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 $\mathbf{x}, \mathbf{y} \in V$, jejichž vyjádření vzhledem k B jsou

$$[\mathbf{x}]_B = (t_1, t_2, \ldots, t_n)^T, \quad [\mathbf{y}]_B = (s_1, s_2, \ldots, s_n)^T \ .$$

Pak $[\mathbf{x}+\mathbf{y}]_B = (t_1+s_1, t_2+s_2, \dots, t_n+s_n)^T$ (viz tvrzení 5.75 o souřadnicích a operacích) a tedy

$$\begin{aligned} f(\mathbf{x}+\mathbf{y}) &= (t_1+s_1)\mathbf{w}_1 + (t_2+s_2)\mathbf{w}_2 + \dots + (t_n+s_n)\mathbf{w}_n \\ &= t_1\mathbf{w}_1 + t_2\mathbf{w}_2 + \dots + t_n\mathbf{w}_n + s_1\mathbf{w}_1 + s_2\mathbf{w}_2 + \dots + s_n\mathbf{w}_n \\ &= f(\mathbf{x}) + f(\mathbf{y}) \ . \end{aligned}$$

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 $\mathbf{x} = (x_1, x_2, \dots, x_n)^T \in T^n$ platí

$$f(\mathbf{x}) = f(x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + \dots + x_n\mathbf{e}_n) = x_1 f(\mathbf{e}_1) + x_2 f(\mathbf{e}_2) + \dots + x_n f(\mathbf{e}_n) \ ,$$

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 vektorové 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 vektorové prostory nad tělesem $\mathbf{T}$, $f : \mathbf{V} \to \mathbf{W}$, $B = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ je báze 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 vektorové prostory nad tělesem $\mathbf{T}$, $B = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ 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 $\mathbf{x} = x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + \dots + x_n\mathbf{v}_n$ vzhledem k bázi B platí

$$f(\mathbf{x}) = f(x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + \dots + x_n\mathbf{v}_n) = x_1 f(\mathbf{v}_1) + x_2 f(\mathbf{v}_2) + \dots + x_n f(\mathbf{v}_n) \ ,$$

pro vyjádření vzhledem k bázi C pak podle tvrzení 5.75 o souřadnicích a operacích platí

$$[f(\mathbf{x})]_C = x_1[f(\mathbf{v}_1)]_C + x_2[f(\mathbf{v}_2)]_C + \dots + x_n[f(\mathbf{v}_n)]_C \ ,$$

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 vektorové 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 $M = ([f(\mathbf{v}_1)]_C \mid [f(\mathbf{v}_2)]_C \mid \cdots \mid [f(\mathbf{v}_n)]_C) = [f]_C^B$. ▲

V definici 5.78 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 6.8. *Jsou-li* B, C *dvě báze konečně generovaného prostoru* $\mathbf{V}$*, pak matice identického zobrazení z* $\mathbf{V}$ *do* $\mathbf{V}$ *vzhledem k bázím* B *a* C *se rovná matici přechodu od báze* B *k bázi* C.

DŮKAZ. Přímý důsledek definic. ▲

Vztah $[\mathbf{x}]_C = [\mathrm{id}]_C^B\,[\mathbf{x}]_B$ z tvrzení 5.79 je nyní důsledkem tvrzení 6.6.

Přesnější označení pro matici přechodu od báze B k bázi C 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.

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 aritmetickém prostoru $\mathbf{T}^i$.

PŘÍKLAD 6.9. 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:

$$\begin{aligned} f(1,1,2)^T &= (2\cdot 1+3\cdot 1+1\cdot 2, 4\cdot 1+2\cdot 2)^T = (2,3)^T \\ f(2,2,0)^T &= (2\cdot 2+3\cdot 2+1\cdot 0, 4\cdot 2+2\cdot 0)^T = (0,3)^T \\ f(3,4,4)^T &= (2\cdot 3+3\cdot 4+1\cdot 4, 4\cdot 3+2\cdot 4)^T = (2,0)^T \end{aligned}$$

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 6.10. 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 4.3.1. ▲

Příklad 6.11. 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 6.12. 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:

$$\begin{aligned}
[1']_B &= [0]_B = (0,0,0,0)^T \\
[x']_B &= [1]_B = (1,0,0,0)^T \\
[(x^2)']_B &= [2x]_B = (0,2,0,0)^T \\
[(x^3)']_B &= [3x^2]_B = (0,0,3,0)^T
\end{aligned}$$

Hledaná matice je

$$[f]_B^B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} .$$

▲

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 6.13. *Jsou-li* $\mathbf{U}, \mathbf{V}, \mathbf{W}$ *vektorové 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 je-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 6.14. *Nechť* $\mathbf{U}, \mathbf{V}$ *jsou vektorové 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 vektorové prostory dimenze* n, B *báze v* $\mathbf{U}$ *a* C *báze ve* $\mathbf{V}$, *pak platí*

$$[f^{-1}]_B^C = \left([f]_C^B\right)^{-1} \quad .$$

Důkaz. Zvolíme libovolné dva 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 6.13 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 6.27 je pak prostor $\mathbf{V}$ také konečně generovaný a má stejnou dimenzi.

Ukážeme si použití předchozích dvou tvrzení na početních příkladech.

Příklad 6.15. 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 6.14:

$$[\mathrm{id}]_B^{K_2} = [\mathrm{id}^{-1}]_B^{K_2} = ([\mathrm{id}]_{K_2}^B)^{-1} = \begin{pmatrix} 2 & -5 \\ 5 & 2 \end{pmatrix}^{-1} = \frac{1}{29}\begin{pmatrix} 2 & 5 \\ -5 & 2 \end{pmatrix} \quad .$$

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 6.11 jsme nahlédli, že matice f vzhledem k B a kanonické bázi je

$$[f]_{K_2}^B = \begin{pmatrix} 2 & 5 \\ 5 & -2 \end{pmatrix} \quad .$$

Pomocí tvrzení 6.13 a užitím $f = f\ \mathrm{id}$ nyní můžeme spočítat matici f vzhledem ke kanonickým bázím:

$$[f]_{K_2}^{K_2} = [f]_{K_2}^B\,[\mathrm{id}]_B^{K_2} = \begin{pmatrix} 2 & 5 \\ 5 & -2 \end{pmatrix} \frac{1}{29}\begin{pmatrix} 2 & 5 \\ -5 & 2 \end{pmatrix} = \frac{1}{29}\begin{pmatrix} -21 & 20 \\ 20 & 21 \end{pmatrix} \quad .$$

▲

Příklad 6.16. 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 6.13 a 6.14:

$$\begin{aligned}[\mathrm{id}]_C^B &= [\mathrm{id}]_C^{K_2}\,[\mathrm{id}]_{K_2}^B = \left([\mathrm{id}]_{K_2}^C\right)^{-1}[\mathrm{id}]_{K_2}^B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{-1}\begin{pmatrix} 2 & 3 \\ 4 & 3 \end{pmatrix} \\ &= \frac{1}{3}\begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 2 & 3 \\ 4 & 3 \end{pmatrix} = 2\begin{pmatrix} 0 & 1 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 3 \end{pmatrix}\end{aligned}$$

Souřadnice $\mathbf{v}$ vzhledem k C jsou

$$[\mathbf{v}]_C = [\mathrm{id}]_C^B\,[\mathbf{v}]_B = \begin{pmatrix} 0 & 2 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 2x_2 \\ x_1 + 3x_2 \end{pmatrix} \quad .$$

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 6.17. V příkladu 6.9 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 6.13 a 6.14 je obzvláště důležitý, jak zjistíme v kapitole o vlastních číslech. Proto jej formulujeme jako samostatné tvrzení.

TVRZENÍ 6.18. *Je-li* $\mathbf{V}$ *konečně generovaný vektorový 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. Speciální typy lineárních zobrazení

Následující definice zavádí terminologii pro různé typy lineárních zobrazení.

DEFINICE 6.19. Nechť $\mathbf{V}$, $\mathbf{W}$ jsou vektorové 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 6.20.

- Rotace a osové souměrnosti jsou automorfismy $\mathbb{R}^2 \to \mathbb{R}^2$.

- Zobrazení přiřazující vektoru z $\mathbf{V}$ souřadnice ve zvolené bázi $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ 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 $\operatorname{Ker} f$ lineárního zobrazení f, je tvořeno těmi vektory, které f zobrazí na nulový vektor. Obraz lineárního zobrazení f budeme značit $\operatorname{Im} f$.

Definice 6.21. 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.

$$\operatorname{Im} f = \{f(\mathbf{x}) : \mathbf{x} \in V\} \ .$$

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 6.22. *Nechť $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení. Pak f je prosté právě tehdy, když* $\operatorname{Ker} f = \{\mathbf{o}\}$.

Důkaz. Je-li f prosté a $\mathbf{x} \in \operatorname{Ker} f$, pak $f(\mathbf{x}) = \mathbf{o} = f(\mathbf{o})$, a protože f je prosté, plyne odtud $\mathbf{x} = \mathbf{o}$. Proto $\operatorname{Ker} f \subseteq \{\mathbf{o}\}$. Opačná inkluze je triviální.

Je-li naopak $\operatorname{Ker} f = \{\mathbf{o}\}$ 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 $\mathbf{x} - \mathbf{y} \in \operatorname{Ker} f$, 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 6.23. *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 6.24. 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

$$[\operatorname{Ker} f]_B = \operatorname{Ker} A = \mathrm{LO}\left\{\begin{pmatrix}-1\\2\\0\end{pmatrix}, \begin{pmatrix}3\\0\\2\end{pmatrix}\right\} \ ,$$

z čehož dopočteme

$$\begin{aligned}\operatorname{Ker} f &= \mathrm{LO}\left\{-1\begin{pmatrix}1\\2\\3\end{pmatrix} + 2\begin{pmatrix}2\\0\\1\end{pmatrix}, 3\begin{pmatrix}1\\2\\3\end{pmatrix} + 2\begin{pmatrix}3\\3\\0\end{pmatrix}\right\} \\ &= \mathrm{LO}\left\{\begin{pmatrix}3\\-2\\-1\end{pmatrix}, \begin{pmatrix}9\\12\\9\end{pmatrix}\right\} = \mathrm{LO}\left\{\begin{pmatrix}3\\-2\\-1\end{pmatrix}, \begin{pmatrix}3\\4\\3\end{pmatrix}\right\} \ .\end{aligned}$$

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

$$[\operatorname{Im} f]_C = \operatorname{Im} A = \mathrm{LO}\left\{\begin{pmatrix}1\\-2\end{pmatrix}\right\}$$

a

$$\operatorname{Im} f = \mathrm{LO}\left\{1\begin{pmatrix}3\\1\end{pmatrix} - 2\begin{pmatrix}-1\\1\end{pmatrix}\right\} = \mathrm{LO}\left\{\begin{pmatrix}5\\-1\end{pmatrix}\right\} \ .$$

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 6.25. *Nechť* $\mathbf{V}$ *a* $\mathbf{W}$ *jsou vektorové 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 6.22 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 6.26. *Nechť* $\mathbf{V}$ *a* $\mathbf{W}$ *jsou vektorové 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 $\mathbf{w} = t_1 f(\mathbf{v}_1) + \dots + t_n f(\mathbf{v}_n)$. Pak pro vektor $\mathbf{x} = t_1\mathbf{v}_1 + \dots + t_n\mathbf{v}_n$ platí $f(\mathbf{x}) = f(t_1\mathbf{v}_1 + \dots + t_n\mathbf{v}_n) = t_1 f(\mathbf{v}_1) + \dots + t_n f(\mathbf{v}_n) = \mathbf{w}$. ▲

Důsledkem předchozích dvou tvrzení je charakterizace izomorfismů.

Tvrzení 6.27. *Nechť* $\mathbf{V}$ *a* $\mathbf{W}$ *jsou vektorové 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 6.28. *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. Důkaz je přenechán čtenáři jako cvičení. ▲

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 5.75. (Vlastnosti uvedené v pozorování 5.77 jsou tak speciálním případem pozorování 6.28.)

Použitím vlastností z pozorování 6.28 na tento "souřadnicový izomorfismus" získáme obecnější verzi věty o dimenzi jádra a obrazu, dříve dokázané v maticové verzi.

VĚTA 6.29 (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 6.23 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 6.28 nyní vyplývá $\dim \operatorname{Ker} f = \dim \operatorname{Ker} A$ a $\dim \operatorname{Im} f = \dim \operatorname{Im} A$. Vztah nyní vyplývá z věty 5.99 o dimenzi jádra a obrazu pro matice. ▲

Souřadnicový izomorfismus 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 6.30. *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) $\Rightarrow$ (2) je bod (4) v pozorování 6.28.

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 6.27 charakterizující izomorfismy. ▲

Dokázaná věta dává 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 6.31. 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.

TVRZENÍ 6.32. *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 $\mathbf{V} \to \mathbf{W}$.

DŮKAZ. Přenecháme jako cvičení. ▲

Definice 6.33. Mějme vektorové prostory $\mathbf{V}$, $\mathbf{W}$ nad stejným tělesem $\mathbf{T}$. Pak množina všech lineárních zobrazení z $\mathbf{V}$ do $\mathbf{W}$ s operacemi definovanými v tvrzení 6.32 tvoří vektorový prostor nad $\mathbf{T}$, značíme jej $\mathrm{Hom}(\mathbf{V}, \mathbf{W})$.

Tvrzení 6.34. *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 $s(f) = [f]^B_C$.

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 $[tf]^B_C = t[f]^B_C$, $[f + g]^B_C = [f]^B_C + [g]^B_C$. 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 6.32) nazýváme duál prostoru $\mathbf{V}$:

Definice 6.35. 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 6.34 izomorfní prostoru $\mathbf{T}^{1\times n}$ všech matic nad $\mathbf{T}$ typu $1 \times n$ tj. prostoru řádkových vektorů. Speciálně:

Tvrzení 6.36. *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 6.28), platí $\dim \mathbf{V}^d = n$. ▲

Podle důkazu tvrzení 6.34 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 6.37. 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 $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ rovná

$$[f]^B = (f(\mathbf{v}_1), f(\mathbf{v}_2), \dots, f(\mathbf{v}_n)) \ .$$

Vzorec z tvrzení 6.6 o matici lineárního zobrazení má pro lineární formy tvar

$$f(\mathbf{x}) = [f]^B [\mathbf{x}]_B \ .$$

Označíme-li $[f]^B = (a_1, \dots, a_n)$ a $[\mathbf{x}]_B = (x_1, \dots, x_n)$, máme

$$f(\mathbf{x}) = (a_1, \dots, a_n)(x_1, \dots, x_n)^T = a_1x_1 + a_2x_2 + \cdots + a_nx_n \ .$$

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 $\tilde{\mathbf{a}}_1, \dots, \tilde{\mathbf{a}}_m$. Pro $i = 1, \dots, m$ označme f_i lineární formu na $\mathbf{T}^n$, jejíž matice vzhledem ke kanonické bázi je $\tilde{\mathbf{a}}_i$, tj.

$$f_i(x_1, \dots, x_n)^T = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n \ .$$

Vektor $\mathbf{x} \in T^n$ je řešením soustavy $A\mathbf{x} = \mathbf{o}$ právě tehdy, když $f_1(\mathbf{x}) = 0, f_2(\mathbf{x}) = 0, \dots, f_m(\mathbf{x}) = 0$. Jinými slovy, $A\mathbf{x} = \mathbf{o}$ právě tehdy, když $\mathbf{x} \in \operatorname{Ker} f_1$, ..., $\mathbf{x} \in \operatorname{Ker} f_m$, neboli $\mathbf{x} \in \operatorname{Ker} f_1 \cap \cdots \cap \operatorname{Ker} f_m$. Jádro je, kromě případu nulové formy, vždy nadrovina (tj. podprostor dimenze $n-1$ v $\mathbf{T}^n$), jak ukazuje následující obecnější tvrzení.

Tvrzení 6.38. *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 6.29 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

$$\mathbf{W}_1 = \operatorname{Ker} f_1, \ \mathbf{W}_2 = \operatorname{Ker} f_1 \cap \operatorname{Ker} f_2, \dots, \mathbf{W}_m = \operatorname{Ker} f_1 \cap \operatorname{Ker} f_2 \cap \cdots \cap \operatorname{Ker} f_m.$$

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 6.39), 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 $\tilde{\mathbf{a}}_1$, ..., $\tilde{\mathbf{a}}_i$.)

Tvrzení 6.39. *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 $\mathbf{U}$ 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 5.103 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 6.40. *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) $g \in \operatorname{LO}\{f_1, \dots, f_k\}$
(2) $\operatorname{Ker} g \supseteq \operatorname{Ker} f_1 \cap \cdots \cap \operatorname{Ker} f_k$

Důkaz. Jednodušší je implikace (1) $\Rightarrow$ (2). Předpokládejme, že $g = t_1 f_1 + \cdots + t_k f_k$ pro nějaké skaláry $t_1, \ldots, t_k \in T$. Pak pro libovolný vektor $\mathbf{x} \in \operatorname{Ker} f_1 \cap \cdots \cap \operatorname{Ker} f_k$ platí $f_1(\mathbf{x}) = f_2(\mathbf{x}) = \cdots = f_k(\mathbf{x}) = \mathbf{o}$, tedy také $g(\mathbf{x}) = (t_1 f_1 + \cdots + t_k f_k)(\mathbf{x}) = t_1 f_1(\mathbf{x}) + \cdots + t_k f_k(\mathbf{x}) = \mathbf{o}$.

Pro důkaz (2) $\Rightarrow$ (1) zvolme nějakou bázi B prostoru $\mathbf{V}$. Označme C matici (typu $k \times n$) s řádkovými vektory $[f_1]^B$, ..., $[f_k]^B$ a D matici (typu $(k+1) \times n$) s řádkovými vektory $[f_1]^B$, ..., $[f_k]^B$, $[g]^B$.

Ukážeme, že $\operatorname{Ker} C = [\operatorname{Ker} f_1 \cap \cdots \cap \operatorname{Ker} f_k]_B$. 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 $[\operatorname{Ker} f_1 \cap \cdots \cap \operatorname{Ker} f_k]_B$ právě tehdy, když $\mathbf{x}$ leží v $\operatorname{Ker} f_1 \cap \ldots \operatorname{Ker} f_k$, neboli $f_1(\mathbf{x}) = \cdots = f_k(\mathbf{x}) = 0$. To nastane právě tehdy, když $[f_1]^B[\mathbf{x}]_B = \cdots = [f_k]^B[\mathbf{x}]_B = 0$ (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 $\operatorname{Ker} D = [\operatorname{Ker} f_1 \cap \cdots \cap \operatorname{Ker} f_k \cap \operatorname{Ker} g]_B$. Z předpokladu, že $\operatorname{Ker} g$ obsahuje $\operatorname{Ker} f_1 \cap \cdots \cap \operatorname{Ker} f_k$ ale plyne $\operatorname{Ker} f_1 \cap \cdots \cap \operatorname{Ker} f_k \cap \operatorname{Ker} g = \operatorname{Ker} f_1 \cap \cdots \cap \operatorname{Ker} f_k$. Platí proto $\operatorname{Ker} C = \operatorname{Ker} D$.

Podle věty 5.99 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 5.88 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 způsoby 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. Předchozí 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 $\mathbf{V}, \mathbf{W}$ vektorové 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 $\mathbf{W}$ vektorové 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 vektorové 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 vektorové 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 vektorové 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 aritmetickém 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 $\mathbf{U}, \mathbf{V}, \mathbf{W}$ vektorové 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 $\mathbf{U}, \mathbf{V}$ vektorové 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 vektorové 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 vektorový 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 vektorové 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 $\mathbf{V}$.

(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 $\mathbf{W}$ vektorové prostory nad tělesem $\mathbf{T}$, $\mathbf{V}$ konečně generovaný vektorový 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 $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ ve $\mathbf{V}$ je posloupnost $(f(\mathbf{v}_1), \dots, f(\mathbf{v}_k))$ lineárně nezávislá ve $\mathbf{W}$,
(c) 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 $\mathbf{W}$.

(18) Jsou-li $\mathbf{V}$ a $\mathbf{W}$ vektorové prostory nad tělesem $\mathbf{T}$, $\mathbf{V}$ konečně generovaný vektorový 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 $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ ve $\mathbf{V}$ je $\{f(\mathbf{v}_1), \dots, f(\mathbf{v}_k)\}$ množina generátorů ve $\mathbf{W}$,
(c) existuje báze $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ prostoru $\mathbf{V}$ taková, že $\{f(\mathbf{v}_1), \dots, f(\mathbf{v}_n)\}$ generuje $\mathbf{W}$.

(19) Jsou-li $\mathbf{V}$ a $\mathbf{W}$ vektorové prostory nad tělesem $\mathbf{T}$, $\mathbf{V}$ konečně generovaný vektorový prostor, a $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak následující tvrzení jsou ekvivalentní.

(a) Zobrazení f je izomorfismus,
(b) pro každou bázi $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ ve $\mathbf{V}$ je $(f(\mathbf{v}_1), \dots, f(\mathbf{v}_k))$ báze ve $\mathbf{W}$,
(c) 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 $\mathbf{W}$.

(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) $\dim(\mathbf{V}) = \dim(\mathbf{W})$.

Klíčové znalosti ze šesté kapitoly nezbytné pro průběžné sledování přednášek s pochopením

(1) Definice lineárního zobrazení.
(2) Každé lineární zobrazení na konečně generovaném vektorovém 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 vektorové prostory jsou isomorfní právě když mají stejnou dimenzi.
(13) Věta o dimenzi jádra a obrazu lineárního zobrazení definovaného na konečně generovaném vektorovém prostoru.

KAPITOLA 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 (přesněji, tato deformace musí body původního obrázku převádět na odpovídající body obrazu). Pokud je determinant A rovný -1, pak zobrazení zachová obsah každého útvaru a orientaci mění.

$A = I_2$ $\qquad$ $\det A = 1{,}3$ $\qquad$ $\det A = -1$

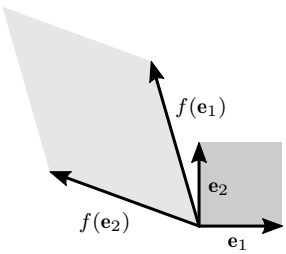
Obrázek 7.1. Vliv determinantu na velikost a orientaci obrazu

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 $\mathbf{v}$.

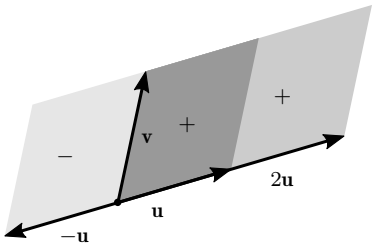
Podíváme se na jiný postup, který se nám rovněž bude hodit v obecnější situaci.



OBRÁZEK 7.2. Jednotkový čtverec a jeho obraz lineárním zobrazením

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

$$\det(t\mathbf{u}|\mathbf{v}) = t\det(\mathbf{u}|\mathbf{v}) = \det(\mathbf{u}|t\mathbf{v}) \quad .$$



OBRÁZEK 7.3. Srovnání $\det(\mathbf{u}|\mathbf{v})$ a $\det(t\mathbf{u}|\mathbf{v})$

Z následujícího obrázku 7.4 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.

$$\det(\mathbf{u}|\mathbf{v}_1 + \mathbf{v}_2) = \det(\mathbf{u}|\mathbf{v}_1) + \det(\mathbf{u}|\mathbf{v}_2)$$

Na obrázku 7.4 jsou všechny použité rovnoběžníky kladně orientované. Obrázek 7.5 ukazuje, že rovnost

$$\det(\mathbf{u}_1 + \mathbf{u}_2|\mathbf{v}) = \det(\mathbf{u}_1|\mathbf{v}) + \det(\mathbf{u}_2|\mathbf{v})$$

platí i v případě, kdy jsou některé rovnoběžníky orientované záporně.

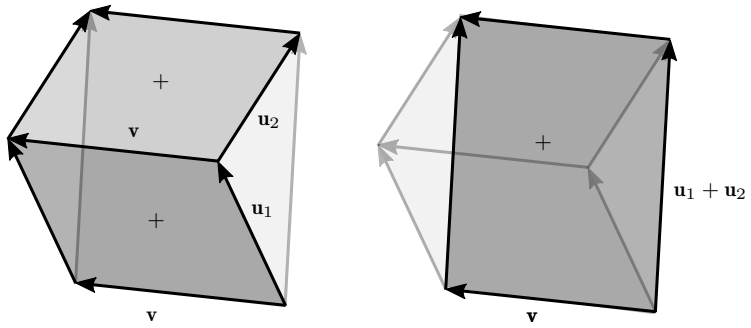
Ještě si uvědomíme, že

$$\det(\mathbf{e}_1, \mathbf{e}_2) = 1, \quad \det(\mathbf{e}_2, \mathbf{e}_1) = -1 \ , \quad \det(\mathbf{e}_1, \mathbf{e}_1) = \det(\mathbf{e}_2, \mathbf{e}_2) = 0$$

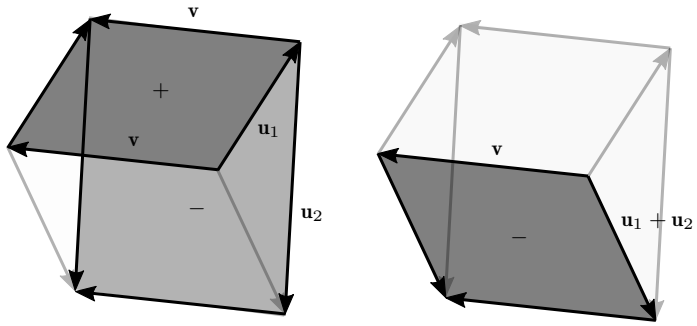
protože první matice odpovídá identickému zobrazení, které nemění obsah ani orientaci, druhá matice odpovídá překlopení kolem osy prvního kvadrantu, která nemění obsah a mění orientaci, třetí a čtvrtá matice odpovídá zobrazení, která čtverci přiřadí „zdegenerovaný rovnoběžník“ – úsečku.

Z odvozených vztahů již jde spočítat determinant obecné matice

$$A = (\mathbf{u}|\mathbf{v}) = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad .$$



OBRÁZEK 7.4. Srovnání $\det(\mathbf{u}_1|\mathbf{v}) + \det(\mathbf{u}_2|\mathbf{v})$ (vlevo) a $\det(\mathbf{u}_1 + \mathbf{u}_2|\mathbf{v})$ (vpravo)



OBRÁZEK 7.5. Srovnání $\det(\mathbf{u}_1|\mathbf{v}) + \det(\mathbf{u}_2|\mathbf{v})$ (vlevo; $\det(\mathbf{u}_2|\mathbf{v})$ záporný) a $\det(\mathbf{u}_1 + \mathbf{u}_2|\mathbf{v})$ (vpravo)

$$\begin{aligned}
\det(A) = \det(\mathbf{u}|\mathbf{v}) &= \det(a_{11}\mathbf{e}_1 + a_{21}\mathbf{e}_2|a_{12}\mathbf{e}_1 + a_{22}\mathbf{e}_2) \\
&= \det(a_{11}\mathbf{e}_1|a_{12}\mathbf{e}_1 + a_{22}\mathbf{e}_2) + \det(a_{21}\mathbf{e}_2|a_{12}\mathbf{e}_1 + a_{22}\mathbf{e}_2) = \\
&= \det(a_{11}\mathbf{e}_1|a_{12}\mathbf{e}_1) + \det(a_{11}\mathbf{e}_1|a_{22}\mathbf{e}_2) + \\
&\quad + \det(a_{21}\mathbf{e}_2|a_{12}\mathbf{e}_1) + \det(a_{21}\mathbf{e}_2|a_{22}\mathbf{e}_2) = \\
&= a_{11}a_{12}\det(\mathbf{e}_1|\mathbf{e}_1) + a_{11}a_{22}\det(\mathbf{e}_1|\mathbf{e}_2) + \\
&\quad + a_{21}a_{12}\det(\mathbf{e}_2|\mathbf{e}_1) + a_{21}a_{22}\det(\mathbf{e}_2|\mathbf{e}_2) = \\
&= a_{11}a_{22} - a_{21}a_{12}
\end{aligned}$$

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, je součástí přednášky z teorie míry ve druhém ročníku.

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 z 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 $\pi\pi^{-1} = \pi^{-1}\pi = \mathrm{id}_X$.

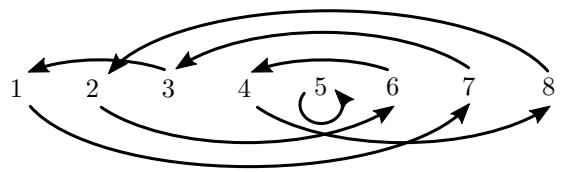
Tím pádem nemusíme při skládání psát závorky a také můžeme řešit jednoduché rovnice typu $\alpha\rho\beta = \gamma$, kde α, β, γ jsou dané permutace, podobným způsobem jako pro čísla, akorát musíme dát pozor na nekomutativitu.

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

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

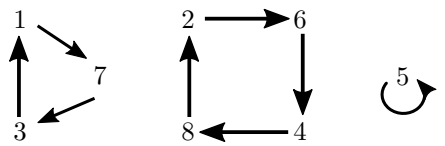
Tabulkou můžeme zapsat libovolné zobrazení z X do X (nebo i do jiné množiny). To, že π je permutace, se v tabulce projeví tak, že v druhém řádku bude každý prvek množiny X právě jednou.

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. Když graf trochu překreslíme, vidíme, že permutace je sjednocením nezávislých



Obrázek 7.6. Obrázek permutace

cyklů.



Obrázek 7.7. Lepší obrázek permutace

To není náhoda, každá permutace je složením nezávislých cyklů.

Definice 7.2. *Cyklus délky k* je permutace na X splňující $\pi(x_1) = x_2$, $\pi(x_2) = x_3$, ..., $\pi(x_{k-1}) = x_k$, $\pi(x_k) = x_1$ a $\pi(y) = y$ pro každé $y \in X \setminus \{x_1, x_2, \ldots, x_k\}$, kde x_1, x_2, ..., x_k jsou po dvou různé prvky X. Zapisujeme $\pi = (x_1\ x_2\ \ldots\ x_k)$.

Cykly nazýváme *nezávislé*, pokud jsou množiny prvků vyskytující se v cyklech disjunktní.

Transpozice je cyklus délky 2, tj. permutace tvaru $\pi = (x\ y)$.

Všimněte si, že pořadí prvků v cyklu můžeme cyklicky otočit a dostaneme stejnou permutaci:

$$(x_1\ x_2\ \dots\ x_k) = (x_2\ \dots\ x_k\ x_1) = \dots = (x_k\ x_1\ x_2\ \dots\ x_{k-1})$$

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 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 7 a permutace ρ prvek 7 zobrazí na 4, takže složená permutace $\rho\pi$ zobrazí prvek 1 na prvek 4, tj. za 1 napíšeme číslo 4. Číslo 4 permutace π zobrazí na 8 a permutace ρ zobrazí číslo 8 na 2, takže píšeme 2, 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 $\rho\pi$. Má ale stejnou strukturu – má stejně jako $\rho\pi$ 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.

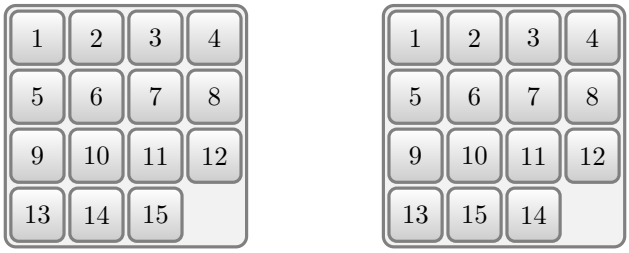
(1) Identická permutace má 0 cyklů sudé délky.
(2) Inverzní permutace má stejný počet cyklů sudé délky.
(3) Pokud π lze zapsat jako složení k transpozic, tj. $\operatorname{sgn}(\pi) = (-1)^k$, a ρ lze zapsat jako složení l transpozic, tj. $\operatorname{sgn}(\rho) = (-1)^l$, pak $\pi\rho$ lze zapsat 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.

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



Obrázek 7.8. Hra 15

$\pi(i) = j$, 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 $(16\ i)\pi$.

Obarvíme ještě desku hlavolamu dvěma barvami jako šachovnici 4×4, tj. aby bílé místo vždy hranově sousedilo pouze s černými místy a naopak. Zvolme třeba obarvení, kdy levý horní roh (a také pravý dolní) je bílý.

Budeme si všímat parity permutace π a barvy prázdného políčka. Na začátku vyjdeme z pozice odpovídající liché permutaci (14 15) a prázdné políčko je bílé. Po provedení jednoho tahu permutace π změní paritu a rovněž se změní barva prázdného políčka, protože bílá místa sousedí pouze s černými a naopak. Z toho plyne, že

- po provedení sudého počtu tahů bude π lichá a prázdné políčko bude bílé;
- po provedení lichého počtu tahů bude π sudá a prázdné políčko bude černé.

Ani v jednom z obou případů nemůžeme získat základní pozici, pro kterou je permutace π sudá (je to identická permutace) a prázdné políčko je bílé. ▲

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

$$\begin{vmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{vmatrix} = \cos^2(\alpha) + \sin^2(\alpha) = 1 \ ,$$

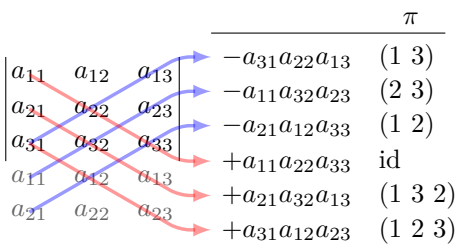
což není překvapivé, protože rotace o α nemění ani obsah ani orientaci.

(Při zápisu determinantu pomocí svislých čar vynecháváme kulaté závorky.) ▲

PŘÍKLAD 7.16. V případě $n = 3$ máme šest permutací v S_3 – identická permutace a trojcykly jsou sudé, transpozice jsou liché. Odpovídající sčítanci jsou:

π	
id	$a_{11}a_{22}a_{33}$
(1 2 3)	$a_{21}a_{32}a_{13}$
(1 3 2)	$a_{31}a_{12}a_{23}$
(2 3)	$-a_{11}a_{32}a_{23}$
(1 3)	$-a_{31}a_{22}a_{13}$
(1 2)	$-a_{21}a_{12}a_{33}$

a opět dostáváme vzorec odvozený výše. Mnemotechnickou pomůckou je tzv. *Sarrusovo pravidlo* na obrázku.



OBRÁZEK 7.9. Sarrusovo pravidlo

▲

Počítat matice z definice není vhodné už pro matice řádu 3, je lepší využít jiné metody. Sarrusovo pravidlo tedy nebudeme používat. V případě $n = 4$ má již výraz 24 členů (vypište je jako cvičení) a definice je pro výpočet již zcela nevhodná. Všimněte si, že **pravidlo podobné Sarrusovu pro matice řádu $n > 3$ neplatí**.

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* $\det(A) = a_{11}a_{22}\dots a_{nn}$.

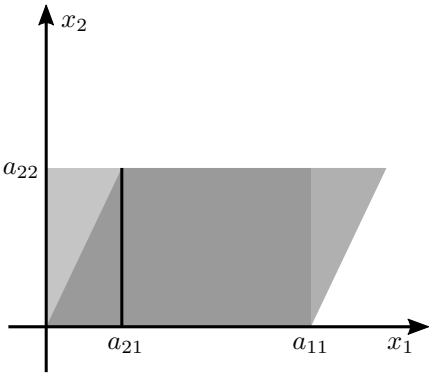
DŮKAZ. Podívejme se na jeden sčítanec $\operatorname{sgn}(\pi)a_{\pi(1),1}a_{\pi(2),2}\dots a_{\pi(n),n}$ v definici determinantu. Pokud je jeden z činitelů v tomto součinu nulový, celý sčítanec je roven nule a můžeme jej ignorovat. První sloupec matice A je celý nulový, až na hodnotu a_{11}, která může být nenulová. Pokud tedy $\pi(1) > 1$, pak $a_{\pi(1),1} = 0$ a sčítanec je nulový. Předpokládejme proto $\pi(1) = 1$. Podobně, pokud $\pi(2) > 2$ můžeme na sčítanec zapomenout, protože $a_{\pi(2),2} = 0$. Takže můžeme předpokládat $\pi(2) \leq 2$. Ale $\pi(2)$ nemůže být 1, protože máme $\pi(1) = 1$ a π je prosté zobrazení, čili $\pi(2) = 2$. Postupně dostáváme $\pi(3) = 3$, $\pi(4) = 4$, ..., $\pi(n) = n$.

Jediný možný 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 7.10. 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.

Podobně bychom mohli dokázat, že determinant dolní trojúhelníkové matice je součin prvků na diagonále. Dělat to ale nebudeme, dokážeme obecněji, že determinant se nezmění transponováním.

TVRZENÍ 7.18. *Pro libovolnou čtvercovou matici A platí* $\det(A) = \det\left(A^T\right)$.



Obrázek 7.10. Determinant dolní trojúhelníkové matice řádu 2

Důkaz. Sčítanec v definici $\det\left(A^T\right)$ odpovídající permutaci π je

$$\operatorname{sgn}(\pi) a_{1,\pi(1)} a_{2,\pi(2)} \dots a_{n,\pi(n)} \quad .$$

Součin lze přeuspořádat na

$$\operatorname{sgn}(\pi) a_{\pi^{-1}(1),1} a_{\pi^{-1}(2),2} \dots a_{\pi^{-1}(n),n} \quad ,$$

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

$$\det(A) = \sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{1,\pi(1)} a_{2,\pi(2)} \dots a_{n,\pi(n)} \quad ,$$

což je trochu tradičnější verze definice.

Tvrzení se hodí 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 $\mathbf{u} = (b_1, b_2, \dots, b_n)^T$, platí

$$\begin{aligned}
&\det(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_{i-1}|\ \mathbf{v}_i + \mathbf{u}\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n)\\
&= \sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(i-1),i-1}(a_{\pi(i),i} + b_{\pi(i)}) a_{\pi(i+1),i+1} \dots a_{\pi(n),n}\\
&= \sum_{\pi\in S_n} (\operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(n),n} +\\
&\qquad + \operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(i-1),i-1} b_{\pi(i)} a_{\pi(i+1),i+1} \dots a_{\pi(n),n})\\
&= \sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(n),n}\\
&\qquad + \sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(i-1),i-1} b_{\pi(i)} a_{\pi(i+1),i+1} \dots a_{\pi(n),n}\\
&= \det(\mathbf{v}_1|\dots|\mathbf{v}_{i-1}|\ \mathbf{v}_i\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n) + \det(\mathbf{v}_1|\dots|\mathbf{v}_{i-1}|\ \mathbf{u}\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n)\ .
\end{aligned}$$

V úpravách jsme roznásobili závorku a rozdělili sumu na dvě části.

(2) K důkazu tohoto bodu stačí vytknout t před sumu:

$$\begin{aligned}
&\det(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_{i-1}|\ t\mathbf{v}_i\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n)\\
&= \sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(i-1),i-1}(t a_{\pi(i),i}) a_{\pi(i+1),i+1} \dots a_{\pi(n),n}\\
&= t \sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(n),n}\\
&= t\ \det(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n)\ .
\end{aligned}$$

(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 $a_{i,\rho(j)}$. Z toho plyne, že pro $\pi \in S_n$ a $k \in \{1, 2, \dots, n\}$ bude prvek na místě $(k, \pi(k))$ v matici $(\mathbf{v}_{\rho(1)}|\mathbf{v}_{\rho(2)}|\dots|\mathbf{v}_{\rho(n)})$ roven $a_{k,\rho(\pi(k))}$ (pozor, záleží tu na pořadí řeckých písmen). K rozepsání determinantu použijeme alternativní

definici.

$$\begin{aligned}
&\det\left(\mathbf{v}_{\rho(1)}|\mathbf{v}_{\rho(2)}|\dots|\mathbf{v}_{\rho(n)}\right)\\
&=\sum_{\pi\in S_n}\operatorname{sgn}(\pi)a_{1,\rho(\pi(1))}a_{2,\rho(\pi(2))}\cdots a_{n,\rho(\pi(n))}\\
&=\sum_{\pi\in S_n}\operatorname{sgn}(\rho)\operatorname{sgn}(\rho\pi)a_{1,\rho\pi(1)}a_{2,\rho\pi(2)}\cdots a_{n,\rho\pi(n)}\\
&=\operatorname{sgn}(\rho)\sum_{\pi\in S_n}\operatorname{sgn}(\rho\pi)a_{1,\rho\pi(1)}a_{2,\rho\pi(2)}\cdots a_{n,\rho\pi(n)}\\
&=\operatorname{sgn}(\rho)\sum_{\substack{\pi\in S_n\\ \sigma=\rho\pi}}\operatorname{sgn}(\sigma)a_{1,\sigma(1)}a_{2,\sigma(2)}\cdots a_{n,\sigma(n)}\\
&=\operatorname{sgn}(\rho)\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)a_{1,\sigma(1)}a_{2,\sigma(2)}\cdots a_{n,\sigma(n)}\\
&=\operatorname{sgn}(\rho)\det\left(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n\right)
\end{aligned}$$

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

$$\begin{aligned}
\det(B)=&\sum_{\pi\in S_n,\operatorname{sgn}(\pi)=1}\big(\operatorname{sgn}(\pi)b_{1,\pi(1)}b_{2,\pi(2)}\dots b_{n,\pi(n)}+\\
&\qquad+\operatorname{sgn}((i\ j)\pi)b_{1,(i\ j)\pi(1)}b_{2,(i\ j)\pi(2)}\dots b_{n,(i\ j)\pi(n)}\big)\\
=&\sum_{\pi\in S_n,\operatorname{sgn}(\pi)=1}\big(\operatorname{sgn}(\pi)b_{1,\pi(1)}b_{2,\pi(2)}\dots b_{n,\pi(n)}-\\
&\qquad-\operatorname{sgn}(\pi)b_{1,\pi(1)}b_{2,\pi(2)}\dots b_{n,\pi(n)}\big)\\
=&\ 0\ ,
\end{aligned}$$

kde jsme použili $\operatorname{sgn}((i\ j)\pi)=-\operatorname{sgn}(\pi)$ a fakt, že B má shodný i-tý a j-tý sloupec.

Tím jsem dokázali pomocné tvrzení a důkaz čtvrtého bodu snadno dokončíme užitím předchozích.

$$\begin{aligned}
&\det\left(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_{i-1}|\mathbf{v}_i+t\mathbf{v}_j|\mathbf{v}_{i+1}|\dots|\mathbf{v}_n\right)\\
&=\det\left(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n\right)+\det\left(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_{i-1}|\ t\mathbf{v}_j\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n\right)\\
&=\det\left(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n\right)+t\det\left(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_{i-1}|\ \mathbf{v}_j\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n\right)\\
&=\det\left(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n\right)
\end{aligned}$$

▲

Protože determinant matice se shoduje s determinantem transponované matice (tvrzení 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 rovnoběžník bude 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 je jeho obor hodnot 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 4.82 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 z 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 $R = E_1E_2\dots E_k$ (podle tvrzení 4.89), takže dostáváme

$$\begin{aligned}\det(RB) &= \det(E_1E_2\dots E_kB) = \det(E_1)\det(E_2\dots E_kB) = \dots \\ &= \det(E_1)\det(E_2)\dots\det(E_k)\det(B) = \dots = \det(R)\det(B)\end{aligned}$$

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 5.92 o hodnosti součinu: $\operatorname{rank}(AB) \le \operatorname{rank}(A) < n$. 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

$$1 = \det(I) = \det\left(AA^{-1}\right) = \det(A)\det\left(A^{-1}\right) \quad ,$$

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*

$$x_j = \frac{\det(A_j)}{\det(A)} \quad ,$$

kde A_j je matice, která vznikne z A nahrazením j-tého sloupce vektorem $\mathbf{b}$, tj.

$$A_j = (\mathbf{a}_1|\mathbf{a}_2|\dots|\mathbf{a}_{j-1}|\mathbf{b}|\mathbf{a}_{j+1}|\dots|\mathbf{a}_n) \quad .$$

Důkaz. Vztah $A\mathbf{x} = \mathbf{b}$ můžeme zapsat jako

$$x_1\mathbf{a}_1 + x_2\mathbf{a}_2 + \dots + x_n\mathbf{a}_n = \mathbf{b} \quad .$$

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 determinantu 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 $j \in \{1, 2, \dots, n\}$, pak*

$$\det(A) = \sum_{i=1}^{n} a_{ij} A_{ij} = a_{1j}A_{1j} + a_{2j}A_{2j} + \cdots + a_{nj}A_{nj} \ .$$

DŮKAZ. Potřebujeme dokázat, že koeficient u a_{ij}, vytkneme-li tento prvek ze všech členů, které jej obsahují, je rovný A_{ij}. Pro pohodlnost zvolíme trochu jiný postup důkazu.

1. krok. Pokud $a_{nn} = 1$ a všechny ostatní prvky v n-tém sloupci jsou nulové, pak $\det(A) = A_{nn}$.

Platí

$$\begin{aligned} \det(A) &= \sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(n),n} \\ &= \sum_{\pi \in S_n, \pi(n)=n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(n),n} \\ &= \sum_{\pi \in S_n, \pi(n)=n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(n-1),n-1} = \\ &= (-1)^{n+n} \sum_{\pi \in S_{n-1}} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(n-1),n-1} = A_{nn} \ . \end{aligned}$$

V druhé úpravě jsme vynechali nulové sčítance, ve třetí jsme použili $a_{nn} = 1$, ve čtvrté jsme použili $(-1)^{(n-1)+(n-1)} = 1$ a skutečnost, že znaménko permutace $\pi \in S_n$, pro kterou $\pi(n) = n$, je stejné jako znaménko permutace π zúžené na množinu $\{1, 2, \dots, n-1\}$ (to platí, protože tyto dvě permutace mají stejný redukovaný cyklický zápis).

2. krok. Pro libovolné $i, j \in \{1, 2, \dots, n\}$, pokud $a_{ij} = 1$ a všechny ostatní prvky v j-tém sloupci jsou nulové, pak $\det(A) = A_{ij}$.

Posuneme-li v matici A řádek i na poslední místo a potom sloupec j na poslední místo, dostaneme matici B, jejíž determinant je B_{nn} podle 1. kroku. Posunutí i-tého řádku na n-té místo odpovídá permutaci řádků $\sigma = (n\ (n-1)\ \dots\ i)$ a posunutí j-tého sloupce na n-té místo odpovídá permutaci sloupců $\rho = (n\ (n-1)\ \dots\ j)$. Podle bodu (3) tvrzení 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 $j, k \in \{1, 2, \ldots, n\}$, $j \neq k$, 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 5.94), 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 $\operatorname{adj}(A)$ stejného řádu, která má na místě (i, j) prvek A_{ji}.

Řádkovou i sloupcovou verzi vět o rozvoji a falešném rozvoji jde formulovat maticovým vztahem.

Věta 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.

$$\operatorname{adj}(A)=\begin{pmatrix} \begin{vmatrix} 4 & -2 \\ 2 & 5 \end{vmatrix} & -\begin{vmatrix} 1 & -3 \\ 2 & 5 \end{vmatrix} & \begin{vmatrix} 1 & -3 \\ 4 & -2 \end{vmatrix} \\ -\begin{vmatrix} 3 & -2 \\ 0 & 5 \end{vmatrix} & \begin{vmatrix} -2 & -3 \\ 0 & 5 \end{vmatrix} & -\begin{vmatrix} -2 & -3 \\ 3 & -2 \end{vmatrix} \\ \begin{vmatrix} 3 & 4 \\ 0 & 2 \end{vmatrix} & -\begin{vmatrix} -2 & 1 \\ 0 & 2 \end{vmatrix} & \begin{vmatrix} -2 & 1 \\ 3 & 4 \end{vmatrix} \end{pmatrix}$$

$$=\begin{pmatrix} 24 & -11 & 10 \\ -15 & -10 & -13 \\ 6 & 4 & -11 \end{pmatrix}$$

Determinant matice A by teď bylo neefektivní počítat zvlášť. Stačí spočítat například prvek na místě $(3,3)$ v součinu $A\operatorname{adj}(A)$.

$$\det(A)=0\cdot 10+2\cdot(-13)+5\cdot(-11)=-81.$$

Vidíme, že A je regulární a platí

$$A^{-1}=-\frac{1}{81}\begin{pmatrix} 24 & -11 & 10 \\ -15 & -10 & -13 \\ 6 & 4 & -11 \end{pmatrix}=\frac{1}{81}\begin{pmatrix} -24 & 11 & -10 \\ 15 & 10 & 13 \\ -6 & -4 & 11 \end{pmatrix}.$$

▲

7.5. Vandermondův determinant

Tzv. *Vandermondova matice* vzniká při interpolaci polynomem. Budeme hledat polynom f nad tělesem $\mathbf{T}$ stupně nejvýše $n-1$, tj.

$$f=k_0+k_1x+\dots+k_{n-1}x^{n-1},\quad k_0,k_1,\dots k_{n-1}\in T\ ,$$

který splňuje podmínky

$$f(a_1)=b_1,\ f(a_2)=b_2,\ \dots\ ,f(a_n)=b_n\ ,$$

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.

$$\begin{vmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^{n-1} \end{vmatrix} = \begin{vmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ 0 & a_2 - a_1 & a_2^2 - a_1^2 & \dots & a_2^{n-1} - a_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_n - a_1 & a_n^2 - a_1^2 & \dots & a_n^{n-1} - a_1^{n-1} \end{vmatrix}$$

$$= \begin{vmatrix} a_2 - a_1 & a_2^2 - a_1^2 & \dots & a_2^{n-1} - a_1^{n-1} \\ a_3 - a_1 & a_3^2 - a_1^2 & \dots & a_3^{n-1} - a_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_n - a_1 & a_n^2 - a_1^2 & \dots & a_n^{n-1} - a_1^{n-1} \end{vmatrix}$$

Nyní přičteme $(-a_1)$-násobek předposledního sloupce k poslednímu, ..., $(-a_1)$-násobek druhého sloupce ke třetímu, a nakonec $(-a_1)$-násobek prvního sloupce ke druhému. Dostaneme matici

$$\begin{vmatrix} a_2 - a_1 & a_2(a_2 - a_1) & a_2^2(a_2 - a_1) & \dots & a_2^{n-2}(a_2 - a_1) \\ a_3 - a_1 & a_3(a_3 - a_1) & a_3^2(a_3 - a_1) & \dots & a_3^{n-2}(a_3 - a_1) \\ \vdots & \vdots & \ddots & \vdots & \\ a_n - a_1 & a_n(a_n - a_1) & a_n^2(a_n - a_1) & \dots & a_n^{n-2}(a_n - a_1) \end{vmatrix}$$

Vytkneme z prvního řádku výraz $a_2 - a_1$, z druhého výraz $a_3 - a_1$, atd., čímž dostaneme rekurentní vztah

$$V(a_1, \dots, a_n) = (a_2 - a_1)(a_3 - a_1) \dots (a_n - a_1) V(a_2, \dots, a_n)$$

a užitím indukčního předpokladu odvodíme

$$V(a_1, \dots, a_n) = (a_2 - a_1)(a_3 - a_1) \dots (a_n - a_1) \prod_{2 \le i < j \le n} a_j - a_i = \prod_{1 \le i < j \le n} a_j - a_i$$

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 $\prod_{1 \le i < j \le n} a_j - a_i$.

7.6. Orientace vektorového prostoru

Při odvození vzorce pro determinant v sekci 7.1 jsme intuitivně používali pojem orientace, který teď přesněji zavedeme.

Definice 7.41. Dvě báze B a B' reálného vektorového prostoru $\mathbf{V}$ dimenze n nazýváme *souhlasně orientované*, pokud je determinant matice přechodu $[\mathrm{id}]_{B'}^{B}$ kladný. V opačném případě říkáme, že báze jsou *nesouhlasně orientované*.

Relace souhlasné orientovanosti je reflexivní, protože $\det\left([\mathrm{id}]_B^B\right) = \det(I_n) = 1$, symetrická, protože $\det\left([\mathrm{id}]_{B'}^{B}\right) = (\det\left([\mathrm{id}]_B^{B'}\right))^{-1}$, a tranzitivní, protože

$$\det\left([\mathrm{id}]_{B'}^{B}\right) \det\left([\mathrm{id}]_{B''}^{B'}\right) = \det\left([\mathrm{id}]_{B''}^{B}\right).$$

Tato relace je tedy ekvivalencí na množině bází vektorového prostoru $\mathbf{V}$. Množina matic se tímto rozpadá na dvě disjunktní třídy. Každá z nich sestává se souhlasně orientovaných bází a dvě báze patřící do různých tříd jsou orientované nesouhlasně.

OBRAZEK

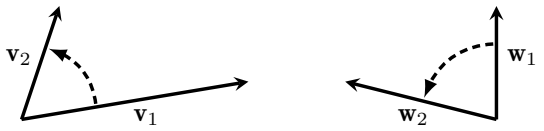
Definice 7.42. *Orientací* vektorového prostoru $\mathbf{V}$ rozumíme výběr jedné ze tříd ekvivalence relace souhlasné orientovanosti. Báze v této třídě nazveme *kladně orientované* a ve druhé třídě *záporně orientované*. Vektorový prostor spolu s volbou orientace nazýváme *orientovaný vektorový prostor*.

Volba orientace umožňuje pro každou nadrovinu $\mathrm{LO}\{\mathbf{v}_1, \dots, \mathbf{v}_{n-1}\}$ rozdělit prostor na „dvě strany“. Vektory $\mathbf{v}_n$, pro něž je báze $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ kladně orientovaná tvoří jednu stranu a vektory, pro něž $\mathbf{v}_n$ je báze $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ tvoří druhou stranu. Vektory $\mathbf{v}_n$, pro které $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ není báze, jsou právě vektory hraniční nadroviny $\mathrm{LO}\{\mathbf{v}_1, \dots, \mathbf{v}_{n-1}\}$.

OBRAZEK

Z definice 7.41 souhlasné orientace vyplývá, že zaměníme-li jeden vektor v bázi za opačný, kladně orientované báze se změní na záporně orientovanou a naopak (protože determinant v definici bude -1). Orientace báze se rovněž změní, pokud prohodíme dva vektory v bázi (determinant bude opět -1).

V prostoru dimenze 2 si také můžeme orientaci představit jako volbu kladného směru otáčení. Dvě báze $(\mathbf{v}_1, \mathbf{v}_2)$ a $(\mathbf{w}_1, \mathbf{w}_2)$ jsou souhlasně orientované právě tehdy, když „směr otáčení“ od $\mathbf{v}_1$ k $\mathbf{v}_2$ je stejný jako „směr otáčení“ od $\mathbf{w}_1$ k $\mathbf{w}_2$.



Obrázek 7.11. Souhlasně orientované báze $(\mathbf{v}_1, \mathbf{v}_2)$ a $(\mathbf{w}_1, \mathbf{w}_2)$ v $\mathbb{R}^2$ mají stejný směr otáčení.

V našem fyzikálním trojrozměrném prostoru se orientace často volí tzv. *pravidlem pravé ruky*. Ukazovák, prostředník ohnutý kolmo k dlani a palec (v tomto pořadí) udávají kladnou orientaci.

OBRAZEK

V aritmetických vektorových prostorech $\mathbb{R}^n$ je přirozené definovat kanonickou bázi jako kladně orientovanou. Báze $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ je pak kladně orientovaná právě tehdy, když je determinant $\det\left([\mathrm{id}]^B_{K_n}\right) = \det(\mathbf{v}_1 | \dots | \mathbf{v}_n)$ kladný.

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 $\mathrm{sgn}(\pi) = (-1)^{n+k}$.

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 $X = \{1, 2, \dots, n\}$, 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 id_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 $y \in X \setminus \{x_1, x_2, \dots, x_k\}$, kde x_1, x_2, ..., x_k jsou po dvou různé prvky X. Zapisujeme $\pi = (x_1\ x_2\ \dots\ x_k)$.

(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 množině 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 $i, j \in \{1, 2, \ldots, n\}$, pak *algebraickým doplňkem* (též *kofaktorem*) prvku a_{ij} matice A rozumíme skalár

$$m_{ij} = (-1)^{i+j} \det(M_{ij}) \quad ,$$

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 $j \in \{1, 2, \ldots, n\}$, pak

$$\det(A) = \sum_{i=1}^{n} a_{ij} m_{ij} = a_{1j} m_{1j} + a_{2j} m_{2j} + \cdots + a_{nj} m_{nj} \quad .$$

(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 $j, k \in \{1, 2, \ldots, n\}$, $j \neq k$, pak

$$0 = \sum_{i=1}^{n} a_{ij} m_{ik} = a_{1j} m_{1k} + a_{2j} m_{2k} + \cdots + a_{nj} m_{nk} \quad .$$

(38) Pro libovolnou čtvercovou matici A platí

$$\operatorname{adj}(A)\, A = A \operatorname{adj}(A) = \det(A)\, I_n \quad .$$

Speciálně, pokud A je regulární, pak

$$A^{-1} = \frac{\operatorname{adj}(A)}{\det(A)} \quad .$$

(39) Úloha na nalezení polynomu stupně nejvýše $n-1$ s koeficienty v tělese $\mathbf{T}$, který má předepsané hodnoty v n bodech $a_1, a_2, \ldots, a_n \in \mathbf{T}$ vede na řešení soustavy lineární rovnic a maticí

$$\begin{pmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \ldots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \ldots & a_n^{n-1} \end{pmatrix} \quad .$$

(40) Tato matice se nazývá *Vandermondova matice* a její determinant *Vandermondův determinant* určený prvky $a_1, a_2, \ldots, a_n$.

(41) Hodnota Vandermondova determinantu určeného prvky $a_1, a_2, \ldots, a_n$ je

$$\prod_{1 \le i < j \le n} a_j - a_i \quad .$$

(42) Vandermondova matice určená prvky $a_1, a_2, \ldots, a_n$ je regulární právě když jsou prvky $a_1, a_2, \ldots, a_n$ 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 $\det(A) = \det\left(A^T\right)$, determinant trojúhelníkové matice.

(5) Vliv elementárních úprav matice na hodnotu jejího determinantu.
(6) Determinant součinu je součin determinantů (pro čtvercové matice stejných řádů).
(7) Matice je regulární právě když má nenulový determinant.
(8) Věta o rozvoji determinantu podle řádku nebo podle sloupce.

KAPITOLA 8

Skalární součin

Cíl. *Pomocí skalárního součinu počítáme v reálných nebo komplexních vektorových prostorech velikosti vektorů a úhly mezi nimi. Významnou aplikací skalárního součinu je hledání dobrých aproximací vektorů v podprostoru, což umožňuje například hledat rozumná „řešení“ neřešitelných soustav vektorových rovnic nebo aproximovat funkci jednoduššími funkcemi.*

V abstraktním vektorovém prostoru nemáme metrické pojmy jako délka vektoru nebo úhel mezi dvěma vektory (co například znamená délka funkce nebo matice?). Tyto pojmy zavedeme přidáním skalárního součinu. Nejprve se podíváme na důležitý příklad skalárního součinu v aritmetických vektorových prostorech nad $\mathbb{R}$ a nad $\mathbb{C}$ – *standardní skalární součin.*

8.1. Standardní skalární součin v $\mathbb{R}^n$ a $\mathbb{C}^n$

8.1.1. Motivace. Standardní skalární součin dvou reálných n-složkových aritmetických vektorů (tj. prvků $\mathbb{R}^n$) je reálné číslo definované jednoduchou formulkou, viz definice 8.4. Pomocí standardního skalárního součinu pak *definujeme* eukleidovskou délku vektoru a úhel mezi vektory.

Abychom se přesvědčili, že takto definované pojmy jsou v souladu s geometrickou intuicí v prostorech $\mathbb{R}^2$ a $\mathbb{R}^3$ (a $\mathbb{R}$), budeme na chvíli předpokládat znalosti elementární geometrie a zavedeme standardní skalární součin $\mathbf{u} \cdot \mathbf{v}$ aritmetických vektorů $\mathbf{u}, \mathbf{v} \in \mathbb{R}^2$ (nebo $\mathbf{u}, \mathbf{v} \in \mathbb{R}^3$) alternativně, a to pro nenulové vektory vztahem

$$\mathbf{u} \cdot \mathbf{v} = \|\mathbf{u}\| \, \|\mathbf{v}\| \, \cos\alpha \ ,$$

kde $\|\mathbf{u}\|$, $\|\mathbf{v}\|$ značí délky vektorů $\mathbf{u}$, $\mathbf{v}$ a α je úhel, který tyto vektory svírají. Pokud je jeden z vektorů $\mathbf{u}$, $\mathbf{v}$ nulový, definujeme $\mathbf{u} \cdot \mathbf{v} = 0$. Všimněte si, že jsou-li dva nenulové vektory rovnoběžné a souhlasně orientované (tj. jeden je kladným násobkem druhého), pak je jejich standardní skalární součin roven součinu délek, a jsou-li na sebe kolmé, pak je jejich součin roven 0.

Pomocí tohoto pojmu lze vyjádřit délku vektoru i úhel mezi dvěma vektory. Z uvedeného vztahu totiž vyplývá, že délka vektoru $\mathbf{u}$ je $\sqrt{\mathbf{u} \cdot \mathbf{u}}$ a úhel mezi nenulovými vektory $\mathbf{u}$ a $\mathbf{v}$ je ten úhel $\alpha \in [0, \pi]$, pro který platí $\cos\alpha = (\mathbf{u} \cdot \mathbf{v})/(\|\mathbf{u}\| \, \|\mathbf{v}\|)$. Podstatnější výhody jsou, že standardní skalární součin lze spočítat jednoduchým vzorcem a má příjemné vlastnosti, zejména linearitu (viz tvrzení 8.6), které značně usnadňují výpočty.

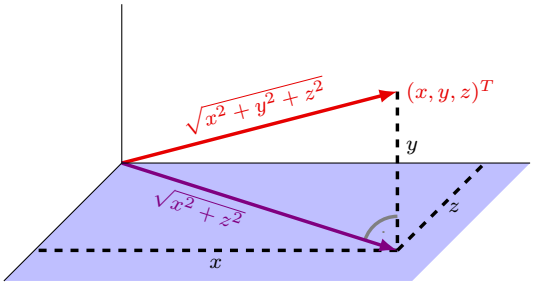
Předvedeme dvě odvození zmíněného jednoduchého vzorce v dimenzi 2. Označíme $\mathbf{u} = (x_1, x_2)^T$ a $\mathbf{v} = (y_1, y_2)^T$ a ukážeme

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = x_1 y_1 + x_2 y_2.$$

První odvození využívá Pythagorovu větu a kosinovou větu. Z Pythagorovy věty vidíme

$$\|\mathbf{u}\| = \sqrt{x_1^2 + x_2^2}, \quad \|\mathbf{v}\| = \sqrt{y_1^2 + y_2^2}, \quad \|\mathbf{u} - \mathbf{v}\| = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2} \ .$$

(Obrázek znázorňuje situaci v dimenzi 3.)



Obrázek 8.1. Eukleidovská norma v $\mathbb{R}^3$

Je-li $(\mathbf{u}, \mathbf{v})$ lineárně nezávislá posloupnost, pak podle kosinové věty použité pro trojúhelník o stranách $\mathbf{u}$, $\mathbf{v}$ a $\mathbf{u} - \mathbf{v}$ platí

$$\|\mathbf{u} - \mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2\,\|\mathbf{u}\|\,\|\mathbf{v}\|\,\cos\alpha \ .$$

Stejný vztah platí i pro případ, že $(\mathbf{u}, \mathbf{v})$ je lineárně závislá posloupnost, jak se snadno přesvědčíte.

OBRAZEK N1 - kosinova veta

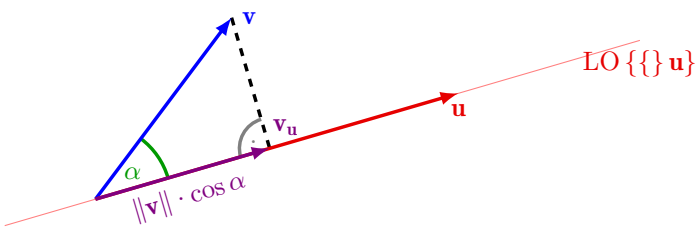
Dosazením a úpravou nyní dostáváme

$$\begin{aligned} 2\,\|\mathbf{u}\|\,\|\mathbf{v}\|\,\cos\alpha &= -\,\|\mathbf{u} - \mathbf{v}\|^2 + \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 \\ &= -(x_1 - y_1)^2 - (x_2 - y_2)^2 + (x_1^2 + x_2^2) + (y_1^2 + y_2^2) \\ &= 2x_1y_1 + 2x_2y_2 \ , \end{aligned}$$

což je po vydělení 2 to, co jsme chtěli. V dimenzi 3 by se analogický vztah ukázal podobně.

Druhé odvození je o něco delší, ale jinak má řadu výhod. Nevyužívá Pythagorovu ani kosinovou větu, je podobné odvození vzorce pro determinant a poskytne nám další důležitý geometrický význam standardního skalárního součinu.

Tímto geometrickým významem začneme. Budeme uvažovat případ, že oba vektory $\mathbf{u}, \mathbf{v}$ jsou nenulové. Výraz $\|\mathbf{v}\|\cos\alpha$ udává orientovanou délku kolmé (též zvané ortogonální nebo pravoúhlé) projekce vektoru $\mathbf{v}$ na přímku LO $\{\mathbf{u}\}$, přičemž znaménko je kladné, pokud vektory $\mathbf{u}$ a $\mathbf{v}$ svírají ostrý úhel, a je záporné pokud svírají tupý úhel.



Obrázek 8.2. Geometrický význam standardního skalárního součinu

Na $\mathbf{u} \cdot \mathbf{v}$ se tedy můžeme dívat jako na součin délky vektoru $\mathbf{u}$ a orientované délky kolmé projekce vektoru $\mathbf{v}$ na přímku LO $\{\mathbf{u}\}$. Symetricky, $\mathbf{u} \cdot \mathbf{v}$ je rovno součinu délky vektoru $\mathbf{v}$ a orientované délky kolmé projekce vektoru $\mathbf{u}$ na přímku LO $\{\mathbf{v}\}$.

Z toho můžeme nahlédnout (viz obrázek), že skalární součin je lineární v první proměnné, tj. pro libovolné $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w} \in \mathbb{R}^2$ (i nulové) a $t \in \mathbb{R}$ platí

$$(t\mathbf{u}) \cdot \mathbf{v} = t(\mathbf{u} \cdot \mathbf{v}), \quad (\mathbf{u} + \mathbf{v}) \cdot \mathbf{w} = \mathbf{u} \cdot \mathbf{w} + \mathbf{v} \cdot \mathbf{w} \ .$$

OBRAZEK N4 - linearita

Ze symetrie nebo z podobného obrázku získáme linearitu v druhé proměnné:

$$\mathbf{u} \cdot (t\mathbf{v}) = t(\mathbf{u} \cdot \mathbf{v}), \quad \mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w} \ .$$

Vlastnosti linearity a symetrie budeme požadovat pro každý skalární součin na $\mathbb{R}^2$. Standardní skalární součin se vyděluje tím, že vektory $\mathbf{e}_1, \mathbf{e}_2$ kanonické báze jsou na sebe kolmé a mají jednotkovou délku, takže

$$\mathbf{e}_1 \cdot \mathbf{e}_2 = \mathbf{e}_2 \cdot \mathbf{e}_1 = 0, \quad \mathbf{e}_1 \cdot \mathbf{e}_1 = 1, \quad \mathbf{e}_2 \cdot \mathbf{e}_2 = 1 \ .$$

Nyní již odvozovaný vztah dostaneme přímočarým výpočtem:

$$\begin{aligned}
\mathbf{u} \cdot \mathbf{v} &= (x_1\mathbf{e}_1 + x_2\mathbf{e}_2) \cdot (y_1\mathbf{e}_1 + y_2\mathbf{e}_2) \\
&= (x_1\mathbf{e}_1) \cdot (y_1\mathbf{e}_1 + y_2\mathbf{e}_2) + (x_2\mathbf{e}_2) \cdot (y_1\mathbf{e}_1 + y_2\mathbf{e}_2) \\
&= (x_1\mathbf{e}_1) \cdot (y_1\mathbf{e}_1) + (x_1\mathbf{e}_1) \cdot (y_2\mathbf{e}_2) + (x_2\mathbf{e}_2) \cdot (y_1\mathbf{e}_1) + (x_2\mathbf{e}_2) \cdot (y_2\mathbf{e}_2) \\
&= x_1y_1(\mathbf{e}_1 \cdot \mathbf{e}_1) + x_1y_2(\mathbf{e}_1 \cdot \mathbf{e}_2) + x_2y_1(\mathbf{e}_2 \cdot \mathbf{e}_1) + x_2y_2(\mathbf{e}_2 \cdot \mathbf{e}_2) \\
&= x_1y_1 + x_2y_2 \ .
\end{aligned}$$

Drobnou úpravou postupu bychom odvodili analogický vzorec pro standardní skalární součin v $\mathbb{R}^3$.

Závěrem motivační části několik příkladů.

Příklad 8.1. Standardní skalární součin můžeme využít k novému náhledu na rovnici přímky v rovině. Máme-li dánu rovnici

$$a_1x_1 + a_2x_2 = b \ ,$$

ve které je aspoň jeden z koeficientů a_1, a_2 nenulový, množina všech řešení $(x_1, x_2)^T \in \mathbb{R}^2$ tvoří nějakou přímku v rovině. Označíme-li $\mathbf{a} = (a_1, a_2)^T$ a $\mathbf{x} = (x_1, x_2)^T$, můžeme rovnici přímky pomocí standardního skalárního součinu přepsat do tvaru

$$\mathbf{a} \cdot \mathbf{x} = b \ .$$

Použijeme rovnost $\mathbf{a} \cdot \mathbf{x} = \|\mathbf{a}\| \, \|\mathbf{x}\| \cos\alpha$, kde α je úhel, který svírají vektory $\mathbf{a}$ a $\mathbf{x}$. Protože $\mathbf{a} \neq \mathbf{o}$, platí $\|\mathbf{a}\| \neq 0$ a poslední rovnici můžeme přepsat do tvaru

$$\|\mathbf{x}\| \cos\alpha = \frac{b}{\|\mathbf{a}\|} \ .$$

Na levé straně dostáváme orientovanou délku kolmé projekce proměnného vektoru $\mathbf{x}$ do směru vektoru $\mathbf{a}$, zatímco pravá strana závisí pouze na koeficientech rovnice $a_1x_1 + a_2x_2 = b$ a je tedy konstantní. Množinu všech řešení rovnice tak tvoří vektory, které mají daný průmět do směru vektoru $\mathbf{a}$. Z toho vidíme, že množina všech řešení rovnice $a_1x_1 + a_2x_2 = b$ tvoří přímku v rovině kolmou na vektor $\mathbf{a}$, pokud je aspoň jeden z koeficientů a_1, a_2 nenulový. Vektor $\mathbf{a}$ se nazývá *normálový vektor* této přímky.

OBRAZEK N3 - přímka s normálovým vektorem

To, že vektor $\mathbf{a}$ je kolmý na směrové vektory přímky můžeme také vidět následujícím způsobem. Víme, že vektor $\mathbf{y} = (y_1, y_2)^T$ je směrový vektor přímky s rovnicí $a_1x_1 + a_2x_2 = b$ právě tehdy, když řeší příslušnou homogenní „soustavu“ (jedné rovnice o dvou neznámých) $a_1y_1 + a_2y_2 = 0$. Levá strana je ale rovná $\mathbf{a} \cdot \mathbf{y}$. ▲

Pomocí standardního skalárního součinu můžeme také snadno najít rovnici přímky v rovině procházející dvěma různými body.

PŘÍKLAD 8.2. Najdeme rovnici $a_1x_1 + a_2x_2 = b$ přímky l v rovině procházející body $P = (1, 3)$ a $Q = (2, 1)$. Vektor $\mathbf{u}$ s počátečním bodem P a koncovým bodem Q je rovnoběžný s přímkou l, má souřadnice $(2, 1)^T - (1, 3)^T = (1, -2)^T$ a je kolmý na libovolný normálový vektor přímky l. Za normálový vektor tedy můžeme zvolit například $\mathbf{a} = (2, 1)^T$. Tím jsme našli koeficienty $a_1 = 2$ a $a_2 = 1$ rovnice přímky l. Ta se tedy rovná $2x_1 + 1x_2 = b$ a souřadnice $(1, 3)^T$ bodu P ji musí splňovat. Číslo b se proto rovná $b = 2 \cdot 1 + 1 \cdot 3 = 5$. Jedna z možných rovnic přímky l je tedy $2x_1 + x_2 = 5$.

V první kapitole jsme rovnici přímky procházející dvěma různými body hledali pomocí parametrického tvaru přímky. Přímý postup využívající skalární součin je mnohem rychlejší. ▲

PŘÍKLAD 8.3. Podobně jako v rovině vyjádříme také v prostoru množinu všech řešení rovnice

$$a_1x_1 + a_2x_2 + a_3x_3 = b$$

pomocí skalárního součinu ve tvaru

$$\mathbf{a} \cdot \mathbf{x} = b \ .$$

Je-li aspoň jeden z koeficientů a_1, a_2, a_3 nenulový, je vektor $\mathbf{a} = (a_1, a_2, a_3)^T$ nenulový a vektor neznámých $\mathbf{x} = (x_1, x_2, x_3)^T$ splňuje rovnici

$$\|\mathbf{x}\| \cos\alpha = \frac{b}{\|\mathbf{a}\|} \ .$$

Vektor $\mathbf{x} = (x_1, x_2, x_3)^T$ je tedy řešením rovnice $a_1x_1 + a_2x_2 + a_3x_3 = b$ právě tehdy, když je orientovaná délka jeho kolmé projekce do směru vektoru $\mathbf{a}$ rovná $b/\|\mathbf{a}\|$. Množinou řešení je proto rovina kolmá na vektor $\mathbf{a}$, který opět nazýváme *normálový*.

Uvědomíme si ještě, jaký vektor $\mathbf{z}$ je pravoúhlou projekcí vektoru $\mathbf{x}$ do směru vektoru $\mathbf{a}$. Víme, že délka vektoru $\mathbf{z}$ je $|b|/\|\mathbf{a}\|$ a tento vektor je nezáporným násobkem vektoru $\mathbf{a}$, pokud $b/\|\mathbf{a}\| \geq 0$, a záporným násobkem $\mathbf{a}$, pokud $b/\|\mathbf{a}\| < 0$. Protože vektor $\mathbf{a}/\|\mathbf{a}\|$ má stejný směr jako $\mathbf{a}$ a jednotkovou délku, vidíme, že v obou případech platí

$$\mathbf{z} = \frac{b}{\|\mathbf{a}\|} \frac{\mathbf{a}}{\|\mathbf{a}\|} = \frac{b}{\|\mathbf{a}\|^2} \mathbf{a} \ .$$

Množinu řešení rovnice $a_1x_1 + a_2x_2 + a_3x_3 = b$ můžeme tedy přesněji popsat jako množinu těch vektorů, jejichž kolmá projekce na přímku $\mathrm{LO}\{\mathbf{a}\}$ je rovná vektoru $(b/\|\mathbf{a}\|^2)\mathbf{a}$. ▲

8.1.2. Standardní skalární součin v $\mathbb{R}^n$. Motivační úvahy snad čtenáře přesvědčily o smysluplnosti následujících definic.

DEFINICE 8.4. Pro dva n-složkové aritmetické vektory $\mathbf{u} = (x_1, x_2, \ldots, x_n)^T$, $\mathbf{v} = (y_1, y_2, \ldots, y_n)^T \in \mathbb{R}^n$ definujeme jejich *standardní skalární součin* jako reálné číslo

$$\mathbf{u} \cdot \mathbf{v} = x_1y_1 + x_2y_2 + \cdots + x_ny_n \ .$$

Všimněme si, že standardní skalární součin lze napsat pomocí maticového součinu

$$\mathbf{u} \cdot \mathbf{v} = \mathbf{u}^T \mathbf{v} \ ,$$

kde řádkový vektor $\mathbf{u}^T$ chápeme jako matici typu $1 \times n$, sloupcový vektor $\mathbf{v}$ chápeme jako matici typu $n \times 1$ a výslednou matici $\mathbf{u}^T\mathbf{v}$ typu 1×1 ztotožňujeme s jejím jediným prvkem.

Pomocí standardního skalárního součinu definujeme eukleidovskou délku (též zvanou normu) vektoru $\mathbf{u} \in \mathbb{R}^n$.

Definice 8.5. *Eukleidovská norma* nebo také *eukleidovská délka* vektoru $\mathbf{u} \in \mathbb{R}^n$ je číslo

$$\|\mathbf{u}\| = \sqrt{\mathbf{u} \cdot \mathbf{u}} \ .$$

Eukleidovskou normu vektoru $\mathbf{u} = (x_1, x_2, \ldots, x_n)^T$ lze také psát

$$\|\mathbf{u}\| = \sqrt{\mathbf{u}^T \mathbf{u}} = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2} \ .$$

Pro $n = 2$ a $n = 3$ jde o stejný vzorec, který v elementární geometrii plyne z Pythagorovy věty. Pro $n = 1$ dostáváme $\|\mathbf{u}\| = \|(x_1)\| = |x_1|$.

Úhel mezi nenulovými vektory $\mathbf{u}$ a $\mathbf{v}$ z $\mathbb{R}^n$ definujeme jako to jednoznačně určené reálné číslo $\alpha \in [0, \pi]$, které splňuje

$$\mathbf{u} \cdot \mathbf{v} = \|\mathbf{u}\| \ \|\mathbf{v}\| \ \cos\alpha \ .$$

To, že takové číslo existuje, vyplývá z Cauchyho-Schwarzovy nerovnosti, kterou ve větě 8.33 dokážeme obecněji. Dva vektory nazýváme *kolmé* (nebo *ortogonální*), pokud $\mathbf{u} \cdot \mathbf{v} = 0$. V definici kolmosti můžou být vektory nulové; nulový vektor je podle této definice kolmý ke všem vektorům.

Základní algebraické vlastnosti standardního skalárního součinu shrnuje následující tvrzení. Jejich geometrický význam byl vysvětlený v předchozí části.

Tvrzení 8.6. *Jsou-li* $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{R}^n$ *libovolné reálné aritmetické vektory a* $t \in \mathbb{R}$ *skalár, pak platí*

(1) $\mathbf{u} \cdot \mathbf{v} = \mathbf{v} \cdot \mathbf{u}$,
(2) $\mathbf{u} \cdot (t\mathbf{v}) = t(\mathbf{u} \cdot \mathbf{v})$,
(3) $\mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w}$,
(4) $\mathbf{u} \cdot \mathbf{u} \geq 0$, *a* $\mathbf{u} \cdot \mathbf{u} = 0$ *právě když* $\mathbf{u} = \mathbf{o}$.

Důkaz. Všechna tvrzení plynou okamžitě z definice standardního skalárního součinu. K výpočtům je výhodné používat maticový zápis. Například třetí vlastnost ověříme výpočtem

$$\mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{u}^T(\mathbf{v} + \mathbf{w}) = \mathbf{u}^T\mathbf{v} + \mathbf{u}^T\mathbf{w} = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w} \ ,$$

použili jsme pouze distributivitu násobení matic vzhledem k jejich sčítání.

Poslední tvrzení plyne z toho, že pro $\mathbf{u} = (x_1, x_2, \ldots, x_n)^T$ platí

$$\mathbf{u} \cdot \mathbf{u} = \mathbf{u}^T\mathbf{u} = x_1^2 + x_2^2 + \cdots + x_n^2 \ .$$

▲

První rovnost se nazývá *symetrie*, další dvě rovnosti říkají, že standardní skalární součin je *lineární vzhledem ke druhé složce*. Ze symetrie pak plyne, že je také *lineární vzhledem k první složce*. Poslední čtvrtá vlastnost se nazývá *pozitivní definitnost* standardního skalárního součinu.

Analogicky jako v dimenzi 2 vzorec v definici 8.4 plyne ze symetrie, linearity a předpokladu, že vektory kanonické báze $(\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n)$ prostoru $\mathbb{R}^n$ splňují

$$\mathbf{e}_i \cdot \mathbf{e}_j = 0 \ \text{ pokud } \ i \neq j, \quad \mathbf{e}_i \cdot \mathbf{e}_i = 1 \ .$$

Výpočet je následující.

$$\begin{aligned}\mathbf{u} \cdot \mathbf{v} &= \left(\sum_{i=1}^n x_i\mathbf{e}_i\right) \cdot \left(\sum_{i=1}^n y_i\mathbf{e}_i\right) = \sum_{i=1}^n \sum_{j=1}^n (x_i\mathbf{e}_i) \cdot (y_j\mathbf{e}_j) \\ &= \sum_{i=1}^n \sum_{j=1}^n x_i y_j (\mathbf{e}_i \cdot \mathbf{e}_j) = \sum_{i=1}^n x_i y_i \ .\end{aligned}$$

PŘÍKLAD 8.7. V příkladech 8.1 a 8.3 jsme ukázali interpretaci řešení jedné lineární rovnice o dvou nebo třech reálných neznámých pomocí skalárního součinu. Uvažujme nyní obecnou soustavu m vektorových rovnic o n neznámých $A\mathbf{x} = \mathbf{b}$ nad reálnými čísly. Víme, že množina všech řešení je tvaru $\mathbf{x}_p + \operatorname{Ker} A$, kde $\mathbf{x}_p$ je libovolné řešení soustavy.

Směrové vektory tohoto útvaru (tj. prvky $\operatorname{Ker} A$) jsou právě řešení příslušné homogenní soustavy $A\mathbf{x} = \mathbf{o}$. Označíme-li $\tilde{\mathbf{a}}_1, \dots, \tilde{\mathbf{a}}_m \in \mathbb{R}^n$ řádkové vektory matice A, můžeme vztah $A\mathbf{x} = \mathbf{o}$ ekvivalentně psát

$$\tilde{\mathbf{a}}_1 \cdot \mathbf{x} = 0,\ \tilde{\mathbf{a}}_2 \cdot \mathbf{x} = 0,\ \dots,\ \tilde{\mathbf{a}}_m \cdot \mathbf{x} = 0\ .$$

To znamená, že $\mathbf{x}$ leží v $\operatorname{Ker} A$ právě tehdy, když je kolmý ke všem řádkovým vektorům matice A.

Symetricky můžeme říct, že každý řádkový vektor matice A je kolmý ke všem prvkům $\operatorname{Ker} A$. Z věty 8.79 o ortogonálním doplňku vyplyne silnější tvrzení: vektor je kolmý ke všem prvkům $\operatorname{Ker} A$ právě tehdy, když leží v lineárním obalu řádků matice A, tj. v prostoru $\operatorname{Im} A^T$. ▲

8.1.3. Aritmetický prostor $\mathbb{C}^n$. Nad komplexními čísly je standardní skalární součin aritmetických vektorů definován trochu jiným způsobem.

DEFINICE 8.8. Pro dva komplexní aritmetické vektory $\mathbf{u} = (x_1,\ x_2,\ \dots,\ x_n)^T$ a $\mathbf{v} = (y_1, y_2, \dots, y_n)^T$ definujeme *standardní skalární součin* $\mathbf{u} \cdot \mathbf{v}$ předpisem

$$\mathbf{u} \cdot \mathbf{v} = \overline{x_1} y_1 + \overline{x_2} y_2 + \dots + \overline{x_n} y_n\ ,$$

kde $\overline{x}$ značí číslo komplexně sdružené k x, tj. $\overline{a + bi} = a - bi$.

Pro reálné vektory tato definice souhlasí s předchozí, protože komplexní sdružování s reálnými čísly nic nedělá. Tato definice má výhodu v tom, že skalární součin $\mathbf{u} \cdot \mathbf{u}$ je vždy nezáporné reálné číslo, neboť je součtem druhých mocnin absolutních hodnot $\overline{x_i} x_i = |x_i|^2$ složek vektoru $\mathbf{u}$. Proto komplexní aritmetické vektory mají nezápornou reálnou délku ve smyslu následující definice.

DEFINICE 8.9. *Eukleidovskou délku* nebo také *eukleidovskou normu* aritmetického vektoru $\mathbf{u} = (x_1,\ x_2,\ \dots,\ x_n)^T \in \mathbb{C}^n$ definujeme jako

$$\|\mathbf{u}\| = \sqrt{\mathbf{u} \cdot \mathbf{u}} = \sqrt{\overline{x_1} x_1 + \overline{x_2} x_2 + \dots + \overline{x_n} x_n} = \sqrt{|x_1|^2 + |x_2|^2 + \dots + |x_n|^2}\ .$$

Eukleidovská délka $\|\mathbf{u}\|$ je reálné číslo, které je nulové právě tehdy, když $\mathbf{u} = \mathbf{o}$. Pokud bychom definovali skalární součin bez komplexního sdružování, výraz $\mathbf{u} \cdot \mathbf{u}$ by nebyl vždy reálný a byl by roven nule i pro některé nenulové vektory.

Eukleidovská délka vektoru $\mathbf{u} = (a_1 + b_1 i, \dots, a_n + b_n i)^T$, kde $a_1, \dots, a_n$ a $b_1, \dots, b_n$ jsou reálná čísla, je podle definice

$$\|\mathbf{u}\| = \sqrt{|a_1 + b_1 i|^2 + \dots + |a_n + b_n i|^2} = \sqrt{a_1^2 + b_1^2 + \dots + a_n^2 + b_n^2}\ ,$$

což je totéž jako eukleidovská délka $(2n)$-složkového reálného vektoru $(a_1, b_1, \dots, a_n, b_n)^T$. Všimněte si ale, že skalární součin n-složkových komplexních aritmetických vektorů se obecně nerovná skalárnímu součinu příslušných $(2n)$-složkových reálných.

V reálném případě můžeme standardní skalární součin definovat maticovým součinem $\mathbf{u}^T \mathbf{v}$. Abychom mohli maticově zapsat standardní skalární součin nad komplexními čísly, zavedeme pojem hermitovsky sdružené matice.

DEFINICE 8.10. *Hermitovsky sdružená matice* k matici $A = (a_{ij})_{m \times n}$ je matice $A^* = (b_{ji})_{n \times m}$, kde $b_{ji} = \overline{a_{ij}}$ pro libovolné indexy $i \in \{1, 2, \dots, m\}$ a $j \in \{1, 2, \dots, n\}$.

Hermitovsky sdruženou matici k A tedy dostaneme transponováním a následným nahrazením všech prvků prvky komplexně sdruženými. Hermitovské sdružování se chová k ostatním operacím podobně jako transponování, viz cvičení. Speciálně, pokud je definován součin komplexních matic AB, platí

$$(AB)^* = B^* A^* \ .$$

Stejně tak $(A^*)^* = A$ pro každou komplexní matici A. Všimněme si také, že pokud jsou všechny prvky matice A reálné, platí $A^* = A^T$.

Příklad 8.11.

$$\begin{pmatrix} 1+2i & 3 & i \\ 0 & 3-2i & 4i \end{pmatrix}^* = \begin{pmatrix} 1-2i & 0 \\ 3 & 3+2i \\ -i & -4i \end{pmatrix}$$

▲

Pomocí hermitovského sdružování můžeme také standardní skalární součin komplexních vektorů zapsat pomocí součinu matic:

$$\mathbf{u} \cdot \mathbf{v} = \mathbf{u}^* \mathbf{v} \ .$$

Následující jednoduché tvrzení shrnuje základní vlastnosti standardního skalárního součinu v aritmetickém prostoru $\mathbb{C}^n$.

Tvrzení 8.12. *Pro libovolné tři vektory* $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{C}^n$ *a komplexní číslo* t *platí*

(1) $\mathbf{u} \cdot \mathbf{v} = \overline{\mathbf{v} \cdot \mathbf{u}}$,
(2) $\mathbf{u} \cdot (t\,\mathbf{v}) = t\,(\mathbf{u} \cdot \mathbf{v})$,
(3) $\mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w}$,
(4) $\mathbf{u} \cdot \mathbf{u}$ *je nezáporné reálné číslo, a* $\mathbf{u} \cdot \mathbf{u} = 0$ *právě když* $\mathbf{u} = \mathbf{o}$.

Důkaz. Tentokrát dokážeme první rovnost, důkaz ostatních vlastností ponecháme jako cvičení. Než se do toho pustíme, připomeneme úmluvu, že čtvercovou matici (a) řádu 1 obsahující jediný prvek a budeme v případě potřeby ztotožňovat s prvkem a. Při tomto ztotožnění platí $(a)^* = \bar{a}$.

Při ověření použijeme známou vlastnost, že pro každé komplexní číslo z platí $\bar{\bar{z}} = z$. Pak platí

$$\mathbf{u} \cdot \mathbf{v} = \mathbf{u}^* \mathbf{v} = \overline{\overline{\mathbf{u}^* \mathbf{v}}} = \overline{(\mathbf{u}^* \mathbf{v})^*} = \overline{\mathbf{v}^* \mathbf{u}} = \overline{\mathbf{v} \cdot \mathbf{u}} \ .$$

▲

První vlastnost je „skorosymetrie“. Druhá a třetí rovnost říkají, že standardní skalární součin nad komplexními čísly je lineární v druhé proměnné. V první proměnné ale lineární není. Platí pouze následující dvě rovnosti.

Pozorování 8.13. *Pro libovolné tři vektory* $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{C}^n$ *a komplexní číslo* t *platí*

(1) $(t\mathbf{u}) \cdot \mathbf{v} = \bar{t}\ (\mathbf{u} \cdot \mathbf{v})$.
(2) $(\mathbf{u} + \mathbf{v}) \cdot \mathbf{w} = \mathbf{u} \cdot \mathbf{w} + \mathbf{v} \cdot \mathbf{w}$,

Důkaz. Obě rovnosti lze dokázat pouze použitím vlastností z tvrzení 8.12:

$$(t\mathbf{u}) \cdot \mathbf{v} = \overline{\mathbf{v} \cdot (t\mathbf{u})} = \overline{t(\mathbf{v} \cdot \mathbf{u})} = \bar{t}\,\overline{\overline{\mathbf{u} \cdot \mathbf{v}}} = \bar{t}\ (\mathbf{u} \cdot \mathbf{v})$$

$$(\mathbf{u} + \mathbf{v}) \cdot \mathbf{w} = \overline{\mathbf{w} \cdot (\mathbf{u} + \mathbf{v})} = \overline{\mathbf{w} \cdot \mathbf{u} + \mathbf{w} \cdot \mathbf{v}} = \overline{\mathbf{w} \cdot \mathbf{u}} + \overline{\mathbf{w} \cdot \mathbf{v}} = \mathbf{u} \cdot \mathbf{w} + \mathbf{v} \cdot \mathbf{w}$$

▲

8.2. Obecný skalární součin

Obecně definujeme skalární součin jako zobrazení, které přiřazuje každé dvojici prvků nějakého vektorového prostoru nad $\mathbb{R}$ nebo $\mathbb{C}$ skalár a které má podobné vlastnosti jako standardní skalární součin. Důvodem pro takové zobecnění je opět daleko širší možnost využití, například na prostory funkcí.

Skalární součin prvků $\mathbf{u}$ a $\mathbf{v}$ budeme značit $\langle \mathbf{u}, \mathbf{v} \rangle$, značení $\mathbf{u} \cdot \mathbf{v}$ budeme používat pouze pro standardní skalární součin v $\mathbb{R}^n$ nebo $\mathbb{C}^n$.

Za základ definice obecného skalárního součinu vezmeme vlastnosti standardního skalárního součinu shrnuté v tvrzeních 8.6 a 8.12. Všimněme si také, že standardní skalární součin na prostoru $\mathbb{R}^n$ má všechny vlastnosti standardního skalárního součinu na prostoru $\mathbb{C}^n$, protože standardní skalární součin dvou reálných vektorů je reálné číslo a pro každé reálné číslo a platí $\bar{a} = a$.

Definice 8.14. Je-li $\mathbf{V}$ vektorový prostor nad $\mathbb{R}$ (resp. nad $\mathbb{C}$), pak se zobrazení $\langle\, , \rangle$ z $V \times V$ do $\mathbb{R}$ (resp do $\mathbb{C}$), které dvojici $\mathbf{u}, \mathbf{v}$ přiřadí skalár $\langle \mathbf{u}, \mathbf{v} \rangle$, nazývá *skalární součin* na $\mathbf{V}$, pokud pro libovolné $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ a $t \in \mathbb{R}$ (resp. $t \in \mathbb{C}$) platí

(SSS) $\langle \mathbf{u}, \mathbf{v} \rangle = \overline{\langle \mathbf{v}, \mathbf{u} \rangle}$,
(SL1) $\langle \mathbf{u}, t\mathbf{v} \rangle = t \langle \mathbf{u}, \mathbf{v} \rangle$,
(SL2) $\langle \mathbf{u}, \mathbf{v} + \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{u}, \mathbf{w} \rangle$,
(SP) $\langle \mathbf{u}, \mathbf{u} \rangle$ je nezáporné reálné číslo, které je nulové právě tehdy, když $\mathbf{u} = \mathbf{o}$.

Zdůrazněme ještě jednou, že **skalární součin definujeme pouze pro vektorové prostory nad tělesem $\mathbb{R}$ nebo $\mathbb{C}$.**

První axiom je „skorosymetrie“, další dva axiomy říkají, že i obecný skalární součin je lineární vzhledem ke druhé složce, poslední je pozitivní definitnost. Axiomy jsou stejné pro reálný i komplexní případ, důkazy proto budeme většinou provádět jen pro komplexní prostory.

Začneme jednoduchými důsledky axiomů v předcházející definici.

Pozorování 8.15. *Je-li $\mathbf{V}$ vektorový prostor nad $\mathbb{R}$ (resp. nad $\mathbb{C}$) se skalárním součinem $\langle\, , \rangle$, pak pro libovolné $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ a skalár t platí*

(1) $\langle \mathbf{u}, \mathbf{o} \rangle = 0 = \langle \mathbf{o}, \mathbf{u} \rangle$
(2) $\langle t\mathbf{u}, \mathbf{v} \rangle = \bar{t} \langle \mathbf{u}, \mathbf{v} \rangle$
(3) $\langle \mathbf{u} + \mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{w} \rangle + \langle \mathbf{v}, \mathbf{w} \rangle$

Důkaz. Druhou a třetí vlastnost jsme dokázali už v pozorování 8.13, neboť jsme i tam použili pouze axiomy z definice 8.14. Zbývá první vlastnost:

$$\langle \mathbf{u}, \mathbf{o} \rangle = \langle \mathbf{u}, 0\mathbf{o} \rangle = 0 \langle \mathbf{u}, \mathbf{o} \rangle = 0,$$

zbytek plyne z vlastnosti (SSS). ▲

8.2.1. Příklady.

Příklad 8.16. Standardní skalární součin v $\mathbb{R}^n$ (resp. $\mathbb{C}^n$) je skalárním součinem v $\mathbb{R}^n$ (resp. $\mathbb{C}^n$) ve smyslu definice 8.14. Všechny axiomy jsme už ověřili v tvrzeních 8.6 a 8.12. ▲

Příklad 8.17. Představme si $\mathbb{R}^2$ jako (nekonečný) list papíru a podívejme se na papír z jiné vzdálenosti a z jiného úhlu. Tím se nám změní vnímané délky vektorů a úhly mezi nimi. Uvažujme například situaci, kdy délka vektoru $\mathbf{e}_1$ zůstane 1, délka vektoru $\mathbf{e}_2$ bude 2 a vektory $\mathbf{e}_1$ a $\mathbf{e}_2$ budou svírat úhel $\pi/3$.

V části o standardním skalárním součinu na $\mathbb{R}^n$ jsme viděli, že formulka pro tento součin plyne z linearity a předpokladu kolmosti různých vektorů kanonické báze a toho, že mají délku 1. Zkusíme podobným způsobem zavést skalární součin pro „šikmý pohled“ na rovinu. To znamená, že bude platit

$$\langle \mathbf{e}_i, \mathbf{e}_j \rangle = (\text{„délka“ } \mathbf{e}_i)(\text{„délka“ } \mathbf{e}_j) \cos \alpha,$$

kde α je „úhel“, který svírají vektory $\mathbf{e}_i$ a $\mathbf{e}_j$. To znamená, že

$$\begin{aligned}\langle \mathbf{e}_1, \mathbf{e}_1 \rangle &= 1 \cdot 1 \cdot \cos 0 = 1\\ \langle \mathbf{e}_2, \mathbf{e}_2 \rangle &= 2 \cdot 2 \cdot \cos 0 = 4\\ \langle \mathbf{e}_1, \mathbf{e}_2 \rangle &= 1 \cdot 2 \cdot \cos(\pi/3) = 1 = \langle \mathbf{e}_2, \mathbf{e}_1 \rangle\end{aligned}$$

Podobným výpočtem jako v případě standardního skalárního součinu získáme vzorec

$$\begin{aligned}\left\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle &= \langle x_1\mathbf{e}_1 + x_2\mathbf{e}_2, y_1\mathbf{e}_1 + y_2\mathbf{e}_2 \rangle\\ &= x_1y_1 \langle \mathbf{e}_1, \mathbf{e}_1 \rangle + x_1y_2 \langle \mathbf{e}_1, \mathbf{e}_2 \rangle + x_2y_1 \langle \mathbf{e}_2, \mathbf{e}_1 \rangle + x_2y_2 \langle \mathbf{e}_2, \mathbf{e}_2 \rangle\\ &= x_1y_1 + x_1y_2 + x_2y_1 + 4x_2y_2 \ .\end{aligned}$$

Tento vztah lze maticově zapsat

$$\left\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle = (x_1 \ x_2) \begin{pmatrix} 1 & 1 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \ .$$

Snadno ověříme, že takto definovaný součin splňuje axiomy symetrie a linearity. Splňuje také axiom (SP): Je-li $\mathbf{u} = (x_1, x_2)^T$, pak platí

$$\langle \mathbf{u}, \mathbf{u} \rangle = x_1^2 + 2x_1x_2 + 4x_2^2 = (x_1 + x_2)^2 + 3x_2^2 \ .$$

Odtud plyne, že $\langle \mathbf{u}, \mathbf{u} \rangle \geq 0$ pro každý vektor $\mathbf{u} \in \mathbb{R}^2$ a $\langle \mathbf{u}, \mathbf{u} \rangle = 0$ právě když $x_2 = 0$ a $x_1 + x_2 = 0$, tj. právě když $\mathbf{u} = (x_1, x_2)^T = (0, 0)^T$. ▲

Zobecníme předchozí příklad „nestandardního“ skalárního součinu na aritmetickém prostoru.

Je-li A čtvercová matice nad $\mathbb{R}$ (resp. $\mathbb{C}$) řádu n, pak zobrazení z $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ (resp. $\mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$) definované vztahem

$$\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}^* A\mathbf{v}$$

vždy splňuje axiomy linearity, tj. axiomy (SL1) a (SL2) (cvičení). Snadno lze také zjistit, pro které matice A platí „skorosymetrie“ (SSS).

Pozorování 8.18. *Matice $A = (a_{ij}) \in \mathbb{C}^{n\times n}$ splňuje rovnost $\mathbf{u}^*A\mathbf{v} = \overline{\mathbf{v}^*A\mathbf{u}}$ pro každé dva vektory $\mathbf{u}, \mathbf{v} \in \mathbb{C}^n$ právě když $A^* = A$.*

Důkaz. Pokud platí $A^* = A$, pak $\overline{\mathbf{v}^*A\mathbf{u}} = (\mathbf{v}^*A\mathbf{u})^* = \mathbf{u}^*A^*\mathbf{v} = \mathbf{u}^*A\mathbf{v}$. Pokud naopak rovnost $A^* = A$ neplatí, existují indexy $i, j \in \{1, 2, \ldots, n\}$ takové, že $a_{ij} \neq \overline{a_{ji}}$. Pak pro prvky $\mathbf{e}_i, \mathbf{e}_j$ kanonické báze v $\mathbb{C}^n$ platí

$$\mathbf{e}_i^*A\mathbf{e}_j = a_{ij} \neq \overline{a_{ji}} = \overline{\mathbf{e}_j^*A\mathbf{e}_i} \ .$$

▲

Definice 8.19. Komplexním čtvercovým maticím splňujícím rovnost $A^* = A$ říkáme *hermitovské*.

Všimněte si, že reálná čtvercová matice je hermitovská právě tehdy, když je symetrická.

Pro obecnou hermitovskou (symetrickou) matici A, zobrazení definované $\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}^*A\mathbf{v}$ nemusí splňovat podmínku (SP). Má-li matice $A \in \mathbb{C}^{n\times n}$ splňovat podmínku (SP), musí být regulární. Pro singulární matici A totiž existuje nenulový vektor $\mathbf{u} \in \mathbb{C}^n$, pro který platí $A\mathbf{u} = \mathbf{o}$. Pro tento vektor $\mathbf{u}$ pak platí $\mathbf{u}^*A\mathbf{u} = 0$ a matice A tak podmínku (SP) nesplňuje. Ani regularita matice A ale není postačující pro splnění podmínky (SP). Lze si to snadno ověřit na matici

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

Definice 8.20. Reálná nebo komplexní čtvercová matice A řádu n se nazývá *pozitivně definitní*, pokud je A hermitovská a $\mathbf{u}^* A\mathbf{u}$ je nezáporné reálné číslo pro libovolné $\mathbf{u}$ z prostoru $\mathbb{R}^n$ resp. $\mathbb{C}^n$, přičemž $\mathbf{u}^* A\mathbf{u}$ se rovná 0 právě když $\mathbf{u} = \mathbf{o}$.

Shrnutím dosavadních úvah dostáváme:

Pozorování 8.21. *Je-li A čtvercová matice nad $\mathbb{R}$ (resp. $\mathbb{C}$) řádu n, pak zobrazení z $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ (resp. $\mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$) definované vztahem*

$$\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}^* A\mathbf{v}$$

je skalární součin právě tehdy, když je matice A pozitivně definitní.

Pozitivně definitní matice hrají v lineární algebře a jejích aplikacích důležitou roli. Příkladem pozitivně definitních matic jsou matice typu $A = B^* B$, kde B je regulární matice řádu n nad $\mathbb{R}$ (resp. nad $\mathbb{C}$). Snadno totiž spočteme, že v takovém případě pro každý vektor $\mathbf{u} \in \mathbb{C}^n$ platí

$$\mathbf{u}^* A\mathbf{u} = \mathbf{u}^* B^* B\mathbf{u} = (\mathbf{u}^* B^*)(B\mathbf{u}) = (B\mathbf{u})^*(B\mathbf{u}) = (B\mathbf{u}) \cdot (B\mathbf{u}) \ .$$

V posledním výrazu používáme standardní skalární součin na $\mathbb{C}^n$, který podmínku (SP) splňuje. Takže $\mathbf{u}^* A\mathbf{u} = \|B\mathbf{u}\|^2 \geq 0$ pro každý vektor $\mathbf{u} \in \mathbb{C}^n$, přičemž rovnost nule nastává právě když $B\mathbf{u} = \mathbf{o}$. A poslední rovnost vzhledem k regularitě matice B nastává právě když $\mathbf{u} = \mathbf{o}$.

Později ukážeme (tvrzení 10.22), že platí i opak, tj. každá pozitivně definitní matice A je tvaru $A = B^* B$ pro nějakou regulární matici B. Dokonce platí, že každý skalární součin na $\mathbb{R}^n$ (a na $\mathbb{C}^n$) můžeme vyjádřit ve tvaru

$$\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}^* B^* B\mathbf{v},$$

kde B je jednoznačně určená dolní trojúhelníková matice. (Pro reálné matice plyne existence z tvrzení 11.10 a věty 11.33.)

Pro $A = I_n$ dostáváme standardní skalární součin. Jako ukázku jiného konkrétního příkladu vezmeme

$$B = \begin{pmatrix} \sqrt{3}/2 & 0 \\ 1/2 & 2 \end{pmatrix} \ ,$$

tedy

$$A = B^* B = B^T B = \begin{pmatrix} \sqrt{3}/2 & 1/2 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} \sqrt{3}/2 & 0 \\ 1/2 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 4 \end{pmatrix}.$$

Příslušný skalární součin v $\mathbb{C}^2$ je dán vztahem

$$\langle \mathbf{u}, \mathbf{v} \rangle = (\overline{x_1}, \overline{x_2}) \begin{pmatrix} 1 & 1 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \overline{x_1} y_1 + \overline{x_1} y_2 + \overline{x_2} y_1 + 4\overline{x_2} y_2 \ ,$$

kde $\mathbf{u} = (x_1, x_2)^T$ a $\mathbf{v} = (y_1, y_2)^T$. Stejný vztah (kde nemusíme komplexně sdružovat) definuje skalární součin v $\mathbb{R}^2$, tentýž jako v předchozím příkladu.

Příklad 8.22. Příkladem skalárního součinu na prostoru $\mathbb{C}^{m \times n}$ komplexních matic typu $m \times n$ je

$$\langle A, B \rangle = \sum_{i=1}^{m} \sum_{j=1}^{n} \overline{a_{ij}}\, b_{ij} \ .$$

Stejný vzorec (bez nutnosti komplexního sdružování) definuje skalární součin na $\mathbb{R}^{m \times n}$. ▲

Příklad 8.23. Na prostoru spojitých reálných funkcí na intervalu $[0, 2\pi]$ je

$$\langle f, g \rangle = \int_0^{2\pi} f\, g$$

skalární součin.

Obecnější příklad skalárního součinu na prostoru všech spojitých reálných funkcí na intervalu $[0, 2\pi]$ je definovaný předpisem

$$\langle f, g\rangle = \int_0^{2\pi} f\, g\, h \ ,$$

kde h je nějaká spojitá kladná funkce na intervalu $[0, 2\pi]$, říkáme jí váhová funkce.

Podobně, na prostoru všech spojitých komplexních funkcí na stejném intervalu je

$$\langle f, g\rangle = \int_0^{2\pi} \overline{f}\, g\, h \ ,$$

skalární součin.

Skalární součiny toho typu se používají pro aproximaci funkcí. ▲

Příklad 8.24. Prostor ℓ_2 je tvořen posloupnostmi $(a_n)_{n=1}^{\infty}$ komplexních čísel splňujícími

$$\sum_{n=1}^{\infty} |a_n|^2 < \infty \ .$$

(Je třeba si rozmyslet, že tato množina tvoří spolu s přirozenými operacemi sčítání a násobení skalárem vektorový prostor. Jediný obtížnější krok je uzavřenost na sčítání.) Na tomto prostoru je

$$\langle (a_n)_{n=1}^{\infty}, (b_n)_{n=1}^{\infty}\rangle = \sum_{n=1}^{\infty} \overline{a_n} b_n \ .$$

skalární součin. ▲

Příklad 8.25. Důležité příklady skalárního součinu pochází z teorie pravděpodobnosti. Vektorový prostor tvoří náhodné veličiny na nějakém pevně zvoleném pravděpodobnostím prostoru. Tzv. kovariance, která, zhruba řečeno, měří míru závislosti jedné veličiny na druhé, splňuje všechny vlastnosti skalárního součinu až na implikaci zleva doprava v podmínce (SP) – $\langle \mathbf{u}, \mathbf{u}\rangle$ může být nula i pro nenulovou veličinu $\mathbf{u}$. (Tento drobný technický nedostatek lze odstranit ztotožněním veličin, jejichž rozdíl má nulový rozptyl.) ▲

8.2.2. Norma. Normu vektoru v prostoru se skalárním součinem zavedeme stejným vztahem jakým jsme vyjádřili eukleidovskou normu (délku) pomocí standardního skalárního součinu.

Definice 8.26. Nechť $\mathbf{V}$ je vektorový prostor se skalárním součinem $\langle\, ,\rangle$. *Normou* vektoru $\mathbf{u} \in V$ rozumíme reálné číslo

$$\|\mathbf{u}\| = \sqrt{\langle \mathbf{u}, \mathbf{u}\rangle} \ .$$

Vektor $\mathbf{u}$ se nazývá *jednotkový*, pokud $\|\mathbf{u}\| = 1$.

Definice dává smysl, protože výraz pod odmocninou je podle (SP) vždy nezáporné reálné číslo. Norma závisí na skalárním součinu, takže když používáme symbol normy, musí být z kontextu jasné, se kterým skalárním součinem pracujeme. Podobně i pro další pojmy jako úhel nebo kolmost, které budou zavedeny později.

Příklad 8.27. Norma vektoru $\mathbf{u} = (1, 1)^T$ v prostoru $\mathbb{R}^2$ se standardním skalárním součinem je $\|\mathbf{u}\| = \sqrt{\mathbf{u}^T\mathbf{u}} = \sqrt{2}$. Norma vektoru $\mathbf{u}$ v prostoru $\mathbb{R}^2$ se skalárním součinem

$$\left\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle = x_1y_1 + x_1y_2 + x_2y_1 + 4x_2y_2 = (x_1, x_2) \begin{pmatrix} 1 & 1 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

je ale $\|\mathbf{u}\| = \sqrt{\langle \mathbf{u}, \mathbf{u}\rangle} = \sqrt{7}$. ▲

PŘÍKLAD 8.28. Norma vektoru $(1+i, 2, 3-2i)^T$ v prostoru $\mathbb{C}^3$ se standardním skalárním součinem je

$$\left\| \begin{pmatrix} 1+i \\ 2 \\ 3-2i \end{pmatrix} \right\| = \sqrt{\begin{pmatrix} 1+i \\ 2 \\ 3-2i \end{pmatrix} \cdot \begin{pmatrix} 1+i \\ 2 \\ 3-2i \end{pmatrix}} = \sqrt{|1+i|^2 + |2|^2 + |3-2i|^2} = \sqrt{19} \ .$$

▲

PŘÍKLAD 8.29. Norma matice $A = (a_{ij})$ v prostoru $\mathbb{C}^{m\times n}$ (nebo $\mathbb{R}^{m\times n}$) je

$$\|A\| = \sqrt{\sum_{i=1}^{m} \sum_{j=1}^{n} |a_{ij}|^2} \ .$$

Říká se jí *Frobeniova norma* matice A. ▲

PŘÍKLAD 8.30. Uvažujme prostor $\mathbf{V}$ spojitých reálných funkcí na intervalu $[0,1]$ se skalárním součinem

$$\langle f, g \rangle = \int_0^1 f\, g$$

Norma funkce f je

$$\sqrt{\int_0^1 f^2} \ ,$$

neboli odmocnina obsahu plochy vymezené funkcí f^2, osou x a přímkami $x = 0$ a $x = 1$. V tomto smyslu tedy norma vyjadřuje, jak moc se funkce liší od nuly na intervalu $[0,1]$.

Konkrétně např. norma funkce x^2 je

$$\|x^2\| = \sqrt{\int_0^1 x^4\, dx} = \sqrt{\frac{1}{5}} \ .$$

▲

Norma určená skalárním součinem má následující vlastnosti.

TVRZENÍ 8.31. *Nechť* $\mathbf{V}$ *je vektorový prostor nad* $\mathbb{R}$ *(resp.* $\mathbb{C}$*) se skalárním součinem* $\langle\, , \rangle$, $\mathbf{u}, \mathbf{v} \in V$ *a* $t \in \mathbb{R}$ *(resp.* $t \in \mathbb{C}$*). Pak platí*

(1) $\|\mathbf{u}\| \geq 0$, *přičemž* $\|\mathbf{u}\| = 0$ *právě tehdy, když* $\mathbf{u} = \mathbf{o}$,
(2) $\|t\mathbf{u}\| = |t|\, \|\mathbf{u}\|$,
(3) $\|\mathbf{u}+\mathbf{v}\|^2 + \|\mathbf{u}-\mathbf{v}\|^2 = 2\,\|\mathbf{u}\|^2 + 2\,\|\mathbf{v}\|^2$ *(rovnoběžníkové pravidlo).*

DŮKAZ.

(1) Snadný důsledek (SP).
(2) Použitím (SL1) dostáváme

$$\|t\mathbf{u}\| = \sqrt{\langle t\mathbf{u}, t\mathbf{u}\rangle} = \sqrt{t\bar{t}\,\langle \mathbf{u}, \mathbf{u}\rangle} = \sqrt{|t|^2\,\langle \mathbf{u}, \mathbf{u}\rangle} = |t|\sqrt{\langle \mathbf{u}, \mathbf{u}\rangle} = |t|\,\|\mathbf{u}\| \ .$$

(3) Ve výpočtu stačí použít (SL2).

$$\begin{aligned} \|\mathbf{u}+\mathbf{v}\|^2 + \|\mathbf{u}-\mathbf{v}\|^2 &= \langle \mathbf{u}+\mathbf{v}, \mathbf{u}+\mathbf{v}\rangle + \langle \mathbf{u}-\mathbf{v}, \mathbf{u}-\mathbf{v}\rangle \\ &= \langle \mathbf{u}, \mathbf{u}\rangle + \langle \mathbf{u}, \mathbf{v}\rangle + \langle \mathbf{v}, \mathbf{u}\rangle + \langle \mathbf{v}, \mathbf{v}\rangle \\ &\quad + \langle \mathbf{u}, \mathbf{u}\rangle - \langle \mathbf{u}, \mathbf{v}\rangle - \langle \mathbf{v}, \mathbf{u}\rangle + \langle \mathbf{v}, \mathbf{v}\rangle \\ &= 2\,\langle \mathbf{u}, \mathbf{u}\rangle + 2\,\langle \mathbf{v}, \mathbf{v}\rangle = 2\,\|\mathbf{u}\|^2 + 2\,\|\mathbf{v}\|^2 \ . \end{aligned}$$

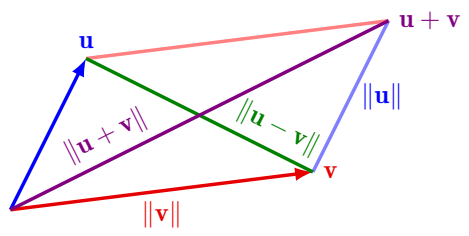
▲

Důsledkem (1) a (2) je, že pro nenulový vektor $\mathbf{u}$ je jeho násobek

$$\frac{\mathbf{u}}{\|\mathbf{u}\|}$$

jednotkový vektor. Říkáme, že vektor $\mathbf{u}/\|\mathbf{u}\|$ vznikl z $\mathbf{u}$ *znormováním.*

Rovnoběžníkové pravidlo je ilustrováno na obrázku.



Obrázek 8.3. Rovnoběžníkové pravidlo

Tak zvané polarizační identity vyjadřují reálnou a imaginární část skalárního součinu pouze pomocí norem vektorů. Skalární součin je tedy určen normami vektorů.

Tvrzení 8.32 (polarizační identity). *Nechť* $\mathbf{V}$ *je vektorový prostor nad* $\mathbb{R}$ *(resp.* $\mathbb{C}$*) se skalárním součinem* $\langle\,,\rangle$ *a* $\mathbf{u},\mathbf{v}\in V$*. Pak platí*

(1) $\operatorname{Re}(\langle\mathbf{u},\mathbf{v}\rangle)=\frac{1}{2}(\|\mathbf{u}+\mathbf{v}\|^2-\|\mathbf{u}\|^2-\|\mathbf{v}\|^2)$,

(2) $\operatorname{Im}(\langle\mathbf{u},\mathbf{v}\rangle)=\frac{1}{2}(\|\mathbf{u}-i\mathbf{v}\|^2-\|\mathbf{u}\|^2-\|\mathbf{v}\|^2)$,

kde $\operatorname{Re}(x)$ *značí reálnou a* $\operatorname{Im}(x)$ *imaginární část čísla* x*.*

Důkaz. Ze (SL2) a (SSS) vypočteme

$$\|\mathbf{u}+\mathbf{v}\|^2=\langle\mathbf{u},\mathbf{u}\rangle+\langle\mathbf{u},\mathbf{v}\rangle+\langle\mathbf{v},\mathbf{u}\rangle+\langle\mathbf{v},\mathbf{v}\rangle=\|\mathbf{u}\|^2+\|\mathbf{v}\|^2+\langle\mathbf{u},\mathbf{v}\rangle+\overline{\langle\mathbf{u},\mathbf{v}\rangle}\ .$$

Protože $x+\overline{x}=2\operatorname{Re}(x)$, dostáváme

$$2\operatorname{Re}(\langle\mathbf{u},\mathbf{v}\rangle)=\|\mathbf{u}+\mathbf{v}\|^2-\|\mathbf{u}\|^2-\|\mathbf{v}\|^2\ .$$

Druhou identitu necháme jako cvičení. ▲

Různé další varianty polarizační identity jsou ve cvičeních.

8.2.3. Cauchyho-Schwarzova nerovnost, úhel. Pro vektory $\mathbf{u},\mathbf{v}\in\mathbb{R}^3$ jsme nahlédli, že $\mathbf{u}\cdot\mathbf{v}=\|\mathbf{u}\|\,\|\mathbf{v}\|\cos\alpha$. Z toho také vyplývá, že absolutní hodnota $|\mathbf{u}\cdot\mathbf{v}|$ nemůže být větší než součin norem $\|\mathbf{u}\|\,\|\mathbf{v}\|$, protože kosinus úhlu je vždy v intervalu $[-1,1]$.

Vztah $\langle\mathbf{u},\mathbf{v}\rangle=\|\mathbf{u}\|\,\|\mathbf{v}\|\cos\alpha$ jde naopak použít pro zavedení úhlu mezi dvěma prvky v libovolném reálném vektorovém prostoru se skalárním součinem. Aby byl úhel dobře definován, musíme dokázat, že obecně platí $|\langle\mathbf{u},\mathbf{v}\rangle|\le\|\mathbf{u}\|\,\|\mathbf{v}\|$. Tato nerovnost platí i v komplexních vektorových prostorech, nazývá se Cauchyho-Schwarzova nerovnost (též Bunjakovského nerovnost, nebo Cauchyho-Schwarzova-Bunjakovského nerovnost, apod.) a je asi jednou z nejdůležitějších nerovností v matematice.

Věta 8.33 (Cauchyho-Schwarzova nerovnost). *Nechť* $\mathbf{V}$ *je vektorový prostor (nad* $\mathbb{R}$ *nebo* $\mathbb{C}$*) se skalárním součinem* $\langle\,,\rangle$ *a* $\mathbf{u},\mathbf{v}\in V$*. Pak platí*

$$|\langle\mathbf{u},\mathbf{v}\rangle|\le\|\mathbf{u}\|\,\|\mathbf{v}\|\ ,$$

přičemž rovnost nastává právě tehdy, když $(\mathbf{u},\mathbf{v})$ *je lineárně závislá posloupnost.*

Důkaz. Pokud je posloupnost $(\mathbf{u}, \mathbf{v})$ lineárně závislá, pak $\mathbf{u} = t\mathbf{v}$ nebo $\mathbf{v} = t\mathbf{u}$ pro nějaké $t \in \mathbb{C}$. V prvním případě je

$$|\langle \mathbf{u}, \mathbf{v} \rangle| = |\langle t\mathbf{v}, \mathbf{v} \rangle| = |\bar{t} \langle \mathbf{v}, \mathbf{v} \rangle| = |t| \, \|\mathbf{v}\|^2$$

a

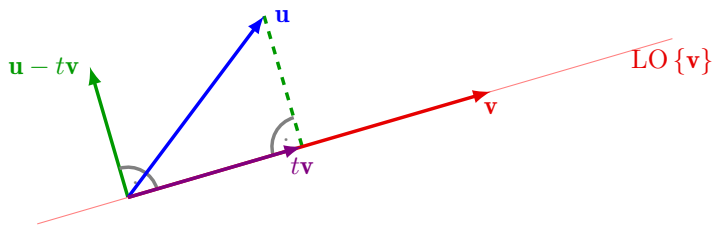
$$\|\mathbf{u}\| \, \|\mathbf{v}\| = \|t\mathbf{v}\| \, \|\mathbf{v}\| = |t| \, \|\mathbf{v}\|^2 \quad .$$

V případě $\mathbf{v} = t\mathbf{u}$ se rovnost $|\langle \mathbf{u}, \mathbf{v} \rangle| = \|\mathbf{u}\| \, \|\mathbf{v}\|$ odvodí podobně.

Nyní předpokládáme, že $(\mathbf{u}, \mathbf{v})$ je lineárně nezávislá posloupnost a odvodíme ostrou nerovnost. Díky lineární nezávislosti pro libovolné $t \in \mathbb{C}$ platí

$$0 < \|\mathbf{u} - t\mathbf{v}\|^2 \quad .$$

Zvolíme $t \in \mathbb{C}$ tak, aby platilo $\langle \mathbf{v}, \mathbf{u} - t\mathbf{v} \rangle = 0$. Geometrický význam v případě standardního skalárního součinu v $\mathbb{R}^n$ je vyznačen na obrázku: vektor $t\mathbf{v}$ je ortogonální projekcí vektoru $\mathbf{u}$ na $\mathrm{LO}\{\mathbf{v}\}$. Později dáme této intuici přesný význam pro obecný skalární součin.



Obrázek 8.4. K důkazu Cauchy-Schwarzovy nerovnosti

Vztah $\langle \mathbf{v}, \mathbf{u} - t\mathbf{v} \rangle = 0$ je ekvivalentní $\langle \mathbf{v}, \mathbf{u} \rangle - t \langle \mathbf{v}, \mathbf{v} \rangle = 0$, což je ekvivalentní

$$t = \frac{\langle \mathbf{v}, \mathbf{u} \rangle}{\|\mathbf{v}\|^2} \quad .$$

(Nulou nedělíme, protože prvek $\mathbf{v}$ je nenulový podle předpokladu o lineární nezávislosti $(\mathbf{u}, \mathbf{v})$.)

Při této volbě t dostáváme

$$\begin{aligned} 0 < \|\mathbf{u} - t\mathbf{v}\|^2 &= \langle \mathbf{u} - t\mathbf{v}, \mathbf{u} - t\mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{u} - t\mathbf{v} \rangle - \bar{t} \langle \mathbf{v}, \mathbf{u} - t\mathbf{v} \rangle \\ &= \langle \mathbf{u}, \mathbf{u} - t\mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{u} \rangle - t \langle \mathbf{u}, \mathbf{v} \rangle = \|\mathbf{u}\|^2 - \frac{\langle \mathbf{v}, \mathbf{u} \rangle}{\|\mathbf{v}\|^2} \langle \mathbf{u}, \mathbf{v} \rangle \\ &= \|\mathbf{u}\|^2 - \frac{\overline{\langle \mathbf{u}, \mathbf{v} \rangle} \langle \mathbf{u}, \mathbf{v} \rangle}{\|\mathbf{v}\|^2} = \|\mathbf{u}\|^2 - \frac{|\langle \mathbf{u}, \mathbf{v} \rangle|^2}{\|\mathbf{v}\|^2} \quad . \end{aligned}$$

Po vynásobení $\|\mathbf{v}\|^2$, drobné úpravě a odmocnění (oba výrazy, z nichž se počítá druhá mocnina jsou kladné) vyjde dokazovaná nerovnost:

$$\begin{aligned} 0 &< \|\mathbf{u}\|^2 - \frac{|\langle \mathbf{u}, \mathbf{v} \rangle|^2}{\|\mathbf{v}\|^2} \\ 0 &< \|\mathbf{u}\|^2 \, \|\mathbf{v}\|^2 - |\langle \mathbf{u}, \mathbf{v} \rangle|^2 \\ |\langle \mathbf{u}, \mathbf{v} \rangle|^2 &< \|\mathbf{u}\|^2 \, \|\mathbf{v}\|^2 \\ |\langle \mathbf{u}, \mathbf{v} \rangle| &< \|\mathbf{u}\| \, \|\mathbf{v}\| \quad . \end{aligned}$$

▲

PŘÍKLAD 8.34. Pro standardní skalární součin v $\mathbb{C}^n$ říká Cauchyho-Schwarzova nerovnost

$$|\overline{x_1}y_1+\overline{x_2}y_2+\cdots+\overline{x_n}y_n| \leq \sqrt{|x_1|^2+|x_2|^2+\cdots+|x_n|^2}\,\sqrt{|y_1|^2+|y_2|^2+\cdots+|y_n|^2}\ .$$

V případě skalárního součinu na $\mathbb{C}^2$ daného vzorcem

$$\left\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle = (\overline{x_1}, \overline{x_2}) \begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

dostáváme

$$\begin{aligned} &|5\overline{x_1}y_1 - 2\overline{x_1}y_2 - 2\overline{x_2}y_1 + \overline{x_2}y_2| \\ &\qquad \leq \sqrt{5|x_1|^2 - 4\mathrm{Re}\,(\overline{x_1}x_2) + |x_2|^2}\ \sqrt{5|y_1|^2 - 4\mathrm{Re}\,(\overline{y_1}y_2) + |y_2|^2}\ . \end{aligned}$$

Pro prostor spojitých reálných funkcí na intervalu $[0, 2\pi]$ se skalárním součinem $\langle f, g\rangle = \int_0^{2\pi} fg$ Cauchyho-Schwarzova nerovnost znamená

$$\left|\int_0^{2\pi} fg\right| \leq \sqrt{\int_0^{2\pi} f^2}\ \sqrt{\int_0^{2\pi} g^2}\ .$$

▲

Důležitým důsledkem Cauchyho-Schwarzovy nerovnosti je trojúhelníková nerovnost.

DŮSLEDEK 8.35 (Trojúhelníková nerovnost). *Nechť* $\mathbf{V}$ *je vektorový prostor se skalárním součinem* $\langle\,,\rangle$ *a* $\mathbf{u}, \mathbf{v} \in V$. *Pak platí*

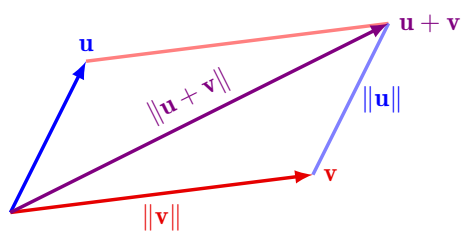
$$\|\mathbf{u}+\mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\|\ .$$

DŮKAZ.

$$\begin{aligned} \|\mathbf{u}+\mathbf{v}\|^2 &= \langle \mathbf{u}+\mathbf{v}, \mathbf{u}+\mathbf{v}\rangle = \langle \mathbf{u}, \mathbf{u}\rangle + \langle \mathbf{u}, \mathbf{v}\rangle + \overline{\langle \mathbf{u}, \mathbf{v}\rangle} + \langle \mathbf{v}, \mathbf{v}\rangle \\ &= \|\mathbf{u}\|^2 + 2\,\mathrm{Re}\,(\langle \mathbf{u}, \mathbf{v}\rangle) + \|\mathbf{v}\|^2 \leq \|\mathbf{u}\|^2 + 2\,|\langle \mathbf{u}, \mathbf{v}\rangle| + \|\mathbf{v}\|^2 \\ &\leq \|\mathbf{u}\|^2 + 2\,\|\mathbf{u}\|\,\|\mathbf{v}\| + \|\mathbf{v}\|^2 = (\|\mathbf{u}\| + \|\mathbf{v}\|)^2 \end{aligned}$$

Cauchyho-Schwarzovu nerovnost jsme použili v předposlední úpravě. Výrazy pod druhými mocninami jsou kladné, takže nerovnost plyne odmocněním. ▲

Geometrický význam je patrný z obrázku.



OBRÁZEK 8.5. Trojúhelníková nerovnost

Cauchyho-Schwarzova nerovnost nám umožňuje definovat úhel mezi prvky reálného vektorového prostoru se skalárním součinem.

DEFINICE 8.36. Nechť $\mathbf{V}$ je vektorový prostor nad $\mathbb{R}$ se skalárním součinem $\langle\,,\rangle$ a $\mathbf{o} \neq \mathbf{u}, \mathbf{v} \in V$. *Úhlem mezi prvky* $\mathbf{u}$ *a* $\mathbf{v}$ rozumíme reálné číslo $\alpha \in [0, \pi]$ splňující

$$\cos\alpha = \frac{\langle \mathbf{u}, \mathbf{v}\rangle}{\|\mathbf{u}\|\,\|\mathbf{v}\|}$$

Úhel mezi dvěma prvky existuje a je určen jednoznačně, protože zlomek je v intervalu $[-1,1]$ podle Cauchyho-Schwarzovy nerovnosti a funkce cos vzájemně jednoznačně zobrazuje $[0,\pi]$ na interval $[-1,1]$.

Pro libovolný skalární součin v vektorovém prostoru nad reálnými čísly tedy máme vztah

$$\langle \mathbf{u}, \mathbf{v} \rangle = \|\mathbf{u}\| \, \|\mathbf{v}\| \cos\alpha \ .$$

Z tohoto vztahu snadno odvodíme kosinovou větu.

TVRZENÍ 8.37 (Kosinová věta). *Nechť* $\mathbf{V}$ *je vektorový prostor nad* $\mathbb{R}$ *se skalárním součinem* $\langle\,,\rangle$ *a* $\mathbf{o} \neq \mathbf{u}, \mathbf{v} \in V$. *Pak platí*

$$\|\mathbf{u}-\mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2\,\|\mathbf{u}\|\,\|\mathbf{v}\| \cos\alpha \ ,$$

kde α *je úhel mezi vektory* $\mathbf{u}$ *a* $\mathbf{v}$.

DŮKAZ.

$$\begin{aligned}\|\mathbf{u}-\mathbf{v}\|^2 &= \langle \mathbf{u}-\mathbf{v}, \mathbf{u}-\mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{u} \rangle - 2\,\langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{v}, \mathbf{v} \rangle \\ &= \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2\,\|\mathbf{u}\|\,\|\mathbf{v}\| \cos\alpha\end{aligned}$$

▲

8.2.4. Obecné normy. Někdy bývá přirozenější měřit délku prvků ve vektorovém prostoru jiným způsobem, než pomocí normy definované skalárním součinem.

DEFINICE 8.38. Je-li $\mathbf{V}$ vektorový prostor nad $\mathbb{C}$ (nebo nad $\mathbb{R}$), pak zobrazení $\|\cdot\|$, které přiřazuje každému prvku $\mathbf{u}$ reálné číslo $\|\mathbf{u}\|$, nazýváme *norma* na prostoru $\mathbf{V}$, pokud platí pro každé dva prvky $\mathbf{u}, \mathbf{v} \in V$ a každý skalár t

(1) $\|\mathbf{u}\| \geq 0$, přičemž $\|\mathbf{u}\| = 0$ právě tehdy, když $\mathbf{u} = \mathbf{o}$,
(2) $\|t\mathbf{u}\| = |t|\,\|\mathbf{u}\|$,
(3) $\|\mathbf{u}+\mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\|$.

Norma pochází ze skalárního součinu právě tehdy, když splňuje rovnoběžníkové pravidlo, viz cvičení.

Existuje mnoho norem, které nepochází ze skalárního součinu, například v $\mathbb{R}^n$ máme normu

$$\left\|(x_1, x_2, \ldots, x_n)^T\right\| = |x_1| + |x_2| + \cdots + |x_n| \ ,$$

která měří vzdálenost, když se můžeme pohybovat pouze pravoúhlým směrem (proto se jí někdy říká manhattanská norma). Jiným příkladem normy na $\mathbb{R}^n$ nepocházející ze skalárního součinu je norma

$$\left\|(x_1, x_2, \ldots, x_n)^T\right\| = \max\{|x_i| : i = 1, 2 \ldots, n\} \ .$$

OBRAZEK N5 - l_1-norma

8.3. Kolmost

8.3.1. Kolmé vektory a množiny. V reálném vektorovém prostoru se skalárním součinem platí vztah $\langle \mathbf{u}, \mathbf{v} \rangle = \|\mathbf{u}\| \, \|\mathbf{v}\| \cos \alpha$. Nenulové vektory tedy svírají úhel $\pi/2$ právě tehdy, když je jejich skalární součin nula. To motivuje následující definici kolmosti vektorů, která funguje i pro komplexní prostory.

Definice 8.39. Nechť $\mathbf{V}$ je vektorový prostor nad $\mathbb{R}$ nebo $\mathbb{C}$ se skalárním součinem $\langle \, , \rangle$.

Prvky $\mathbf{u}, \mathbf{v} \in V$ nazýváme *kolmé* (nebo *ortogonální*) a píšeme $\mathbf{u} \perp \mathbf{v}$, pokud $\langle \mathbf{u}, \mathbf{v} \rangle = 0$.

Říkáme, že prvek $\mathbf{v} \in V$ *je kolmý na množinu* $M \subseteq V$, pokud $\mathbf{v}$ je kolmý na každý prvek z množiny M, což zapisujeme $\mathbf{v} \perp M$.

Říkáme, že množiny $M, N \subseteq V$ jsou *kolmé*, zapisujeme $M \perp N$, pokud každý prvek množiny M je kolmý na každý prvek množiny N.

Pozor, podle této definice stěna *není* kolmá na podlahu – ne všechny vektory stěny jsou kolmé k vektorům podlahy. Jako snadné cvičení si rozmyslete, že je-li množina M kolmá na množinu N, pak v jejich průniku může být pouze nulový vektor.

Jednoduchým důsledkem definice je následující pozorování.

Tvrzení 8.40. *Je-li* $\mathbf{V}$ *vektorový prostor se skalárním součinem* $\langle \, , \rangle$ *a* $M, N \subseteq V$*, pak* $M \perp N$ *právě když* $M \perp \mathrm{LO}\, N$*, a to nastane právě když* $\mathrm{LO}\, M \perp \mathrm{LO}\, N$*.*

Důkaz. Dokážeme ekvivalenci prvních dvou tvrzení. Předpokládáme tedy $M \perp N$. Je-li $\mathbf{x} \in M$ a $\mathbf{y} \in \mathrm{LO}\, N$, existuje vyjádření $\mathbf{y} = a_1\mathbf{u}_1 + a_2\mathbf{u}_2 + \cdots + a_k\mathbf{u}_k$ pro nějaké prvky $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k \in N$ a skaláry $a_1, a_2, \ldots, a_k$. Potom

$$\begin{aligned} \langle \mathbf{x}, \mathbf{y} \rangle &= \langle \mathbf{x}, a_1\mathbf{u}_1 + a_2\mathbf{u}_2 + \cdots + a_k\mathbf{u}_k \rangle \\ &= a_1 \langle \mathbf{x}, \mathbf{u}_1 \rangle + a_2 \langle \mathbf{x}, \mathbf{u}_2 \rangle + \cdots + a_k \langle \mathbf{x}, \mathbf{u}_k \rangle = 0 \ . \end{aligned}$$

Proto $M \perp \mathrm{LO}\, N$. Opačná implikace je zřejmá. Ekvivalence druhých dvou tvrzení plyne z ekvivalence prvních dvou. ▲

Dokázané tvrzení se zejména používá v situaci, kdy chceme ověřit, že nějaký vektor $\mathbf{v} \in V$ je kolmý na podprostor $W \leq \mathbf{V}$. Podle tvrzení k tomu stačí ověřit, že $\mathbf{v}$ je kolmý na všechny vektory z nějaké množiny generátorů podprostoru W.

8.3.2. Ortogonální a ortonormální množiny.

Definice 8.41. Nechť $\mathbf{V}$ je vektorový prostor nad $\mathbb{R}$ nebo $\mathbb{C}$ se skalárním součinem $\langle \, , \rangle$ a M množina, nebo posloupnost, prvků V. Pak M se nazývá

- *ortogonální*, pokud $\mathbf{u} \perp \mathbf{v}$ pro libovolné dva různé prvky množiny (nebo posloupnosti) M;
- *ortonormální*, pokud je ortogonální a každý vektor v M je jednotkový.

Z vlastnosti (SSS) plyne, že ortogonalita dvou prvků nezávisí na jejich pořadí. Protože pro libovolný vektor $\mathbf{v}$ platí $\langle \mathbf{v}, \mathbf{o} \rangle = 0$, nulový vektor je kolmý k jakémukoliv vektoru.

Z vlastnosti (SL1) vidíme, že jsou-li dva prvky kolmé, pak jsou kolmé i jejich libovolné násobky. Máme-li ortogonální množinu nenulových prvků $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$, můžeme z ní vytvořit ortonormální množinu *znormováním*, tj.

$$\left\{ \frac{\mathbf{v}_1}{\|\mathbf{v}_1\|}, \frac{\mathbf{v}_2}{\|\mathbf{v}_2\|}, \ldots, \frac{\mathbf{v}_k}{\|\mathbf{v}_k\|} \right\}$$

je ortonormální.

Z geometrického náhledu v $\mathbb{R}^3$ vidíme, že ortogonální posloupnost nenulových vektorů je lineárně nezávislá. Platí to zcela obecně.

Tvrzení 8.42. *Je-li* $\mathbf{V}$ *vektorový prostor se skalárním součinem* $\langle\,,\rangle$*, pak každá ortogonální posloupnost nenulových prvků* V *je lineárně nezávislá.*

Důkaz. Je-li $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ ortogonální posloupnost prvků V a platí-li

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

pak skalárním vynásobením obou stran zleva vektorem $\mathbf{v}_i$ $(i \in \{1, 2, \ldots, k\})$ a využitím (SL1), (SL2) a kolmosti dostáváme

$$\begin{aligned} \langle\, \mathbf{v}_i, a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k \rangle &= \langle\, \mathbf{v}_i, \mathbf{o} \rangle \\ a_1 \langle\, \mathbf{v}_i, \mathbf{v}_1 \rangle + a_2 \langle\, \mathbf{v}_i, \mathbf{v}_2 \rangle + \cdots + a_k \langle\, \mathbf{v}_i, \mathbf{v}_k \rangle &= 0 \\ a_i \langle\, \mathbf{v}_i, \mathbf{v}_i \rangle &= 0 \ . \end{aligned}$$

Protože vektor $\mathbf{v}_i$ je nenulový, platí podle (SP) vztah $\langle\, \mathbf{v}_i, \mathbf{v}_i \rangle = \|\mathbf{v}_i\|^2 > 0$, takže z odvozeného vztahu vyplývá $a_i = 0$. Ukázali jsme tak, že pouze triviální lineární kombinace prvků $\mathbf{v}_i$ se rovná nulovému vektoru, takže posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ je lineárně nezávislá (viz bod (3) tvrzení 5.37). ▲

Z tvrzení vyplývá, že ortogonální posloupnost n nenulových vektorů v prostoru dimenze n je ortogonální báze, protože je lineárně nezávislá a lineárně nezávislá posloupnost n vektorů v prostoru dimenze n je báze podle bodu (4) v pozorování 5.67.

Příklad 8.43. V prostoru $\mathbb{R}^n$ (nebo $\mathbb{C}^n$) se standardním skalárním součinem je kanonická báze ortonormální. ▲

Příklad 8.44. Posloupnost vektorů $((1, 2, 2)^T, (-2, -1, 2)^T)$ v $\mathbb{R}^3$ (nebo $\mathbb{C}^3$) se standardním skalárním součinem je ortogonální, ale není ortonormální. Znormováním dostaneme ortonormální posloupnost

$$\left(\frac{1}{3}(1, 2, 2)^T, \frac{1}{3}(-2, -1, 2)^T\right) \ .$$

Tuto posloupnost lze doplnit na ortonormální bázi – posloupnost

$$\left(\frac{1}{3}(1, 2, 2)^T, \frac{1}{3}(-2, -1, 2)^T, \frac{1}{3}(2, -2, 1)^T\right)$$

je ortonormální, takže je to podle poznámky za předchozím tvrzením ortonormální báze. Později budeme pomocí Gramova-Schmidtova ortogonalizačního procesu umět každou ortogonální (resp. ortonormální) posloupnost nenulových vektorů v konečně generovaném prostoru doplnit do ortogonální (resp. ortonormální) báze. ▲

Příklad 8.45. V prostoru $\mathbb{R}^2$ se skalárním součinem daným

$$\langle\, (x_1, x_2)^T, (y_1, y_2)^T \rangle = (x_1, x_2) \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = 2x_1y_1 + x_1y_2 + x_2y_1 + x_2y_2$$

(ověřte, že je to skutečně skalární součin) je posloupnost

$$\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \end{pmatrix}\right)$$

ortogonální, protože

$$\left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \end{pmatrix} \right\rangle = (1, 0) \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -1 \\ 2 \end{pmatrix} = (2, 1) \begin{pmatrix} -1 \\ 2 \end{pmatrix} = 0 \ ,$$

tedy tvoří ortogonální bázi. Spočítáme normy vektorů a vytvoříme ortonormální bázi.

$$\left\|\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right\| = \sqrt{(1,0)\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}} = \sqrt{(2,1)\begin{pmatrix} 1 \\ 0 \end{pmatrix}} = \sqrt{2}$$

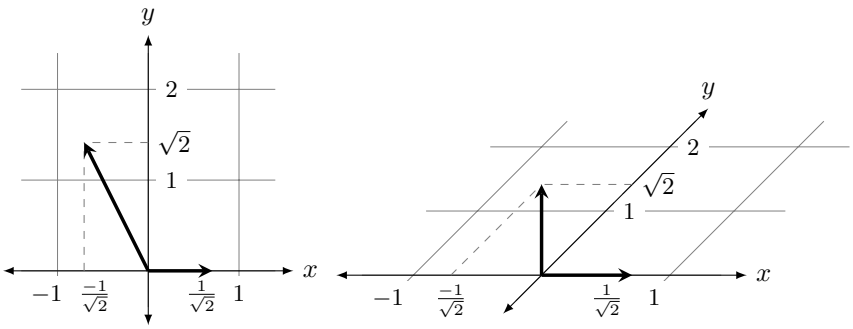
$$\left\|\begin{pmatrix} -1 \\ 2 \end{pmatrix}\right\| = \sqrt{(-1,2)\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} -1 \\ 2 \end{pmatrix}} = \sqrt{(0,1)\begin{pmatrix} -1 \\ 2 \end{pmatrix}} = \sqrt{2}$$

Posloupnost

$$\left(\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 2 \end{pmatrix}\right)$$

je tedy ortonormální báze.

Pokud si nakreslíme tyto dva vektory jako kolmé vektory jednotkové velikosti a ostatní vektory kreslíme v tomto souřadném systému, pak délky a úhly při daném skalárním součinu jsou běžné eukleidovské délky a úhly na obrázku. Tento fakt dokážeme v tvrzení 8.50.



▲

Příklad 8.46. V prostoru spojitých funkcí na intervalu $[0, 2\pi]$ se skalárním součinem

$$\langle f, g\rangle = \int_0^{2\pi} fg$$

je množina $\{1, \sin x, \cos x, \sin(2x), \cos(2x), \dots\}$ ortogonální. Toto je základní fakt Fourierovy analýzy, jedné z velmi důležitých oblastí matematiky. ▲

Poznámka. Odvodíme maticové kritérium na to, kdy je posloupnost sloupcových vektorů reálné nebo komplexní matice A typu $m \times n$ ortonormální vzhledem ke standardnímu skalárnímu součinu v $\mathbb{C}^m$.

Uvažujme tedy standardní skalární součin na $\mathbb{C}^m$. Posloupnost sloupcových vektorů matice $A = (\mathbf{a}_1|\dots|\mathbf{a}_n)$ je ortonormální právě tehdy, když $\mathbf{a}_i \cdot \mathbf{a}_j = 0$ pro každé $i \neq j \in \{1, \dots, n\}$ a $\mathbf{a}_i \cdot \mathbf{a}_i = 1$ pro každé $i \in \{1, \dots, n\}$. Skalár $\mathbf{a}_i \cdot \mathbf{a}_j = \mathbf{a}_i^* \mathbf{a}_j$ je ale roven prvku na místě (i, j) v matici A^*A.

$$A^*A = \begin{pmatrix} \mathbf{a}_1^*\mathbf{a}_1 & \mathbf{a}_1^*\mathbf{a}_2 & \cdots & \mathbf{a}_1^*\mathbf{a}_k \\ \mathbf{a}_2^*\mathbf{a}_1 & \mathbf{a}_2^*\mathbf{a}_2 & \cdots & \mathbf{a}_2^*\mathbf{a}_k \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_k^*\mathbf{a}_1 & \mathbf{a}_k^*\mathbf{a}_2 & \cdots & \mathbf{a}_k^*\mathbf{a}_k \end{pmatrix} = \begin{pmatrix} \mathbf{a}_1 \cdot \mathbf{a}_1 & \mathbf{a}_1 \cdot \mathbf{a}_2 & \cdots & \mathbf{a}_1 \cdot \mathbf{a}_k \\ \mathbf{a}_2 \cdot \mathbf{a}_1 & \mathbf{a}_2 \cdot \mathbf{a}_2 & \cdots & \mathbf{a}_2 \cdot \mathbf{a}_k \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_k \cdot \mathbf{a}_1 & \mathbf{a}_k \cdot \mathbf{a}_2 & \cdots & \mathbf{a}_k \cdot \mathbf{a}_k \end{pmatrix}.$$

Vidíme, že sloupce matice A tvoří ortonormální posloupnost právě tehdy, když $A^*A = I_n$. Matici A^*A nazveme v definici 8.61 Gramovou maticí posloupnosti vektorů $(\mathbf{a}_1, \dots, \mathbf{a}_n)$.

Podobně, posloupnost řádkových vektorů reálné nebo komplexní matice A je ortonormální vzhledem ke standardnímu skalárnímu součinu právě tehdy, když platí $AA^* = I_m$.

Jednoduchým důsledkem definice kolmosti je zobecnění Pythagorovy věty pro libovolný skalární součin.

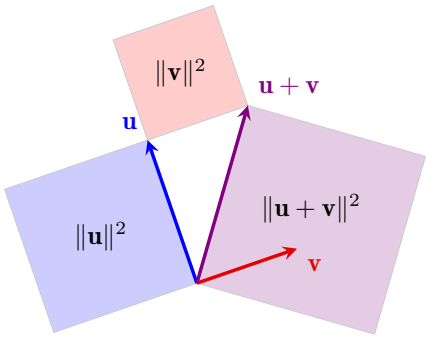
TVRZENÍ 8.47 (Pythagorova věta). *Je-li* $\mathbf{V}$ *vektorový prostor se skalárním součinem* $\langle\,,\rangle$ *a jsou-li vektory* $\mathbf{u}, \mathbf{v} \in V$ *kolmé, pak platí*

$$\|\mathbf{u}+\mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 \quad .$$

DŮKAZ.

$$\|\mathbf{u}+\mathbf{v}\|^2 = \langle \mathbf{u}+\mathbf{v}, \mathbf{u}+\mathbf{v}\rangle = \langle \mathbf{u}, \mathbf{u}\rangle + \langle \mathbf{u}, \mathbf{v}\rangle + \langle \mathbf{v}, \mathbf{u}\rangle + \langle \mathbf{v}, \mathbf{v}\rangle$$

Díky kolmosti jsou prostřední dva členy nulové, takže výraz je roven $\|\mathbf{u}\|^2 + \|\mathbf{v}\|^2$. ▲



Indukcí lze Pythagorovu větu zobecnit na libovolný konečný počet prvků. Je-li $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ ortogonální množina, pak

$$\|\mathbf{v}_1 + \mathbf{v}_2 + \cdots + \mathbf{v}_k\|^2 = \|\mathbf{v}_1\|^2 + \|\mathbf{v}_2\|^2 + \cdots + \|\mathbf{v}_k\|^2 \quad .$$

Existuje zobecnění Pythagorovy věty na nekonečné ortogonální množiny, tzv. *Parsevalova identita.*

8.3.3. Souřadnice vzhledem k ortonormální bázi. Souřadnice prvků vektorového prostoru vzhledem k ortonormální bázi se počítají velmi snadno.

TVRZENÍ 8.48. *Je-li* $\mathbf{V}$ *vektorový prostor se skalárním součinem* $\langle\,,\rangle$, $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ *nějaká ortonormální báze ve* $\mathbf{V}$ *a* $\mathbf{u} \in V$, *pak platí*

$$\mathbf{u} = \langle \mathbf{v}_1, \mathbf{u}\rangle \mathbf{v}_1 + \langle \mathbf{v}_2, \mathbf{u}\rangle \mathbf{v}_2 + \cdots + \langle \mathbf{v}_n, \mathbf{u}\rangle \mathbf{v}_n \quad .$$

Jinými slovy,

$$[\mathbf{u}]_B = (\langle \mathbf{v}_1, \mathbf{u}\rangle, \langle \mathbf{v}_2, \mathbf{u}\rangle, \ldots, \langle \mathbf{v}_n, \mathbf{u}\rangle)^T \quad .$$

DŮKAZ. Označme $[\mathbf{u}]_B = (a_1, a_2, \ldots, a_n)^T$, neboli

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

Podobně jako v důkazu lineární nezávislosti ortogonální posloupnosti nenulových vektorů skalárně vynásobíme obě strany zleva vektorem $\mathbf{v}_i$ a dostaneme

$$\begin{aligned}
\langle \mathbf{v}_i, \mathbf{u}\rangle &= \langle \mathbf{v}_i, a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n\rangle \\
\langle \mathbf{v}_i, \mathbf{u}\rangle &= a_1 \langle \mathbf{v}_i, \mathbf{v}_1\rangle + a_2 \langle \mathbf{v}_i, \mathbf{v}_2\rangle + \cdots + a_n \langle \mathbf{v}_i, \mathbf{v}_n\rangle \\
\langle \mathbf{v}_i, \mathbf{u}\rangle &= a_i \langle \mathbf{v}_i, \mathbf{v}_i\rangle = a_i \quad ,
\end{aligned}$$

takže $a_i = \langle \mathbf{v}_i, \mathbf{u}\rangle$. ▲

Souřadnicím vzhledem k ortonormální bázi se někdy říká *Fourierovy koeficienty* vzhledem k této bázi. Obecněji z důkazu vidíme, že pro ortogonální bázi B platí

$$[\mathbf{u}]_B = \left(\frac{\langle \mathbf{v}_1, \mathbf{u} \rangle}{\|\mathbf{v}_1\|^2}, \frac{\langle \mathbf{v}_2, \mathbf{u} \rangle}{\|\mathbf{v}_2\|^2}, \ldots, \frac{\langle \mathbf{v}_n, \mathbf{u} \rangle}{\|\mathbf{v}_n\|^2} \right)^T .$$

Příklad 8.49. Určíme souřadnice vektoru $\mathbf{u} = (3+i, 2, i)^T \in \mathbb{C}^3$ vzhledem k ortonormální bázi

$$B = (\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) = \left(\frac{1}{3} \begin{pmatrix} i \\ 2i \\ 2i \end{pmatrix}, \frac{1}{3} \begin{pmatrix} -2 \\ -1 \\ 2 \end{pmatrix}, \frac{1}{3} \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix} \right)$$

prostoru $\mathbb{C}^3$ se standardním skalárním součinem.

$$\begin{aligned} [\mathbf{u}]_B &= (\mathbf{v}_1^* \mathbf{u}, \mathbf{v}_2^* \mathbf{u}, \mathbf{v}_3^* \mathbf{u})^T \\ &= \left(\frac{1}{3}(-i, -2i, -2i) \begin{pmatrix} 3+i \\ 2 \\ i \end{pmatrix}, \frac{1}{3}(-2, -1, 2) \begin{pmatrix} 3+i \\ 2 \\ i \end{pmatrix}, \right. \\ &\qquad \left. \frac{1}{3}(2, -2, 1) \begin{pmatrix} 3+i \\ 2 \\ i \end{pmatrix} \right)^T \\ &= \left(\frac{1}{3}(3-7i), -\frac{8}{3}, \frac{1}{3}(2+3i) \right)^T . \end{aligned}$$

Skutečně

$$\begin{pmatrix} 3+i \\ 2 \\ i \end{pmatrix} = \frac{1}{3}(3-7i) \cdot \frac{1}{3} \begin{pmatrix} i \\ 2i \\ 2i \end{pmatrix} - \frac{8}{3} \cdot \frac{1}{3} \begin{pmatrix} -2 \\ -1 \\ 2 \end{pmatrix} + \frac{1}{3}(2+3i) \cdot \frac{1}{3} \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix} .$$

▲

Vzhledem k ortonormální bázi přechází skalární součin na standardní. Přesněji řečeno, skalární součin dvou vektorů je roven standardnímu skalárnímu součinu souřadnic těchto vektorů vzhledem k ortonormální bázi.

Tvrzení 8.50. *Je-li* $\mathbf{V}$ *vektorový prostor se skalárním součinem* $\langle , \rangle$, $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ *jeho ortonormální báze, a* $\mathbf{u}, \mathbf{w} \in V$, *pak*

$$\langle \mathbf{u}, \mathbf{w} \rangle = [\mathbf{u}]_B^* [\mathbf{w}]_B .$$

Důkaz. Označme $[\mathbf{u}]_B = (a_1, a_2, \ldots, a_n)^T$, $[\mathbf{w}]_B = (b_1, b_2, \ldots, b_n)^T$, tedy

$$\mathbf{u} = a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2 + \cdots + a_n \mathbf{v}_n, \quad \mathbf{w} = b_1 \mathbf{v}_1 + b_2 \mathbf{v}_2 + \cdots + b_n \mathbf{v}_n .$$

Pomocí (SL2), (SL1) a ortonormality postupně dostáváme

$$\begin{aligned} \langle \mathbf{u}, \mathbf{w} \rangle &= \left\langle \sum_{i=1}^n a_i \mathbf{v}_i, \sum_{i=1}^n b_i \mathbf{v}_i \right\rangle = \sum_{i=1}^n \sum_{j=1}^n \langle a_i \mathbf{v}_i, b_j \mathbf{v}_j \rangle \\ &= \sum_{i=1}^n \sum_{j=1}^n \overline{a_i} b_j \langle \mathbf{v}_i, \mathbf{v}_j \rangle = \sum_{i=1}^n \overline{a_i} b_i = [\mathbf{u}]_B^* [\mathbf{w}]_B . \end{aligned}$$

▲

Tvrzení ospravedlňuje poznámku z příkladu 8.45 – pokud si nakreslíme vektory ortonormální báze jako jednotkové navzájem kolmé vektory a ostatní vektory kreslíme v tomto souřadném systému, pak délky a úhly při daném skalárním součinu jsou běžné eukleidovské délky a úhly na obrázku.

PŘÍKLAD 8.51. V prostoru $\mathbb{R}^2$ se skalárním součinem

$$\left\langle (x_1,x_2)^T,(y_1,y_2)\right\rangle^T = (x_1,x_2)\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = 2x_1y_1 + x_1y_2 + x_2y_1 + x_2y_2$$

je posloupnost

$$B = \left(\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 2 \end{pmatrix}\right)$$

ortonormální báze (viz příklad 8.45). Uvažujme vektory $\mathbf{u} = (2,3)^T$ a $\mathbf{v} = (1,1)^T$. Z tvrzení 8.48 spočteme jejich souřadnice vzhledem k B a pak vypočítáme skalární součin podle tvrzení 8.50.

$$[\mathbf{u}]_B = \left(\left\langle \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \mathbf{u}\right\rangle, \left\langle \frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 2 \end{pmatrix}, \mathbf{u}\right\rangle\right)^T = \frac{1}{\sqrt{2}}\begin{pmatrix} 7 \\ 3 \end{pmatrix}$$

$$[\mathbf{v}]_B = \left(\left\langle \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \mathbf{v}\right\rangle, \left\langle \frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 2 \end{pmatrix}, \mathbf{v}\right\rangle\right)^T = \frac{1}{\sqrt{2}}\begin{pmatrix} 3 \\ 1 \end{pmatrix}$$

$$\langle \mathbf{u},\mathbf{v}\rangle = [\mathbf{u}]_B \cdot [\mathbf{v}]_B = \frac{1}{\sqrt{2}}(7,3)\ \frac{1}{\sqrt{2}}\begin{pmatrix} 3 \\ 1 \end{pmatrix} = 12\ .$$

Stejný výsledek dostaneme přímo ze vzorce definující tento skalární součin. ▲

8.4. Ortogonální projekce a ortogonalizace

Nyní se seznámíme s pojmem ortogonální (pravoúhlé, kolmé) projekce vektoru na podprostor. Tato projekce je v jistém smyslu nejlepší aproximací daného vektoru v podprostoru, čehož se využívá v aplikacích. Ortogonální projekce je také základem jednoho z nejdůležitějších algoritmů v lineární algebře – Gramovy-Schmidtovy ortogonalizace. Jeho důležitost je srovnatelná s Gaussovou eliminací.

8.4.1. Ortogonální projekce.

DEFINICE 8.52. Je-li $\mathbf{V}$ vektorový prostor se skalárním součinem $\langle\,,\rangle$, $\mathbf{v} \in V$ a W podprostor $\mathbf{V}$, pak prvek $\mathbf{w} \in W$ nazýváme *ortogonální projekce* vektoru $\mathbf{v}$ *na podprostor* W, pokud platí $(\mathbf{v}-\mathbf{w}) \perp W$.

Z definice snadno odvodíme, že pokud $\mathbf{v} \in W$, pak ortogonální projekcí $\mathbf{w}$ na W je vektor $\mathbf{w} = \mathbf{v}$. Platí totiž $\mathbf{v} - \mathbf{w} = \mathbf{o} \perp W$. Později (Důsledek **??**) uvidíme, že ortogonální projekce je ve skutečnosti lineární zobrazení.

Vektor $\mathbf{v}-\mathbf{w}$ budeme někdy nazývat *kolmice* vektoru $\mathbf{v}$ na podprostor W, nebo také *chybový vektor* aproximace vektoru $\mathbf{v}$ v podprostoru W.

OBRAZEK

Následující *věta o aproximaci* je jednoduchým, ale velmi důležitým, důsledkem Pythagorovy věty. Dokazuje intuitivně pochopitelný fakt, že ortogonální projekce vektoru na podprostor je, pokud existuje, určená jednoznačně a minimalizuje vzdálenost vektoru $\mathbf{v}$ od vektorů podprostoru W.

VĚTA 8.53. *Je-li W podprostor vektorového prostoru $\mathbf{V}$ se skalárním součinem $\langle\,,\rangle$, $\mathbf{v} \in V$ a $\mathbf{w}$ ortogonální projekce prvku $\mathbf{v}$ na podprostor W, pak pro každý prvek $\mathbf{w} \neq \mathbf{u} \in W$ platí*

$$\|\mathbf{v}-\mathbf{w}\| < \|\mathbf{v}-\mathbf{u}\|\ .$$

Ortogonální projekce vektoru $\mathbf{v}$ na podprostor W je určena jednoznačně, pokud existuje.

Důkaz. Protože $\mathbf{w}$ je ortogonální projekce $\mathbf{v}$ na W, je $(\mathbf{v}-\mathbf{w}) \perp W$, speciálně platí $(\mathbf{v}-\mathbf{w}) \perp (\mathbf{w}-\mathbf{u})$, protože vektor $\mathbf{w}-\mathbf{u}$ leží v W jakožto rozdíl dvou vektorů v W. Podle Pythagorovy věty platí

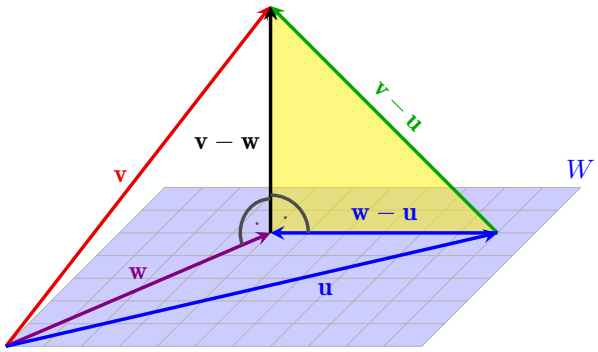
$$\|\mathbf{v}-\mathbf{u}\|^2 = \|(\mathbf{v}-\mathbf{w})+(\mathbf{w}-\mathbf{u})\|^2 = \|\mathbf{v}-\mathbf{w}\|^2 + \|\mathbf{w}-\mathbf{u}\|^2 > \|\mathbf{v}-\mathbf{w}\|^2 \quad ,$$

kde poslední nerovnost plyne z $\mathbf{w}-\mathbf{u} \neq \mathbf{o}$.

Kdyby oba vektory $\mathbf{w}, \mathbf{u} \in W$ byly ortogonálními projekcemi $\mathbf{v}$ na W, platilo by podle právě dokázaného

$$\|\mathbf{v}-\mathbf{w}\| < \|\mathbf{v}-\mathbf{u}\| < \|\mathbf{v}-\mathbf{w}\| \quad ,$$

což nelze. Ortogonální projekce $\mathbf{v}$ na W je proto určena jednoznačně. ▲



Obrázek 8.6. Důkaz věty o aproximaci

Ve smyslu předchozí věty je ortogonální projekce $\mathbf{w}$ vektoru $\mathbf{v}$ na podprostor W nejlepší aproximací vektoru $\mathbf{v}$ v tomto podprostoru. Má totiž nejmenší normu chybového vektoru $\mathbf{v}-\mathbf{w}$ mezi všemi možnými vektory z $\mathbf{w} \in W$.

Kdy ortogonální projekce existuje a jak ji hledat? Následující tvrzení ukazuje, že ortogonální projekce na $\mathbf{W}$ existuje, pokud ve $\mathbf{W}$ máme konečnou ortonormální bázi. Navíc poskytuje jednoduchý vzorec na její výpočet. Později uvidíme, že každý konečně generovaný prostor se skalárním součinem má (konečnou) ortonormální bázi, takže v libovolném prostoru se skalárním součinem existuje ortogonální projekce libovolného vektoru na libovolný konečně generovaný podprostor.

Tvrzení 8.54. *Je-li* $\mathbf{V}$ *vektorový prostor se skalárním součinem* $\langle\,,\rangle$, $\mathbf{v} \in V$, *a* $\mathbf{W}$ *konečně generovaný podprostor prostoru* $\mathbf{V}$ *s ortonormální bází* $B = (\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k)$, *pak prvek*

$$\mathbf{w} = \langle \mathbf{u}_1, \mathbf{v}\rangle \mathbf{u}_1 + \langle \mathbf{u}_2, \mathbf{v}\rangle \mathbf{u}_2 + \cdots + \langle \mathbf{u}_k, \mathbf{v}\rangle \mathbf{u}_k \quad ,$$

je ortogonální projekcí vektoru $\mathbf{v}$ *na podprostor* W.

Jinými slovy, ortogonální projekcí vektoru $\mathbf{v}$ *na podprostor* W *je vektor* $\mathbf{w}$ *se souřadnicemi*

$$[\mathbf{w}]_B = (\langle \mathbf{u}_1, \mathbf{v}\rangle, \langle \mathbf{u}_2, \mathbf{v}\rangle, \cdots, \langle \mathbf{u}_k, \mathbf{v}\rangle)^T \quad .$$

Důkaz. Libovolný prvek $\mathbf{w}$ podprostoru $\mathbf{W}$ můžeme vyjádřit jako lineární kombinaci prvků ortonormální báze $(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k)$. Prvek

$$\mathbf{w} = a_1\mathbf{u}_1 + a_2\mathbf{u}_2 + \cdots + a_k\mathbf{u}_k$$

je podle definice ortogonální projekcí prvku $\mathbf{v}$ na podprostor $W = \mathrm{LO}\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\}$ právě když je prvek $\mathbf{v}-\mathbf{w}$ ortogonální ke každému prvku podprostoru $\mathbf{W}$ a to podle

tvrzení 8.40 nastává právě když je ortogonální ke každému prvku $\mathbf{u}_i$. Pro každé $i = 1, 2, \ldots, k$ je prvek $\mathbf{u}_i$ kolmý k prvku $\mathbf{v} - \mathbf{w}$ právě když

$$\begin{aligned} 0 &= \langle \mathbf{u}_i, \mathbf{v} - \mathbf{w} \rangle = \langle \mathbf{u}_i, \mathbf{v} \rangle - \langle \mathbf{u}_i, \mathbf{w} \rangle \\ &= \langle \mathbf{u}_i, \mathbf{v} \rangle - \langle \mathbf{u}_i, a_1\mathbf{u}_1 + a_2\mathbf{u}_2 + \cdots + a_k\mathbf{u}_k \rangle \\ &= \langle \mathbf{u}_i, \mathbf{v} \rangle - a_1 \langle \mathbf{u}_i, \mathbf{u}_1 \rangle - a_2 \langle \mathbf{u}_i, \mathbf{u}_2 \rangle - \cdots - a_k \langle \mathbf{u}_i, \mathbf{u}_k \rangle \\ &= \langle \mathbf{u}_i, \mathbf{v} \rangle - a_i \langle \mathbf{u}_i, \mathbf{u}_i \rangle = \langle \mathbf{u}_i, \mathbf{v} \rangle - a_i \ , \end{aligned}$$

tj. právě když $a_i = \langle \mathbf{u}_i, \mathbf{v} \rangle$. ▲

Všimněte si, že vzorec pro výpočet ortogonální projekce na podprostor s ortonormální bází je stejný jako vzorec z tvrzení 8.48 pro souřadnice prvku vzhledem k ortonormální bázi. Tvrzení 8.48 je speciálním případem předešlého tvrzení, kdy $V = W$.

Pokud báze $(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k)$ v podprostoru $\mathbf{W}$ není ortonormální, ale pouze ortogonální, napřed ji normalizujeme

$$\frac{\mathbf{u}_1}{\|\mathbf{u}_1\|}, \frac{\mathbf{u}_2}{\|\mathbf{u}_2\|}, \ldots, \frac{\mathbf{u}_k}{\|\mathbf{u}_k\|}$$

a pak použijeme předchozí tvrzení. Dostaneme tak vyjádření ortogonální projekce $\mathbf{w}$ prvku $\mathbf{v}$ na podprostor W ve tvaru

$$\begin{aligned} \mathbf{w} &= \left\langle \frac{\mathbf{u}_1}{\|\mathbf{u}_1\|}, \mathbf{v} \right\rangle \frac{\mathbf{u}_1}{\|\mathbf{u}_1\|} + \left\langle \frac{\mathbf{u}_2}{\|\mathbf{u}_2\|}, \mathbf{v} \right\rangle \frac{\mathbf{u}_2}{\|\mathbf{u}_2\|} + \cdots + \left\langle \frac{\mathbf{u}_k}{\|\mathbf{u}_k\|}, \mathbf{v} \right\rangle \frac{\mathbf{u}_k}{\|\mathbf{u}_k\|} \\ &= \frac{\langle \mathbf{u}_1, \mathbf{v} \rangle}{\|\mathbf{u}_1\|^2} \mathbf{u}_1 + \frac{\langle \mathbf{u}_2, \mathbf{v} \rangle}{\|\mathbf{u}_2\|^2} \mathbf{u}_2 + \cdots + \frac{\langle \mathbf{u}_k, \mathbf{v} \rangle}{\|\mathbf{u}_k\|^2} \mathbf{u}_k \ . \end{aligned}$$

Dokázali jsme tak následující důsledek.

Důsledek 8.55. *Je-li* $\mathbf{V}$ *vektorový prostor se skalárním součinem* $\langle , \rangle$, $\mathbf{v} \in V$, *a* $\mathbf{W}$ *konečně generovaný podprostor* $\mathbf{V}$ *s ortogonální bází* $B = (\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k)^T$, *pak prvek*

$$\mathbf{w} = \frac{\langle \mathbf{u}_1, \mathbf{v} \rangle}{\|\mathbf{u}_1\|^2} \mathbf{u}_1 + \frac{\langle \mathbf{u}_2, \mathbf{v} \rangle}{\|\mathbf{u}_2\|^2} \mathbf{u}_2 + \cdots + \frac{\langle \mathbf{u}_k, \mathbf{v} \rangle}{\|\mathbf{u}_k\|^2} \mathbf{u}_k$$

je ortogonální projekcí vektoru $\mathbf{v}$ *na podprostor* $\mathbf{W}$.

Pomocí souřadnic vzhledem k ortogonální bázi B poslední důsledek zapíšeme ve tvaru

$$[\mathbf{w}]_B = \left(\frac{\langle \mathbf{u}_1, \mathbf{v} \rangle}{\|\mathbf{u}_1\|^2}, \frac{\langle \mathbf{u}_2, \mathbf{v} \rangle}{\|\mathbf{u}_2\|^2}, \ldots, \frac{\langle \mathbf{u}_k, \mathbf{v} \rangle}{\|\mathbf{u}_k\|^2} \right) \ .$$

V případě podprostoru $W = \mathrm{LO}\{\mathbf{u}\}$ dimenze 1 dostáváme projekci $\mathbf{w}$ libovolného prvku $\mathbf{v} \in \mathbf{V}$ na podprostor $\mathrm{LO}\{\mathbf{u}\}$ jako

$$\mathbf{w} = \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\|\mathbf{u}\|^2} \mathbf{u} \ .$$

To odpovídá závěru příkladu 8.3.

Příklad 8.56. V aritmetickém prostoru $\mathbb{R}^3$ se standardním skalárním součinem je $((1, 1, 2)^T, (2, 0, -1)^T)$ ortogonální posloupnost. Ortogonální projekce $\mathbf{w}$

vektoru $\mathbf{v} = (1,2,3)^T$ na rovinu $W = \mathrm{LO}\left\{(1,1,2)^T, (2,0,-1)^T\right\}$ je tedy

$$\begin{aligned}\mathbf{w} &= \frac{(1,1,2)(1,2,3)^T}{(1,1,2)(1,1,2)^T}\begin{pmatrix}1\\1\\2\end{pmatrix} + \frac{(2,0,-1)(1,2,3)^T}{(2,0,-1)(2,0,-1)^T}\begin{pmatrix}2\\0\\-1\end{pmatrix}\\ &= \frac{9}{6}\begin{pmatrix}1\\1\\2\end{pmatrix} - \frac{1}{5}\begin{pmatrix}2\\0\\-1\end{pmatrix} = \frac{1}{10}\begin{pmatrix}11\\15\\32\end{pmatrix}\ .\end{aligned}$$

Jde skutečně o ortogonální projekci vektoru $\mathbf{v}$ na podprostor W, protože chybový vektor $\mathbf{v}-\mathbf{w} = \frac{1}{10}(-1,5,-2)^T$ je kolmý na oba dva generátory $(1,1,2)^T$, $(2,0,-1)^T$ prostoru W.

Vektor $\mathbf{w}$ je podle věty 8.53 ten jednoznačně určený vektor v W, pro který je chyba $\|\mathbf{v}-\mathbf{w}\|$ nejmenší možná. ▲

Příklad 8.57. V $\mathbb{R}^2$ se skalárním součinem

$$\left\langle (x_1,x_2)^T, (y_1,y_2)\right\rangle^T = (x_1,x_2)\begin{pmatrix}2 & 1\\1 & 1\end{pmatrix}\begin{pmatrix}y_1\\y_2\end{pmatrix} = 2x_1y_1 + x_1y_2 + x_2y_1 + x_2y_2$$

je ortogonální projekce vektoru $\mathbf{v} = (1,0)^T$ na přímku $\mathrm{LO}\left\{(0,1)^T\right\}$ rovná

$$\mathbf{w} = \frac{(0,1)\begin{pmatrix}2 & 1\\1 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}}{(0,1)\begin{pmatrix}2 & 1\\1 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}\ .$$

Skutečně, chybový vektor $\mathbf{v}-\mathbf{w} = (1,-1)^T$ je kolmý na $(0,1)^T$, protože

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

▲

Příklad 8.58. Najdeme nejlepší aproximaci funkce x^2 ve tvaru $a + b\sin x + c\cos x$ (kde $a,b,c \in \mathbb{R}$) ve smyslu, že

$$\int_{-\pi}^{\pi} \left(x^2 - (a + b\sin x + c\cos x)\right)^2\, dx$$

je co nejmenší.

Protože

$$0 = \int_{-\pi}^{\pi} \sin x\, dx = \int_{-\pi}^{\pi} \cos x\, dx = \int_{-\pi}^{\pi} \sin x\cos x\, dx\ ,$$

je posloupnost funkcí $(1, \sin x, \cos x)$ ortogonální. Hledaná nejlepší aproximace je funkce x^2 je tedy

$$\frac{\int_{-\pi}^{\pi} x^2\, dx}{\int_{-\pi}^{\pi} 1\, dx}\cdot 1 + \frac{\int_{-\pi}^{\pi} x^2(\sin x)\, dx}{\int_{-\pi}^{\pi}(\sin x)^2\, dx}\cdot \sin x + \frac{\int_{-\pi}^{\pi} x^2(\cos x)\, dx}{\int_{-\pi}^{\pi}(\cos x)^2\, dx}\cdot \cos x \approx 3.29 - 4\cos x$$

▲

8.4.2. Gramova matice. Tvrzení 8.54 dává vzorec na výpočet ortogonální projekce vektoru $\mathbf{v} \in V$ na konečně generovaný podprostor $\mathbf{W}$, známe-li v $\mathbf{W}$ nějakou ortonormální bázi. Odvození vzorce z důkazu tohoto tvrzení lze obecněji použít v případě, že v $\mathbf{W}$ máme dánu obecnou množinu generátorů, tj. ne nutně ortogonální.

Tvrzení 8.59. *Je-li* $\mathbf{W}$ *konečně generovaný podprostor vektorového prostoru* $\mathbf{V}$ *se skalárním součinem* $\langle\,,\rangle$, $\mathbf{v} \in V$ *a* $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\}$ *množina generátorů prostoru* $\mathbf{W}$, *pak vektor*

$$\mathbf{w} = a_1\mathbf{u}_1 + \cdots + a_k\mathbf{u}_k$$

je ortogonální projekcí vektoru $\mathbf{v}$ *na* W *právě tehdy, když je aritmetický vektor* $(a_1, \dots, a_k)^T$ *řešením soustavy lineárních rovnic*

$$\left(\begin{array}{cccc|c} \langle \mathbf{u}_1, \mathbf{u}_1 \rangle & \langle \mathbf{u}_1, \mathbf{u}_2 \rangle & \cdots & \langle \mathbf{u}_1, \mathbf{u}_k \rangle & \langle \mathbf{u}_1, \mathbf{v} \rangle \\ \langle \mathbf{u}_2, \mathbf{u}_1 \rangle & \langle \mathbf{u}_2, \mathbf{u}_2 \rangle & \cdots & \langle \mathbf{u}_2, \mathbf{u}_k \rangle & \langle \mathbf{u}_2, \mathbf{v} \rangle \\ \vdots & & \ddots & \vdots & \vdots \\ \langle \mathbf{u}_k, \mathbf{u}_1 \rangle & \langle \mathbf{u}_k, \mathbf{u}_2 \rangle & \cdots & \langle \mathbf{u}_k, \mathbf{u}_k \rangle & \langle \mathbf{u}_k, \mathbf{v} \rangle \end{array}\right) .$$

Důkaz. Definice ortogonální projekce $\mathbf{w}$ prvku $\mathbf{v}$ na podprostor $\mathbf{W}$ říká, že musí platit $(\mathbf{v} - \mathbf{w}) \perp \mathbf{W}$, což platí právě když $(\mathbf{v} - \mathbf{w}) \perp \mathbf{u}_i$ pro každé $i = 1, 2, \dots, k$, neboli právě když $\langle \mathbf{u}_i, \mathbf{w} \rangle = \langle \mathbf{u}_i, \mathbf{v} \rangle$.

Pro každé $i = 1, \dots, k$ je součin $\langle \mathbf{u}_i, \mathbf{w} \rangle$ z linearity roven

$$\langle \mathbf{u}_i, \mathbf{w} \rangle = \langle \mathbf{u}_i, a_1\mathbf{u}_1 + \cdots + a_k\mathbf{u}_k \rangle = a_1 \langle \mathbf{u}_i, \mathbf{u}_1 \rangle + a_2 \langle \mathbf{u}_i, \mathbf{u}_2 \rangle + \cdots + a_k \langle \mathbf{u}_i, \mathbf{u}_k \rangle \ .$$

Rovnost $\langle \mathbf{u}_i, \mathbf{w} \rangle = \langle \mathbf{u}_i, \mathbf{v} \rangle$ je tedy ekvivalentní rovnosti

$$a_1 \langle \mathbf{u}_i, \mathbf{u}_1 \rangle + a_2 \langle \mathbf{u}_i, \mathbf{u}_2 \rangle + \cdots + a_k \langle \mathbf{u}_i, \mathbf{u}_k \rangle = \langle \mathbf{u}_i, \mathbf{v} \rangle \ .$$

▲

V případě, že je v přechozím tvrzení posloupnost $B = (\mathbf{u}_1, \dots, \mathbf{u}_k)$ lineárně nezávislá (tedy tvoří bázi prostoru $\mathbf{W}$), pak lze závěr formulovat přehledněji tak, že souřadnice $[\mathbf{w}]_B$ ortogonální projekce $\mathbf{w}$ vektoru $\mathbf{v}$ na podprostor W jsou řešením uvedené soustavy rovnic.

Příklad 8.60. V prostoru reálných polynomů se skalárním součinem $\langle f, g \rangle = \int_0^1 fg$ najdeme ortogonální projekci $\mathbf{w}$ polynomu $\mathbf{v} = x^2$ na podprostor $\mathbf{W} = \mathrm{LO}\{\mathbf{u}_1, \mathbf{u}_2\} = \mathrm{LO}\{1, x\}$ polynomů stupně nejvýše 1.

Projekce je $\mathbf{w} = a + bx$ s neznámými koeficienty $a, b \in \mathbb{R}$, které podle předchozího tvrzení najdeme jako řešení soustavy

$$\left(\begin{array}{cc|c} \langle \mathbf{u}_1, \mathbf{u}_1 \rangle & \langle \mathbf{u}_1, \mathbf{u}_2 \rangle & \langle \mathbf{u}_1, \mathbf{v} \rangle \\ \langle \mathbf{u}_2, \mathbf{u}_1 \rangle & \langle \mathbf{u}_2, \mathbf{u}_2 \rangle & \langle \mathbf{u}_2, \mathbf{v} \rangle \end{array}\right) = \left(\begin{array}{cc|c} \int_0^1 1 & \int_0^1 x & \int_0^1 x^2 \\ \int_0^1 x & \int_0^1 x^2 & \int_0^1 x^3 \end{array}\right) = \left(\begin{array}{cc|c} 1 & \frac{1}{2} & \frac{1}{3} \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} \end{array}\right) .$$

Řešením soustavy dostaneme vektor $(a, b)^T = (-\frac{1}{6}, 1)^T$. Ortogonální projekce polynomu $\mathbf{v} = x^2$ je tedy

$$\mathbf{w} = a\mathbf{u}_1 + b\mathbf{u}_2 = -\frac{1}{6} + x \ .$$

▲

Matice soustavy z tvrzení 8.59 si také vysloužila vlastní jméno.

Definice 8.61. Jsou-li $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k$ prvky vektorového prostoru se skalárním součinem $\langle , \rangle$, pak čtvercovou matici

$$\begin{pmatrix} \langle \mathbf{u}_1, \mathbf{u}_1 \rangle & \langle \mathbf{u}_1, \mathbf{u}_2 \rangle & \cdots & \langle \mathbf{u}_1, \mathbf{u}_k \rangle \\ \langle \mathbf{u}_2, \mathbf{u}_1 \rangle & \langle \mathbf{u}_2, \mathbf{u}_2 \rangle & \cdots & \langle \mathbf{u}_2, \mathbf{u}_k \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle \mathbf{u}_k, \mathbf{u}_1 \rangle & \langle \mathbf{u}_k, \mathbf{u}_2 \rangle & \cdots & \langle \mathbf{u}_k, \mathbf{u}_k \rangle \end{pmatrix}$$

řádu k nazýváme *Gramova matice* posloupnosti vektorů $(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k)$.

Tvrzení 8.62. *Buď* $B = (\langle \mathbf{u}_i, \mathbf{u}_j \rangle)_{k \times k}$ *Gramova matice posloupnosti prvků* $(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k)$ *vektorového prostoru* $\mathbf{V}$ *se skalárním součinem* $\langle , \rangle$. *Pak matice* B *je regulární právě tehdy, když je posloupnost* $(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k)$ *lineárně nezávislá.*

Důkaz. Použijeme tvrzení 8.59 na vektor $\mathbf{v} = \mathbf{o}$, jehož ortogonální projekce je $\mathbf{w} = \mathbf{o}$. Matice soustavy z tvrzení je rovná B a pravá strana je nulová. Víme tedy, že $a_1\mathbf{u}_1 + \cdots + a_k\mathbf{u}_k = \mathbf{o}$ platí právě tehdy, když $(a_1, \ldots, a_k)^T$ je řešením homogenní soustavy rovnic s maticí B. Z toho vyplývá, že $a_1\mathbf{u}_1 + \cdots + a_k\mathbf{u}_k = \mathbf{o}$ pro nějaký nenulový vektor $(a_1, \ldots, a_k)^T$ (ekvivalentně $(\mathbf{u}_1, \ldots, \mathbf{u}_k)$ je lineárně závislá) právě tehdy, když homogenní soustava rovnic s maticí B má netriviální řešení (ekvivalentně B je singulární). ▲

Přeformulujeme si tvrzení 8.59 pro případ aritmetických vektorových prostorů se standardním skalárním součinem. Výhodné je v tomto případě používat maticový jazyk. Uvažujme tedy prostor $\mathbf{V} = \mathbb{R}^n$ nebo $\mathbf{V} = \mathbb{C}^n$, vektor $\mathbf{v} \in V$ a podprostor W prostoru $\mathbf{V}$ generovaný vektory $\mathbf{u}_1, \ldots, \mathbf{u}_k$. Označme $A = (\mathbf{u}_1 | \ldots | \mathbf{u}_k)$ – je to reálná nebo komplexní matice typu $n \times k$. Podprostor W je lineární obal sloupců této matice, takže $W = \operatorname{Im} A$. Výraz $a_1\mathbf{u}_1 + \cdots + a_k\mathbf{u}_k$ můžeme maticově zapsat jako $A\mathbf{x}$, kde $\mathbf{x} = (a_1, \ldots, a_k)^T$. Gramova matice je rovná A^*A (viz výpočet v poznámce) a pravá strana soustavy v tvrzení je rovná $A^*\mathbf{v}$. Tvrzení tedy v této situaci dává následující důsledek.

Důsledek 8.63. *Nechť A je reálná nebo komplexní matice typu $n \times k$ a $\mathbf{v} \in \mathbb{R}^n$ (resp. $\mathbf{v} \in \mathbb{C}^n$). Pak vektor $A\mathbf{x}$ (kde $\mathbf{x} \in \mathbb{R}^k$ nebo $\mathbf{x} \in \mathbb{C}^k$) je ortogonální projekcí vektoru $\mathbf{v}$ na podprostor $\operatorname{Im} A$ právě tehdy, když*

$$A^*A\mathbf{x} = A^*\mathbf{v} \ .$$

Důkaz. Důkaz jsme již provedli výše užitím tvrzení 8.59. Maticově jde důkaz přímo provést velmi rychle: Vektor $A\mathbf{x}$ je ortogonální projekcí vektoru $\mathbf{v}$ na $\operatorname{Im} A$ právě když $(\mathbf{v} - A\mathbf{x}) \perp \operatorname{Im} A$, což je právě když každý sloupec matice A je kolmý na $(\mathbf{v} - A\mathbf{x})$, to nastane právě když $A^*(\mathbf{v} - A\mathbf{x}) = \mathbf{o}$, a to je po drobné úpravě ekvivalentní $A^*A\mathbf{x} = A^*\mathbf{v}$. ▲

Gramovu matici lze vyjádřit ve tvaru A^*A i v obecném případě: Je-li $\mathbf{W}$ konečně generovaný vektorový prostor se skalárním součinem $\langle\, , \rangle$ a B je jeho ortonormální báze, pak Gramova matice posloupnosti $(\mathbf{u}_1, \ldots, \mathbf{u}_k)$ je rovná A^*A pro matici

$$A = ([\mathbf{u}_1]_B | [\mathbf{u}_2]_B | \cdots | [\mathbf{u}_k]_B) \ ,$$

protože podle tvrzení 8.50 o výpočtu skalárního součinu ze souřadnic vzhledem k ortonormální bázi platí

$$\begin{aligned} A^*A &= \begin{pmatrix} [\mathbf{u}_1]_B^*[\mathbf{u}_1]_B & [\mathbf{u}_1]_B^*[\mathbf{u}_2]_B & \cdots & [\mathbf{u}_1]_B^*[\mathbf{u}_k]_B \\ [\mathbf{u}_2]_B^*[\mathbf{u}_1]_B & [\mathbf{u}_2]_B^*[\mathbf{u}_2]_B & \cdots & [\mathbf{u}_2]_B^*[\mathbf{u}_k]_B \\ \vdots & \vdots & \ddots & \vdots \\ [\mathbf{u}_k]_B^*[\mathbf{u}_1]_B & [\mathbf{u}_k]_B^*[\mathbf{u}_2]_B & \cdots & [\mathbf{u}_k]_B^*[\mathbf{u}_k]_B \end{pmatrix} \\ &= \begin{pmatrix} \langle \mathbf{u}_1, \mathbf{u}_1 \rangle & \langle \mathbf{u}_1, \mathbf{u}_2 \rangle & \cdots & \langle \mathbf{u}_1, \mathbf{u}_k \rangle \\ \langle \mathbf{u}_2, \mathbf{u}_1 \rangle & \langle \mathbf{u}_2, \mathbf{u}_2 \rangle & \cdots & \langle \mathbf{u}_2, \mathbf{u}_k \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle \mathbf{u}_k, \mathbf{u}_1 \rangle & \langle \mathbf{u}_k, \mathbf{u}_2 \rangle & \cdots & \langle \mathbf{u}_k, \mathbf{u}_k \rangle \end{pmatrix} \ . \end{aligned}$$

8.4.3. Gramova-Schmidtova ortogonalizace. Nyní dokážeme, že v každém konečně generovaném vektorovém prostoru se skalárním součinem existuje ortonormální báze. Existenci ortonormální báze dokážeme pomocí algoritmu, kterému se říká *Gramova-Schmidtova ortogonalizace*.

Tento algoritmus dostane *na vstupu* nějakou lineárně nezávislou posloupnost

$$(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$$

prvků vektorového prostoru $\mathbf{V}$ se skalárním součinem. *Na výstupu* vydá ortonormální posloupnost

$$(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k)$$

prvků prostoru $\mathbf{V}$, která splňuje podmínku

$$\mathrm{LO}\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_i\} = \mathrm{LO}\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_i\}$$

pro každé $i = 1, 2, \ldots, k$.

Popíšeme variantu Gramovy-Schmidtovy ortogonalizace s průběžným normováním. První krok je jednoduchý – normalizujeme vektor $\mathbf{v}_1$, tj. položíme

$$\mathbf{u}_1 = \frac{\mathbf{v}_1}{\|\mathbf{v}_1\|} \ ,$$

pak platí také $\mathrm{LO}\{\mathbf{u}_1\} = \mathrm{LO}\{\mathbf{v}_1\}$. Z předpokladu lineární nezávislosti posloupnosti $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ vyplývá, že vektor $\mathbf{v}_1$ je nenulový, takže normalizaci můžeme provést.

V dalších krocích provádíme postupně pro $i = 2, 3, \ldots, k$ následující operace.

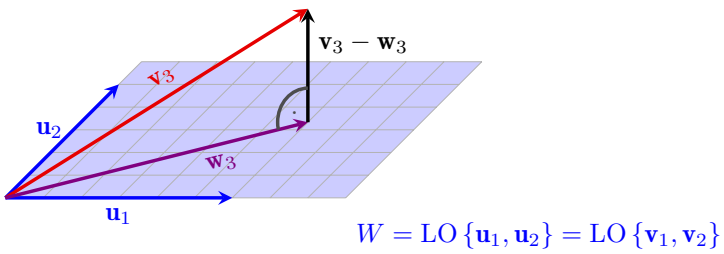
(ia) **ortogonalizace**: najdeme kolmici vektoru $\mathbf{v}_i$ na podprostor $\mathrm{LO}\{\mathbf{u}_1, \ldots, \mathbf{u}_{i-1}\}$. Podle tvrzení 8.54 ji můžeme vypočítat vztahem

$$\mathbf{v}_i - \mathbf{w}_i = \mathbf{v}_i - \langle \mathbf{u}_1, \mathbf{v}_i \rangle \ \mathbf{u}_1 - \langle \mathbf{u}_2, \mathbf{v}_i \rangle \ \mathbf{u}_2 - \cdots - \langle \mathbf{u}_{i-1}, \mathbf{v}_i \rangle \ \mathbf{u}_{i-1},$$

kde $\mathbf{w}_i$ značí ortogonální projekci vektoru $\mathbf{v}_i$ na daný podprostor;

(ib) **normalizace**: položíme

$$\mathbf{u}_i = \frac{\mathbf{v}_i - \mathbf{w}_i}{\|\mathbf{v}_i - \mathbf{w}_i\|} \ .$$



Obrázek 8.7. Krok (3a)

Ověříme, že algoritmus funguje, tj. že algoritmus proběhne (to v našem případě znamená, že v (ib) nikdy nedělíme nulou) a že výsledná n-tice $(\mathbf{u}_1, \ldots, \mathbf{u}_n)$ je ortonormální posloupnost splňující $\mathrm{LO}\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_i\} = \mathrm{LO}\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_i\}$ pro každé $i = 1, 2, \ldots, k$. To dokážeme indukcí.

Předpokládejme, že jsme již spočítali prvních $i-1$ vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_{i-1}$, které tvoří ortonormální posloupnost takovou, že $\mathrm{LO}\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{i-1}\} = \mathrm{LO}\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{i-1}\}$. V kroku (ia) je vektor $\mathbf{v}_i - \mathbf{w}_i$ kolmý na všechny vektory v $\mathrm{LO}\{\mathbf{u}_1, \ldots, \mathbf{u}_{i-1}\}$ podle definice ortogonální projekce a kolmice. Speciálně je tento vektor kolmý na vektory $\mathbf{u}_1, \ldots, \mathbf{u}_{i-1}$, které jsou také navzájem kolmé podle indukčního předpokladu. Posloupnost $(\mathbf{u}_1, \ldots, \mathbf{u}_{i-1}, \mathbf{v}_i - \mathbf{w}_i)$ je tedy ortogonální.

Zdůvodníme, že vektor $\mathbf{v}_i - \mathbf{w}_i$ nemůže být nulový. V opačném případě je $\mathbf{v}_i = \mathbf{w}_i$, neboli ortogonální projekce vektoru $\mathbf{v}_i$ na podprostor $\mathrm{LO}\{\mathbf{u}_1, \ldots, \mathbf{u}_{i-1}\} = \mathrm{LO}\{\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}\}$ (indukční předpoklad) je rovná $\mathbf{v}_i$. To znamená, že $\mathbf{v}_i$ v tomto podprostoru leží, což je spor s lineární nezávislostí $(\mathbf{v}_1, \ldots, \mathbf{v}_i)$.

Protože je vektor $\mathbf{v}_i - \mathbf{w}_i$ nenulový, jeho norma je rovněž nenulová a normalizaci v kroku (ib) můžeme provést. Nyní víme, že $(\mathbf{u}_1, \ldots, \mathbf{u}_i)$ je ortonormální a zbývá ověřit rovnost

$$\mathrm{LO}\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_i\} = \mathrm{LO}\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_i\} \quad .$$

Ověříme nejprve inkluzi $\subseteq$ – stačí ověřit, že vektory $\mathbf{u}_1, \ldots, \mathbf{u}_i$ leží v lineárním obalu napravo. Z indukčního předpokladu víme, že $\mathrm{LO}\{\mathbf{u}_1, \ldots, \mathbf{u}_{i-1}\} = \mathrm{LO}\{\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}\}$. Speciálně, každý z vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_{i-1}$ leží v $\mathrm{LO}\{\mathbf{v}_1, \ldots, \mathbf{v}_i\}$. Vektor $\mathbf{u}_i$ je, jak vidíme z jeho výpočtu, lineární kombinací $\mathbf{v}_i, \mathbf{u}_1, \ldots, \mathbf{u}_{i-1}$. Leží proto také v $\mathrm{LO}\{\mathbf{u}_1, \ldots, \mathbf{u}_{i-1}, \mathbf{v}_i\} \subseteq \mathrm{LO}\{\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_i\}$.

Důkaz opačné inkluze je rovněž snadný. Vektory $\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}$ leží v lineárním obalu vlevo díky indukčnímu předpokladu, vektor $\mathbf{v}_i$ díky vyjádření $\mathbf{v}_i = \|\mathbf{v}_i - \mathbf{w}_i\|\, \mathbf{u}_i + \mathbf{w}_i$, ve kterém oba vektory $\mathbf{u}_i$ a $\mathbf{w}_i$ v lineárním obalu $\mathrm{LO}\{\mathbf{u}_1, \ldots, \mathbf{u}_i\}$ zřejmě leží.

Dokázali jsme následující větu.

Věta 8.64. *Gramova-Schmidtova ortogonalizace převede libovolnou lineárně nezávislou posloupnost* $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ *prvků vektorového prostoru se skalárním součinem na ortonormální posloupnost* $(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k)$*, pro kterou platí*

$$\mathrm{LO}\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_i\} = \mathrm{LO}\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_i\}$$

pro každé $i = 1, 2, \ldots, k$.

Pokud chceme najít pouze ortogonální bázi, stačí vynechat v algoritmu kroky (ib). V takovém případě hledáme ortogonální projekci $\mathbf{w}_i$ vektoru $\mathbf{v}_i$ na podprostor $\mathrm{LO}\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{i-1}\}$ s ortogonální bází $(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{i-1})$ a k jejímu výpočtu musíme použít důsledek 8.55 místo tvrzení 8.54. Výpočtu norem vektorů $\mathbf{v}_i - \mathbf{w}_i$ se tím ale nevyhneme (s výjimkou toho posledního).

Příklad 8.65. V podprostoru

$$W = \mathrm{LO}\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\} = \mathrm{LO}\left\{(1,2,0,1)^T, (1,-1,1,0)^T, (0,1,1,3)^T\right\}$$

prostoru $\mathbb{R}^4$ se standardním skalárním součinem najdeme ortonormální bázi ($\mathbf{u}_1$, $\mathbf{u}_2$, $\mathbf{u}_3$). Použijeme Gramovu-Schmidtovou ortogonalizaci na posloupnost vektorů $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$. Postupně počítáme

$$\mathbf{u}_1 = \frac{\mathbf{v}_1}{\|\mathbf{v}_1\|} = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix} \quad ,$$

$$\mathbf{w}_2 = \langle \mathbf{u}_1, \mathbf{v}_2 \rangle\, \mathbf{u}_1 = \frac{1}{\sqrt{6}}(1,2,0,1) \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \end{pmatrix} \frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix} = -\frac{1}{6} \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix} \quad ,$$

$$\mathbf{v}_2 - \mathbf{w}_2 = \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \end{pmatrix} + \frac{1}{6} \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{6} \begin{pmatrix} 7 \\ -4 \\ 6 \\ 1 \end{pmatrix} \quad ,$$

$$\mathbf{u}_2 = \frac{\mathbf{v}_2 - \mathbf{w}_2}{\|\mathbf{v}_2 - \mathbf{w}_2\|} = \frac{1}{\sqrt{102}} \begin{pmatrix} 7 \\ -4 \\ 6 \\ 1 \end{pmatrix} \quad .$$

$$
\begin{aligned}
\mathbf{w}_3 &= \langle \mathbf{u}_1, \mathbf{v}_3 \rangle \mathbf{u}_1 + \langle \mathbf{u}_2, \mathbf{v}_3 \rangle \mathbf{u}_2 \\
&= \frac{1}{\sqrt{6}}(1,2,0,1) \begin{pmatrix} 0 \\ 1 \\ 1 \\ 3 \end{pmatrix} \frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix} + \frac{1}{\sqrt{102}}(7,-4,6,1) \begin{pmatrix} 0 \\ 1 \\ 1 \\ 3 \end{pmatrix} \frac{1}{\sqrt{102}} \begin{pmatrix} 7 \\ -4 \\ 6 \\ 1 \end{pmatrix} \\
&= \frac{5}{6} \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix} + \frac{5}{102} \begin{pmatrix} 7 \\ -4 \\ 6 \\ 1 \end{pmatrix} = \frac{1}{102} \begin{pmatrix} 120 \\ 150 \\ 30 \\ 90 \end{pmatrix} = \frac{5}{17} \begin{pmatrix} 4 \\ 5 \\ 1 \\ 3 \end{pmatrix} \ , \\
\mathbf{v}_3 - \mathbf{w}_3 &= \begin{pmatrix} 0 \\ 1 \\ 1 \\ 3 \end{pmatrix} - \frac{5}{17} \begin{pmatrix} 4 \\ 5 \\ 1 \\ 3 \end{pmatrix} = \frac{4}{17} \begin{pmatrix} -5 \\ -2 \\ 3 \\ 9 \end{pmatrix} \ , \\
\mathbf{u}_3 &= \frac{\mathbf{v}_3 - \mathbf{w}_3}{\|\mathbf{v}_3 - \mathbf{w}_3\|} = \frac{1}{\sqrt{119}} \begin{pmatrix} -5 \\ -2 \\ 3 \\ 9 \end{pmatrix} \ .
\end{aligned}
$$

Získali jsme tak ortonormální posloupnost

$$
\left(\frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{102}} \begin{pmatrix} 7 \\ -4 \\ 6 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{119}} \begin{pmatrix} -5 \\ -2 \\ 3 \\ 9 \end{pmatrix} \right) \ ,
$$

která je ortonormální bází podprostoru $W = \mathrm{LO}\left\{(1,2,0,1)^T, (1,-1,1,0)^T, (0,1,1,3)^T\right\}$.

▲

Při řešení předchozího příkladu jsme neověřovali předpoklad, že daná posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ je lineárně nezávislá. Není to nutné, protože algoritmus pro Gramovu-Schmidtovu ortogonalizaci sám pozná, je-li některý z daných prvků $\mathbf{v}_i$ lineárně závislý na předchozích. Pokud by takový prvek $\mathbf{v}_i$ existoval, pro první z nich by platilo

$$
\mathbf{v}_i \in \mathrm{LO}\left\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{i-1}\right\} = \mathrm{LO}\left\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{i-1}\right\} \ .
$$

Ortogonální projekce $\mathbf{w}_i$ prvku $\mathbf{v}_i$ na podprostor $\mathrm{LO}\left\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{i-1}\right\}$ by se rovnala $\mathbf{v}_i$ a rozdíl $\mathbf{v}_i - \mathbf{w}_i$ by byl nulový vektor. V kroku (ib) by se algoritmus ozval, že má dělit číslem 0, a zastavil by se. Gramovu-Schmidtovu ortogonalizaci tak můžeme použít ke zjištění, je-li nějaká posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ prvků vektorového prostoru se skalárním součinem lineárně závislá nebo nezávislá.

Další příklad ukazuje ortogonalizaci v prostoru funkcí.

Příklad 8.66. V prostoru reálných polynomů se skalárním součinem $\langle f, g \rangle = \int_0^1 fg$ budeme ortogonalizovat posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) = (1, x, x^2)$. Zároveň spočítáme ortogonální projekci vektoru x^2 na podprostor $\mathrm{LO}\left\{1, x\right\}$, neboli aproximaci vektoru x^2 funkcí tvaru $a + bx$, která je nejlepší vzhledem k danému skalárnímu součinu.

$$
\mathbf{u}_1 = \frac{\mathbf{v}_1}{\|\mathbf{v}_1\|} = \frac{1}{\sqrt{\int_0^1 1^2 dx}} 1 = 1 \ ,
$$

$$\mathbf{w}_2 = \langle \mathbf{u}_1, \mathbf{v}_2 \rangle \mathbf{u}_1 = \left(\int_0^1 (1 \cdot x)\, dx \right) \cdot 1 = \frac{1}{2} \ ,$$

$$\mathbf{v}_2 - \mathbf{w}_2 = x - \frac{1}{2} \ ,$$

$$\mathbf{u}_2 = \frac{\mathbf{v}_2 - \mathbf{w}_2}{\|\mathbf{v}_2 - \mathbf{w}_2\|} = \frac{x - \frac{1}{2}}{\sqrt{\int_0^1 (x - \frac{1}{2})^2\, dx}} = 2\sqrt{3}x - \sqrt{3} \ .$$

$$\begin{aligned} \mathbf{w}_3 &= \langle \mathbf{u}_1, \mathbf{v}_3 \rangle \mathbf{u}_1 + \langle \mathbf{u}_2, \mathbf{v}_3 \rangle \mathbf{u}_2 \\ &= \left(\int_0^1 (1 \cdot x^2)\, dx \right) 1 + \left(\int_0^1 \left(2\sqrt{3}x - \sqrt{3} \right) x^2\, dx \right) \left(2\sqrt{3}x - \sqrt{3} \right) = x - \frac{1}{6} \ , \end{aligned}$$

$$\mathbf{v}_3 - \mathbf{w}_3 = x^2 - x + \frac{1}{6},$$

$$\mathbf{u}_3 = \frac{\mathbf{v}_3 - \mathbf{w}_3}{\|\mathbf{v}_3 - \mathbf{w}_3\|} = \frac{x^2 - x + \frac{1}{6}}{\sqrt{\int_0^1 \left(x^2 - x + \frac{1}{6} \right)^2\, dx}} = \frac{x^2 - x + \frac{1}{6}}{\sqrt{\frac{1}{180}}} = \sqrt{180} \left(x^2 - x + \frac{1}{6} \right).$$

Získali jsme tak ortonormální bázi

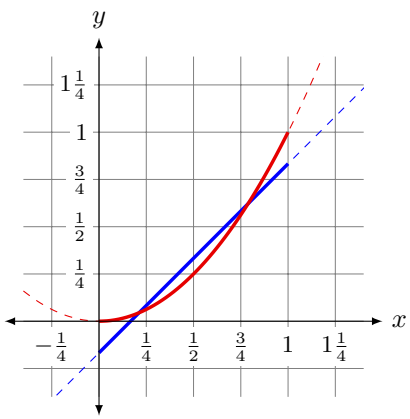
$$\left(1, 2\sqrt{3}x - \sqrt{3}, \sqrt{180} \left(x^2 - x + \frac{1}{6} \right) \right)$$

prostoru LO $\left\{ 1, x, x^2 \right\}$ polynomů stupně nejvýše 2.

Ortogonální projekce (a hledaná aproximace) vektoru $\mathbf{v}_3 = x^2$ na podprostor LO $\{1, x\} = \text{LO}\{\mathbf{v}_1, \mathbf{v}_2\} = \text{LO}\{\mathbf{u}_1, \mathbf{u}_2\}$ je vektor

$$\mathbf{w}_3 = x - 1/6 \ .$$

Chybový vektor, tj. rozdíl $\mathbf{v}_3 - \mathbf{w}_3$ je $x^2 - x + \frac{1}{6}$, jeho velikost je $\sqrt{1/180}$.



Obrázek 8.8. K příkladu 8.66

▲

Gramova-Schmidtova ortogonalizace obecně není numericky stabilní. Její stabilitu lze vylepšit tak, že jednotlivé algebraické operace při výpočtu děláme v jiném pořadí, ale tak, aby se výsledek nezměnil. Tomu se říká *modifikovaná Gramova-Schmidtova ortogonalizace*. Existují i jiné numericky stabilní ortogonalizační postupy, například algoritmus využívající Householderovy transformace, nebo algoritmus využívající Givensovy rotace.

PŘÍKLAD 8.67. V aritmetice se zaokrouhlováním na tři platná místa vyjde Gramovou-Schmidtovou ortogonalizací (vzhledem ke standardnímu skalárnímu součinu v $\mathbb{R}^3$)

$$\left(\begin{pmatrix} 1 \\ 10^{-3} \\ 10^{-3} \end{pmatrix}, \begin{pmatrix} 1 \\ 10^{-3} \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 10^{-3} \end{pmatrix}\right)$$

posloupnost

$$\left(\begin{pmatrix} 1 \\ 10^{-3} \\ 10^{-3} \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ -0{,}709 \\ -0{,}709 \end{pmatrix}\right) .$$

Druhý a třetí vektor příliš kolmé nevyšly. Je to způsobené tím, že původní vektory jsou skoro rovnoběžné. ▲

8.4.4. QR-rozklad. QR-rozklad je maticová formulace Gramovy-Schmidtovy ortogonalizace v aritmetických vektorových prostorech se standardním skalárním součinem. Ze vzorce pro Gramovu-Schmidtovu ortogonalizaci vidíme, že původní vektory $\mathbf{v}_i$ lze vyjádřit jako lineární kombinaci vektorů $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_i$, které jsou navzájem ortogonální a jednotkové. Použijeme-li tento fakt na lineárně nezávislou posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ reálných (nebo komplexních) n-složkových aritmetických vektorů, získáme vyjádření matice $A = (\mathbf{v}_1|\mathbf{v}_2|\ldots|\mathbf{v}_k)$ jako součinu matice $(\mathbf{u}_1|\mathbf{u}_2|\ldots|\mathbf{u}_k)$ s ortonormální posloupností sloupců a horní trojúhelníkové matice řádu k. Tomuto vyjádření říkáme QR-rozklad. Později v tvrzení 8.86 ukážeme, že QR-rozklad reguální matice je jednoznačný.

TVRZENÍ 8.68 (o QR-rozkladu). *Je-li A reálná nebo komplexní matice typu $n \times k$ s lineárně nezávislou posloupností sloupcových vektorů, pak existuje matice Q typu $n \times k$ nad stejným tělesem s ortonormální posloupností sloupců (vzhledem ke standardnímu skalárnímu součinu) a horní trojúhelníková matice R řádu k s kladnými reálnými prvky na hlavní diagonále taková, že platí $A = QR$.*

DŮKAZ. Označíme $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ posloupnost sloupcových vektorů matice A. Na tuto posloupnost provedeme Gramovu-Schmidtovu ortogonalizaci, tj. volme pro každé $i = 1, 2, \ldots, k$

$$\begin{aligned} \mathbf{w}_i &= \langle \mathbf{u}_1, \mathbf{v}_i \rangle \mathbf{u}_1 + \langle \mathbf{u}_2, \mathbf{v}_i \rangle \mathbf{u}_2 + \cdots + \langle \mathbf{u}_{i-1}, \mathbf{v}_i \rangle \mathbf{u}_{i-1} \ , \\ \mathbf{u}_i &= \frac{\mathbf{v}_i - \mathbf{w}_i}{\|\mathbf{v}_i - \mathbf{w}_i\|} \ . \end{aligned}$$

(Pro $i = 1$ bude podle této definice $\mathbf{w}_1$ prázný součet, tj. $\mathbf{w}_1 = \mathbf{o}$ je projekce $\mathbf{u}_1$ na nulový podprostor.)

Z toho získáme vyjádření

$$\begin{aligned} \mathbf{v}_i &= \|\mathbf{v}_i - \mathbf{w}_i\| \, \mathbf{u}_i + \mathbf{w}_i \\ &= \|\mathbf{v}_i - \mathbf{w}_i\| \, \mathbf{u}_i + \langle \mathbf{u}_1, \mathbf{v}_i \rangle \mathbf{u}_1 + \langle \mathbf{u}_2, \mathbf{v}_i \rangle \mathbf{u}_2 + \cdots + \langle \mathbf{u}_{i-1}, \mathbf{v}_i \rangle \mathbf{u}_{i-1} \\ &= \langle \mathbf{u}_1, \mathbf{v}_i \rangle \mathbf{u}_1 + \langle \mathbf{u}_2, \mathbf{v}_i \rangle \mathbf{u}_2 + \cdots + \langle \mathbf{u}_{i-1}, \mathbf{v}_i \rangle \mathbf{u}_{i-1} + \|\mathbf{v}_i - \mathbf{w}_i\| \, \mathbf{u}_i \ , \end{aligned}$$

což můžeme maticově zapsat ve tvaru

$$(\mathbf{v}_1|\mathbf{v}_2|\ldots|\mathbf{v}_k) = (\mathbf{u}_1|\ldots|\mathbf{u}_k) \begin{pmatrix} \|\mathbf{v}_1 - \mathbf{w}_1\| & \langle \mathbf{u}_1, \mathbf{v}_2 \rangle & \ldots & \langle \mathbf{u}_1, \mathbf{v}_k \rangle \\ 0 & \|\mathbf{v}_2 - \mathbf{w}_2\| & \ldots & \langle \mathbf{u}_2, \mathbf{v}_k \rangle \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \|\mathbf{v}_k - \mathbf{w}_k\| \end{pmatrix} .$$

Provádíme-li Gramovu-Schmidtovu ortogonalizaci vzhledem ke standardnímu součinu, dostáváme požadovaný rozklad

$$(\mathbf{v}_1|\mathbf{v}_2|\ldots|\mathbf{v}_k) = (\mathbf{u}_1|\ldots|\mathbf{u}_k) \begin{pmatrix} \|\mathbf{v}_1 - \mathbf{w}_1\| & \mathbf{u}_1^* \mathbf{v}_2 & \ldots & \mathbf{u}_1^* \mathbf{v}_k \\ 0 & \|\mathbf{v}_2 - \mathbf{w}_2\| & \ldots & \mathbf{u}_2^* \mathbf{v}_k \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \|\mathbf{v}_k - \mathbf{w}_k\| \end{pmatrix} .$$

▲

PŘÍKLAD 8.69. Vypočítáme QR-rozklad reálné matice

$$A = (\mathbf{v}_1|\mathbf{v}_2|\mathbf{v}_3) = \begin{pmatrix} 1 & 1 & 0 \\ 2 & -1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 3 \end{pmatrix} .$$

Gramovu-Schmidtovu ortogonalizaci posloupnosti sloupcových vektorů $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ v aritmetickém prostoru se standardním skalárním součinem jsme spočítali už v příkladu 8.65. Našli jsme tam ortonormální posloupnost

$$(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3) = \left(\frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{102}} \begin{pmatrix} 7 \\ -4 \\ 6 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{119}} \begin{pmatrix} -5 \\ -2 \\ 3 \\ 9 \end{pmatrix} \right) .$$

Z výpočtu také můžeme vyčíst všechny prvky matice R z důkazu předchozí věty. Dostaneme

$$\begin{pmatrix} 1 & 1 & 0 \\ 2 & -1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{6} & 7/\sqrt{102} & -5/\sqrt{119} \\ 2/\sqrt{6} & -4/\sqrt{102} & -2/\sqrt{119} \\ 0 & 6/\sqrt{102} & 3/\sqrt{119} \\ 1/\sqrt{6} & 1/\sqrt{102} & 9/\sqrt{119} \end{pmatrix} \begin{pmatrix} \sqrt{6} & -1/\sqrt{6} & 5/\sqrt{6} \\ 0 & \sqrt{102}/6 & 5/\sqrt{102} \\ 0 & 0 & 4\sqrt{119}/17 \end{pmatrix} .$$

▲

QR-rozklad lze použít při řešení reálných (komplexních) soustav lineárních rovnic $A\mathbf{x} = \mathbf{b}$ s danou regulární maticí A a různými vektory pravých stran $\mathbf{b}$ podobným způsobem, jakým lze použít LU-rozklad. Spočteme QR-rozklad matice $A = QR$. Protože Q má ortonormální posloupnost sloupců, platí $Q^*Q = I_n$ (viz poznámka), takže $Q^* = Q^{-1}$, protože Q je čtvercová. Rovnici $A\mathbf{x} = \mathbf{b}$ přepíšeme do tvaru $QR\mathbf{x} = \mathbf{b}$ a vynásobíme $Q^* = Q^{-1}$. Soustava

$$R\mathbf{x} = Q^*\mathbf{b}$$

má horní trojúhelníkovou matici, můžeme ji proto vyřešit zpětnou substitucí. Algoritmus pro QR-rozklad je numericky stabilnější než Gaussova eliminace, která vede na LU-rozklad. Vyžaduje ale zhruba n^3 aritmetických operací, což je třikrát více než výpočet LU-rozkladu.

8.4.5. Existence ortonormální báze. Důsledkem Gramovy-Schmidtovy ortogonalizace (věta 8.64) je následující věta o existenci ortonormální báze.

VĚTA 8.70. *Je-li* $\mathbf{W}$ *podprostor konečně generovaného vektorového prostoru* $\mathbf{V}$ *se skalárním součinem, pak každou ortonormální (ortogonální) bázi v podprostoru* $\mathbf{W}$ *lze doplnit na ortonormální (ortogonální) bázi celého prostoru* $\mathbf{V}$.

Speciálně, v každém konečně generovaném vektorovém prostoru se skalárním součinem existuje ortonormální báze.

DŮKAZ. Nechť $(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k)$ ortonormální báze $\mathbf{W}$. Tuto lineárně nezávislou posloupnost můžeme doplnit vektory $\mathbf{v}_{k+1}, \ldots, \mathbf{v}_n$ na bázi $\mathbf{V}$ (viz důsledek 5.64). Gramova-Schmidtova ortogonalizace z posloupnosti $(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k, \mathbf{v}_{k+1}, \ldots, \mathbf{v}_n)$ vytvoří ortonormální posloupnost, přičemž prvních k prvků nezmění. (Můžeme ji také „spustit“ až od $(k+1)$-ního cyklu).

Totéž uděláme v případě pouhé ortogonální báze $(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k)$ podprostoru $\mathbf{W}$, Gramovu-Schmidtovu ortogonalizaci použijeme bez normalizačních kroků (ib).

▲

Pomocí existence ortonormální báze lze dokázat řadu užitečných věcí. První příkladem je následující věta, která formalizuje intuitivní tvrzení, že každý konečně generovaný vektorový prostor se skalárním součinem je „v podstatě stejný“ jako aritmetický vektorový prostor se standardním skalárním součinem.

VĚTA 8.71. *Je-li* $\mathbf{V}$ *vektorový prostor dimenze* n *nad* $\mathbb{R}$ *(nebo nad* $\mathbb{C}$*) se skalárním součinem* $\langle\, , \rangle$*, pak existuje izomorfismus* $f : \mathbf{V} \to \mathbb{R}^n$ *(nebo* $f : \mathbf{V} \to \mathbb{C}^n$*), pro který platí*

$$\langle \mathbf{u}, \mathbf{v} \rangle = f(\mathbf{u}) \cdot f(\mathbf{v})$$

pro každé dva prvky $\mathbf{u}, \mathbf{v} \in \mathbf{V}$.

DŮKAZ. V prostoru $\mathbf{V}$ zvolíme ortonormální bázi B a definujeme f předpisem $f(\mathbf{u}) = [\mathbf{u}]_B$. Podle tvrzení 6.27 je f izomorfizmus mezi $\mathbf{V}$ a $\mathbb{R}^n$ (nebo $\mathbb{C}^n$). Podle tvrzení 8.50 platí

$$\langle \mathbf{u}, \mathbf{v} \rangle = [\mathbf{u}]_B^* \, [\mathbf{v}]_B = f(\mathbf{u}) \cdot f(\mathbf{v}) \ .$$

▲

Dalším důskedkem je pozitivní definitnost Gramovy matice lineárně nezávislé posloupnosti.

TVRZENÍ 8.72. *Gramova matice* $B = (\langle \mathbf{u}_i, \mathbf{u}_j \rangle)_{k\times k}$ *lineárně nezávislé posloupnosti prvků* $(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k)$ *vektorového prostoru* $\mathbf{V}$ *se skalárním součinem* $\langle\,,\rangle$ *je* B *pozitivně definitní.*

DŮKAZ. Ze skorosymetrie (SSS) skalárního součinu plyne, že je matice B je hermitovská. Označme $\mathbf{W}$ podprostor prostoru $\mathbf{V}$ generovaný vektory $\mathbf{u}_1, \dots, \mathbf{u}_k$ a zvolme nějakou ortonormální bázi C prostoru $\mathbf{W}$. Výpočet na konci sekce 8.4.2 ukazuje, že $B = A^*A$ pro matici $A = ([\mathbf{u}_1]_C | \cdots | [\mathbf{u}_k]_C)$. Matice A je regulární, protože je čtvercová a její sloupce tvoří lineárně nezávislou posloupnost. Pozitivní definitnost matic tvaru A^*A pro regulární matici A jsme ale již ověřili za definicí 8.20 pozitivně definitních matic. ▲

A konečně si také můžeme dokázat, že ortogonální projekce lineární zobrazení (tvrzení platí i pro prostory, které nejsou konečně generované, ale důkaz vynecháme).

TVRZENÍ 8.73. *Je-li* $\mathbf{V}$ *vektorový prostor se skalárním součinem* $\langle\,,\rangle$, $\mathbf{v} \in V$ *a* $\mathbf{W}$ *konečně generovaný podprostor* $\mathbf{V}$, *pak je ortogonální projekce z* $\mathbf{V}$ *do* $\mathbf{W}$ *lineárním zobrazením.*

DŮKAZ. Označme $f\colon \mathbf{V} \to \mathbf{W}$ tuto ortogonální projekci. Zvolme ortonormální bázi $(\mathbf{u}_1, \dots, \mathbf{u}_k)$ prostoru $\mathbf{W}$. Z tvrzení 8.54 máme $f(\mathbf{v}) = \sum_{i=1}^{k} \langle \mathbf{u}_i, \mathbf{v} \rangle \mathbf{u}_i$. Nyní už lze snadno z definice ověřit, že $f(\mathbf{v} + \mathbf{v}') = f(\mathbf{v}) + f(\mathbf{v}')$ a $f(t\mathbf{v}) = tf(\mathbf{v})$ (klíčovou ingrediencí důkazu je, že pro každé $i = 1, 2, \dots, k$ je zobrazení $\mathbf{v} \mapsto \langle \mathbf{u}_i, \mathbf{v} \rangle$ lineární formou). ▲

8.4.6. Ortogonální doplněk. Největší množina prvků kolmá na danou množinu $M \subseteq V$ se nazývá ortogonální doplněk.

DEFINICE 8.74. Je-li $\mathbf{V}$ prostor se skalárním součinem $\langle\,,\rangle$ a $M \subseteq V$, pak *ortogonální doplněk* $M^\perp$ množiny M je množina všech prvků V kolmých na každý prvek M, tj.

$$M^\perp = \{\mathbf{v} \in V : \mathbf{v} \perp M\} \ .$$

Podle definice M je kolmá na $M^\perp$ a $M^\perp$ je největší taková množina vzhledem k inkluzi. Další jednoduché vlastnosti ortogonálního doplňku jsou:

TVRZENÍ 8.75. *Je-li* $\mathbf{V}$ *prostor se skalárním součinem* $\langle\,,\rangle$ *a* $M, N \subseteq V$, *pak platí*

(1) $M^\perp = (\mathrm{LO}\, M)^\perp$,
(2) $M^\perp$ *je podprostor* $\mathbf{V}$,
(3) *je-li* $M \subseteq N$, *pak* $N^\perp \subseteq M^\perp$.

DŮKAZ. Platí $\mathbf{v} \in M^\perp$ právě když $\mathbf{v} \perp M$ což je právě když $\mathbf{v} \perp \mathrm{LO}\, M$ podle tvrzení 8.40, a to je právě když $\mathbf{v} \in (\mathrm{LO}\, M)^\perp$.

K důkazu (2) stačí ověřit, že ortogonální doplněk $M^\perp$ je neprázdný a uzavřený na sčítání a násobení skalárem. Je neprázdný, protože obsahuje nulový vektor. Je-li $\mathbf{u}, \mathbf{v} \in M^\perp$, platí pro každé $\mathbf{w} \in M$, že $\mathbf{u} \perp \mathbf{w}$ a $\mathbf{v} \perp \mathbf{w}$, a tedy $\langle \mathbf{w}, \mathbf{u} + \mathbf{v} \rangle = \langle \mathbf{w}, \mathbf{u} \rangle + \langle \mathbf{w}, \mathbf{v} \rangle = 0$, což dokazuje $\mathbf{u} + \mathbf{v} \in M^\perp$. Podobně lze dokázat uzavřenost $M^\perp$ na skalární násobky.

Stejně snadné je ověřit (3). Je-li $\mathbf{v} \in N^\perp$, platí $\mathbf{v} \perp N \supseteq M$, tj. také $\mathbf{v} \perp M$ a tedy $\mathbf{v} \in M^\perp$. ▲

PŘÍKLAD 8.76. Určíme ortogonální doplněk roviny $U = \mathrm{LO}\left\{(1,2,5)^T, (0,1,1)^T)\right\}$ v prostoru $\mathbb{R}^3$ se standardním skalárním součinem. Podle (1) je $U^\perp$ rovná množině všech vektorů $\mathbf{x}$ kolmých na oba generátory, tj. množině vektorů, pro které $(1,2,5)\mathbf{x} = 0$ a $(0,1,1)\mathbf{x} = 0$. Maticově

$$\begin{pmatrix} 1 & 2 & 5 \\ 0 & 1 & 1 \end{pmatrix} \mathbf{x} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} .$$

Hledáme tedy řešení homogenní soustavy s maticí, jejíž řádkové vektory jsou generátory U,

$$U^\perp = \mathrm{Ker} \begin{pmatrix} 1 & 2 & 5 \\ 0 & 1 & 1 \end{pmatrix} = \mathrm{LO}\left\{ \begin{pmatrix} -3 \\ -1 \\ 1 \end{pmatrix} \right\} .$$

Obecněji, je-li $(\mathbf{u}, \mathbf{v})$ lineárně nezávislá posloupnost vektorů v prostoru $\mathbb{R}^3$, pak ortogonální doplněk množiny $M = \{\mathbf{u}, \mathbf{v}\}$ je přímka kolmá na rovinu $\mathrm{LO}\{\mathbf{u}, \mathbf{v}\}$. Ortogonálním doplňkem nenulového vektoru (nebo jeho lineárního obalu) je rovina. Intuitivně jsou tato trvzení zřejmá, formálně je zdůvodníme níže. ▲

V příkladu jsme viděli, že k určení ortogonálního doplňku množiny vektorů $M = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k\}$ (nebo podprostoru $\mathrm{LO}\, M$) v aritmetickém vektorovém prostoru $\mathbb{R}^n$ se standardním skalárním součinem stačí napsat vektory $\mathbf{v}_1^T, \mathbf{v}_2^T, \dots, \mathbf{v}_k^T$ do řádků matice A a vyřešit příslušnou homogenní soustavu. Toto pozorování lze maticově zapsat

$$\{v_1, \dots, v_k\}^\perp = (\mathrm{Im}\, A^T)^\perp = \mathrm{Ker}\, A \ .$$

Vlastně jsme jen zopakovali úvahu z příkladu 8.7, kde jsme nahlédli, že řešení homogenní soustavy rovnic $A\mathbf{x} = \mathbf{o}$ jsou právě vektory kolmé na všechny řádky matice A (ekvivalentně na všechny prvky řádkového prostoru matice A).

V $\mathbb{C}^n$ se standardním skalárním součinem je ještě třeba přidat komplexní sdružování:

$$(\mathrm{Im}\, A^*)^\perp = \mathrm{Ker}\, A \ .$$

Čili $\mathrm{Ker}\, A$ je rovno ortogonálnímu doplňku komplexně sdružených řádků matice A.

Obecněji, počítáme-li vzhledem k ortonormální bázi, pak skalární součin se chová jako standardní (viz tvrzení 8.50), takže ortogonální doplněk množiny vektorů můžeme spočítat podobně.

TVRZENÍ 8.77. *Nechť* $\mathbf{V}$ *je konečně generovaný prostor se skalárním součinem* $\langle\, , \rangle$, B *jeho ortonormální báze,* $M = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k\}$. *Označíme* A *matici s řádky* $[\mathbf{v}_1]_B^*$, $[\mathbf{v}_2]_B^*$, ..., $[\mathbf{v}_k]_B^*$. *Pak*

$$[M^\perp]_B = \mathrm{Ker}\, A \ .$$

DŮKAZ. Z definice vyjádření podmnožiny vzhledem k bázi, definice ortogonálního doplňku a tvrzení 8.50 máme

$$\begin{aligned} [M^\perp]_B &= \{[\mathbf{u}]_B : \mathbf{u} \in M^\perp\} = \{[\mathbf{u}]_B : \langle \mathbf{v}_1, \mathbf{u}\rangle = \langle \mathbf{v}_2, \mathbf{u}\rangle = \dots = \langle \mathbf{v}_k, \mathbf{u}\rangle = 0\} \\ &= \{[\mathbf{u}]_B : [\mathbf{v}_1]_B^*[\mathbf{u}]_B = [\mathbf{v}_2]_B^*[\mathbf{u}]_B = \dots = [\mathbf{v}_k]_B^*[\mathbf{u}]_B = 0\} \\ &= \{\mathbf{x} : A\mathbf{x} = \mathbf{o}\} = \mathrm{Ker}\, A \ . \end{aligned}$$

▲

PŘÍKLAD 8.78. V $\mathbb{C}^3$ je dán skalární součin $\langle\, , \rangle$ takový, že báze

$$B = \left(\begin{pmatrix} 1 \\ i \\ i \end{pmatrix}, \begin{pmatrix} 1 \\ 1+i \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right)$$

je ortonormální. Určíme ortogonální doplněk N přímky $\mathrm{LO}\{\mathbf{v}\}$, kde

$$\mathbf{v} = \begin{pmatrix} 3 \\ 1+2i \\ i \end{pmatrix} .$$

Souřadnice vektoru $\mathbf{v}$ vzhledem k bázi B je

$$[\mathbf{v}]_B = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} .$$

Z vlastnosti (1) v tvrzení 8.75 vyplývá, že N je rovno ortogonálnímu doplňku množiny $\{\mathbf{v}\}$. Vyjádření N v bázi B je proto podle tvrzení 8.77 rovno

$$[N]_B = \mathrm{Ker}\,(1\ 1\ 1) = \mathrm{LO}\left\{ \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} \right\} ,$$

takže

$$\begin{aligned} N = \mathrm{LO}\,\{\mathbf{v}\}^{\perp} &= \mathrm{LO}\left\{ -\begin{pmatrix} 1 \\ i \\ i \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, -\begin{pmatrix} 1 \\ i \\ i \end{pmatrix} + \begin{pmatrix} 1 \\ 1+i \\ 0 \end{pmatrix} \right\} \\ &= \mathrm{LO}\left\{ \begin{pmatrix} 0 \\ -i \\ -i \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -i \end{pmatrix} \right\} = \mathrm{LO}\left\{ \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -i \end{pmatrix} \right\} . \end{aligned}$$

▲

Následující věta shrnuje důležité vlastnosti ortogonálních doplňků podprostoru. Jde o další užitečný důsledek věty 8.70 o existenci ortonormální báze.

VĚTA 8.79. *Nechť* $\mathbf{V}$ *je vektorový prostor se skalárním součinem* $\langle\,,\rangle$ *a* $\mathbf{W}$ *je konečně generovaný podprostor* $\mathbf{V}$. *Pak platí*

(1) $V = W \oplus W^{\perp}$,
(2) $(W^{\perp})^{\perp} = W$.
(3) *Každý vektor* $\mathbf{v} \in V$ *má jednoznačně určenou ortogonální projekci na* W *a také jednoznačně určenou ortogonální projekci na* $W^{\perp}$.
(4) *Je-li* $\mathbf{V}$ *konečně generovaný prostor dimenze* n, *pak* $\dim(\mathbf{W}^{\perp}) = n - \dim(\mathbf{W})$,

DŮKAZ. Podle věty 8.70 existuje ortonormální báze prostoru $\mathbf{W}$ (se skalárním součinem zděděným z prostoru $\mathbf{V}$). Zvolme tedy nějakou ortonormální bázi $(\mathbf{w}_1, \ldots, \mathbf{w}_k)$ prostoru $\mathbf{W}$, tj. $\dim \mathbf{W} = k$.

(1). Pro každý vektor $\mathbf{v} \in V$ existuje podle tvrzení 8.54 ortogonální projekce $\mathbf{w}$ na podprostor W. V součtu $\mathbf{v} = \mathbf{w} + (\mathbf{v} - \mathbf{w})$ je první vektor z W a druhý vektor z $W^{\perp}$. To ukazuje, že $V = W + W^{\perp}$. Navíc W je kolmý na $W^{\perp}$, takže jejich jediným společným vektorem je $\mathbf{o}$. Platí tedy $W \cap W^{\perp} = \{\mathbf{o}\}$ a $W + W^{\perp} = V$, což zapisujeme jako $V = W \oplus W^{\perp}$.

(2). Podprostor W je kolmý na $W^{\perp}$, takže W je podmnožinou $(W^{\perp})^{\perp}$. K důkazu druhé inkluze uvažujme libovolný vektor $\mathbf{v} \in (W^{\perp})^{\perp}$ a snažme se ukázat $\mathbf{v} \in W$. Jako v přechozím bodu, vektor $\mathbf{v}$ má ortogonální projekci $\mathbf{w}$ na W. Podle definice ortogonální projekce je $\mathbf{v} - \mathbf{w} \in W^{\perp}$, speciálně $\mathbf{w} \perp (\mathbf{v} - \mathbf{w})$, protože $\mathbf{w} \in W$. Vektor $\mathbf{v} \in (W^{\perp})^{\perp}$ je kolmý na každý vektor z $W^{\perp}$, platí tedy $\mathbf{v} \perp (\mathbf{v} - \mathbf{w})$. Nyní

$$\|\mathbf{v} - \mathbf{w}\|^2 = \langle \mathbf{v} - \mathbf{w}, \mathbf{v} - \mathbf{w} \rangle = \langle \mathbf{v}, \mathbf{v} - \mathbf{w} \rangle - \langle \mathbf{w}, \mathbf{v} - \mathbf{w} \rangle = 0 - 0 ,$$

z čehož plyne $\mathbf{v} - \mathbf{w} = \mathbf{o}$, protože skalární součin je pozitivně definitní. Ukázali jsme $\mathbf{v} = \mathbf{w} \in W$, jak jsme chtěli.

(3). Jednoznačnost ortogonální projekce vektoru $\mathbf{v} \in V$ byla dokázána ve větě 8.53, existence ortogonální projekce $\mathbf{w}$ vektoru $\mathbf{v}$ na W v tvrzení 8.54. Vektor $\mathbf{v} - \mathbf{w}$ leží v prostoru $W^\perp$. Protože $\mathbf{v} - (\mathbf{v} - \mathbf{w}) = \mathbf{w} \in W = (W^\perp)^\perp$ podle předchozího bodu, je $\mathbf{v} - \mathbf{w}$ ortogonální projekcí vektoru $\mathbf{v}$ na podprostor $W^\perp$.

(4). Z věty o dimenzi součtu a průniku 5.103 a bodu (1) spočítáme

$$\dim \mathbf{W}^\perp = \dim(\mathbf{W} + \mathbf{W}^\perp) + \dim(\mathbf{W} \cap \mathbf{W}^\perp) - \dim \mathbf{W} = \dim(\mathbf{V}) + 0 - k = n - k \ .$$

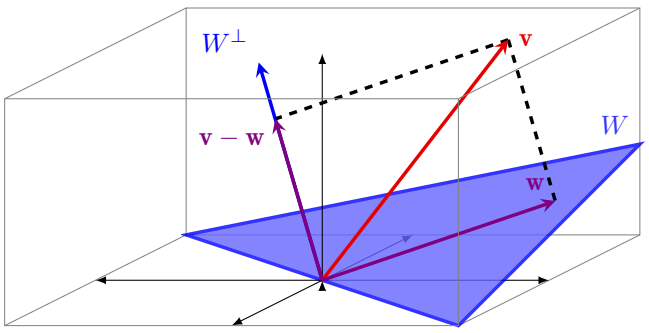
▲

Ve větě se předpokládá, že podprostor $\mathbf{W}$ je konečně generovaný, ale $\mathbf{V}$ být konečně generovaný nemusí. To odpovídá například situaci z příkladu 8.58, kde $\mathbf{V}$ je prostor spojitých funkcí a $\mathbf{W}$ je podprostor generovaný konečně mnoha spojitými funkcemi. Předpoklad, že $\mathbf{W}$ je konečně generovaný nelze vynechat, viz cvičení.

Jedno pozorování učiněné v důkazu věty si zaslouží zdůraznit. Ortogonální projekce $\mathbf{w}$ vektoru $\mathbf{v}$ na prostor W dává rozklad

$$\mathbf{v} = \mathbf{w} + (\mathbf{v} - \mathbf{w}), \qquad \text{kde } \mathbf{w} \in W \ \text{ a } \ (\mathbf{v} - \mathbf{w}) \in W^\perp,$$

a kolmice – vektor $\mathbf{v} - \mathbf{w}$ – je zároveň ortogonální projekcí vektoru $\mathbf{v}$ na podprostor $\mathbf{W}^\perp$.



Dokázaná věta nám také umožňuje zdůvodnit tvrzení v příkladu 8.7 o interpretaci řešení soustavy lineárních rovnic $A\mathbf{x} = \mathbf{b}$ nad reálnými čísly. V příkladu jsme si všimli, že vektor $\mathbf{x}$ je směrovým vektorem množiny řešení (tj. $\mathbf{x} \in \operatorname{Ker} A$) právě tehdy, když je kolmý ke všem řádkovým vektorům matice A. To nastane právě tehdy, když je kolmý k řádkovému prostoru. Maticově zapsáno, $\operatorname{Ker} A = (\operatorname{Im} A^T)^\perp$. Z bodu (2) nyní také máme

$$\operatorname{Im} A^T = ((\operatorname{Im} A^T)^\perp)^\perp = (\operatorname{Ker} A)^\perp \ ,$$

slovy, vektor je kolmý ke všem prvkům $\operatorname{Ker} A$ právě tehdy, když leží v lineárním obalu řádků matice A. Ještě trochu jinak, normálové vektory množiny všech řešení soustavy $A\mathbf{x} = \mathbf{o}$ jsou právě lineární kombinace řádků matice A.

Bod (1) nám také dává rozklad

$$\operatorname{Ker} A \oplus \operatorname{Im} A^T = \mathbb{R}^n,$$

kde n je počet sloupců matice A.

Nad komplexními čísly vychází stejné vztahy, jen je potřeba transponování nahradit hermitovským sdružováním a reálné prostory $\mathbb{R}^n, \mathbb{R}^m$ komplexními prostory $\mathbb{C}^n, \mathbb{C}^m$.

Příklad 8.80. Pro matici

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

máme

$$\operatorname{Ker} A = \operatorname{LO}\left\{(-1,5,3)^T\right\}, \quad \operatorname{Im} A^T = \operatorname{LO}\left\{(1,2,-3)^T, (1,-1,2)^T\right\} \ .$$

Přímku $\operatorname{Ker} A$ tvoří právě vektory kolmé na rovinu $\operatorname{Im} A^T$, rovinu $\operatorname{Im} A^T$ tvoří právě vektory kolmé na přímku $\operatorname{Ker} A$ a platí $\operatorname{Ker} A \oplus \operatorname{Im} A^T = \mathbb{R}^3$. ▲

8.5. Unitární a ortogonální zobrazení a matice

Lineární zobrazení mezi prostory se skalárními součiny se nazývá unitární (v reálném případě ortogonální), pokud zachovává skalární součin a tím pádem i odvozené pojmy jako normu, kolmost, v reálném případě úhel. Představa je taková, že zatímco obecné lineární zobrazení může objekty lineárně deformovat (např. zkosení), nebo dokonce degenerovat (např. projekce na přímku v nějakém směru), ortogonální zobrazení objekty může pouze rotovat nebo ještě překlápět podle nadroviny. Této intuici lze dát přesný smysl, v kapitole o vlastních číslech to provedeme pro ortogonální zobrazení $\mathbb{R}^2 \to \mathbb{R}^2$ a $\mathbb{R}^3 \to \mathbb{R}^3$.

Nejdůležitějším speciálním případem jsou unitární (ortogonální) zobrazení mezi stejnými prostory, tzv. unitární (ortogonální) operátory. Unitární operátory jsou základní objekty v kvantové mechanice.

8.5.1. Unitární a ortogonální matice. Začneme maticovou verzí unitárních (ortogonálních) operátorů na aritmetických prostorech. Čtvercová matice Q je unitární (ortogonální), pokud příslušné zobrazení f_Q je unitární (ortogonální) operátor na aritmetickém vektorovém prostoru se standardním skalárním součinem, viz bod (6) tvrzení 8.82. Takové matice jsme v této kapitole už několikrát potkali v následující formě.

Definice 8.81. Čtvercová komplexní (resp. reálná) matice řádu n se nazývá *unitární* (resp. *ortogonální*), pokud její sloupce tvoří ortonormální posloupnost vzhledem ke standardnímu skalárnímu součinu v $\mathbb{C}^n$ (resp. $\mathbb{R}^n$).

Standardní pojmenování ortogonální matice je poněkud matoucí, smysluplnější by bylo nazývat ji ortonormální.

Následující tvrzení shrnuje řadu různých ekvivalentních definic.

Tvrzení 8.82. *Je-li Q komplexní (resp. reálná) čtvercová matice řádu n, pak jsou následující tvrzení ekvivalentní.*

(1) *Q je unitární (resp. ortogonální),*
(2) *$Q^*Q = I_n$,*
(3) *Q^* je unitární (resp. ortogonální),*
(4) *$QQ^* = I_n$,*
(5) *Q^T je unitární (resp. ortogonální), ekvivalentně, řádky matice Q tvoří ortonormální posloupnost,*
(6) *zobrazení f_Q zachovává standardní skalární součin, tj. pro libovolné $\mathbf{u}, \mathbf{v} \in \mathbb{C}^n$ (resp. $\mathbb{R}^n$) platí $Q\mathbf{u} \cdot Q\mathbf{v} = \mathbf{u} \cdot \mathbf{v}$.*

Speciálně, každá unitární (ortogonální) matice je regulární a platí $Q^{-1} = Q^*$.

Důkaz. Ekvivalenci (1) a (2) jsme nahlédli v poznámce : $Q^*Q = I_n$ je maticovým zápisem skutečnosti, že Q má ortonormální posloupnost sloupců. Podobně (3) a (4) jsou také ekvivalentní. Pokud platí $Q^*Q = I_n$ nebo $QQ^* = I_n$, pak z věty 4.82 charakterizující regulární matice vyplývá $Q^{-1} = Q^*$ a platí tudíž i druhá z rovností. To dokazuje dodatek a ekvivalenci (2) a (4). Body (1), (2), (3), (4) jsou tedy ekvivalentní.

Ekvivalence (3) $\Leftrightarrow$ (5) je zajímavá jenom v komplexním případě. K důkazu si stačí uvědomit, že pro libovolné $\mathbf{u}, \mathbf{v} \in \mathbb{C}^n$ je $\overline{\mathbf{u}} \cdot \overline{\mathbf{v}}$ číslo komplexně sdružené k

$\mathbf{u} \cdot \mathbf{v}$, kde $\overline{\mathbf{u}}$ značí aritmetický vektor, který je po složkách komplexně sdružený k $\mathbf{u}$. Z toho plyne, že sloupce matice Q^* tvoří ortonormální posloupnost právě když sloupce matice Q^T tvoří ortonormální posloupnost.

Nakonec ukážeme, že z (2) plyne (6) a z (6) plyne (1). Je-li $Q^*Q = I_n$, pak pro libovolné $\mathbf{u}, \mathbf{v} \in \mathbb{C}^n$ (resp. $\mathbb{R}^n$) platí

$$(Q\,\mathbf{u}) \cdot (Q\,\mathbf{v}) = (Q\,\mathbf{u})^* Q\,\mathbf{v} = \mathbf{u}^* Q^* Q\,\mathbf{v} = \mathbf{u}^*\mathbf{v} = \mathbf{u} \cdot \mathbf{v} \ .$$

Pokud f_Q zachovává standardní skalární součin, pak speciálně $(Q\mathbf{e}_i) \cdot (Q\mathbf{e}_j) = \mathbf{e}_i \cdot \mathbf{e}_j = \delta_{ij}$ pro libovolná $i, j \in \{1, \dots, n\}$. Na levé straně je ale skalární součin i-tého a j-tého sloupce matice Q, tato matice je proto unitární (ortogonální). ▲

Důsledek 8.83.

(1) *Součin dvou unitárních (resp. ortogonálních) matic téhož řádu je opět unitární (resp. ortogonální) matice.*

(2) *Determinant unitární (resp. ortogonální) matice má absolutní hodnotu* 1.

Důkaz. (1) Jsou-li A, B dvě unitární (nebo ortogonální) matice těhož řádu, pak podle bodu (2) tvrzení 8.82 platí $(AB)^*(AB) = B^*A^*AB = B^*B = I_n$, tedy AB je rovněž unitární (ortogonální).

(2) Je-li Q unitární (nebo ortogonální) matice, pak $1 = \det I_n = \det QQ^* = \det Q \det Q* = \det Q(\det Q) = |\det Q|$. V předposlední rovnosti využíváme faktu, že $\det Q = \det Q^T$ a $\det \bar{Q} = \overline{\det Q}$. ▲

Příklad 8.84. Intuitivně vidíme, že rotace a zrcadlení podle podprostorů v $\mathbb{R}^2$ nebo $\mathbb{R}^3$ zachovávají normy a úhly, zachovávají tedy skalární součin. Podle tvrzení 8.82, bod (6), jsou jejich matice vzhledem ke kanonickým bázím ortogonální. ▲

Z tvrzení 8.82 vyplývá, že unitární a ortogonální matice je velmi snadné invertovat – stačí je hermitovsky sdružit, v reálném případě transponovat. Na příkladě ukážeme trochu sofistikovanější použití.

Příklad 8.85. Reálná matice

$$A = \begin{pmatrix} 1 & 0 & -13 \\ 2 & 3 & 2 \\ 3 & -2 & 3 \end{pmatrix}$$

sice není ortogonální, ale můžeme vypozorovat, že má ortogonální posloupnost sloupců. To umožňuje rozložit matici A na součin ortogonální a diagonální:

$$A = QR = \begin{pmatrix} \frac{1}{\sqrt{14}} & 0 & \frac{-13}{\sqrt{182}} \\ \frac{2}{\sqrt{14}} & \frac{3}{\sqrt{13}} & \frac{2}{\sqrt{182}} \\ \frac{3}{\sqrt{14}} & \frac{-2}{\sqrt{13}} & \frac{3}{\sqrt{182}} \end{pmatrix} \begin{pmatrix} \sqrt{14} & 0 & 0 \\ 0 & \sqrt{13} & 0 \\ 0 & 0 & \sqrt{182} \end{pmatrix}$$

Všimněte si, že jde vlastně o QR-rozklad matice A. Nyní máme $A^{-1} = (QR)^{-1} = R^{-1}Q^{-1} = R^{-1}Q^T$, čili

$$A^{-1} = \begin{pmatrix} \frac{1}{\sqrt{14}} & 0 & 0 \\ 0 & \frac{1}{\sqrt{13}} & 0 \\ 0 & 0 & \frac{1}{\sqrt{182}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{14}} & \frac{2}{\sqrt{14}} & \frac{3}{\sqrt{14}} \\ 0 & \frac{3}{\sqrt{13}} & \frac{-2}{\sqrt{13}} \\ \frac{-13}{\sqrt{182}} & \frac{2}{\sqrt{182}} & \frac{3}{\sqrt{182}} \end{pmatrix} = \begin{pmatrix} \frac{1}{14} & \frac{2}{14} & \frac{3}{14} \\ 0 & \frac{3}{13} & \frac{-2}{13} \\ \frac{-13}{182} & \frac{2}{182} & \frac{3}{182} \end{pmatrix}$$

▲

Vlastnosti unitárních a ortogonálních matic pomohou dokázat jednoznačnost QR-rozkladu regulárních matic.

Tvrzení 8.86. *Je-li A regulární (reálná nebo komplexní) matice řádu n a $A = Q_1R_1 = Q_2R_2$ jsou dva QR-rozklady matice A, pak platí $Q_1 = Q_2$ a $R_1 = R_2$.*

Důkaz. Důkaz budeme formulovat pro reálný případ, abychom se vyhnuli nadměrnému závorkování.

Jsou-li $A = Q_1R_1 = Q_2R_2$ dva QR-rozklady regulární matice A, plyne odtud

$$Q_2^{-1}Q_1 = R_2R_1^{-1} \ .$$

Označíme si tento součin $C = (\mathbf{c}_1|\mathbf{c}_2|\cdots|\mathbf{c}_n) = (c_{ij})$. Součin $Q_2^{-1}Q_1$ je ortogonální jakožto součin dvou ortogonálních matic a součin $R_2R_1^{-1}$ je horní trojúhelníková matice s kladnými prvky na hlavní diagonále. Platí proto $c_{i1} = 0$ pro $i > 1$ a tedy $1 = \|\mathbf{c}_1\| = |c_{11}|$ a tedy $c_{11} = 1$, neboť c_{11} je kladné reálné číslo. To znamená, že $\mathbf{c}_1 = \mathbf{e}_1$.

Dále postupujeme indukcí podle indexu sloupců $\mathbf{c}_j$ a dokážeme $\mathbf{c}_j = \mathbf{e}_j$ pro každé $j = 1, 2, \ldots, n$. Pro $j = 1$ jsme to právě ověřili. Předpokládejme nyní, že pro nějaké $j > 1$ a $j \leq n$ platí $\mathbf{c}_i = \mathbf{e}_i$ pro každé $i = 1, 2, \ldots, j-1$. Z rovností $\mathbf{c}_i \cdot \mathbf{c}_j = 0$ pro $i < j$ (Q je ortogonální) a indukčního předpokladu $\mathbf{c}_i = \mathbf{e}_i$ plyne $0 = \mathbf{e}_i \cdot \mathbf{c}_j = c_{ij}$ pro každé $i < j$. Matice $(c_{ij}) = R_2R_1^{-1}$ je horní trojúhelníková, proto také $c_{ij} = 0$ pro každé $i > j$. Z rovnosti $\|\mathbf{c}_j\| = 1$ (opět ortogonalita matice C) pak plyne $c_{jj}^2 = 1$ a tedy $c_{jj} = 1$, neboli $\mathbf{c}_j = \mathbf{e}_j$.

Indukcí jsme tak dokázali, že $Q_2^{-1}Q_1 = R_2R_1^{-1} = I_n$ a tedy $Q_1 = Q_2$ a $R_1 = R_2$. ▲

8.5.2. Unitární a ortogonální zobrazení. Nyní budeme uvažovat lineární zobrazení mezi dvěma potenciálně různými prostory $\mathbf{V}$ a $\mathbf{W}$ opatřené skalárními součiny. Tyto součiny i indukované normy rozlišíme dolním indexem. V případě unitárních operátorů, tj. v případě $\mathbf{V} = \mathbf{W}$, se většinou implicitně rozumí, že se shodují i skalární součiny $\langle\,,\rangle_V = \langle\,,\rangle_W$.

Definice 8.87. Nechť $\mathbf{V}$ a $\mathbf{W}$ jsou vektorové prostory nad $\mathbb{C}$ (resp. $\mathbb{R}$) se skalárními součiny $\langle\,,\rangle_V, \langle\,,\rangle_W$. Lineární zobrazení $f : \mathbf{V} \to \mathbf{W}$ nazýváme *unitární* (resp. *ortogonální*), pokud zachovává skalární součin, tj. pro libovolné $\mathbf{u}, \mathbf{v} \in V$ platí

$$\langle f(\mathbf{u}), f(\mathbf{v})\rangle_W = \langle \mathbf{u}, \mathbf{v}\rangle_V \ .$$

Je snadné si rozmyslet, že ze zachovávání skalárního součinu plyne zachovávání odvozené normy, kolmosti, apod. Zajímavější v následujícím tvrzení jsou opačné implikace.

Tvrzení 8.88. *Nechť $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení mezi komplexními (resp. reálnými) vektorovými prostory $\mathbf{V}$, $\mathbf{W}$ se skalárními součiny $\langle\,,\rangle_V, \langle\,,\rangle_W$. Pak následující tvrzení jsou ekvivalentní.*

(1) *f je unitární (resp. f je ortogonální),*
(2) *f zachovává normu, tj. pro libovolný vektor $\mathbf{v} \in V$ platí $\|f(\mathbf{v})\|_W = \|\mathbf{v}\|_V$,*
(3) *f zachovává ortonormalitu, tj. je-li $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ ortonormální posloupnost ve $\mathbf{V}$, pak $(f(\mathbf{v}_1), \ldots, f(\mathbf{v}_n))$ je ortonormální posloupnost v $\mathbf{W}$.*
(4) *f zobrazuje jednotkové vektory ve $\mathbf{V}$ na jednotkové vektory v $\mathbf{W}$.*

Speciálně, každé unitární (ortogonální) zobrazení je prosté.

Důkaz. Implikace (1) $\Rightarrow$ (3) $\Rightarrow$ (4) a (1) $\Rightarrow$ (2) $\Rightarrow$ (4) jsou přímočaré, například (1) $\Rightarrow$ (2) se dokáže výpočtem

$$\|f(\mathbf{v})\|_W = \sqrt{\langle f(\mathbf{v}), f(\mathbf{v})\rangle_W} = \sqrt{\langle \mathbf{v}, \mathbf{v}\rangle_V} = \|\mathbf{v}\|_V \ .$$

Implikace (4) $\Rightarrow$ (2) plyne z linearity f a vlastností normy: libovolný nenulový vektor $\mathbf{v}$ napíšeme ve tvaru $\mathbf{v} = t\mathbf{u}$, kde $t = \|\mathbf{v}\|_V$ je kladné reálné číslo a $\mathbf{u} = \mathbf{v}/\|\mathbf{v}\|_V$ je jednotkový, a spočítáme

$$\|f(\mathbf{v})\|_W = \|f(t\mathbf{u})\|_W = \|tf(\mathbf{u})\|_W = t\,\|f(\mathbf{u})\|_W = t\,\|\mathbf{v}\|_V \ .$$

Zachovávání normy nulového vektoru je zřejmé.

Nyní stačí dokázat, že z (2) plyne (1). Tato implikace je důsledkem polarizačních identit, které vyjadřují skalární součin pomocí normy. Na ukázku srovnáme reálné části, podobně by se postupovalo pro imaginární.

$$\begin{aligned}\operatorname{Re}(\langle f(\mathbf{u}), f(\mathbf{v})\rangle_W) &= \frac{1}{2}(\|f(\mathbf{u})+f(\mathbf{v})\|_W^2 - \|f(\mathbf{u})\|_W^2 - \|f(\mathbf{v})\|_W^2)\\ &= \frac{1}{2}(\|f(\mathbf{u}+\mathbf{v})\|_W^2 - \|f(\mathbf{u})\|_W^2 - \|f(\mathbf{v})\|_W^2)\\ &= \frac{1}{2}(\|\mathbf{u}+\mathbf{v}\|_V^2 - \|\mathbf{u}\|_V^2 - \|\mathbf{v}\|_V^2)\\ &= \operatorname{Re}(\langle \mathbf{u}, \mathbf{v}\rangle_V)\ .\end{aligned}$$

Z bodu (2) vyplývá, že obrazem nenulového vektoru je opět nenulový vektor. Unitární nebo ortogonální zobrazení má proto triviální jádro, takže je prosté. ▲

Zachovávání kolmosti k unitaritě lineárního zobrazení nestačí – stejnolehlost s koeficientem různým od ± 1 normu nezachovává, ale kolmost ano.

Dokázané tvrzení můžeme použít na aritmetické prostory se standardním součinem a zobrazení f_Q určené čtvercovou komplexní nebo reálnou maticí Q. Tím získáme další podmínky ekvivalentní unitaritě (ortogonalitě). Například ekvivalence unitarity se zachováváním normy v této situaci říká, že čtvercová komplexní matice Q je unitární právě tehdy, když pro libovolný vektor $\mathbf{v} \in \mathbb{C}^n$ platí $\|Q\mathbf{v}\| = \|\mathbf{v}\|$.

Nakonec si ještě přesně ujasníme vztah unitárních (ortogonálních) zobrazení a unitárních (ortogonálních) matic.

Tvrzení 8.89. *Nechť* $\mathbf{V}$ *a* $\mathbf{W}$ *jsou konečně generované vektorové prostory nad* $\mathbb{C}$ *(resp.* $\mathbb{R}$*) se skalárními součiny* $\langle\,,\rangle_V, \langle\,,\rangle_W$, $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ *a* C *jsou po řadě ortonormální báze prostorů* $\mathbf{V}$ *a* $\mathbf{W}$, *a* $f : \mathbf{V} \to \mathbf{W}$ *je lineární zobrazení. Pak* f *je unitární (resp. ortogonální) právě tehdy, když* $[f]_C^B$ *má ortonormální posloupnost sloupců vzhledem ke standardnímu skalárnímu součinu.*

Speciálně, je-li $\mathbf{V} = \mathbf{W}$, *pak* f *je unitární (resp. ortogonální) právě když* $[f]_C^B$ *je unitární (resp. ortogonální).*

Důkaz. Je-li f unitární, pak je posloupnost $(f(\mathbf{v}_1), \dots, f(\mathbf{v}_n))$ ortonormální v $\mathbf{W}$ podle předchozího tvrzení. Z tvrzení 8.50 potom vyplývá, že pro $i \neq j$ platí $[f(\mathbf{v}_i)]_C \cdot [f(\mathbf{v}_j)]_C = \langle f(\mathbf{v}_i), f(\mathbf{v}_j)\rangle_W = 0$. Posloupnost sloupců matice $[f]_C^B$, tj. posloupnost $([f(\mathbf{v}_1)]_C, \dots, [f(\mathbf{v}_n)]_C)$, je tedy ortonormální vzhledem ke standardnímu skalárnímu součinu.

Má-li naopak $[f]_C^B$ ortonormální posloupnost sloupců, pak obrácením předchozí úvahy dostáváme, že $(f(\mathbf{v}_1), \dots, f(\mathbf{v}_n))$ je ortonormální posloupnost v $\mathbf{W}$. Ověříme třeba, že f zachovává normu, což podle přechozího tvrzení stačí. Libovolný vektor $\mathbf{u} \in V$ lze psát jako $\mathbf{u} = a_1\mathbf{v}_1 + \dots + a_n\mathbf{v}_n$. Podle Pythagorovy věty máme $\|\mathbf{u}\|^2 = a_1^2 + \dots + a_n^2$, protože posloupnost $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ je ortonormální. Ze stejného důvodu je $\|f(\mathbf{u})\|^2 = \|a_1 f(\mathbf{v}_1) + \dots + a_n f(\mathbf{v}_n)\|^2 = a_1^2 + \dots + a_n^2$. Máme proto $\|f(\mathbf{u})\|^2 = \|\mathbf{u}\|^2$, jak jsme chtěli.

Dodatek plyne z definice unitární matice a dokázané ekvivalence. ▲

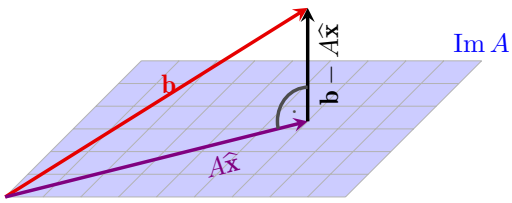
8.6. Aplikace: aproximace a optimalizace

8.6.1. Metoda nejmenších čtverců. Při řešení praktických problémů se často stává, že vedou na soustavu rovnic $A\mathbf{x} = \mathbf{b}$ s reálnými nebo komplexními koeficienty, která nemá řešení. Řekněme, že $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ je matice typu $m \times n$ nad $\mathbb{R}$ nebo $\mathbb{C}$, typicky $m >> n$. Taková soustava může například vzniknout sestavením rovnic z velkého množství měření, která jsou zatížená chybami. Chceme nalézt „co nejlepší“ přibližné řešení $\widehat{\mathbf{x}}$ v tom smyslu, aby vektor $A\widehat{\mathbf{x}}$ byl co nejblíže pravé straně soustavy $\mathbf{b}$, tj. aby norma $\|\mathbf{b} - A\widehat{\mathbf{x}}\|$ byla co nejmenší možná.

Metoda nejmenších čtverců je založená na měření normy vektorů pomocí eukleidovské normy (odtud její název), která je určená standardním skalárním součinem v $\mathbb{R}^n$ (nebo v $\mathbb{C}^n$).

Definice 8.90. Nechť $A\mathbf{x} = \mathbf{b}$ je soustava lineárních rovnic s reálnými (nebo komplexními) koeficienty. Každý vektor $\widehat{\mathbf{x}} \in \mathbb{R}^n$ (nebo $\widehat{\mathbf{x}} \in \mathbb{C}^n$), který minimalizuje eukleidovskou normu $\|\mathbf{b} - A\mathbf{x}\|$, se nazývá *přibližné řešení* (nebo *aproximace řešení*) *soustavy* $A\mathbf{x} = \mathbf{b}$ *metodou nejmenších čtverců.*

Vektor je tvaru $A\mathbf{x}$ pro nějaké $\mathbf{x} \in \mathbb{R}^n$ ($\mathbf{x} \in \mathbb{C}^n$) právě když leží ve sloupcovém prostoru $\operatorname{Im} A$ matice A. Podle věty 8.53 o aproximaci je mezi všemi vektory $\operatorname{Im} A$ nejblíže k $\mathbf{b}$ ortogonální projekce vektoru $\mathbf{b}$ na podprostor $\operatorname{Im} A$. Přibližnými řešeními soustavy $A\mathbf{x} = \mathbf{b}$ metodou nejmenších čtverců jsou tedy právě ty vektory $\widehat{\mathbf{x}}$, pro které $A\widehat{\mathbf{x}}$ je rovno ortogonální projekci vektoru $\mathbf{b}$ na podprostor $\operatorname{Im} A$.



Obrázek 8.9. Krok (3a)

Jak takové vektory $\widehat{\mathbf{x}}$ spočítat nám říká důsledek 8.63 o projekci aritmetických vektorů na podprostor.

Tvrzení 8.91. *Je-li A matice typu $m \times n$ nad $\mathbb{R}$ nebo $\mathbb{C}$ a $\mathbf{b} \in \mathbb{R}^m$ (resp. $\mathbb{C}^m$), pak množina všech přibližných řešení soustavy $A\mathbf{x} = \mathbf{b}$ metodou nejmenších čtverců je rovna množině všech (přesných) řešení soustavy*

$$A^* A\widehat{\mathbf{x}} = A^*\mathbf{b} \ .$$

Matice A^*A je Gramova matice posloupnosti sloupcových vektorů matice A. Podle tvrzení 8.62 je tedy A^*A regulární právě když má matice A lineárně nezávislou posloupnost sloupcových vektorů. V takovém případě existuje inverzní matice $(A^*A)^{-1}$ a jednoznačně určenou aproximaci $\widehat{\mathbf{x}}$ řešení soustavy $A\mathbf{x} = \mathbf{b}$ metodou nejmenších čtverců můžeme vyjádřit ve tvaru

$$\widehat{\mathbf{x}} = (A^*A)^{-1} A^*\mathbf{b} \ .$$

Příklad 8.92. Řešení reálné soustavy $(A|\mathbf{b})$, kde

$$(A|\mathbf{b}) = \left(\begin{array}{cc|c} 2 & 0 & 3 \\ 1 & 1 & 5 \\ -2 & -1 & -2 \end{array}\right) \ ,$$

metodou nejmenších čtverců je řešení soustavy

$$A^T A\widehat{\mathbf{x}} = A^T\mathbf{b}$$

$$\begin{pmatrix} 2 & 1 & -2 \\ 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 1 & 1 \\ -2 & -1 \end{pmatrix} \widehat{\mathbf{x}} = \begin{pmatrix} 2 & 1 & -2 \\ 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 3 \\ 5 \\ -2 \end{pmatrix}$$

$$\begin{pmatrix} 9 & 3 \\ 3 & 2 \end{pmatrix} \widehat{\mathbf{x}} = \begin{pmatrix} 15 \\ 7 \end{pmatrix} \ .$$

Eliminací dostaneme $\widehat{\mathbf{x}} = (x_1, x_2)^T = (1, 2)^T$.

Součin $A(1,2)^T = (2,3,-4)$ je ortogonální projekcí $\mathbf{w}$ vektoru $\mathbf{b}$ na podprostor $\operatorname{Im} A$. Rozdíl mezi vektorem pravých stran $\mathbf{b}$ a vektorem $\mathbf{w} = A\hat{\mathbf{x}}$ je potom

$$\mathbf{b} - \mathbf{w} = (3,5,-2)^T - (2,3,-4)^T = (1,2,2)^T$$

a vzdálenost $\mathbf{b}$ od $\operatorname{Im} A$ je tedy

$$\|\mathbf{b} - \mathbf{w}\| = \sqrt{1^2 + 2^2 + 2^2} = 3 \ .$$

▲

8.6.2. (Lineární) regrese. Jedním z často využívaných příkladů použití metody nejmenších čtverců je *lineární regrese*. V této úloze chceme „co nejlépe“ proložit přímku $y = ax + b$ danými naměřenými hodnotami (x_1, y_1), (x_2, y_2), ..., (x_n, y_n). Přesněji řečeno, hledáme aproximaci „řešení“ soustavy

$$\left(\begin{array}{cc|c} x_1 & 1 & y_1 \\ x_2 & 1 & y_2 \\ \vdots & \vdots & \vdots \\ x_n & 1 & y_n \end{array}\right) .$$

Vidíme, že posloupnost sloupcových vektorů matice soustavy je lineárně nezávislá, pokud se liší aspoň dvě hodnoty x_i pro $i = 1, 2, \ldots, n$.

Příklad 8.93. Metodou nejmenších čtverců proložíme body $(0,1)$, $(1,1)$, $(2,2)$, $(3,4)$, $(4,5)$ v $\mathbb{R}^2$ přímku $y = ax + b$. Dvojice koeficientů (a,b) je přibližným řešením soustavy lineárních rovnic

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

metodou nejmenších čtverců. Vyřešíme příslušnou soustavu rovnic z tvrzení 8.91:

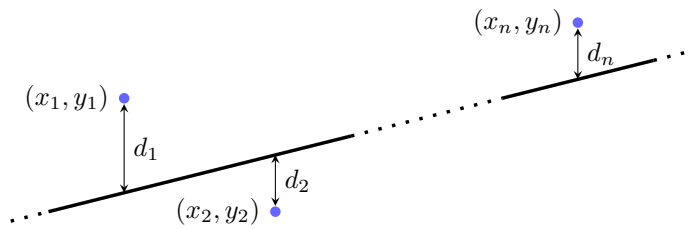
$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 2 & 1 \\ 3 & 1 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 2 \\ 4 \\ 5 \end{pmatrix} ,$$

$$\begin{pmatrix} 30 & 10 \\ 10 & 5 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 37 \\ 13 \end{pmatrix} .$$

Řešení vyjde $(a,b)^T = (11/10, 2/5)$ takže hledaná přímka je

$$y = \frac{11}{10}x + \frac{2}{5} \ .$$

▲



Obrázek 8.10. Lineární regrese – minimalizujeme $\sum d_i^2$.

Daty můžeme prokládat složitější útvary, jako paraboly, polynomy vyššího stupně, elipsy (např. při hledání dráhy planety), apod. Také takové úlohy vedou na hledání řešení soustavy metodou nejmenších čtverců.

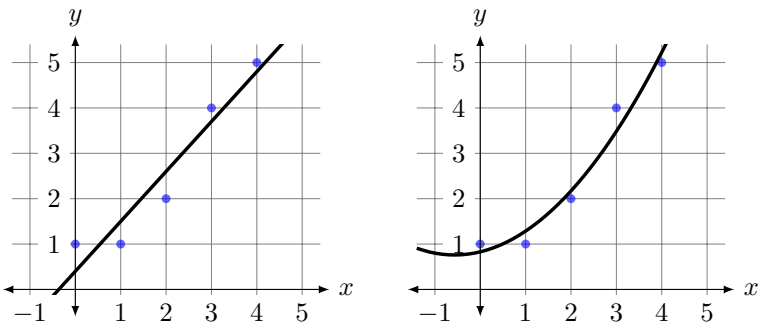
PŘÍKLAD 8.94. Stejnými body proložíme „co nejlépe“ parabolu $y = ax^2+bx+c$. Koeficienty jsou řešením soustavy

$$\left(\begin{array}{ccc|c} 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 4 & 2 & 1 & 2 \\ 9 & 3 & 1 & 4 \\ 16 & 4 & 1 & 5 \end{array}\right)$$

metodou nejmenších čtverců. Vyjde $(a, b, c)^T = 1/70(15, 17, 58)^T$,

$$y = \frac{3}{14}x^2 + \frac{17}{70}x + \frac{29}{35}$$

▲



Metodu řešení posledních dvou příkladů můžeme zobecnit následujícím způsobem. Chceme danými daty (x_1, y_1), (x_2, y_2), ..., (x_n, y_n) „co nejlépe“ proložit funkci, která je lineární kombinací předem zvolených reálných funkcí $f_1(x), f_2(x), \ldots, f_q(x)$, kterým se v některých oborech říká *regresory*. V prvním z příkladů těmito funkcemi byla konstantní funkce $f_1(x) = 1$ a lineární funkce $f_2(x) = x$. Ve druhém z příkladů jsme si k těmto dvěma funkcím přidali ještě kvadratickou funkci $f_3(x) = x^2$.

Hledáme tedy reálná čísla $c_1, c_2, \ldots, c_q$ taková, že lineární kombinace

$$\hat{f}(x) = c_1 f_1(x) + c_2 f_2(x) + \cdots + c_q f_q(x)$$

minimalizuje eukleidovskou vzdálenost mezi vektorem $\mathbf{y} = (y_1, y_2, \ldots, y_n)^T$ a vektorem $\mathbf{w} = (\hat{f}(x_1), \hat{f}(x_2), \ldots, \hat{f}(x_n))^T$, tj. eukleidovskou normu vektoru $\mathbf{y} - \mathbf{w}$. Potom pro každé $i = 1, 2, \ldots, n$ platí

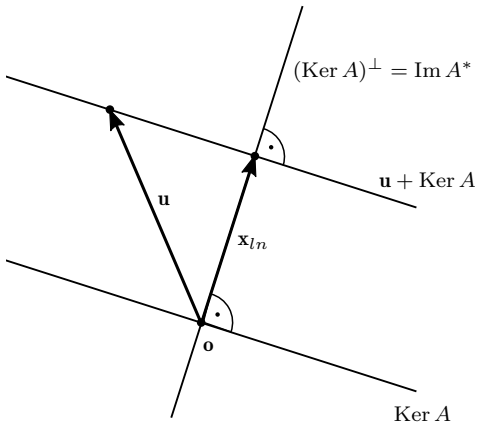
$$\hat{f}(x_i) = c_1 f_1(x_i) + c_2 f_2(x_i) + \cdots + c_q f_q(x_i)$$

což můžeme zapsat maticově ve tvaru $\mathbf{w} = A\widehat{\mathbf{c}}$, kde $A = (f_j(x_i))_{n\times q}$ a $\widehat{\mathbf{c}} = (c_1, c_2, \ldots, c_q)^T$. Ve sloupcovém prostoru $\operatorname{Im} A$ matice A tak hledáme vektor $A\widehat{\mathbf{c}}$, který minimalizuje vzdálenost od vektoru $\mathbf{y}$. Vektor $\widehat{\mathbf{c}}$ tedy najdeme jako přibližné řešení soustavy $\mathbf{y} = A\mathbf{c}$ metodou nejmenších čtverců, tj. jako (pravé) řešení soustavy

$$A^T A\widehat{\mathbf{c}} = A^T\mathbf{y} \ .$$

8.6.3. Řešení s nejmenší normou. Jiné praktické situace vedou na řešení soustavy $A\mathbf{x} = \mathbf{b}$ s reálnými nebo komplexními koeficienty, která je sice řešitelná, ale podurčená – má nekonečně mnoho řešení. Typicky jde o soustavu, která má daleko více neznámých než rovnic, tj. A je typu $m \times n$, $m << n$. Zajímá nás často řešení, které má co nejmenší normu. Pro eukleidovskou normu indukovanou standardním skalárním součinem lze i tuto úlohu vyřešit našimi prostředky.

Množina řešení řešitelné soustavy $A\mathbf{x} = \mathbf{b}$ je tvaru $\mathbf{u} + \operatorname{Ker} A$, kde $\mathbf{u}$ je libovolné řešení dané soustavy. Obrázek 8.11 vede k domněnce, že řešení s nejmenší normou existuje právě jedno a je rovno ortogonální projekci vektoru $\mathbf{u}$ na $(\operatorname{Ker} A)^\perp = \operatorname{Im} A^*$.



OBRÁZEK 8.11. Řešení soustavy lineárních rovnic s nejmenší normou

Následující tvrzení ukazuje, že tato intuice je správná.

TVRZENÍ 8.95. *Nechť $A\mathbf{x} = \mathbf{b}$ je soustava lineárních rovnic nad $\mathbb{R}$ nebo nad $\mathbb{C}$, která má alespoň jedno řešení $\mathbf{u}$. Pak existuje právě jedno řešení $\mathbf{x}_{ln}$ soustavy $A\mathbf{x} = \mathbf{b}$, které minimalizuje eukleidovskou normu $\|\mathbf{x}\|$. Vektor $\mathbf{x}_{ln}$ je roven ortogonální projekci vektoru $\mathbf{u}$ na podprostor $\operatorname{Im} A^*$ a platí $\mathbf{x}_{ln} = A^*\mathbf{z}$, kde $\mathbf{z}$ je libovolné řešení soustavy $AA^*\mathbf{z} = \mathbf{b}$.*

DŮKAZ. Předpokládejme, že $\mathbf{u}$ je řešení soustavy $A\mathbf{x} = \mathbf{b}$ a označme $\mathbf{x}_{ln}$ jeho ortogonální projekci na $\operatorname{Im} A^*$. Z důsledku 8.63 o projekci v aritmetických prostorech použitého na matici A^* plyne, že $\mathbf{x}_{ln} = A^*\mathbf{z}$, kde $\mathbf{z}$ je libovolné řešení soustavy $AA^*\mathbf{z} = A\mathbf{u} = \mathbf{b}$ (z toho také vidíme, že $\mathbf{x}_{ln}$ nezávisí na volbě partikulárního řešení $\mathbf{u}$).

Zbývá ukázat, že $\mathbf{x}_{ln}$ je řešením soustavy a že toto řešení jako jediné minimalizuje eukleidovskou normu $\|\mathbf{x}\|$. První fakt je jednoduchý – platí $A\mathbf{x}_{ln} = AA^*\mathbf{z} = \mathbf{b}$.

Druhou skutečnost ukážeme podobně jako v důkazu věty 8.53 o aproximaci. Uvažujme libovolné jiné řešení $\mathbf{v} \neq \mathbf{x}_{ln}$ soustavy $A\mathbf{x} = \mathbf{b}$. Vektor $\mathbf{v} - \mathbf{x}_{ln}$ leží v $\operatorname{Ker} A$ (protože je rozdílem dvou řešení soustavy) a je proto kolmý na $\mathbf{x}_{ln} \in \operatorname{Im} A^* = (\operatorname{Ker} A)^\perp$ (náležení do $\operatorname{Im} A^*$ plyne z vyjádření $\mathbf{x}_{ln} = A^*\mathbf{z}$). Z Pythagorovy věty plyne

$$\|\mathbf{v}\| = \sqrt{\|\mathbf{x}_{ln}\|^2 + \|\mathbf{v} - \mathbf{x}_{ln}\|^2} > \sqrt{\|\mathbf{x}_{ln}\|^2} = \|\mathbf{x}_{ln}\| \ .$$

Mezi všemi řešeními soustavy $A\mathbf{x} = \mathbf{b}$ je tedy $\mathbf{x}_{ln}$ ten jediný vektor, který minimalizuje normu $\|\mathbf{x}\|$. ▲

V případě, že A má lineárně nezávislou posloupnost řádků, je matice AA^* regulární, protože je to Gramova matice komplexně sdružených řádkových vektorů matice A. V takovém případě má rovnice $AA^*\mathbf{z} = \mathbf{b}$ právě jedno řešení $\mathbf{z} = (AA^*)^{-1}\mathbf{b}$ a řešení soustavy $A\mathbf{x} = \mathbf{b}$ s nejmenší normou je tedy

$$\mathbf{x}_{ln} = A^*(AA^*)^{-1}\mathbf{b} \ .$$

V tomto případě je matice $A^*(AA^*)^{-1}$ inverzní zprava k matici A.

PŘÍKLAD 8.96. Najdeme řešení s nejmenší normou pro reálnou soustavu rovnic

$$(A|\mathbf{b}) = \left(\begin{array}{ccc|c} 1 & 2 & 3 & 18 \\ -1 & 1 & 1 & 7 \end{array}\right) \ .$$

Nejprve najdeme řešení soustavy $AA^T\mathbf{z} = \mathbf{b}$. Protože

$$(AA^T|\mathbf{b}) = \left(\begin{array}{cc|c} 14 & 4 & 18 \\ 4 & 3 & 7 \end{array}\right) ,$$

vidíme, že $\mathbf{z} = (1,1)^T$. Hledané řešení s nejmenší normou je

$$\mathbf{x}_{ln} = A^T \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \\ 4 \end{pmatrix} .$$

▲

Příklad 8.97. Dořešíme úlohu z části 2.1.3. Tam jsme dospěli k soustavě lineárních rovnic s rozšířenou maticí

$$\left(\begin{array}{cccccccc|c} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 15/2 & 13/2 & 11/2 & 9/2 & 7/2 & 5/2 & 3/2 & 1/2 & 4 \end{array}\right) .$$

Označíme matici soustavy A a vektor pravých stran $\mathbf{b} = (0,4)^T$. Připomeňme, že v této konkrétní aplikaci vektor $\mathbf{x} = (x_1, x_2, \ldots, x_8)^T \in \mathbb{R}^8$ řeší soustavu $A\mathbf{x} = \mathbf{b}$ právě když pomocí sil $x_1, \ldots, x_8$ přemístíme těleso z počáteční klidové polohy v bodě 0 do klidové polohy v bodě 4 během 8 vteřin. Každá síla x_i působí na těleso po dobu jedné vteřiny v časovém intervalu $[i-1, i]$. Protože $\operatorname{rank}(A) = 2$, je soustava $A\mathbf{x} = \mathbf{b}$ řešitelná pro jakoukoliv pravou stranu $\mathbf{b}$ a $\dim(\operatorname{Ker} A) = 6$.

Energii $E(\mathbf{x})$, kterou spotřebujeme, zvolíme-li řešení $\mathbf{x} = (x_1, x_2, \ldots, x_8)^T$, jsme v části 2.1.3 spočítali jako

$$E(x_1, x_2, \ldots, x_8) = \frac{1}{2}(x_1^2 + x_2^2 + \cdots + x_7^2 + x_8^2) = \frac{1}{2}\|\mathbf{x}\|^2 .$$

Hledáme-li to řešení soustavy $A\mathbf{x} = \mathbf{b}$, které spotřebuje co nejméně energie, hledáme řešení $\mathbf{x}_{ln}$, které má nejmenší euklidovskou normu. Podle Tvrzení 8.95 se $\mathbf{x}_{ln}$ rovná ortogonální projekci jakéhokoliv partikulárního řešení řešení soustavy $A\mathbf{x} = \mathbf{b}$ na podprostor $\operatorname{Im}(A^T)$. A tuto ortogonální projekci najdeme ve tvaru $\mathbf{x}_{ln} = A^T\mathbf{z}$, kde $\mathbf{z}$ je libovolné řešení soustavy $AA^T\mathbf{z} = \mathbf{b}$.

Soustava

$$(AA^T|\mathbf{b}) = \left(\begin{array}{cc|c} 8 & 32 & 0 \\ 32 & 170 & 4 \end{array}\right)$$

má řešení $\mathbf{z} = (z_1, z_2)^T = (-8/21, 2/21)^T$ a proto

$$\mathbf{x}_{ln} = -\frac{8}{21}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + \frac{2}{21}\begin{pmatrix} 15/2 \\ 13/2 \\ 11/2 \\ 9/2 \\ 7/2 \\ 5/2 \\ 3/2 \\ 1/2 \end{pmatrix} = \begin{pmatrix} 7/21 \\ 5/21 \\ 3/21 \\ 1/21 \\ -1/21 \\ -3/21 \\ -5/21 \\ -7/21 \end{pmatrix} .$$

Spotřebujeme při něm energii

$$\frac{1}{2}\|\mathbf{x}_{ln}\|^2 = \frac{84}{441} \doteq \frac{1}{5} .$$

Srovnejme si tuto energii s energetickou náročností jiných řešení soustavy $A\mathbf{x} = \mathbf{b}$. Energetická náročnost řešení $\mathbf{u} = (4, -4, 0, 0, 0, 0, 0, 0)^T$, kdy to v první vteřině hodně rozjedeme, ve druhém vteřině dobrzdíme do klidového stavu v poloze 4, a pak si „dáme dvacet“, je $(1/2)\|\mathbf{u}\|^2 = 16$. Jiné řešení $\mathbf{v} = (1, -1, 1, -1, 1, -1, 1, -1)^T$, tzv. „cukací“, kdy to v každé liché vteřině rozjedeme na rychlost rovnou 1 a v následující vteřině dobrzdíme zpět na rychlost 0, vyžaduje energii $(1/2)\|\mathbf{v}\|^2 = 4$. ▲

Aproximaci neřešitelné soustavy a hledání řešení s nejmenší normou můžeme zkombinovat a vyřešit problém nalezení aproximace řešení soustavy $A\mathbf{x} = \mathbf{b}$ metodou nejmenších čtverců, které má navíc co nejmenší normu (viz cvičení).

8.7. Orientovaný objem

Determinant $\det(\mathbf{v}_1|\ldots|\mathbf{v}_n)$ udává orientovaný n-rozměrný objem rovnoběžnostěnu určeného vektory $\mathbf{v}_1, \ldots, \mathbf{v}_n$ v aritmetickém vektorovém prostoru $\mathbb{R}^n$ se standardním měřením délek (tj. se standardním skalárním součinem). Tento koncept lze zobecnit na libovolný orientovaný reálný vektorový prostor $\mathbf{V}$ se skalárním součinem $\langle\,,\rangle$.

Rovnoběžnostěnem určeným vektory $\mathbf{v}_1, \dots, \mathbf{v}_n$ rozumíme množinu

$$\{t_1\mathbf{v}_1 + \dots + t_n\mathbf{v}_n : t_1, \dots, t_i \in [0,1]\} \ .$$

Orientovaný objem můžeme popsat obdobným postupem jako v kapitole o determinantech, přičemž roli kanonické báze bude hrát kladně orientovaná ortonormální báze $B = (\mathbf{w}_1, \dots, \mathbf{w}_n)$ – vektory v této bázi jsou jednotkové, navzájem kolmé a kladně orientované, takže chceme aby rovnoběžnostěn jimi určený měl objem 1.

Definice 8.98. Nechť $\mathbf{V}$ je reálný orientovaný vektorový prostor dimenze n se skalárním součinem $\langle\,,\rangle$ a $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$. *Orientovaný objem* rovnoběžnostěnu určeného vektory $\mathbf{v}_1, \dots, \mathbf{v}_n$ definujeme vztahem

$$\mathrm{vol}_n(\mathbf{v}_1, \dots, \mathbf{v}_n) = \det\left([\mathbf{v}_1]_B | \dots | [\mathbf{v}_n]_B\right) \ ,$$

kde B je libovolná kladně orientovaná ortonormální báze prostoru $\mathbf{V}$. *Objem* stejného rovnoběžnostěnu definujeme jako absolutní hodnotu orientovaného objemu.

Objem nezávisí na konkrétní volbě kladně orientované ortonormální báze B: Označme C jinou kladně orientovanou bázi prostoru $\mathbf{V}$. Matice přechodu $X = [\mathrm{id}]_C^B$ od B k C je ortogonální, takže její determinant je ± 1 (důsledek 8.83). Navíc B a C jsou souhlasně orientované, takže determinant je 1. Z toho dostáváme

$$\begin{aligned}\det\left([\mathbf{v}_1]_C | \dots | [\mathbf{v}_n]_C\right) &= \det\left(X[\mathbf{v}_1]_B | \dots | X[\mathbf{v}_n]_B\right) = \det\left(X([\mathbf{v}_1]_B | \dots | [\mathbf{v}_n]_B)\right) \\ &= \det(X)\det\left([\mathbf{v}_1]_B | \dots | [\mathbf{v}_n]_B\right) = \det\left([\mathbf{v}_1]_B | \dots | [\mathbf{v}_n]_B\right)\end{aligned}$$

Orientovaný objem je nulový právě tehdy, když je posloupnost $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ lineárně závislá. V opačném případě je roven determinantu matice přechodu od $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ k B a má kladné znaménko právě tehdy, když je báze $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ kladně orientovaná. Při změně orientace orientovaný objem změní znaménko a objem se nezmění.

Připomeňme, že souřadnice vektoru $\mathbf{v}$ vzhledem k ortonormální bázi můžeme vypočítat pomocí skalárních součinů s bázovými vektory:

$$[\mathbf{v}]_B = \left(\langle \mathbf{w}_1, \mathbf{v}\rangle, \dots, \langle \mathbf{w}_n, \mathbf{v}\rangle\right)^T$$

To je obsahem tvrzení 8.48, složky vyjádření jsme nazývali Fourierovy koeficienty. Definici tedy můžeme přepsat

$$\mathrm{vol}_n(\mathbf{v}_1, \dots, \mathbf{v}_n) = \det\begin{pmatrix} \langle \mathbf{w}_1, \mathbf{v}_1\rangle & \langle \mathbf{w}_1, \mathbf{v}_2\rangle & \dots & \langle \mathbf{w}_1, \mathbf{v}_n\rangle \\ \langle \mathbf{w}_2, \mathbf{v}_1\rangle & \langle \mathbf{w}_2, \mathbf{v}_2\rangle & \dots & \langle \mathbf{w}_2, \mathbf{v}_n\rangle \\ \vdots & & & \vdots \\ \langle \mathbf{w}_n, \mathbf{v}_1\rangle & \langle \mathbf{w}_n, \mathbf{v}_2\rangle & \dots & \langle \mathbf{w}_n, \mathbf{v}_n\rangle \end{pmatrix}$$

Příklad 8.99. V prostoru $\mathbb{R}^2$ se skalárním součinem

$$\left\langle (x_1, x_2)^T, (y_1, y_2)\right\rangle^T = (x_1, x_2)\begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = 4x_1y_1 + 2x_1y_2 + 2x_2y_1 + 2x_2y_2$$

orientovaném tak, že báze $(\mathbf{e}_1, \mathbf{e}_2)$ je kladně orientovaná, vypočítáme orientovaný objem rovnoběžnostěnu (lépe řečeno, orientovaný obsah rovnoběžníku) určeného vektory $\mathbf{v}_1 = (-3, 4)^T$, $\mathbf{v}_2 = (0, 2)^T$.

Gramovou-Schmidtovou ortogonalizací získáme ortonormální bázi

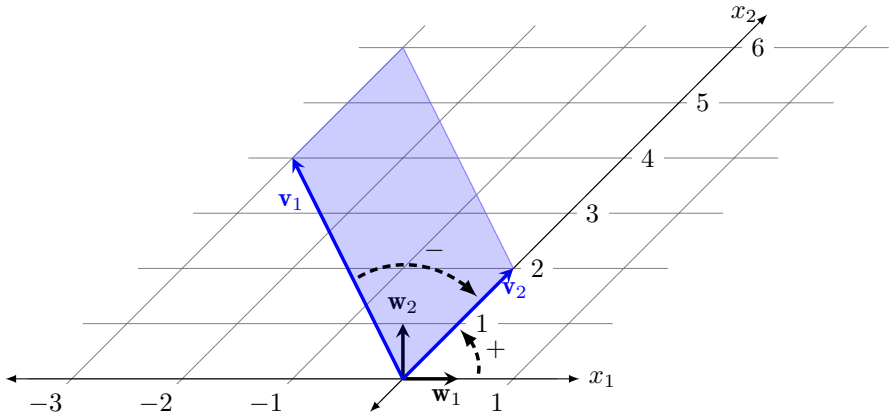
$$B = (\mathbf{w}_1, \mathbf{w}_2) = \left(\frac{1}{2}\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} -1 \\ 2 \end{pmatrix}\right)$$

Tato báze je kladně orientovaná, protože matice přechodu od B ke kladně orientované bázi K_2 má determinant $1 > 0$.

Podle odvozeného vzorce je nyní orientovaný objem roven

$$\begin{aligned}\mathrm{vol}_2(\mathbf{v}_1,\mathbf{v}_2) &= \det\left([\mathbf{v}_1]_B|[\mathbf{v}_2]_B\right) = \det\begin{pmatrix} \langle \mathbf{w}_1,\mathbf{v}_1\rangle & \langle \mathbf{w}_1,\mathbf{v}_2\rangle \\ \langle \mathbf{w}_2,\mathbf{v}_1\rangle & \langle \mathbf{w}_2,\mathbf{v}_2\rangle \end{pmatrix} \\ &= \det\begin{pmatrix} -2 & 2 \\ 4 & 2 \end{pmatrix} = -12\end{aligned}$$

▲



Obrázek 8.12. Obsah rovnoběžníku určeného vektory $\mathbf{v}_1$ a $\mathbf{v}_2$.

Ukážeme, jak lze objem spočítat bez znalosti ortonormální báze. Označme $A = ([\mathbf{v}_1]_B|\dots|[\mathbf{v}_n]_B)$ matici, jejíž determinant je orientovaný objem. V matici A^TA je na pozici (i,j) číslo $[\mathbf{v}_i]_B^T[\mathbf{v}_j]_B = [\mathbf{v}_i]_B\cdot[\mathbf{v}_j]_B$. Vzhledem k ortonormální bázi skalární součin přechází ve standardní (viz tvrzení 8.50), takže tento výraz je roven $\langle \mathbf{v}_i,\mathbf{v}_j\rangle$. To znamená, že A^TA je Gramova matice vektorů $\mathbf{v}_1,\dots,\mathbf{v}_n$! Protože $\det\left(A^TA\right) = (\det(A))^2$ dostáváme následující tvrzení.

Tvrzení 8.100. *Nechť* $\mathbf{V}$ *je reálný orientovaný vektorový prostor dimenze* n *se skalárním součinem* $\langle\,,\rangle$ *a* $\mathbf{v}_1,\dots,\mathbf{v}_n \in V$. *Pak*

$$(\mathrm{vol}_n(\mathbf{v}_1,\dots,\mathbf{v}_n))^2 = \det\begin{pmatrix} \langle \mathbf{v}_1,\mathbf{v}_1\rangle & \langle \mathbf{v}_2,\mathbf{v}_1\rangle & \dots & \langle \mathbf{v}_n,\mathbf{v}_1\rangle \\ \langle \mathbf{v}_1,\mathbf{v}_2\rangle & \langle \mathbf{v}_2,\mathbf{v}_2\rangle & \dots & \langle \mathbf{v}_n,\mathbf{v}_2\rangle \\ \vdots & & & \vdots \\ \langle \mathbf{v}_1,\mathbf{v}_n\rangle & \langle \mathbf{v}_2,\mathbf{v}_n\rangle & \dots & \langle \mathbf{v}_n,\mathbf{v}_n\rangle \end{pmatrix}.$$

Slovy, objem je rovný odmocnině Gramova determinantu.

Příklad 8.101. Uvažujme stejný orientovaný prostor se skalárním součinem jako v předchozím příkladu a stejné vektory $\mathbf{v}_1 = (-3,4)^T, \mathbf{v}_2 = (0,2)^T$. Bez počítání ortonormální báze nyní můžeme objem vypočítat pomocí předchozího tvrzení.

$$|\mathrm{vol}_2(\mathbf{v}_1,\mathbf{v}_2)| = \sqrt{\det\begin{pmatrix} \langle \mathbf{v}_1,\mathbf{v}_1\rangle & \langle \mathbf{v}_1,\mathbf{v}_2\rangle \\ \langle \mathbf{v}_2,\mathbf{v}_1\rangle & \langle \mathbf{v}_2,\mathbf{v}_2\rangle \end{pmatrix}} = \sqrt{\det\begin{pmatrix} 20 & 4 \\ 4 & 8 \end{pmatrix}} = 12$$

(Svislé závorky zde znamenají absolutní hodnotu, nikoliv determinant.) Chceme-li znát orientovaný objem, všimneme si, že determinant matice přechodu od $(\mathbf{v}_1,\mathbf{v}_2)$ ke K_2 je -6, takže báze $(\mathbf{v}_1,\mathbf{v}_2)$ je záporně orientovaná, a proto $\mathrm{vol}_2(\mathbf{v}_1,\mathbf{v}_2) = -12$. ▲

Příklad 8.102. V prostoru $\mathbb{R}^3$ se standardním součinem určíme obsah rovnoběžníku určeného vektory $\mathbf{v}_1 = (1,2,3)^T$ a $\mathbf{v}_2 = (3,1,-1)^T$. Přesněji řečeno,

chceme určit 2-rozměrný objem tohoto rovnoběžníku v prostoru $\mathrm{LO}\{\mathbf{v}_1, \mathbf{v}_2\}$ se zúžením standardního skalárního součinu v $\mathbb{R}^3$ na tento podprostor.

Pokud bychom počítali obsah z definice, museli bychom nejprve nalézt nějakou ortogonální bázi v $\mathrm{LO}\{\mathbf{v}_1, \mathbf{v}_2\}$. Použitím předchozího tvrzení je ale výpočet velmi snadný:

$$|\mathrm{vol}_2(\mathbf{v}_1, \mathbf{v}_2)| = \sqrt{\det \begin{pmatrix} \mathbf{v}_1 \cdot \mathbf{v}_1 & \mathbf{v}_1 \cdot \mathbf{v}_2 \\ \mathbf{v}_2 \cdot \mathbf{v}_1 & \mathbf{v}_2 \cdot \mathbf{v}_2 \end{pmatrix}} = \sqrt{\det \begin{pmatrix} 14 & 2 \\ 2 & 11 \end{pmatrix}} = 5\sqrt{6}$$

V prostoru $\mathrm{LO}\{\mathbf{v}_1, \mathbf{v}_2\}$ nemáme žádnou přirozenou orientaci zděděnou z $\mathbb{R}^3$, takže pro výpočet orientovaného obsahu bychom orientaci nejprve museli zadat. ▲

8.8. Vektorový součin

Výpočty v reálných prostorech dimenze 3 usnadňuje vektorový součin. Tento pojem probereme pouze informativně, principy budeme vysvětlovat na aritmetickém vektorovém prostoru $\mathbb{R}^3$ s kladně orientovanou kanonickou bází a standardním skalárním součinem. Definice a tvrzení budeme formulovat obecně a rozmyšlení důkazů přenecháme čtenáři.

Zafixujeme si nějak vektory $\mathbf{v}_1, \mathbf{v}_2$, pro konkrétní představu např. $\mathbf{v}_1 = (1, 2, 3)^T$ a $\mathbf{v}_2 = (-1, 1, 4)^T$. Orientovaný objem rovnoběžnostěnu určeného pevnými vektory $\mathbf{v}_1, \mathbf{v}_2$ a proměnným vektorem $\mathbf{z} = (z_1, z_2, z_3)^T$ je lineární forma f. V našem konkrétním případě je

$$f((z_1, z_2, z_3)^T) = \det \begin{pmatrix} 1 & -1 & z_1 \\ 2 & 1 & z_2 \\ 3 & 4 & z_3 \end{pmatrix} = 5z_1 - 7z_2 + 3z_3$$

Hodnotu formy f na vektoru $\mathbf{z}$ můžeme vyjádřit jako skalární součin jistého (jednoznačně určeného) vektoru $\mathbf{q}$ a vektoru (z_1, z_2, z_3):

$$f(\mathbf{z}) = (5, -7, 3)^T \cdot \mathbf{z}, \qquad \text{tedy } \mathbf{q} = (5, -7, 3)^T$$

Tento vektor $\mathbf{q}$ nazýváme vektorový součin vektorů $\mathbf{v}_1, \mathbf{v}_2$ a značíme $\mathbf{q} = \mathbf{v}_1 \times \mathbf{v}_2$. To motivuje následující definici.

Definice 8.103. Nechť $\mathbf{V}$ je reálný orientovaný vektorový prostor dimenze 3 se skalárním součinem $\langle\, , \rangle$ a $\mathbf{v}_1, \mathbf{v}_2 \in V$. *Vektorovým součinem* vektorů $\mathbf{v}_1, \mathbf{v}_2$ rozumíme jednoznačně určený vektor $\mathbf{v}_1 \times \mathbf{v}_2$, pro který platí

$$\mathrm{vol}_3(\mathbf{v}_1, \mathbf{v}_2, \mathbf{z}) = \langle\, \mathbf{v}_1 \times \mathbf{v}_2, \mathbf{z} \rangle \quad .$$

pro všechny vektory $\mathbf{z}$ z $\mathbf{V}$.

Vrátíme se k $\mathbb{R}^3$ a ukážeme, jak lze obecně spočítat vektorový součin $\mathbf{v}_1 = (x_1, x_2, x_3)^T$ a $\mathbf{v}_2 = (y_1, y_2, y_3)^T$. Pro libovolný vektor $\mathbf{z} = (z_1, z_2, z_3)^T$ dostáváme z rozvoje determinantu $\det(\mathbf{v}_1|\mathbf{v}_2|\mathbf{z})$ podle třetího sloupce

$$\det(\mathbf{v}_1|\mathbf{v}_2|\mathbf{z}) = (x_2y_3 - x_3y_2)z_1 - (x_1y_3 - x_3y_1)z_2 + (x_1y_2 - x_2y_1)z_3 \ ,$$

takže podle definice je

$$\mathbf{v}_1 \times \mathbf{v}_2 = (x_2y_3 - x_3y_2, -x_1y_3 + x_3y_1, x_1y_2 - x_2y_1)^T \quad .$$

To je vzorec, který nejspíše znáte ze střední školy. Alternativně lze vzorec získat postupně dosazením $\mathbf{z} = \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ do definice. Pro obecný prostor vyjde stejný vzorec vzhledem k libovolné kladně orientované ortonormální bázi.

Tvrzení 8.104. *Nechť $\mathbf{V}$ je reálný orientovaný vektorový prostor dimenze 3 se skalárním součinem $\langle\, , \rangle$, B je kladně orientovaná ortonormální báze $\mathbf{V}$, $\mathbf{v}_1, \mathbf{v}_2 \in V$, $[\mathbf{v}_1]_B = (x_1, x_2, x_3)^T$ a $[\mathbf{v}_2]_B = (y_1, y_2, y_3)^T$. Pak*

$$[\mathbf{v}_1 \times \mathbf{v}_2]_B = (x_2y_3 - x_3y_2, -x_1y_3 + x_3y_1, x_1y_2 - x_2y_1)^T \quad .$$

Nyní nalezneme geometrický význam směru a délky vektorového součinu.

Nejprve dokážeme kolmost vektorového součiny na oba parametry. Jsou-li vektory $\mathbf{v}_1, \mathbf{v}_2$ lineárně závislé, pak je determinant $\det(\mathbf{v}_1|\mathbf{v}_2|\mathbf{v}_3)$ rovný nule a vektorový součin je tudíž nulový vektor. Předpokládejme dále, že vektory jsou lineárně nezávislé. Vektor $\mathbf{v}_1 \times \mathbf{v}_2$ je kolmý na oba vektory $\mathbf{v}_1, \mathbf{v}_2$, protože $(\mathbf{v}_1 \times \mathbf{v}_2) \cdot \mathbf{v}_1$ je podle definice rovno $\det(\mathbf{v}_1|\mathbf{v}_2|\mathbf{v}_1) = 0$ a podobně pro vektor $\mathbf{v}_2$. Vektor $\mathbf{v}_1 \times \mathbf{v}_2$ tedy leží v ortogonálním doplňku roviny $\mathrm{LO}\{\mathbf{v}_1, \mathbf{v}_2\}$, což je podprostor dimenze 1. Tím je určen směr.

K určení normy vektorového součinu stačí spočítat $\|\mathbf{v}_1 \times \mathbf{v}_2\|^2 = (\mathbf{v}_1 \times \mathbf{v}_2) \cdot (\mathbf{v}_1 \times \mathbf{v}_2)$. K tomu využijeme tzv. Cauchy-Binetův vzorec, který ve speciálním případě říká

$$\begin{aligned}(\mathbf{v}_1 \times \mathbf{v}_2) \cdot (\mathbf{w}_1 \times \mathbf{w}_2) &= \det\left((\mathbf{v}_1|\mathbf{v}_2)^T(\mathbf{w}_1|\mathbf{w}_2)\right) = \det\begin{pmatrix} \mathbf{v}_1 \cdot \mathbf{w}_1 & \mathbf{v}_1 \cdot \mathbf{w}_2 \\ \mathbf{v}_2 \cdot \mathbf{w}_1 & \mathbf{v}_2 \cdot \mathbf{w}_2 \end{pmatrix} \\ &= (\mathbf{v}_1 \cdot \mathbf{w}_1)(\mathbf{v}_2 \cdot \mathbf{w}_2) - (\mathbf{v}_1 \cdot \mathbf{w}_2)(\mathbf{v}_2 \cdot \mathbf{w}_1)\end{aligned}$$

Vzorec si můžete ověřit přímým výpočtem. Pro normu vektorového součinu dostáváme

$$\|\mathbf{v}_1 \times \mathbf{v}_2\| = \sqrt{(\mathbf{v}_1 \times \mathbf{v}_2) \cdot (\mathbf{v}_1 \times \mathbf{v}_2)} = \sqrt{\det\begin{pmatrix} \mathbf{v}_1 \cdot \mathbf{v}_1 & \mathbf{v}_1 \cdot \mathbf{v}_2 \\ \mathbf{v}_2 \cdot \mathbf{v}_1 & \mathbf{v}_2 \cdot \mathbf{v}_2 \end{pmatrix}}\,.$$

Nakonec si všimneme, že $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_1 \times \mathbf{v}_2)$ je kladně orientovaná báze, protože $\det(\mathbf{v}_1|\mathbf{v}_2|\mathbf{v}_1 \times \mathbf{v}_2) = (\mathbf{v}_1 \times \mathbf{v}_2) \cdot (\mathbf{v}_1 \times \mathbf{v}_2) > 0$. Z toho také plyne, že vektorový součin změní znaménko, změníme-li orientaci prostoru.

Tvrzení 8.105. *Nechť* $\mathbf{V}$ *je reálný orientovaný vektorový prostor dimenze* 3 *se skalárním součinem* $\langle\,,\rangle$ *a* $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{V}$. *Pak platí*

- $\mathbf{v}_1 \times \mathbf{v}_2 = \mathbf{o}$ *právě tehdy, když je posloupnost* $(\mathbf{v}_1, \mathbf{v}_2)$ *lineárně závislá,*
- $\mathbf{v}_1 \times \mathbf{v}_2 \in \mathrm{LO}\{\mathbf{v}_1, \mathbf{v}_2\}^\perp$,
- $\|\mathbf{v}_1 \times \mathbf{v}_2\| = |\mathrm{vol}_2(\mathbf{v}_1, \mathbf{v}_2)| = \|\mathbf{v}_1\|\,\|\mathbf{v}_2\| \sin(\mathrm{uhel}(\mathbf{v}_1, \mathbf{v}_2))$,
- *je-li* $(\mathbf{v}_1, \mathbf{v}_2)$ *lineárně nezávislá posloupnost, pak je* $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_1 \times \mathbf{v}_2)$ *kladně orientovaná báze prostoru* $\mathbf{V}$.

Ve cvičeních najdete řadu užitečných formulek pro vektorový součin.

Na závěr poznamenejme, že v obecné dimenzi n lze definovat vektorový součin $(n-1)$-tice vektorů vztahem

$$\det(\mathbf{v}_1|\ldots|\mathbf{v}_n) = \langle\, \mathbf{v}_1 \times \cdots \times \mathbf{v}_{n-1}, \mathbf{v}_n \rangle\,.$$

Cvičení

1. Jsou-li A, B matice nad tělesem $\mathbb{C}$ typu $m \times n$, C je matice typu $n \times p$ nad $\mathbb{C}$ a $a \in \mathbb{C}$, pak

(1) $(A+B)^* = A^* + B^*$,
(2) $(aA)^* = \overline{a}A^*$,
(3) $(A^*)^* = A$.
(4) $(BC)^* = C^*B^*$.

Dokažte.

2. Nechť A je čtvercová matice nad $\mathbb{C}$. Dokažte, že $\det(A^*) = (\det(A))^*$.

3. Nechť A je regulární matice nad $\mathbb{C}$. Dokažte, že $(A^*)^{-1} = (A^{-1})^*$.

4. Nechť A je čtvercová matice řádu n nad $\mathbb{C}$. Dokažte, že zobrazení $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$ definované vztahem $\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}^* A \mathbf{v}$ splňuje podmínky (SL1) a (SL2).

5. Nechť A je čtvercová matice řádu n nad $\mathbb{C}$. Dokažte, že zobrazení $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$ definované vztahem $\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}^* A \mathbf{v}$ splňuje podmínku (SSS) právě tehdy, když A je hermitovská (tj. $A^* = A$).

6. Nechť B je regulární matice řádu n nad $\mathbb{C}$ a $A = B^*B$. Dokažte, že zobrazení $\mathbb{C}\times\mathbb{C} \to \mathbb{C}$ definované vztahem $\langle \mathbf{u}, \mathbf{v}\rangle = \mathbf{u}^* A\mathbf{v}$ je skalární součin.

7. Dokažte, že v libovolném vektorovém prostoru se skalárním součinem $\langle\, ,\rangle$ platí

- $\mathrm{Re}\,(\langle \mathbf{u}, \mathbf{v}\rangle) = \frac{1}{2}(\|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - \|\mathbf{u} - \mathbf{v}\|^2)$
- $\mathrm{Re}\,(\langle \mathbf{u}, \mathbf{v}\rangle) = \frac{1}{4}(\|\mathbf{u} + \mathbf{v}\|^2 - \|\mathbf{u} - \mathbf{v}\|^2)$
- $\mathrm{Im}\,(\langle \mathbf{u}, \mathbf{v}\rangle) = \frac{1}{2}(\|\mathbf{u} - i\mathbf{v}\|^2 - \|\mathbf{u}\|^2 - \|\mathbf{v}\|^2)$
- $\mathrm{Im}\,(\langle \mathbf{u}, \mathbf{v}\rangle) = \frac{1}{2}(\|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - \|\mathbf{u} + i\mathbf{v}\|^2)$
- $\mathrm{Im}\,(\langle \mathbf{u}, \mathbf{v}\rangle) = \frac{1}{4}(\|\mathbf{u} - i\mathbf{v}\|^2 - \|\mathbf{u} + i\mathbf{v}\|^2)$

$\mathrm{Im}\,(x)$ značí imaginární část čísla $x \in \mathbb{C}$.

8. Nad reálnými čísly lze Cauchyho-Schwarzovu nerovnost dokázat také následujícím způsobem: Výraz $\|\mathbf{u} + t\mathbf{v}\|^2$ definuje kvadratickou funkci. Protože musí být nezáporná, její diskriminant je nekladný a to dává C-S nerovnost. Doplňte detaily.

9. Kdy nastává v trojúhelníkové nerovnosti rovnost?

10. Dokažte, že norma pochází ze skalárního součinu právě tehdy, když splňuje rovnoběžníkové pravidlo.

11. Dokažte, že platí-li $M \perp N$, pak $M \cap N \subseteq \{\mathbf{o}\}$.

12. Dokažte, že v prostorech nad $\mathbb{R}$ se skalárním součinem platí opačná implikace v Pythagorově větě, tj. pokud $\|\mathbf{u} + \mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2$, pak $\mathbf{u} \perp \mathbf{v}$. Platí opačná implikace v prostorech nad $\mathbb{C}$?

13. Nechť $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení a $\mathbf{U} \leq \mathbf{V}$ je doplněk $\mathrm{Ker}\, f$, tj. $\mathrm{Ker}\, f \oplus U = V$. Dokažte, že zúžení f na $\mathbf{U}$ je izomorfismus z $\mathbf{U}$ na obraz f.

14. Dokažte, že determinant Gramovy matice vektorů $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n \in \mathbb{R}^n$ je rovný druhé mocnině determinantu matice

$$(\mathbf{w}_1|\mathbf{w}_2|\ldots|\mathbf{w}_n)\ .$$

Interpretujte geometricky.

15. Využijte QR-rozklad na důkaz následující nerovnosti pro komplexní matici $A = (\mathbf{a}_1|\ldots|\mathbf{a}_n)$ typu $m \times n$ a standardní skalární součin:

$$\det(A^*A) \leq \|\mathbf{a}_1\|^2\, \|\mathbf{a}_2\|^2 \ldots \|\mathbf{a}_n\|^2$$

Připomeňme si geometrický význam determinantu $\det(A^*A)$ a interpretujte nerovnost geoemetricky.

16. OG PROJEKCE NA NEKONECNE GENEROVANY NEMUSI EXISTOVAT

17. Dokažte, že každé zobrazení $f : \mathbb{C}^n \to \mathbb{C}^n$ zachovávající standardní skalární součin je lineární. (TODO: DODELAT)

18. Dokažte, že každé zobrazení $f : \mathbb{C}^n \to \mathbb{C}^n$ zachovávající kolmost je skalární násobek unitárního. (TODO: DODELAT)

19. Dokažte, že matice unitárního operátoru na konečně generovaném prostoru vzhledem k ortonormálním bázím je ortonormální.

20. TODO: nejlepsi aproximace s nejlepsi normou.

21.

- $\mathbf{v}_1 \times \mathbf{v}_2 = -(\mathbf{v}_2 \times \mathbf{v}_1)$
- $(t\mathbf{v}_1) \times \mathbf{v}_2 = t(\mathbf{v}_1 \times \mathbf{v}_2)$
- $(\mathbf{v}_1 + \mathbf{v}_1') \times \mathbf{v}_2 = \mathbf{v}_1 \times \mathbf{v}_2 + \mathbf{v}_1' \times \mathbf{v}_2$
- $\mathbf{v}_1 \times (\mathbf{v}_2 \times \mathbf{v}_3) = \langle \mathbf{v}_1, \mathbf{v}_3\rangle\, \mathbf{v}_2 - \langle \mathbf{v}_1, \mathbf{v}_2\rangle\, \mathbf{v}_3$
- $\mathbf{v}_1 \times (\mathbf{v}_2 \times \mathbf{v}_3) - (\mathbf{v}_1 \times \mathbf{v}_2) \times \mathbf{v}_3 = \langle \mathbf{v}_2, \mathbf{v}_3\rangle\, \mathbf{v}_1 - \langle \mathbf{v}_1, \mathbf{v}_2\rangle\, \mathbf{v}_3$
- $\mathbf{v}_1 \times (\mathbf{v}_2 \times \mathbf{v}_3) + \mathbf{v}_2 \times (\mathbf{v}_3 \times \mathbf{v}_1) + \mathbf{v}_3 \times (\mathbf{v}_1 \times \mathbf{v}_2) = \mathbf{o}$

Shrnutí osmé kapitoly

(1) Pro dva n-složkové aritmetické vektory $\mathbf{u} = (x_1, x_2, \ldots, x_n)^T$, $\mathbf{v} = (y_1, y_2, \ldots, y_n) \in \mathbb{R}^n$ definujeme jejich *standardní skalární součin* jako reálné číslo

$$\mathbf{u} \cdot \mathbf{v} = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n \ .$$

(2) *Eukleidovská norma* nebo také *eukleidovská délka* vektoru $\mathbf{u} \in \mathbb{R}^n$ je číslo

$$\|\mathbf{u}\| = \sqrt{\mathbf{u} \cdot \mathbf{u}} = \sqrt{\mathbf{u}^{\mathbf{T}}\, \mathbf{u}} \ .$$

Eukleidovskou normu vektoru $\mathbf{u} = (x_1, x_2, \ldots, x_n)^T$ tak spočítáme jako

$$\|\mathbf{u}\| = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2} \ .$$

(3) Geometrický význam standardního skalárního součinu je vyjádřen vztahem

$$\mathbf{u} \cdot \mathbf{v} = \|\mathbf{u}\| \ \|\mathbf{v}\| \cos\alpha \ ,$$

kde α je úhel, který vektory $\mathbf{u}$ a $\mathbf{v}$ svírají.

(4) Jiný geometrický význam spočívá v tom, že absolutní hodnota součinu $\|\mathbf{v}\| \cos\alpha$ je délkou ortogonální projekce vektoru $\mathbf{v}$ do přímky určené vektorem $\mathbf{u} \neq \mathbf{o}$. Projekce má stejný směr jako vektor $\mathbf{u}$ v případě, že oba vektory $\mathbf{u}, \mathbf{v}$ svírají úhel menší než $\pi/2$, a má opačný směr, pokud oba vektory svírají úhel větší než $\pi/2$.

(5) Rovnici přímky v rovině $a_1 x_1 + a_2 x_2 = b$ můžeme přepsat pomocí stanardního skalární součinu do tvaru

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = b \ ,$$

a protože v případě rovnice přímky je vektor $(a_1, a_2)^T \neq \mathbf{o}$, jde o množinu všech bodů (x_1, x_2) v rovině, jejichž polohové vektory $\mathbf{x} = (x_1, x_2)^T$ mají stejnou ortogonální projekci do přímky $\mathrm{LO}\,\{\mathbf{a}\}$. Vektor $\mathbf{a}$ nazýváme *normálovým vektorem* přímky $a_1 x_1 + a_2 x_2 = b$.

(6) Jsou-li $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{R}^n$ libovolné reálné aritmetické vektory a $a \in \mathbb{R}$ skalár, pak platí
   (a) $\mathbf{u} \cdot \mathbf{v} = \mathbf{v} \cdot \mathbf{u}$,
   (b) $\mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w}$,
   (c) $\mathbf{u} \cdot (a\mathbf{v}) = a(\mathbf{u} \cdot \mathbf{v})$,
   (d) $\mathbf{u} \cdot \mathbf{u} \geq 0$ a $\mathbf{u} \cdot \mathbf{u} = 0$ právě když $\mathbf{u} = \mathbf{o}$.

(7) Pro dva komplexní aritmetické vektory $\mathbf{u} = (x_1,\ x_2,\ \ldots,\ x_n)^T$ a $\mathbf{v} = (y_1, y_2, \ldots, y_n)^T$ definujeme *standardní skalární součin* $\mathbf{u} \cdot \mathbf{v}$ předpisem

$$\mathbf{u} \cdot \mathbf{v} = \overline{x_1} y_1 + \overline{x_2} y_2 + \cdots + \overline{x_n} y_n \ ,$$

kde $\overline{x}$ značí číslo komplexně sdružené k x, tj. $\overline{a + bi} = a - bi$.

(8) *Eukleidovskou délku* nebo také *eukleidovskou normu* aritmetického vektoru $\mathbf{u} = (x_1,\ x_2,\ \ldots,\ x_n)^T \in \mathbb{C}^n$ definujeme jako

$$\|\mathbf{u}\| = \sqrt{\mathbf{u} \cdot \mathbf{u}} = \sqrt{\overline{x_1} x_1 + \overline{x_2} x_2 + \cdots + \overline{x_n} x_n} = \sqrt{|x_1|^2 + |x_2|^2 + \cdots + |x_n|^2} \ .$$

(9) *Hermitovsky sdružená matice* k matici $A = (a_{ij})_{m \times n}$ je matice $A^* = (b_{ji})_{n \times m}$, kde $b_{ji} = \overline{a_{ij}}$ pro libovolné indexy $i \in \{1, 2, \ldots, m\}$ a $j \in \{1, 2, \ldots, n\}$.

(10) Pro libovolné tři vektory $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{C}^n$ a komplexní číslo a platí
   (a) $\mathbf{u} \cdot \mathbf{v} = \overline{\mathbf{v} \cdot \mathbf{u}}$,
   (b) $\mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w}$,
   (c) $\mathbf{u} \cdot (a\,\mathbf{v}) = a\,(\mathbf{u} \cdot \mathbf{v})$,
   (d) $\mathbf{u} \cdot \mathbf{u}$ je nezáporné reálné číslo, a $\mathbf{u} \cdot \mathbf{u} = 0$ právě když $\mathbf{u} = \mathbf{o}$.

(11) Pro libovolné tři vektory $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{C}^n$ a komplexní číslo a platí

(a) $(\mathbf{u}+\mathbf{v})\cdot\mathbf{w} = \mathbf{u}\cdot\mathbf{w}+\mathbf{v}\cdot\mathbf{w}$,
(b) $(a\mathbf{u})\cdot\mathbf{v} = \overline{a}\,(\mathbf{u}\cdot\mathbf{v})$.

(12) Je-li $\mathbf{V}$ vektorový prostor nad $\mathbb{R}$ (resp. nad $\mathbb{C}$), pak se zobrazení $\langle\,,\rangle$ z $V\times V$ do $\mathbb{R}$ (resp do $\mathbb{C}$), které dvojici $\mathbf{u},\mathbf{v}$ přiřadí skalár $\langle\mathbf{u},\mathbf{v}\rangle$, nazývá *skalární součin* na $\mathbf{V}$, pokud pro libovolné $\mathbf{u},\mathbf{v},\mathbf{w}\in V$ a $a\in\mathbb{R}$ (resp. $a\in\mathbb{C}$) platí
(SSS) $\langle\mathbf{u},\mathbf{v}\rangle = \overline{\langle\mathbf{v},\mathbf{u}\rangle}$,
(SL1) $\langle\mathbf{u},a\mathbf{v}\rangle = a\,\langle\mathbf{u},\mathbf{v}\rangle$,
(SL2) $\langle\mathbf{u},\mathbf{v}+\mathbf{w}\rangle = \langle\mathbf{u},\mathbf{v}\rangle+\langle\mathbf{u},\mathbf{w}\rangle$,
(SP) $\langle\mathbf{u},\mathbf{u}\rangle$ je nezáporné reálné číslo, které je nulové právě tehdy, když $\mathbf{u}=\mathbf{o}$.

(13) Je-li $\mathbf{V}$ vektorový prostor nad $\mathbb{R}$ (resp. nad $\mathbb{C}$) se skalárním součinem $\langle\,,\rangle$, pak pro prvky libovolné $\mathbf{u},\mathbf{v},\mathbf{w}\in V$ a skalár a platí
(a) $\langle\mathbf{u},\mathbf{o}\rangle = 0 = \langle\mathbf{o},\mathbf{u}\rangle$
(b) $\langle a\mathbf{u},\mathbf{v}\rangle = \overline{a}\,\langle\mathbf{u},\mathbf{v}\rangle$
(c) $\langle\mathbf{u}+\mathbf{v},\mathbf{w}\rangle = \langle\mathbf{u},\mathbf{w}\rangle+\langle\mathbf{v},\mathbf{w}\rangle$.

(14) Komplexním maticím A, které splňují rovnost $A^* = A$ říkáme *hermitovské*.

(15) Hermitovská matice A řádu n se nazývá *pozitivně definitní*, pokud $\mathbf{u}^*A\mathbf{u}$ je nezáporné reálné číslo pro libovolné $\mathbf{u}\in\mathbb{C}^n$ a rovná se 0 právě když $\mathbf{u}=\mathbf{o}$.

(16) Je-li A pozitivně definitní, pak zobrazení definované $\langle\mathbf{u},\mathbf{v}\rangle = \mathbf{u}^*A\mathbf{v}$ je skalární součin na $\mathbb{C}^n$ (nebo na $\mathbb{R}^n$).

(17) Každá matice tvaru $A = B^*B$, kde B je regulární, je pozitivně definitní.

(18) Nechť $\mathbf{V}$ je vektorový prostor se skalárním součinem $\langle\,,\rangle$. *Normou* vektoru $\mathbf{u}\in V$ rozumíme reálné číslo

$$\|\mathbf{u}\| = \sqrt{\langle\mathbf{u},\mathbf{u}\rangle}\ .$$

Vektor $\mathbf{u}$ se nazývá *jednotkový*, pokud $\|\mathbf{u}\| = 1$.

(19) Nechť $\mathbf{V}$ je vektorový prostor nad $\mathbb{R}$ (resp. $\mathbb{C}$) se skalárním součinem $\langle\,,\rangle$, $\mathbf{u},\mathbf{v}\in V$ a $t\in\mathbb{R}$ (resp. $t\in\mathbb{C}$). Pak platí
(a) $\|\mathbf{u}\|\geq 0$, přičemž $\|\mathbf{u}\| = 0$ právě tehdy, když $\mathbf{u}=\mathbf{o}$,
(b) $\|t\mathbf{u}\| = |t|\,\|\mathbf{u}\|$,
(c) $\|\mathbf{u}+\mathbf{v}\|^2+\|\mathbf{u}-\mathbf{v}\|^2 = 2\,\|\mathbf{u}\|^2+2\,\|\mathbf{v}\|^2$, (rovnoběžníkové pravidlo),
(d) $\mathrm{Re}\,(\langle\mathbf{u},\mathbf{v}\rangle) = \frac{1}{2}(\|\mathbf{u}+\mathbf{v}\|^2-\|\mathbf{u}\|^2-\|\mathbf{v}\|^2)$, (polarizační identita),
kde $\mathrm{Re}\,(x)$ značí reálnou část x.

(20) Cauchyho-Schwarzova nerovnost. Nechť $\mathbf{V}$ je vektorový prostor se skalárním součinem $\langle\,,\rangle$ a $\mathbf{u},\mathbf{v}\in V$. Pak platí

$$|\,\langle\mathbf{u},\mathbf{v}\rangle\,|\leq\|\mathbf{u}\|\,\|\mathbf{v}\|\ ,$$

přičemž rovnost nastává právě tehdy, když $(\mathbf{u},\mathbf{v})$ je lineárně závislá posloupnost.

(21) Trojúhelníková nerovnost. Nechť $\mathbf{V}$ je vektorový prostor se skalárním součinem $\langle\,,\rangle$ a $\mathbf{u},\mathbf{v}\in V$. Pak platí

$$\|\mathbf{u}+\mathbf{v}\|\leq\|\mathbf{u}\|+\|\mathbf{v}\|\ .$$

(22) Nechť $\mathbf{V}$ je vektorový prostor nad $\mathbb{R}$ se skalárním součinem $\langle\,,\rangle$ a $\mathbf{o}\neq\mathbf{u},\mathbf{v}\in V$. *Úhlem mezi prvky* $\mathbf{u}$ *a* $\mathbf{v}$ rozumíme reálné číslo $\alpha\in[0,\pi]$ splňující

$$\cos\alpha = \frac{\langle\mathbf{u},\mathbf{v}\rangle}{\|\mathbf{u}\|\,\|\mathbf{v}\|}\ .$$

(23) Kosinová věta. Nechť $\mathbf{V}$ je vektorový prostor nad $\mathbb{R}$ se skalárním součinem $\langle\,,\rangle$ a $\mathbf{o} \neq \mathbf{u}, \mathbf{v} \in V$. Pak platí

$$\|\mathbf{u}-\mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2\,\|\mathbf{u}\|\,\|\mathbf{v}\|\cos\alpha \ ,$$

kde α je úhel mezi vektory $\mathbf{u}$ a $\mathbf{v}$.

(24) Je-li $\mathbf{V}$ vektorový prostor nad $\mathbb{C}$ (nebo nad $\mathbb{R}$), pak zobrazení $\|\cdot\|$, které přiřazuje každému prvku $\mathbf{u}$ reálné číslo $\|\mathbf{u}\|$ nazýváme *norma* na prostoru $\mathbf{V}$, pokud platí pro každé dva prvky $\mathbf{u}, \mathbf{v} \in V$ a každý skalár t
 (a) $\|\mathbf{u}\| \geq 0$, přičemž $\|\mathbf{u}\| = 0$ právě tehdy, když $\mathbf{u} = \mathbf{o}$,
 (b) $\|t\mathbf{u}\| = |t|\,\|\mathbf{u}\|$,
 (c) $\|\mathbf{u}+\mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\|$.

(25) Nechť $\mathbf{V}$ je vektorový prostor se skalárním součinem $\langle\,,\rangle$. Prvky $\mathbf{u}, \mathbf{v} \in V$ nazýváme *kolmé* (nebo *ortogonální*) a píšeme $\mathbf{u} \perp \mathbf{v}$, pokud $\langle\,\mathbf{u}, \mathbf{v}\rangle = 0$.

Množina, nebo posloupnost, M prvků V se nazývá *ortogonální*, pokud $\mathbf{u} \perp \mathbf{v}$ pro libovolné dva různé prvky množiny (nebo posloupnosti) M.

Množina (posloupnost) M se nazývá *ortonormální*, pokud je ortogonální a každý vektor v M je jednotkový.

(26) Je-li $\mathbf{V}$ vektorový prostor se skalárním součinem $\langle\,,\rangle$, pak každá ortogonální posloupnost nenulových prvků V je lineárně nezávislá.

(27) Pythagorova věta. Je-li $\mathbf{V}$ vektorový prostor se skalárním součinem $\langle\,,\rangle$ a jsou-li vektory $\mathbf{u}, \mathbf{v} \in V$ kolmé, pak platí

$$\|\mathbf{u}+\mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 \ .$$

(28) Indukcí lze Pythagorovu větu zobecnit na libovolný konečný počet prvků: je-li $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ ortogonální množina, pak

$$\|\mathbf{v}_1 + \mathbf{v}_2 + \cdots + \mathbf{v}_k\|^2 = \|\mathbf{v}_1\|^2 + \|\mathbf{v}_2\|^2 + \cdots + \|\mathbf{v}_k\|^2 \ .$$

(29) Je-li $\mathbf{V}$ vektorový prostor se skalárním součinem $\langle\,,\rangle$, $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ nějaká ortonormální báze ve $\mathbf{V}$ a $\mathbf{u} \in V$, pak platí

$$\mathbf{u} = \langle\,\mathbf{v}_1, \mathbf{u}\rangle\,\mathbf{v}_1 + \langle\,\mathbf{v}_2, \mathbf{u}\rangle\,\mathbf{v}_2 + \cdots + \langle\,\mathbf{v}_n, \mathbf{u}\rangle\,\mathbf{v}_n \ .$$

Jinými slovy,

$$[\mathbf{u}]_B = (\langle\,\mathbf{v}_1, \mathbf{u}\rangle\,, \langle\,\mathbf{v}_2, \mathbf{u}\rangle\,, \ldots, \langle\,\mathbf{v}_n, \mathbf{u}\rangle)^T \ .$$

(30) Souřadnicím vzhledem k ortonormální bázi se někdy říká *Fourierovy koeficienty* vzhledem k této bázi.

(31) Je-li $\mathbf{V}$ vektorový prostor se skalárním součinem $\langle\,,\rangle$, $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ jeho ortonormální báze, a $\mathbf{u}, \mathbf{w} \in V$, pak

$$\langle\,\mathbf{u}, \mathbf{w}\rangle = [\mathbf{u}]_B^* [\mathbf{w}]_B \ .$$

(32) Je-li $\mathbf{V}$ vektorový prostor se skalárním součinem $\langle\,,\rangle$ a $\mathbf{v} \in V$, $M, N \subseteq V$, pak říkáme, že prvek $\mathbf{v}$ *je kolmý na* M, pokud $\mathbf{v}$ je kolmý na každý prvek z množiny M, což zapisujeme $\mathbf{v} \perp M$.

Říkáme, že M *je kolmá na* N a zapisujeme $M \perp N$, pokud každý prvek množiny M je kolmý na každý prvek množiny N.

(33) Je-li $\mathbf{V}$ vektorový prostor se skalárním součinem $\langle\,,\rangle$ a $M, N \subseteq V$, pak $M \perp N$ právě když $M \perp \mathrm{LO}\,N$ což je právě když $\mathrm{LO}\,M \perp \mathrm{LO}\,N$.

(34) Je-li $\mathbf{V}$ prostor se skalárním součinem $\langle\,,\rangle$ a $M \subseteq V$, pak *ortogonální doplněk* $M^\perp$ množiny M je množina všech prvků $\mathbf{V}$ kolmých na každý prvek M, tj.

$$M^\perp = \{\mathbf{v} \in \mathbf{V} : \mathbf{v} \perp M\} \ .$$

(35) Je-li $\mathbf{V}$ prostor se skalárním součinem $\langle\,,\rangle$ a $M, N \subseteq V$, pak platí
 (a) $M^\perp = \mathrm{LO}\,M^\perp$,
 (b) $M^\perp$ je podprostor V,

(c) je-li $M \subseteq N$, pak $N^{\perp} \subseteq M^{\perp}$.

(36) Nechť $\mathbf{V}$ je konečně generovaný prostor se skalárním součinem $\langle\,,\rangle$, B jeho ortonormální báze, $M = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$. Označíme A matici s řádky $[\mathbf{v}_1]_B^*$, $[\mathbf{v}_2]_B^*$, ..., $[\mathbf{v}_k]_B^*$. Pak

$$[M^{\perp}]_B = \operatorname{Ker} A \ .$$

(37) Je-li $\mathbf{V}$ vektorový prostor se skalárním součinem $\langle\,,\rangle$, $\mathbf{v} \in V$ a $\mathbf{W}$ podprostor prostoru $\mathbf{V}$, pak prvek $\mathbf{w} \in W$ nazýváme *ortogonální projekce* $\mathbf{v}$ *na podprostor* $\mathbf{W}$, pokud platí $(\mathbf{v} - \mathbf{w}) \perp W$ neboli $\mathbf{v} - \mathbf{w} \in W^{\perp}$.

(38) Je-li $\mathbf{W}$ podprostor vektorového prostoru $\mathbf{V}$ se skalárním součinem $\langle\,,\rangle$, $\mathbf{v} \in V$ a $\mathbf{w}$ ortogonální projekce prvku $\mathbf{v}$ na podprostor $\mathbf{W}$, pak pro každý prvek $\mathbf{w} \neq \mathbf{u} \in W$ platí

$$\|\mathbf{v} - \mathbf{w}\| < \|\mathbf{v} - \mathbf{u}\| \ .$$

Ortogonální projekce $\mathbf{v}$ na podprostor $\mathbf{W}$ je určena jednoznačně, pokud existuje.

(39) Je-li $\mathbf{V}$ vektorový prostor se skalárním součinem $\langle\,,\rangle$, $\mathbf{v} \in V$, a $\mathbf{W}$ konečně generovaný podprostor $\mathbf{V}$ s ortonormální bází $(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k)^T$, pak prvek

$$\mathbf{w} = \langle \mathbf{u}_1, \mathbf{v}\rangle\, \mathbf{u}_1 + \langle \mathbf{u}_2, \mathbf{v}\rangle\, \mathbf{u}_2 + \cdots + \langle \mathbf{u}_k, \mathbf{v}\rangle\, \mathbf{u}_k$$

je ortogonální projekcí vektoru $\mathbf{v}$ na podprostor $\mathbf{W}$.

(40) Je-li $\mathbf{V}$ vektorový prostor se skalárním součinem $\langle\,,\rangle$, $\mathbf{v} \in V$, a $\mathbf{W}$ konečně generovaný podprostor $\mathbf{V}$ s ortogonální bází $B = (\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k)^T$, pak prvek

$$\mathbf{w} = \frac{\langle \mathbf{u}_1, \mathbf{v}\rangle}{\|\mathbf{u}_1\|^2}\, \mathbf{u}_1 + \frac{\langle \mathbf{u}_2, \mathbf{v}\rangle}{\|\mathbf{u}_2\|^2}\, \mathbf{u}_2 + \cdots + \frac{\langle \mathbf{u}_k, \mathbf{v}\rangle}{\|\mathbf{u}_k\|^2}\, \mathbf{u}_k$$

je ortogonální projekcí vektoru $\mathbf{v}$ na podprostor $\mathbf{W}$.

(41) *Gramova-Schmidtova ortogonalizace* je algoritmus, který dostane *na vstupu* nějakou lineárně nezávislou posloupnost

$$(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$$

prvků vektorového prostoru $\mathbf{V}$ se skalárním součinem. *Na výstupu* vydá ortonormální posloupnost

$$(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k)$$

prvků prostoru $\mathbf{V}$, která splňuje podmínku

$$\mathrm{LO}\,\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_i\} = \mathrm{LO}\,\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_i\}$$

pro každé $i = 1, 2, \ldots, k$.

(42) Gramova-Schmidtova ortogonalizace spočívá v k-násobném iterování cyklu, jehož i-tý průběh sestává ze dvou kroků

(ia) **ortogonalizace**: najdeme kolmici vektoru $\mathbf{v}_i$ na podprostor $\mathrm{LO}\,\{\mathbf{u}_1, \ldots, \mathbf{u}_{i-1}\}$

$$\mathbf{v}_i - \mathbf{w}_i = \mathbf{v}_i - \langle \mathbf{u}_1, \mathbf{v}_i\rangle\, \mathbf{u}_1 - \langle \mathbf{u}_2, \mathbf{v}_i\rangle\, \mathbf{u}_2 - \cdots - \langle \mathbf{u}_{i-1}, \mathbf{v}_i\rangle\, \mathbf{u}_{i-1},$$

(ib) **normalizace**: položíme

$$\mathbf{u}_i = \frac{\mathbf{v}_i - \mathbf{w}_i}{\|\mathbf{v}_i - \mathbf{w}_i\|} \ .$$

(43) Je-li $\mathbf{W}$ podprostor konečně generovaného vektorového prostoru $\mathbf{V}$ se skalárním součinem, pak každou ortonormální (ortogonální) bázi v podprostoru $\mathbf{W}$ lze doplnit na ortonormální (ortogonální) bázi celého prostoru $\mathbf{V}$.

Speciálně, v každém konečně generovaném vektorovém prostoru se skalárním součinem existuje ortonormální báze.

(44) Je-li $\mathbf{V}$ vektorový prostor dimenze n nad $\mathbb{R}$ (nebo nad $\mathbb{C}$) se skalárním součinem $\langle\,,\rangle$, pak existuje izomorfismus $f : \mathbf{V} \to \mathbb{R}^n$ (nebo $f : \mathbf{V} \to \mathbb{C}^n$), pro který platí

$$\langle \mathbf{u}, \mathbf{v}\rangle = f(\mathbf{u}) \cdot f(\mathbf{v})$$

pro každé dva prvky $\mathbf{u}, \mathbf{v} \in \mathbf{V}$.

(45) QR-rozklad. Je-li A reálná nebo komplexní matice typu $n \times k$ s lineárně nezávislými sloupci, pak existuje matice Q typu $n \times k$ nad stejným tělesem s ortonormálními sloupci a horní trojúhelníková matice R řádu k s kladnými reálnými prvky na hlavní diagonále taková, že platí $A = QR$.

(46) Nechť $\mathbf{V}$ je vektorový prostor se skalárním součinem $\langle\,,\rangle$ a $\mathbf{W}$ je konečně generovaný podprostor $\mathbf{V}$. Pak platí
 (a) $V = W \oplus W^\perp$,
 (b) $(W^\perp)^\perp = W$.
 (c) Každý vektor $\mathbf{v} \in V$ má jednoznačně určenou ortogonální projekci na W a také jednoznačně určenou ortogonální projekci na $W^\perp$.
 (d) Je-li $\mathbf{V}$ konečně generovaný prostor dimenze n, pak $\dim(\mathbf{W}^\perp) = n - \dim(\mathbf{W})$,

(47) Je-li A komplexní matice typu $m \times n$, pak $\operatorname{Ker} A = (\operatorname{Im} A^*)^\perp$, $\operatorname{Im} A^* = (\operatorname{Ker} A)^\perp$ a $\operatorname{Ker} A \oplus \operatorname{Im} A^* = \mathbb{C}^n$.

(48) Je-li $\mathbf{W}$ konečně generovaný podprostor vektorového prostoru $\mathbf{V}$ se skalárním součinem $\langle\,,\rangle$, $\mathbf{v} \in V$ a $\{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k\}$ množina generátorů prostoru $\mathbf{W}$, pak vektor

$$\mathbf{w} = a_1\mathbf{u}_1 + \cdots + a_k\mathbf{u}_k$$

je ortogonální projekcí vektoru $\mathbf{v}$ na W právě tehdy, když je aritmetický vektor $(a_1, \dots, a_k)^T$ řešením soustavy lineárních rovnic

$$\left(\begin{array}{cccc|c} \langle \mathbf{u}_1, \mathbf{u}_1\rangle & \langle \mathbf{u}_1, \mathbf{u}_2\rangle & \cdots & \langle \mathbf{u}_1, \mathbf{u}_k\rangle & \langle \mathbf{u}_1, \mathbf{v}\rangle \\ \langle \mathbf{u}_2, \mathbf{u}_1\rangle & \langle \mathbf{u}_2, \mathbf{u}_2\rangle & \cdots & \langle \mathbf{u}_2, \mathbf{u}_k\rangle & \langle \mathbf{u}_2, \mathbf{v}\rangle \\ \vdots & & \ddots & \vdots & \vdots \\ \langle \mathbf{u}_k, \mathbf{u}_1\rangle & \langle \mathbf{u}_k, \mathbf{u}_2\rangle & \cdots & \langle \mathbf{u}_k, \mathbf{u}_k\rangle & \langle \mathbf{u}_k, \mathbf{v}\rangle \end{array}\right) .$$

(49) Jsou-li $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k$ prvky vektorového prostoru se skalárním součinem $\langle\,,\rangle$, pak čtvercovou matici

$$\begin{pmatrix} \langle \mathbf{u}_1, \mathbf{u}_1\rangle & \langle \mathbf{u}_1, \mathbf{u}_2\rangle & \cdots & \langle \mathbf{u}_1, \mathbf{u}_k\rangle \\ \langle \mathbf{u}_2, \mathbf{u}_1\rangle & \langle \mathbf{u}_2, \mathbf{u}_2\rangle & \cdots & \langle \mathbf{u}_2, \mathbf{u}_k\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle \mathbf{u}_k, \mathbf{u}_1\rangle & \langle \mathbf{u}_k, \mathbf{u}_2\rangle & \cdots & \langle \mathbf{u}_k, \mathbf{u}_k\rangle \end{pmatrix}$$

řádu k nazýváme *Gramova matice* posloupnosti vektorů $(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k)$.

(50) Nechť A je reálná nebo komplexní matice typu $n \times k$ a $\mathbf{v} \in \mathbb{R}^n$ (resp. $\mathbf{v} \in \mathbb{C}^n$). Pak vektor $A\mathbf{x}$ (kde $\mathbf{x} \in \mathbb{R}^k$ nebo $\mathbf{x} \in \mathbb{C}^k$) je ortogonální projekcí vektoru $\mathbf{v}$ na podprostor $\operatorname{Im} A$ právě tehdy, když

$$A^*A\mathbf{x} = A^*\mathbf{v} \ .$$

(51) Gramova matice je rovná A^*A, kde

$$A = ([\mathbf{u}_1]_B|[\mathbf{u}_2]_B|\cdots|[\mathbf{u}_k]_B)$$

a B je ortonormální báze nějakého konečně generovaného prostoru obsahujícího vektory $\mathbf{u}_1, \dots, \mathbf{u}_k$.

(52) Pro Gramovu matici $B = (\langle \mathbf{u}_i, \mathbf{u}_j\rangle)$ posloupnosti prvků $(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k)$ vektorového prostoru $\mathbf{V}$ se skalárním součinem $\langle\,,\rangle$ platí
 (a) matice B je regulární právě když je posloupnost $(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k)$ lineárně nezávislá,

(b) matice B je hermitovská (symetrická v reálném případě),
(c) je-li posloupnost $(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k)$ lineárně nezávislá, pak je B pozitivně definitní.

(53) Čtvercová komplexní (resp. reálná) matice řádu n se nazývá *unitární* (resp. *ortogonální*), pokud její sloupce tvoří ortonormální posloupnost vzhledem ke standardnímu skalárnímu součinu v $\mathbb{C}^n$ (resp. $\mathbb{R}^n$).

(54) Je-li Q komplexní (resp. reálná) čtvercová matice řádu n, pak jsou následující tvrzení ekvivalentní.
(a) Q je unitární (resp. ortogonální),
(b) $Q^*Q = I_n$,
(c) Q^* je unitární (resp. ortogonální),
(d) $QQ^* = I_n$,
(e) Q^T je unitární (resp. ortogonální), ekvivalentně, řádky matice Q tvoří ortonormální posloupnost,
(f) zobrazení f_Q zachovává standardní skalární součin, tj. pro libovolné $\mathbf{u}, \mathbf{v} \in \mathbb{C}^n$ (resp. $\mathbb{R}^n$) platí $Q\mathbf{u} \cdot Q\mathbf{v} = \mathbf{u} \cdot \mathbf{v}$.

Speciálně, každá unitární (ortogonální) matice je regulární a platí $Q^{-1} = Q^*$.

(55) Součin dvou unitárních (resp. ortogonálních) matic téhož řádu je opět unitární (resp. ortogonální) matice.

(56) Je-li A regulární (reálná nebo komplexní) matice řádu n a $A = Q_1R_1 = Q_2R_2$ jsou dva QR-rozklady matice A, pak platí $Q_1 = Q_2$ a $R_1 = R_2$.

(57) Nechť $\mathbf{V}$ a $\mathbf{W}$ jsou vektorové prostory nad $\mathbb{C}$ (resp. $\mathbb{R}$) se skalárními součiny $\langle\,,\rangle_V, \langle\,,\rangle_W$. Lineární zobrazení $f : \mathbf{V} \to \mathbf{W}$ nazýváme *unitární* (resp. *ortogonální*), pokud zachovává skalární součin, tj. pro libovolné $\mathbf{u}, \mathbf{v} \in V$ platí

$$\langle f(\mathbf{u}), f(\mathbf{v})\rangle_W = \langle \mathbf{u}, \mathbf{v}\rangle_V \quad .$$

(58) Nechť $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení mezi komplexními (resp. reálnými) vektorovými prostory $\mathbf{V}$, $\mathbf{W}$ se skalárními součiny $\langle\,,\rangle_V, \langle\,,\rangle_W$. Pak následující tvrzení jsou ekvivalentní.
(a) f je unitární (resp. f je ortogonální),
(b) f zachovává normu, tj. pro libovolný vektor $\mathbf{v} \in V$ platí $\|f(\mathbf{v})\|_W = \|\mathbf{v}\|_V$,
(c) f zachovává ortonormalitu, tj. je-li $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ ortonormální posloupnost ve $\mathbf{V}$, pak $(f(\mathbf{v}_1), \ldots, f(\mathbf{v}_n))$ je ortonormální posloupnost v $\mathbf{W}$.
(d) f zobrazuje jednotkové vektory ve $\mathbf{V}$ na jednotkové vektory v $\mathbf{W}$.

Speciálně, každé unitární (ortogonální) zobrazení je prosté.

(59) Nechť $\mathbf{V}$ a $\mathbf{W}$ jsou konečně generované vektorové prostory nad $\mathbb{C}$ (resp. $\mathbb{R}$) se skalárními součiny $\langle\,,\rangle_V, \langle\,,\rangle_W$, $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ a C jsou pořadě ortonormální báze prostorů $\mathbf{V}$ a $\mathbf{W}$, a $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení. Pak f je unitární (resp. ortogonální) právě tehdy, když $[f]_C^B$ má ortonormální posloupnost sloupců vzhledem ke standardnímu skalárnímu součinu.

Speciálně, je-li $\mathbf{V} = \mathbf{W}$, pak f je unitární (resp. ortogonální) právě když $[f]_C^B$ je unitární (resp. ortogonální).

(60) Nechť $A\mathbf{x} = \mathbf{b}$ soustava lineárních rovnic s reálnými (nebo komplexními) koeficienty. Každý vektor $\widehat{\mathbf{x}} \in \mathbb{R}^n$ (nebo $\widehat{\mathbf{x}} \in \mathbb{C}^n$), který minimalizuje eukleidovskou normu $\|\mathbf{b} - A\mathbf{x}\|$, se na nazývá *přibližné řešení* (nebo *aproximace řešení*) *soustavy* $A\mathbf{x} = \mathbf{b}$ *metodou nejmenších čtverců.*

(61) Je-li A matice typu $m \times n$ nad $\mathbb{R}$ nebo $\mathbb{C}$ a $\mathbf{b} \in \mathbb{R}^m$ (resp. $\mathbb{C}^m$), pak množina všech přibližných řešení soustavy $A\mathbf{x} = \mathbf{b}$ metodou nejmenších

čtverců je rovna množině všech (přesných) řešení soustavy

$$A^* A\widehat{\mathbf{x}} = A^*\mathbf{b} \ .$$

(62) Lineární regrese je přibližné řešení soustavy lineárních rovnic

$$a_1 x_i = b, \quad i = 1, 2, \ldots, n$$

s neznámými a, b metodou nejmenších čtverců. Používá se k prokládání přímky množinou bodů (x_i, y_i), $i = 1, 2, \ldots, n$, získanou obvykle nějakým měřením.

(63) Nechť $A\mathbf{x} = \mathbf{b}$ je soustava lineárních rovnic nad $\mathbb{R}$ nebo nad $\mathbb{C}$, která má alespoň jedno řešení $\mathbf{u}$. Pak existuje právě jedno řešení $\mathbf{x}_{ln}$ soustavy $A\mathbf{x} = \mathbf{b}$, které minimalizuje eukleidovskou normu $\|\mathbf{x}\|$. Vektor $\mathbf{x}_{ln}$ je roven ortogonální projekci vektoru $\mathbf{u}$ na podprostor $\operatorname{Im} A^*$ a platí $\mathbf{x}_{ln} = A^*\mathbf{z}$, kde $\mathbf{z}$ je libovolné řešení soustavy $AA^*\mathbf{z} = \mathbf{b}$.

KAPITOLA 9

Vlastní čísla a vlastní vektory

Cíl. *Vlastní čísla a vlastní vektory jsou základní nástroj pro zkoumání lineárních operátorů. Poznatky o vlastních číslech a vektorech použijeme ke studiu rozsáhlé třídy problémů shrnutých pod společný název lineární dynamické systémy.*

V této kapitole pronikneme hlouběji do struktury matic a lineárních operátorů, hlavně na konečně generovaných prostorech. Vyvinutá teorie nám umožní mimo jiné počítat iterace daného operátoru $f : \mathbf{V} \to \mathbf{V}$, tj. výrazy tvaru

$$f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n\times} \ .$$

Spočítat n-tou mocninu lineárního zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^n$ určeného čtvercovou maticí řádu n nad $\mathbf{T}$ znamená spočítat mocninu A^n, protože $(f_A)^n = f_{A^n}$. V řeči matic se tedy naučíme počítat n-tou mocninu čtvercové matice A.

9.1. Lineární dynamické systémy

9.1.1. Diskrétní lineární dynamické systémy. Začneme několika motivujícími příklady.

Příklad 9.1. Jednoduchým příkladem lineárního dynamického systému je úročení vkladu na účtu. Na účet s úrokem 1%, který banka připisuje jednou za rok, vložíme počáteční vklad $x_0 = 1000$ Kč. Po roce budeme mít na účtě částku

$$x_1 = 1000 + 10 = (1 + 0{,}01)1000 = (1 + 0,01)x_0 \ .$$

Po dvou letech to bude částka

$$x_2 = (1 + 0{,}01)x_1 = (1 + 0{,}01)^2 x_0$$

a po k letech budeme mít

$$x_k = (1 + 0{,}01)x_{k-1} = (1 + 0{,}01)^2 x_{k-2} = \cdots = (1 + 0{,}01)^k x_0 \ .$$

Jiná banka nám nabídne účet, na kterém každé čtvrtletí připíše úrok 0,25%. U takové banky budeme mít při počátečním vkladu y_0 po jednom čtvrtletí částku

$$y_1 = 1000 + 2{,}50 = (1 + 0{,}0025)y_0 \ ,$$

po jednom roce to bude $y_4 = (1 + 0{,}0025)^4 y_0$ a po k čtvrtletích to bude $y_k = (1 + 0{,}0025)^k y_0$.

Vybereme si ještě jinou banku, která každý den připisuje úrok (1/365)%. Při počátečním vkladu z_0 budeme mít po roce částku

$$z_{365} = \left(1 + \frac{0{,}01}{365}\right)^{365} z_0 \ .$$

V rámci konkurenčního boje se banky začnou předhánět v tom, kolikrát za rok úrok připisují. U banky, která připisuje úrok $(1/n)\%$ n-krát ročně, bude po roce na účtu částka

$$z_n = \left(1 + \frac{0{,}01}{n}\right)^n z_0 \ .$$

Přechodem k limitě pro $n \to \infty$ nakonec konkurenční boj vyhraje banka **FURT** s reklamním sloganem *„V bance FURT úročíme furt“*, a poté zkrachuje. V jakémkoliv čase t, přičemž jednotkou času je 1 rok, u ní bude při počátečním vkladu z_0 na účtě částka

$$z(t) = \lim_{n\to\infty} \left(1 + \frac{0{,}01t}{n}\right)^n z(0) = e^{0{,}01t} z_0 \ .$$

Po jednom roce tedy na účtě bude $e^{0{,}01} z_0$ korun. ▲

Příklad 9.2. Fibonacciho posloupnost je příkladem *rekurentní posloupnosti* $(a_k)_{k=0}^{\infty}$ definované *rekurentním vztahem*

$$a_{k+2} = a_{k+1} + a_k \quad \text{pro každé } k = 0, 1, 2, \dots \ .$$

Celou posloupnost jednoznačně určují první dva prvky a_0 a a_1. Fibonacciho posloupnost dostaneme volbou $a_0 = 0$ a $a_1 = 1$.

V příkladu 4.42 jsme nahlédli, že platí

$$\begin{pmatrix} a_{k+1} \\ a_{k+2} \end{pmatrix} = C \begin{pmatrix} a_k \\ a_{k+1} \end{pmatrix}, \text{ kde } C = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \ .$$

V terminologii lineárních dynamických systémů nazýváme vektor $\mathbf{x}_k = (a_k, a_{k+1})^T$ *stav systému*, v tomto případě posloupnosti, v čase k. *Vývoj systému* je pak určen vztahem

$$\mathbf{x}_{k+1} = C\,\mathbf{x}_k = f_C(\mathbf{x}_k) \quad \text{pro každé } k \in \mathbb{N}$$

a *počáteční podmínkou* $\mathbf{x}_0 = (a_0, a_1)^T$.

Stav $\mathbf{x}_k$ v čase k se potom rovná

$$\mathbf{x}_k = \begin{pmatrix} a_k \\ a_{k+1} \end{pmatrix} = C^k \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = C^k\,\mathbf{x}_0 = f_C^k(\mathbf{x}_0) \ .$$

K určení k-tého členu posloupnosti nám tedy stačí umět vypočítat k-tou mocninu matice C (nebo operátoru f_C) pro libovolné $k \in \mathbb{N}$. ▲

Jak běžné připisování úroků za daný časový interval tak lineární rekurentní posloupnosti jsou příklady *diskrétních lineárních dynamických systémů*. Tento systém je zadán lineárním zobrazením $f : \mathbf{V} \to \mathbf{V}$ na vektorovém prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ a *počátečním stavem* $\mathbf{x}_0 \in \mathbf{V}$. *Vývoj* tohoto dynamického systému je dán předpisem

$$\mathbf{x}_{k+1} = f(\mathbf{x}_k) \quad \text{pro každé } k = 0, 1, 2, \dots \ .$$

To znamená, že např. $\mathbf{x}_2 = f(\mathbf{x}_1) = f(f(\mathbf{x}_0)) = f^2(\mathbf{x}_0)$. Jednoduchou indukcí podle k ověříme, že pro každé $k \geq 0$ platí

$$\mathbf{x}_k = f^k(\mathbf{x}_0) \ ,$$

kde pro $k = 0$ definujeme $f^0 = \mathrm{id}_V$.

Je-li vektorový prostor $\mathbf{V} = \mathbf{T}^n$ a A matice řádu n nad $\mathbf{T}$, pak lineární zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^n$ určené maticí A definuje diskrétní lineární systém předpisem

$$\mathbf{x}_{k+1} = f_A(\mathbf{x}_k) = A\,\mathbf{x}_k \quad \text{pro každé } k = 0, 1, 2, \dots \ .$$

Pro každé $k \geq 0$ pak platí

$$\mathbf{x}_k = f_A^k(\mathbf{x}_0) = A^k \mathbf{x}_0 \ ,$$

kde A^0 definujeme jako jednotkovou matici.

Zkoumáme-li nějaký diskrétní lineární dynamický systém, zajímá nás průběh posloupnosti stavů $\mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_2, \dots$ v závislosti na počátečním stavu $\mathbf{x}_0$. Nejsnazší to je, pokud se nám podaří najít explicitní vzorec pro k-tý prvek posloupnosti. Ale i bez explicitního vyjádření stavu $\mathbf{x}_k$ si můžeme klást otázky, jaké je limitní chování posloupnosti $(\mathbf{x}_k)_{k=0}^{\infty}$ pro $k \to \infty$, konverguje-li k nějakému limitnímu stavu $\mathbf{x}_\infty$, pokud ano, jak rychle k němu konverguje, atd. Pro různé počáteční stavy může být limitní chování různé. Jedním počátečním stavem není třeba se zabývat. Pokud je $\mathbf{x}_0 = \mathbf{o}$, pak $\mathbf{x}_k = \mathbf{o}$ pro každé k (důsledek linearity operátoru f).

Vývoj diskrétního lineárního dynamického systému v dimenzi 1, tj. v případě, kdy má stavový prostor $\mathbf{V}$ dimenzi 1, je průhledný. V prostoru $\mathbf{V}$ zvolíme jakýkoliv nenulový prvek $\mathbf{u}$ a jednotlivé stavy $\mathbf{x}_k$ budeme vyjadřovat pomocí jejich souřadnic vzhledem k bázi $B = (\mathbf{u})$ ve $\mathbf{V}$, tj. pomocí koeficientu $x_k \in \mathbf{T}$ ve vyjádření $\mathbf{x}_k = x_k\mathbf{u}$. Pro lineární operátor $f : \mathbf{V} \to \mathbf{V}$ daný předpisem $f(\mathbf{u}) = a\,\mathbf{u}$ dostaneme

$$\mathbf{x}_k = f^k(\mathbf{x}_0) = f^k(x_0\mathbf{u}) = x_0\, f^k(\mathbf{u}) = x_0\, a^k\mathbf{u} \quad \text{pro každé } k = 0, 1, 2, \dots \ .$$

Pomocí souřadnic vzhledem k bázi $B = (\mathbf{u})$ vyjádříme $\mathbf{x}_k = x_k\mathbf{u}$ a dostaneme rovnost

$$x_k = a^k x_0 \quad \text{pro každé } k = 0, 1, 2, \dots \ .$$

Jde tedy o geometrickou posloupnost.

Její limitní chování závisí na tom, v jakém tělese $\mathbf{T}$ počítáme. Rozebereme si jej v případě tělesa reálných čísel. V tom případě

- je-li $|a| < 1$, posloupnost $(x_k)_{k=0}^{\infty}$ konverguje k 0 pro jakýkoliv počáteční stav x_0.
- je-li $a = 1$, je posloupnost $(x_k)_{k=0}^{\infty}$ konstantní rovná x_0.
- je-li $a = -1$, posloupnost $(x_k)_{k=0}^{\infty}$ osciluje mezi hodnotami $\pm x_0$.
- je-li $a > 1$, posloupnost se blíží k $\pm\infty$ v závislosti na znaménku x_0.
- je-li $a < -1$, posloupnost $(|x_k|)_{k=0}^{\infty}$ se blíží $+\infty$ a znaménka čísel x_k se střídají.

Jako cvičení si můžete udělat podobný rozbor v případě tělesa $\mathbb{C}$. Nejzajímavější je případ $|a| = 1$. Posloupnost $(x_k)_{k=0}^{\infty}$ může být v takovém případě konstantní, periodicky nabývat konečně mnoha hodnot a nebo můžou být její prvky po dvou různé, všechny ale leží na kružnici o poloměru $|x_0|$.

9.1.2. Spojité lineární dynamické systémy. U těchto systémů sledujeme vývoj stavu „spojitě“, nikoliv po diskrétních časových intervalech. K popisu spojitých procesů je zásadní pojem derivace reálné funkce f reálné proměnné. Připomeňme význam derivace v případě, že $f(t)$ udává hodnotu nějaké veličiny v čase t, například polohu bodu na přímce, množství nějaké látky, a podobně. Derivace funkce f v čase t, kterou budeme značit $f'(t)$, udává okamžitou rychlost změny hodnoty dané veličiny v čase t. Tedy $f'(11) = 2$ znamená, že okamžitá rychlost změny je 2, tj. pokud by rychlost změny veličiny zůstala od času $t = 11$ konstantní, pak by byla hodnota veličiny v čase $t = 12$ rovná $f(11) + 2$, v čase $t = 11{,}03$ rovná $f(11) + 2 \cdot 0{,}03$ a obecně v čase $t = 11 + \delta$ rovná $f(11) + 2\delta$. Například je-li $f(t)$ poloha bodu pohybujícího se po přímce v čase t, pak je $f'(t)$ jeho okamžitá orientovaná rychlost v čase t; je-li $f(t)$ rychlost bodu v čase t, pak je $f'(t)$ jeho okamžité orientované zrychlení.

Uvedeme opět několik motivujících příkladů, které vedou na spojité lineární dynamické systémy.

Příklad 9.3. Spojité úročení vkladů v bance FURT z příkladu 9.1 je navržené tak, že částka $z(t)$ na účtu v čase t by se za rok zvýšila o $0{,}01z(t)$, pokud by v průběhu roku zůstala rychlost růstu částky konstantní. Jinými slovy, manažerky banky se rozhodly, že částka na účtu se bude řídit vztahem

$$z'(t) = 0{,}01\, z(t) \ .$$

Toto je jednodimenzionální příklad spojitého lineárního dynamického systému.

V příkladu 9.1 jsme určili hodnotu $z(t)$ v závislosti na počátečním stavu $z(0)$ limitním výpočtem. Takto lze řešit všechny spojité lineární dynamické systémy, ale my budeme spíše volit přímý postup. V tomto případě stačí použít tvrzení 9.7. ▲

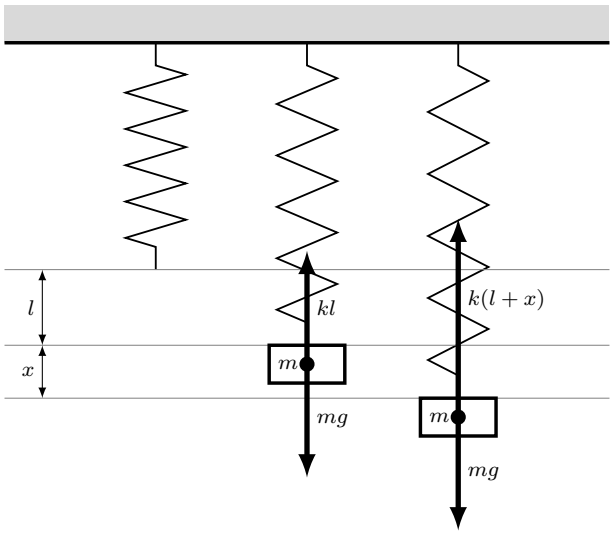
PŘÍKLAD 9.4. Míra radioaktivity jaderného materiálu se měří pomocí *rozpadové konstanty* $k \in (0,1)$, která udává pravděpodobnost, s jakou se jádro rozpadne během jedné vteřiny. Čím větší rozpadová konstanta, tím vyšší pravděpodobnost a tím vyšší radioaktivita materiálu.

Označíme $x(t)$ střední hodnotu počtu radioaktivních jader v čase t (pojem střední hodnoty chápejte intuitivně jako průměrný počet po provedení velkého počtu pokusů). Máme-li $x(t)$ jader a rozpad by probíhal konstantní rychlostí, pak za 1 vteřinu bude o $kx(t)$ jader méně. To znamená, že funkce x splňuje

$$x'(t) = -k\,x(t) \quad \text{pro každé } t \in \mathbb{R} \ .$$

Opět dostáváme jednoduchý spojitý lineární dynamický systém. ▲

PŘÍKLAD 9.5. Na pružinu s koeficientem pružnosti k zavěsíme závaží o hmotnosti m. Pružina se protáhne o délku l. Jak l spočítáme?



V rovnovážném stavu se vyrovnává gravitační síla mg, která táhne závaží směrem dolů, se silou pružiny, která táhne závaží směrem nahoru. Tato síla je podle Hookeova zákona přímo úměrná prodloužení pružiny a koeficient přímé úměrnosti je koeficient pružnosti k. Síla působící směrem vzhůru má proto velikost kl. V rovnovážném stavu pak platí rovnost

$$mg = kl \ ,$$

ze které plyne velikost prodloužení $l = mg/k$.

Když závaží vychýlíme z rovnovážného stavu směrem dolů o $x_1(0) = b$ a pustíme je, začne se pohybovat. Stav závaží v čase t zapíšeme pomocí dvojice čísel $(x_1(t), x_2(t))^T$, kde $x_1(t)$ je odchylka od rovnovážného stavu v čase t a $x_2(t)$ je okamžitá orientovaná rychlost závaží v čase t (řekněme, že směr dolů je kladný).

Směrem dolů na závaží působí konstantní gravitační síla mg, směrem vzhůru síla pružnosti $k(l + x_1(t))$. Celková síla působící na závaží v čase t směrem dolů je potom

$$F(t) = mg - k(l + x_1(t)) = (mg - kl) - kx_1(t) = -kx_1(t) \ ,$$

neboť pro prodloužení l v rovnovážném stavu platí rovnost $mg = kl$. Podle Newtonova zákona síla $F(t)$ uděluje závaží v čase t okamžité orientované zrychlení $a(t)$, které vypočteme ze vztahu $F(t) = a(t)\,m$, neboli

$$a(t) = \frac{F(t)}{m} = -\frac{k}{m}\,x_1(t) \ .$$

Okamžitá orientovaná rychlost je derivací polohy a okamžité orientované zrychlení je derivací orientované rychlosti, tj.

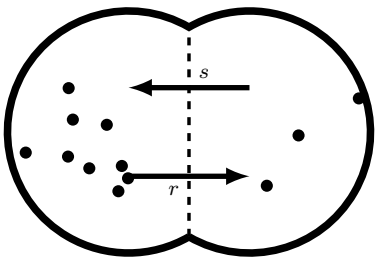
$$x_1'(t) = x_2(t), \quad x_2'(t) = a(t) = -\frac{k}{m}\,x_1(t) \ .$$

Označíme-li $\mathbf{x}(t) = (x_1(t), x_2(t))^T$ a $\mathbf{x}'(t) = (x_1'(t), x_2'(t))^T$ můžeme odvozené vztahy maticově napsat

$$\mathbf{x}'(t) = \begin{pmatrix} x_1'(t) \\ x_2'(t) \end{pmatrix} = \begin{pmatrix} x_2(t) \\ -\frac{k}{m}\, x_1(t) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -\frac{k}{m} & 0 \end{pmatrix} \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 1 \\ -\frac{k}{m} & 0 \end{pmatrix} \mathbf{x}(t)$$

Známe ještě počáteční podmínku $(x_1(0), x_2(0))^T = (b, 0)^T$. ▲

Příklad 9.6. Přes buněčnou blánu mezi dvěma buňkami se šíří nějaká substance, např. vápník, alkohol, vitamín C, apod. Na počátku v čase $t = 0$ je do jedné buňky injektováno jednotkové množství substance. Víme, že rychlost šíření substance přes buněčnou blánu z jedné buňky do druhé je přímo úměrná množství substance v buňce, ze které se substance šíří, koeficient rychlosti šíření z buňky 1 do buňky 2 je $r > 0$, a z buňky 2 do buňky 1 je koeficient rovný $s > 0$. Máme určit množství substance v obou buňkách v čase t.



Označíme si $x_1(t)$, resp. $x_2(t)$, množství substance v buňce 1, resp. 2, v čase t. Rychlost změny množství substance v buňce 1 je $sx_2(t)$ (šíření z buňky 2) minus $rx_1(t)$ (šíření do buňky 2). Podobně pro druhou buňku. Dostáváme rovnice

$$x_1'(t) = -rx_1(t) + sx_2(t) \ ,$$
$$x_2'(t) = rx_1(t) - sx_2(t) \ .$$

Označíme-li $\mathbf{x}(t) = (x_1(t), x_2(t))^T$ a $\mathbf{x}'(t) = (x_1'(t), x_2'(t))^T$, můžeme proces šíření substance mezi buňkami popsat jako spojitý lineární dynamický systém

$$\mathbf{x}'(t) = \begin{pmatrix} -r & s \\ r & -s \end{pmatrix} \mathbf{x}(t)$$

s počáteční podmínkou že $\mathbf{x}(0) = (1, 0)^T$. ▲

Nyní k spojitým lineárním dynamickým systémům obecně.

Stav spojitého dynamického systému v čase $t \in \mathbb{R}$ zapíšeme jako prvek $\mathbf{x}(t) \in \mathbf{V}$, kde $\mathbf{V}$ je nějaký vektorový prostor. V případě spojitých dynamických systémů budeme předpokládat, že $\mathbf{V}$ je aritmetický prostor nad $\mathbb{R}$ nebo nad $\mathbb{C}$. V případě, že $\mathbf{x}(t) \in \mathbb{R}^n$, můžeme stav systému v čase t zapsat jako

$$\mathbf{x}(t) = (x_1(t), x_2(t), \ldots, x_n(t))^T \ ,$$

tj. $\mathbf{x} = (x_1, \ldots, x_n)^T$ je uspořádaná n-tice reálných funkcí jedné reálné proměnné. *Derivací* stavového vektoru v čase t je vektor

$$\mathbf{x}'(t) = (x_1'(t), x_2'(t), \ldots, x'_n(t))^T \ .$$

Vývoj *spojitého lineární dynamického systému* nad $\mathbb{R}$ je definován rovností

$$\mathbf{x}'(t) = f(\mathbf{x}(t)) \quad \text{pro každé } t \in \mathbb{R} \ ,$$

kde $f : \mathbb{R}^n \to \mathbb{R}^n$ je lineární zobrazení, a *počátečním stavem* $\mathbf{x}(0) \in \mathbb{R}^n$. Protože každé lineární zobrazení $f : \mathbb{R}^n \to \mathbb{R}^n$ je tvaru f_A, kde $A = [f]_K^K$ je matice f vzhledem ke kanonickým bázím K a K, můžeme vývoj spojitého lineárního dynamického systému nad $\mathbb{R}$ zapsat také rovnicí

$$\mathbf{x}'(t) = A\,\mathbf{x}(t) \quad \text{pro každé } t \in \mathbb{R} \ ,$$

kde A je reálná matice řádu n.

Je-li $\mathbf{V} = \mathbb{C}^n$, můžeme každý stavový vektor $\mathbf{x}(t)$ zapsat jako

$$\mathbf{x}(t) = (x_1(t) + i\,y_1(t), x_2(t) + i\,y_2(t), \ldots, x_n(t) + i\,y_n(t))^T,$$

kde i je imaginární jednotka a funkce $x_j(t), y_j(t)$ jsou reálné funkce jedné reálné proměnné. Derivací stavového vektoru v čase t je vektor

$$\mathbf{x}'(t) = (x_1'(t) + i\,y_1'(t), x_2'(t) + i\,y_2'(t), \ldots, x_n'(t) + i\,y_n'(t))^T \ .$$

Vývoj *spojitého lineárního dynamického systému* nad $\mathbb{C}$ je definován rovností

$$\mathbf{x}'(t) = f(\mathbf{x}(t)) \quad \text{pro každé } t \in \mathbb{R} \ ,$$

kde $f : \mathbb{C}^n \to \mathbb{C}^n$ je lineární zobrazení a $\mathbf{x}(0) \in \mathbb{C}^n$ je počáteční stav. Také v případě komplexních skalárů můžeme pomocí komplexní matice $A = [f]_K^K$ systém zapsat jako

$$\mathbf{x}'(t) = A\,\mathbf{x}(t) \quad \text{pro každé } t \in \mathbb{R} \ .$$

V mnoha učebnicích bývá derivace stavového vektoru $\mathbf{x}(t)$ označována jako $\underline{\mathbf{x}}(t)$.

Poznamenejme ještě, že obvyklý název pro spojitý lineární dynamický systém

$$\mathbf{x}'(t) = A\mathbf{x}(t), \ \mathbf{x}(0) = \mathbf{b}$$

definovaný maticí A řádu n nad tělesem $\mathbb{R}$ (nebo $\mathbb{C}$) a počátečním stavem $\mathbf{b} \in \mathbb{R}^n$ (nebo $\mathbb{C}^n$), je *soustava lineárních diferenciálních rovnic s konstantními koeficienty* a s *počáteční podmínkou* $\mathbf{x}(0) = \mathbf{b}$.

9.1.3. Vývoj spojitého lineárního dynamického systému v dimenzi 1. V případě reálného spojitého lineárního dynamického systému v dimenzi 1 hledáme reálnou funkci f, která pro každé reálné číslo t splňuje rovnici

$$f'(t) = \lambda\, f(t) \ ,$$

kde λ je pevně zvolené reálné číslo, a která splňuje počáteční podmínku $f(0) = s$.

Jednu takovou funkci lze uhádnout (nebo na ní lze přijít jako v příkladu 9.1):

$$f(t) = s\, e^{\lambda t}, \quad t \in \mathbb{R} \ .$$

Je-li $g : \mathbb{R} \to \mathbb{R}$ jakákoliv funkce splňující $g'(t) = \lambda\, g(t)$ a $g(0) = s$, spočteme

$$(g(t)e^{-\lambda t})' = g'(t)e^{-\lambda t} - g(t)\lambda e^{-\lambda t} = \lambda g(t)(e^{-\lambda t} - e^{-\lambda t}) = 0 \ ,$$

což znamená, že funkce $g(t)e^{-\lambda t}$ je konstantní na $\mathbb{R}$. Její hodnotu získáme volbou $t = 0$, tj.

$$g(0)e^{-\lambda 0} = g(0) = s \ .$$

Platí tedy $g(t)e^{-\lambda t} = s$, neboli $g(t) = s\, e^{\lambda t}$. Dokázali jsme tak následující tvrzení.

Tvrzení 9.7. *Je-li λ reálné číslo, pak existuje právě jedna funkce $f : \mathbb{R} \to \mathbb{R}$ splňující podmínky $f'(t) = \lambda\, f(t)$ pro každé $t \in \mathbb{R}$ a $f(0) = s$:*

$$f(t) = s\, e^{\lambda t} \ .$$

Příklad 9.8. Využijeme právě nalezeného průběhu reálného spojitého lineárního dynamického systému v dimenzi 1 k porovnání rozpadové konstanty $k > 0$ radioaktivní látky s jinou běžně používanou mírou radioaktivity, a to *poločasem rozpadu* T. Ten je definovaný jako doba, za kterou se množství radioaktivních jader průměrně sníží na polovinu. Vývoj střední hodnoty počtu radioktivních jader $f(t)$ v čase t je dán rovnicí $f'(t) = -k\, f(t)$ a počátečním stavem $f(0) = s$, viz příklad 9.4. Podle předchozího tvrzení tedy platí $f(t) = s\, e^{-kt}$ pro každé t. Pro poločas rozpadu T potom platí $f(T) = s/2$, neboli

$$s\, e^{-kT} = s/2 \ ,$$

což po zkrácení s a přirozeném logaritmování vede na rovnost

$$k\,T = \ln 2 \ .$$

▲

Reálný spojitý lineární dynamický systém $f'(t) = \lambda f(t)$ s počáteční podmínkou $f(0) = s \neq 0$ se může vyvíjet v čase třemi různými způsoby v závislosti na hodnotě λ:

- je-li $\lambda < 0$, platí $\lim_{t\to\infty} f(t) = 0$,
- je-li $\lambda = 0$, platí $f(t) = s$ pro každé $t \in \mathbb{R}$,
- je-li $\lambda > 0$, platí $\lim_{t\to\infty} f(t) = \pm\infty$ v závislosti na znaménku s.

Na závěr úvodní motivační části budeme diskutovat řešení komplexního spojitého dynamického systému v dimenzi 1. Při něm hledáme pro komplexní číslo $\lambda = a + bi$ komplexní funkci $z(t) = f(t) + ig(t)$ reálné proměnné splňující podmínku

$$z'(t) = \lambda z(t) \quad \text{pro každé} \quad t \in \mathbb{R}$$

spolu s počáteční podmínkou $z(0) = s = c + di \neq 0$. Řešení vyjde stejně jako v reálném případě

$$z(t) = se^{\lambda t} \ ,$$

akorát teď jsou s a λt komplexní čísla. Podle Eulerovy formule z části 1.4.9 platí

$$z(t) = se^{(a+bi)t} = se^{at}e^{ibt} = se^{at}(\cos(bt) + i\sin(bt)) \ .$$

Absolutní hodnota čísla $z(t)$ je rovná

$$|z(t)| = |s||e^{at}||\cos(bt) + i\sin(bt)| = |s| \cdot |e^{at}|$$

a jeho argument je

$$\arg(z(t)) = \arg(s) + bt \ .$$

Z toho vidíme, že pro absolutní hodnotu mohou nastat následující možnosti.

- $|z(t)| \to \infty$ v případě, že $a = \operatorname{Re}\lambda > 0$,
- $|z(t)| = |s|$ pro každé $t \in \mathbb{R}$, pokud $a = \operatorname{Re}\lambda = 0$,
- $|z(t)| \to 0$, pokud $a = \operatorname{Re}\lambda < 0$.

Pro $b = \operatorname{Im}\lambda \neq 0$ bod $z(t)$ „krouží“ kolem počátku s frekvencí úměrnou b – jeden oběh trvá $2\pi/b$. V případě $b = 0$ se bod pohybuje po přímce v Gaussově rovině.

9.2. Vlastní čísla a vlastní vektory

9.2.1. Definice vlastních čísel a vektorů. V dimenzi 1 nad $\mathbb{R}$ nebo $\mathbb{C}$ umíme předpovědět vývoj jak diskrétních, tak spojitých lineárních dynamických systémů pro jakýkoliv počáteční stav. Podobným způsobem umíme předpovědět vývoj i v dimenzi větší než 1 aspoň pro některé počáteční stavy.

Příklad 9.9. Uvažujme lineární operátor f_A na $\mathbb{R}^2$ určený maticí

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

a diskrétní dynamický systém

$$\mathbf{x}_{k+1} = f_A(\mathbf{x}_k) = A\,\mathbf{x}_k \ .$$

Zvolíme-li počáteční stav $\mathbf{x}_0 = (1,1)^T$, dostáváme

$$\mathbf{x}_1 = f_A\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = 3\begin{pmatrix} 1 \\ 1 \end{pmatrix} = 3\mathbf{x}_0 \ .$$

Dále

$$\mathbf{x}_2 = f_A(\mathbf{x}_1) = f_A(3\mathbf{x}_0) = 3\,f_A(\mathbf{x}_0) = 3^2\mathbf{x}_0$$

a podobně

$$\mathbf{x}_k = f_A^k(\mathbf{x}_0) = 3^k\mathbf{x}_0 \ .$$

Formálně bychom poslední vztah dokázali indukcí podle k.

▲

Řešení příkladu pro počáteční vektor $\mathbf{x}_0 = (1,1)^T$ nám umožnila skutečnost, že $f(\mathbf{x}_0)$ je skalárním násobkem vektoru $\mathbf{x}_0$. To vede k velmi důležité definici vlastních čísel a vektorů.

Definice 9.10. Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na vektorovém prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$, pak skalár $\lambda \in T$ nazýváme *vlastní číslo* operátoru f, pokud existuje nenulový vektor $\mathbf{x} \in V$, pro který platí

$$f(\mathbf{x}) = \lambda\mathbf{x} \ .$$

Je-li λ vlastní číslo operátoru f, pak libovolný prvek $\mathbf{x} \in V$, pro který platí $f(\mathbf{x}) = \lambda\mathbf{x}$, nazýváme *vlastní vektor* operátoru f *příslušný vlastnímu číslu* λ.

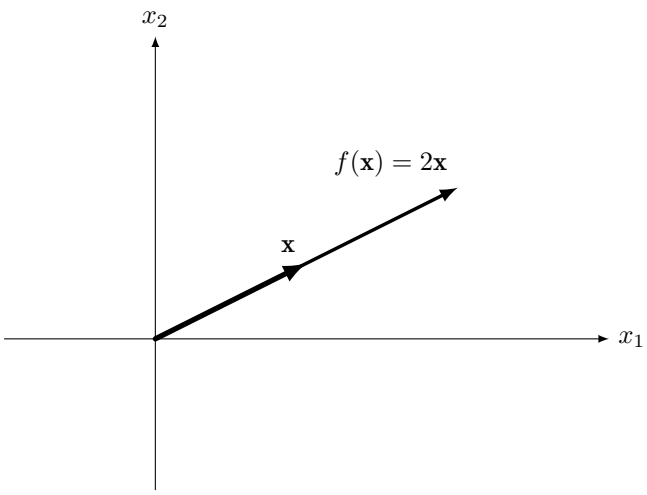
Vlastní čísla a vektory pro čtvercovou matici řádu n nad $\mathbf{T}$ definujeme jako vlastní čísla a vektory příslušného operátoru $f_A : \mathbf{T}^n \to \mathbf{T}^n$. Podobně tomu bude i pro další pojmy v této kapitole. Přeložíme si poslední definici pro případ matic.

Definice 9.11. Je-li A čtvercová matice řádu n nad tělesem $\mathbf{T}$, pak skalár $\lambda \in \mathbf{T}$ nazýváme *vlastní číslo* matice A, pokud existuje nenulový vektor $\mathbf{x} \in T^n$ takový, že

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

Je-li λ vlastní číslo matice A, pak libovolný vektor $\mathbf{x} \in T^n$, pro který platí $A\mathbf{x} = \lambda\mathbf{x}$, nazýváme *vlastní vektor* matice A *příslušný vlastnímu číslu* λ.

Je důležité uvědomit si geometrický význam definice vlastního čísla operátoru. Číslo $\lambda \in \mathbf{T}$ je vlastní číslo operátoru f, pokud existuje nenulový prvek $\mathbf{x} \in V$, který operátor f zobrazí na λ-násobek $\lambda\mathbf{x}$ prvku $\mathbf{x}$, tj. do směru vektoru $\mathbf{x}$. V případě prostoru nad reálnými čísly tak operátor f vektor $\mathbf{x}$ buď „natahuje“ (pokud $\lambda > 1$) nebo „zkracuje“ (pokud $0 < \lambda < 1$), případně navíc „obrací“ (pokud $\lambda < 0$).



Obrázek 9.1. f má vlastní číslo 2, $\mathbf{x}$ je vlastní vektor příslušný 2

Příklad 9.12. Na obrázku 9.2 je nakresleno zobrazení $f_A : \mathbb{R}^2 \to \mathbb{R}^2$ určené maticí

$$A = \begin{pmatrix} 1{,}035 & 0{,}09 \\ 0{,}135 & 0{,}99 \end{pmatrix}$$

tak, že pro některé body $\mathbf{x}$ je zobrazena šipka z $\mathbf{x}$ do $f_A(\mathbf{x}) = A\,\mathbf{x}$.

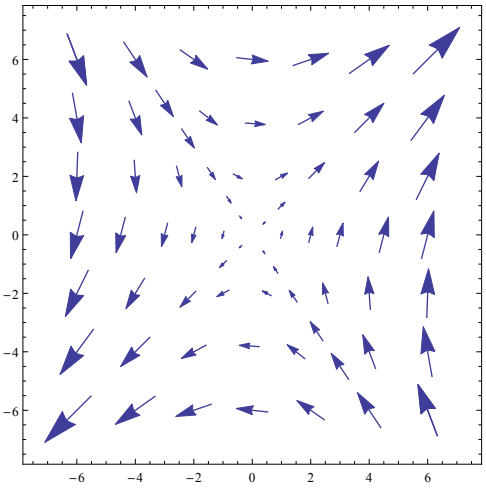
Zobrazení f_A (stejně jako matice A) má dvě vlastní čísla 1,125 a 0,9. Vlastní vektory příslušné 1,125 jsou vektory z LO $\left\{(1,1)^T\right\}$, což na obrázku vidíme tak, že tyto vektory zobrazení f_A natáhne na 1,125-násobek. Vlastní vektory příslušné 0,9 jsou vektory z LO $\left\{(-2,3)^T\right\}$, tyto vektory zobrazení zkrátí na f_A 0,9-násobek.

Na obrázku je také pěkně kvalitativně vidět chování posloupnosti $(f^k(\mathbf{x}_0))_{k=1}^{\infty}$ pro různé počáteční vektory. Výsledek v příští části odůvodníme algebraicky.

▲

Pro každé číslo $\lambda \in \mathbf{T}$ platí, že $f(\mathbf{o}) = \mathbf{o} = \lambda\mathbf{o}$. To ale neznamená, že λ je vlastní číslo f. K tomu, aby λ bylo vlastní číslo f, je nutná existence **nenulového** prvku $\mathbf{x}$, pro který platí $f(\mathbf{x}) = \lambda\mathbf{x}$. V takovém případě pak i nulový vektor je vlastním vektorem příslušným λ.

Číslo 0 může být vlastním číslem operátoru f, k tomu je ale nutná (a stačí) existence vektoru $\mathbf{x} \neq \mathbf{o}$, pro který platí $f(\mathbf{x}) = 0\mathbf{x} = \mathbf{o}$, což nastává právě když $\operatorname{Ker}(f) \neq \{\mathbf{o}\}$, neboli právě když operátor f není prostý (viz tvrzení 6.22). Zformulujeme učiněné pozorování.



Obrázek 9.2. Obrázek zobrazení f_A. Šipka vede z bodu $\mathbf{x}$ do bodu $f_A(\mathbf{x})$.

Pozorování 9.13. *Operátor $f : \mathbf{V} \to \mathbf{V}$ má vlastní číslo 0 právě tehdy, když f není prostý.*

Pro čtvercovou matici A je operátor f_A prostý právě tehdy, když je A regulární, takže maticová verze předchozího pozorování dává další kriterium regularity.

Pozorování 9.14. *Čtvercová matice A má vlastní číslo 0 právě tehdy, když A je singulární.*

Příklad 9.15. Identické zobrazení $f : \mathbf{V} \to \mathbf{V}$ má jediné vlastní číslo 1. Každý vektor z $\mathbf{V}$ je vlastním vektorem příslušným vlastnímu číslu 1. Speciálně, identická matice řádu n nad $\mathbf{T}$ má jediné vlastní číslo 1 a každý vektor z $\mathbf{T}^n$ je vlastním vektorem příslušným vlastnímu číslu 1. ▲

Příklad 9.16. Nulové zobrazení $0 : \mathbf{V} \to \mathbf{V}$ má jediné vlastní číslo 0. Každý vektor z $\mathbf{V}$ je vlastním vektorem příslušným vlastnímu číslu 0. Speciálně, nulová matice řádu n nad $\mathbf{T}$ má jediné vlastní číslo 0 a každý vektor z $\mathbf{T}^n$ je vlastním vektorem příslušným vlastnímu číslu 0. ▲

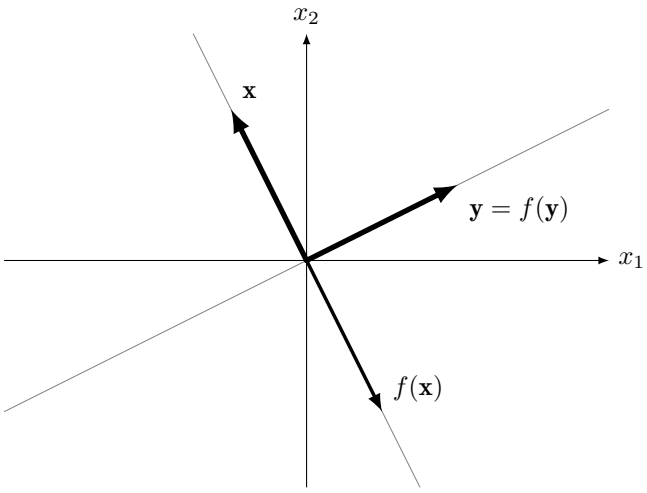
Příklad 9.17. V příkladu 9.9 jsme využili toho, že matice

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

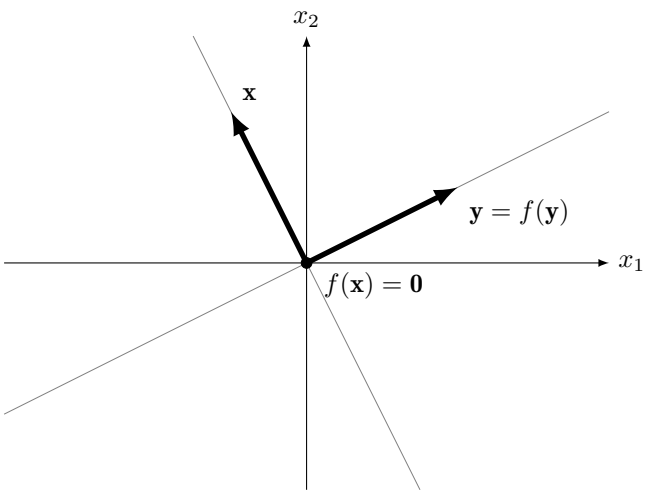
(a lineární operátor f_A) má vlastní číslo 3 a každý vektor z LO $\left\{(1,1)^T\right\}$ je vlastním vektorem matice A příslušným vlastnímu číslu 3. ▲

Příklad 9.18. Osová symetrie $f : \mathbb{R}^2 \to \mathbb{R}^2$ určená přímkou generovanou nenulovým vektorem $(a,b)^T$ má vlastní číslo 1, neboť všechny vektory na ose symetrie se zobrazí samy do sebe a jsou to tedy vlastní vektory příslušné vlastnímu číslu 1. Vektory na přímce kolmé na osu symetrie (generované např. vektorem $(-b,a)^T$) se zobrazují do vektorů opačných, jsou to tedy vlastní vektory příslušné vlastnímu číslu -1. Jiná vlastní čísla než -1 a 1 operátor f nemá, jak vidíme z geometrického náhledu. ▲

Příklad 9.19. Ortogonální projekce $g : \mathbb{R}^2 \to \mathbb{R}^2$ na přímku generovanou $(a,b)^T$ má také dvě vlastní čísla. Jedno je opět 1, protože vektory přímky, na kterou projektujeme, se zobrazují na sebe. Druhé vlastní číslo je 0, protože všechny vektory z přímky kolmé na přímku projekce se zobrazují do nulového vektoru. ▲



Obrázek 9.3. Vlastní čísla osové symetrie



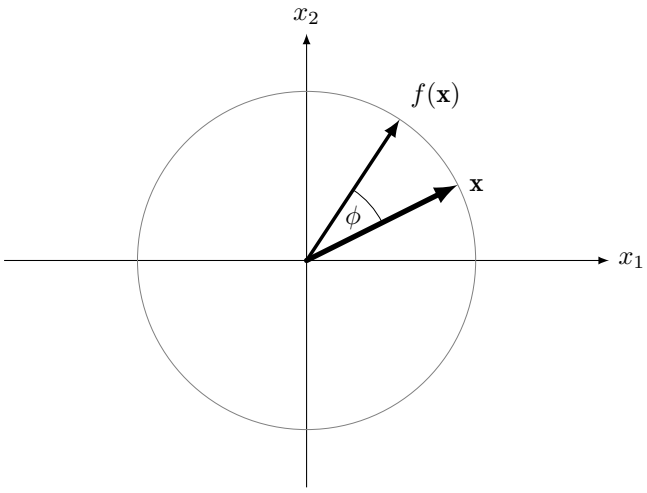
Obrázek 9.4. Vlastní čísla ortogonální projekce

Příklad 9.20. Rotace kolem počátku souřadnic o úhel φ nemá žádné reálné vlastní číslo, pokud φ není násobkem π, neboť v takovém případě se žádný nenulový vektor nezobrazí na svůj násobek. ▲

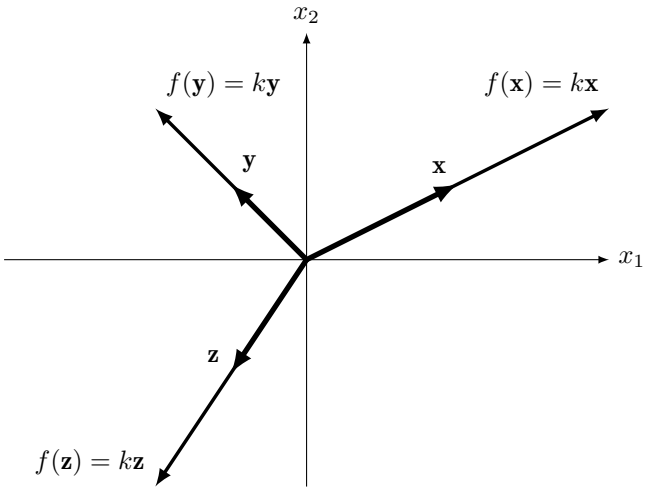
Příklad 9.21. Stejnolehlost v rovině $\mathbb{R}^2$ s koeficientem k, která zobrazuje každý vektor $\mathbf{x}$ do jeho k-násobku $k\mathbf{x}$, má jediné vlastní číslo k, každý vektor $\mathbb{R}^2$ je vlastním vektorem příslušným vlastnímu číslu k. Mezi stejnolehlosti řadíme i mezní případ $k = 0$ (konstantní zobrazení do nulového vektoru), $k = 1$, což je identické zobrazení, a také rotace o úhel 0, a $k = -1$ neboli středová symetrie (a také rotace o úhel π). ▲

V definici vlastních čísel a vektorů nepředpokládáme, že prostor $\mathbf{V}$ má konečnou dimenzi. Důležitým „nekonečnědimenzionálním“ příkladem je operátor derivace.

Příklad 9.22. Označíme D lineární operátor definovaný předpisem $D(f) = f'$ na prostoru $\mathbf{V}$ všech reálných funkcí reálné proměnné, které mají spojité derivace všech řádů.



Obrázek 9.5. Vlastní čísla rotace



Obrázek 9.6. Vlastní čísla stejnolehlosti

Reálné číslo λ je vlastním číslem operátoru D právě když existuje nenulová funkce $f(t) \in \mathbf{V}$, pro kterou platí $D(f) = \lambda f$, neboli

$$f'(t) = \lambda f(t) \quad \text{pro každé} \quad t \in \mathbb{R} \ .$$

V části 9.1.3 jsme ukázali, že pro každé $\lambda \in \mathbb{R}$ jsou všechny funkce splňující poslední rovnost tvaru $f(t) = s\, e^{\lambda t}$, kde s je libovolné reálné číslo – tvrzení 9.7.

Každé reálné číslo je tedy vlastním číslem operátoru D, vlastní vektory příslušné vlastnímu číslu jsou právě prvky LO $\{e^{\lambda t}\}$. ▲

9.2.2. Výpočet vlastních čísel a vlastních vektorů. Na příkladech jste si mohli všimnout, že množina vlastních vektorů příslušných vlastnímu číslu λ vždy tvořila podprostor. To není náhoda.

K důkazu použijeme obrat, který v této kapitole budeme často používat. Uvažujeme lineární operátor $f : \mathbf{V} \to \mathbf{V}$, vektor $\mathbf{x} \in V$ a skalár λ. Vztah $f(\mathbf{x}) = \lambda\mathbf{x}$ lze

ekvivalentně upravit

$$\begin{aligned} f(\mathbf{x}) &= \lambda\mathbf{x} \\ f(\mathbf{x}) &= (\lambda\,\mathrm{id}_V)(\mathbf{x}) \\ f(\mathbf{x}) - (\lambda\,\mathrm{id}_V)(\mathbf{x}) &= \mathbf{o} \\ (f - \lambda\,\mathrm{id}_V)(\mathbf{x}) &= \mathbf{o} \\ \mathbf{x} &\in \mathrm{Ker}\,(f - \lambda\,\mathrm{id}_V) \end{aligned}$$

Odtud plyne následující tvrzení.

Tvrzení 9.23. *Nechť f je lineární operátor na prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$. Pak $\lambda \in T$ je vlastním číslem operátoru f právě tehdy, když operátor $(f - \lambda\,\mathrm{id}_V)$ není prostý.*

Je-li λ vlastním číslem operátoru f, pak množina M_λ všech vlastních vektorů operátoru f příslušných vlastnímu číslu λ je podprostorem $\mathbf{V}$ a platí

$$M_\lambda = \mathrm{Ker}\,(f - \lambda\,\mathrm{id}_V)\ .$$

Důkaz. Podle předchozích úprav, $f(\mathbf{x}) = \lambda\mathbf{x}$ platí právě tehdy, když $\mathbf{x} \in \mathrm{Ker}\,(f - \lambda\,\mathrm{id}_V)$, takže nenulový vektor $\mathbf{x}$ splňující $f(\mathbf{x}) = \lambda\mathbf{x}$ existuje právě tehdy, když je $\mathrm{Ker}\,(f - \lambda\,\mathrm{id}_V)$ netriviální, tedy (viz tvrzení 6.22) právě tehdy, když $f - \lambda\,\mathrm{id}_V$ není prostý.

Druhá část tvrzení pak plyne ze stejného výpočtu a z toho, že jádro je vždy podprostorem (viz tvrzení 6.23). ▲

Explicitně zformulujeme také maticovou verzi. Odvození má v tomto případě podobu

$$\begin{aligned} A\mathbf{x} &= \lambda\mathbf{x} \\ A\mathbf{x} &= \lambda I_n\mathbf{x} \\ A\mathbf{x} - \lambda I_n\mathbf{x} &= \mathbf{o} \\ (A - \lambda I_n)(\mathbf{x}) &= \mathbf{o} \\ \mathbf{x} &\in \mathrm{Ker}\,(A - \lambda I_n) \end{aligned}$$

Tvrzení 9.24. *Je-li A čtvercová matice řádu n nad tělesem $\mathbf{T}$, pak $\lambda \in T$ je vlastním číslem matice A právě tehdy, když je matice $A - \lambda I_n$ singulární.*

Je-li λ vlastním číslem matice A, pak množina M_λ všech vlastních vektorů matice A příslušných vlastnímu číslu λ je podprostorem $\mathbf{T}^n$ a platí

$$M_\lambda = \mathrm{Ker}\,(A - \lambda I_n)\ .$$

Důkaz. Plyne opět z výpočtu před formulací tvrzení spolu s tím, že $\mathrm{Ker}\,(A - \lambda I_n)$ je netriviální právě tehdy, když $A - \lambda I_n$ je singulární (viz větu 4.82 charakterizující regulární matice). ▲

K výpočtu vlastních čísel matice A si uvědomíme, že matice $A - \lambda I_n$ je singulární právě tehdy, když je její determinant nulový.

Pozorování 9.25. *Je-li A čtvercová matice řádu n nad tělesem $\mathbf{T}$, pak $\lambda \in T$ je vlastním číslem matice A právě tehdy, když* $\det\,(A - \lambda I_n) = 0$.

Obecněji, k výpočtu vlastních čísel operátoru f na konečně generovaném prostoru $\mathbf{V}$ zvolíme bázi B prostoru $\mathbf{V}$. Pro každý skalár $\lambda \in T$ je vyjádření jádra operátoru $f - \lambda\,\mathrm{id}_V$ vzhledem k B podle tvrzení 6.23 a 6.34 rovno

$$[\mathrm{Ker}\,(f - \lambda\,\mathrm{id}_V)]_B = \mathrm{Ker}\,[f - \lambda\,\mathrm{id}_V]_B^B = \mathrm{Ker}\,([f]_B^B - \lambda[\mathrm{id}_V]_B^B) = \mathrm{Ker}\,([f]_B^B - \lambda I_n)\ .$$

Dostáváme obecnější verzi předchozího pozorování.

POZOROVÁNÍ 9.26. *Je-li f lineární operátor na konečně generovaném prostoru* $\mathbf{V}$ *dimenze n nad tělesem* $\mathbf{T}$ *a B je báze* $\mathbf{V}$*, pak $\lambda \in T$ je vlastním číslem operátoru f právě když je λ vlastní číslo matice $[f]_B^B$, což nastává právě když* $\det\left([f]_B^B - \lambda I_n\right) = 0$.

Pro lineární operátor f na konečně generovaném prostoru $\mathbf{V}$ s bází B budeme často používat jeho matici $[f]_B^B$ vzhledem k bázím B a B. Proto budeme někdy stručněji hovořit o matici f vzhledem k B.

DEFINICE 9.27. Nechť f je lineární operátor na konečně generovaném prostoru $\mathbf{V}$ a B je báze $\mathbf{V}$. Pak *maticí operátoru f vzhledem k B* rozumíme matici operátoru f vzhledem k bázím B a B.

PŘÍKLAD 9.28. Určíme vlastní čísla a vlastní vektory matice A (= operátoru f_A) z příkladu 9.9.

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

Vypočteme pro obecný skalár $\lambda \in \mathbb{R}$ determinant

$$\det(A - \lambda I_2) = \det \begin{pmatrix} 3-\lambda & 0 \\ 1 & 2-\lambda \end{pmatrix} = (3-\lambda)(2-\lambda) - 0 \cdot 1 = (3-\lambda)(2-\lambda) .$$

Podle pozorování 9.25 má matice A dvě vlastní čísla 2 a 3. Podle tvrzení 9.24 tvoří vlastní vektory příslušné vlastnímu číslu 2 podprostor

$$M_2 = \operatorname{Ker}(A - 2I_2) = \operatorname{Ker} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \operatorname{LO}\left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

a vlastní vektory příslušné vlastnímu číslu 3 tvoří podprostor

$$M_3 = \operatorname{Ker}(A - 3I_2) = \operatorname{Ker} \begin{pmatrix} 0 & 0 \\ 1 & -1 \end{pmatrix} = \operatorname{LO}\left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\} .$$

▲

PŘÍKLAD 9.29. Známe-li lineárně nezávislou dvojici vlastních vektorů matice A řádu 2, můžeme spočítat jakýkoliv stav $\mathbf{x}_k$ diskrétního dynamického systému

$$\mathbf{x}_{k+1} = A\,\mathbf{x}_k$$

určeného maticí A pro každý počáteční stav $\mathbf{x}_0 = (a, b)^T$. Ukážeme si jak na matici

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

z předchozího příkladu.

Tato matice má dvě vlastní čísla $2, 3$, k vlastnímu číslu 2 je příslušný vlastní vektor např. $\mathbf{u}_2 = (0, 1)^T$, k vlastnímu číslu 3 je vlastní vektor například $\mathbf{u}_3 = (1, 1)^T$. Posloupnost B=$(\mathbf{u}_2, \mathbf{u}_3)$ je zjevně lineárně nezávislá a tedy báze v $\mathbb{R}^2$.

Předvedeme elementární odvození vztahu pro $\mathbf{x}_k$, elegantnější pohled bude diskutován v části o diagonalizovatelných operátorech.

Protože $\mathbf{u}_2$ je vlastní vektor příslušný vlastnímu číslu 2, platí

$$A^k \mathbf{u}_2 = 2^k \mathbf{u}_2$$

a analogicky

$$A^k \mathbf{u}_3 = 3^k \mathbf{u}_3 .$$

Libovolný počáteční stav $\mathbf{x}_0 \in \mathbb{R}^2$ vyjádříme jako lineární kombinaci $\mathbf{x}_0 = a\mathbf{u}_2 + b\mathbf{u}_3$ vlastních vektorů matice A (tj. $(a, b)^T = [\mathbf{x}_0]_B$) a spočítáme

$$\begin{aligned} \mathbf{x}_k =& A^k \mathbf{x}_0 = A^k(a\mathbf{u}_2 + b\mathbf{u}_3) = a\,A^k\mathbf{u}_2 + b\,A^k\mathbf{u}_3 = a\,2^k\mathbf{u}_2 + b\,3^k\mathbf{u}_3 \\ =& a\,2^k \begin{pmatrix} 0 \\ 1 \end{pmatrix} + b\,3^k \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} b3^k \\ a2^k + b3^k \end{pmatrix} . \end{aligned}$$

Koeficienty a, b jsou souřadnice vektoru $\mathbf{x}_0$ vzhledem k bázi B, najdeme je jako řešení soustavy lineárních rovnic

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \mathbf{x}_0 \ .$$

▲

PŘÍKLAD 9.30. Vypočteme vlastní čísla a vektory ortogonální projekce v $\mathbb{R}^2$ na přímku určenou vektorem $\mathbf{v} = (1, 2)^T$ (výsledek předem známe z geometrického náhledu, viz příklad 9.19). Označme tento operátor f.

Jedna možnost je najít matici A operátoru f vzhledem ke kanonickým bázím. Pak $f = f_A$ a vlastní čísla a vektory f se vypočítají jako v příkladu 9.28 (jako vlastní čísla a vektory matice A). Ukážeme nejprve tento, méně efektivní, postup.

Obrazy vektorů kanonické báze (tedy jejich ortogonálních projekce na danou přímku) jsou

$$f(\mathbf{e}_1) = \frac{\mathbf{v}^T\mathbf{e}_1}{\|\mathbf{v}\|^2}\mathbf{v} = \frac{1}{5}\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \quad f(\mathbf{e}_2) = \frac{\mathbf{v}^T\mathbf{e}_2}{\|\mathbf{v}\|^2}\mathbf{v} = \frac{1}{5}\begin{pmatrix} 2 \\ 4 \end{pmatrix},$$

takže

$$A = \frac{1}{5}\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \ .$$

Determinant matice $A - \lambda I_2$ je roven

$$\det(A - \lambda I_2) = \det\begin{pmatrix} 1/5 - \lambda & 2/5 \\ 2/5 & 4/5 - \lambda \end{pmatrix} = \lambda^2 - \lambda \ .$$

Matice A má tedy dvě vlastní čísla 1 a 0. Vlastní vektory příslušné vlastnímu číslu 1 tvoří podprostor

$$M_1 = \operatorname{Ker}(A - I_2) = \operatorname{Ker}\begin{pmatrix} -4/5 & 2/5 \\ 2/5 & -1/5 \end{pmatrix} = \operatorname{LO}\left\{\begin{pmatrix} 1 \\ 2 \end{pmatrix}\right\}$$

a vlastní vektory příslušné vlastnímu číslu 0 tvoří podprostor

$$M_0 = \operatorname{Ker}(A) = \operatorname{LO}\left\{\begin{pmatrix} -2 \\ 1 \end{pmatrix}\right\} \ .$$

Výsledek je v souladu z geometrickým náhledem z příkladu 9.19

Početně jednodušší postup je pracovat s maticí vzhledem f vzhledem k jiné bázi. Protože zřejmě $f((1,2)^T) = (1,2)^T$ a $f((-2,1)^T) = (0,0)^T$, je matice f vzhledem k bázi $B = ((1,2)^T, (-2,1)^T)$ a B rovná

$$C = [f]_B^B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

Determinant matice $C - \lambda I_2$ je $(1-\lambda)(-\lambda) = \lambda^2 - \lambda$ a vlastní čísla jsou 0 a 1 podle pozorování 9.25. Podprostory M_1 a M_0 vypočítáme nejprve vzhledem k bázi B:

$$[M_1]_B = [\operatorname{Ker}(f - \mathrm{id}_V)]_B = \operatorname{Ker}([f]_B^B - I_n) = \operatorname{Ker}\begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix} = \operatorname{LO}\left\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right\} \ ,$$

$$[M_0]_B = \operatorname{Ker}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \operatorname{LO}\left\{\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right\} \ .$$

Převodem do kanonické báze dostaneme stejný výsledek jako prvním postupem:

$$M_1 = [M_1]_K = \operatorname{LO}\left\{[\mathrm{id}]_K^B \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right\} = \operatorname{LO}\left\{1\begin{pmatrix} 1 \\ 2 \end{pmatrix} + 0\begin{pmatrix} -2 \\ 1 \end{pmatrix}\right\} = \operatorname{LO}\left\{\begin{pmatrix} 1 \\ 2 \end{pmatrix}\right\} \ ,$$

$$M_0 = [M_2]_K = \operatorname{LO}\left\{[\mathrm{id}]_K^B \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right\} = \operatorname{LO}\left\{0\begin{pmatrix} 1 \\ 2 \end{pmatrix} + 1\begin{pmatrix} -2 \\ 1 \end{pmatrix}\right\} = \operatorname{LO}\left\{\begin{pmatrix} -2 \\ 1 \end{pmatrix}\right\} \ .$$

▲

PŘÍKLAD 9.31. Spočítáme vlastní čísla rotace v $\mathbb{R}^2$ o úhel $\pi/2$ v kladném směru. Matice této rotace vzhledem ke kanonické bázi se rovná

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

příslušný determinant je $\det(A - \lambda I_2) = \lambda^2 + 1$. Vidíme, že matice A nemá žádné reálné vlastní číslo a tedy ani žádný vlastní vektor v $\mathbb{R}^2$.

Považujeme-li matici A za matici nad komplexními čísly, má dvě vlastní čísla i a $-i$. Vlastní vektory příslušné vlastnímu číslu i jsou všechny komplexní násobky vektoru $(i, 1)^T$ a vlastní vektory příslušné vlastnímu číslu $-i$ jsou všechny komplexní násobky vektoru $(i, -1)^T$. ▲

9.2.3. Charakteristický polynom, podobnost. V předchozích příkladech jsme našli vlastní čísla matice A řádu 2 jako kořeny kvadratického polynomu $\det(A - \lambda I_2)$. Obecně víme podle pozorování 9.25, že $\lambda \in \mathbf{T}$ je vlastní číslo matice A právě když platí $\det(A - \lambda I_n) = 0$. V následujícím tvrzení si ukážeme, že $\det(A - \lambda I_n)$ je polynom stupně n pro každou matici A řádu n a uvedeme nějaké jeho koeficienty.

TVRZENÍ 9.32. *Pro každou matici $A = (a_{ij})$ řádu n nad libovolným tělesem $\mathbf{T}$ platí*

(1) $\det(A - \lambda I_n)$ *je polynom stupně n s koeficienty v $\mathbf{T}$,*
(2) *koeficient u λ^n se rovná $(-1)^n$,*
(3) *koeficient u λ^{n-1} se rovná $(-1)^{n-1}(a_{11} + a_{22} + \cdots + a_{nn})$,*
(4) *absolutní člen se rovná $\det A$.*

DŮKAZ. První tři body ukážeme najednou. Označíme si prvky matice $A - \lambda I_n = (b_{ij})$. Z definice determinantu

$$\det(A - \lambda I_n) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) b_{1\pi(1)} b_{2\pi(2)} \cdots b_{n\pi(n)}$$

vidíme, že každý součin je součinem n prvků matice $A - \lambda I_n$, přičemž $b_{ij} = a_{ij}$ pokud $i \neq j$, a $b_{ii} = a_{ii} - \lambda$ pro každé $i = 1, 2, \ldots, n$. Součin odpovídající permutaci π obsahuje tolik činitelů $(a_{ii} - \lambda)$, kolik je prvků $i \in \{1, 2, \ldots, n\}$, pro které platí $\pi(i) = i$, tj. kolik je pevných bodů permutace π. Těch je nejvýše n, proto po roznásobení každého součinu dostaneme nějaký polynom stupně nejvýše n v proměnné λ. Jejich součtem je tedy také polynom stupně nejvýše n v proměnné λ.

Mocnina λ^n se může vyskytnout pouze v součinu, ve kterém je všech n činitelů rovných $a_{ii} - \lambda$, tj. v součinu definovaném identickou permutací na množině $\{1, 2, \ldots, n\}$. Platí

$$\begin{aligned} &\operatorname{sgn}(\mathrm{id}_n)(a_{11} - \lambda)(a_{22} - \lambda) \cdots (a_{nn} - \lambda) \\ &\qquad = (-1)^n \lambda^n + (a_{11} + a_{22} + \cdots + a_{nn})(-1)^{n-1} \lambda^{n-1} + \cdots \quad . \end{aligned}$$

V jakémkoliv součinu, který je definován neidentickou permutací $\pi \in S_n$, se musí vyskytnout aspoň dva činitelé b_{ij}, které neleží na hlavní diagonále matice B, a proto se v něm vyskytuje nejvýše $n - 2$ činitelů obsahujících λ, po roznásobení můžeme dostat nenulové koeficienty pouze u mocnin λ^{n-2} nebo nižších. Koeficienty u λ^n a λ^{n-1} pocházejí proto pouze ze součinu určeného identickou permutací. Tím jsou dokázány body (1), (2) a (3).

Hodnotu absolutního členu c_0 jakéhokoliv polynomu

$$p(\lambda) = c_n \lambda^n + c_{n-1} \lambda^{n-1} + \cdots + c_1 \lambda + c_0$$

získáme tak, že do něho dosadíme hodnotu proměnné $\lambda = 0$. Proto se absolutní člen polynomu $\det(A - \lambda I_n) = \det(A - 0\, I_n) = \det A$. ▲

Definice 9.33. Je-li A čtvercová matice řádu n nad tělesem $\mathbf{T}$, pak *charakteristický polynom matice* A je polynom

$$p_A(\lambda) = \det(A - \lambda I_n) \quad .$$

Příklad 9.34. Charakteristický polynom reálné matice

$$A = \begin{pmatrix} 3 & 7 \\ 4 & 5 \end{pmatrix}$$

je podle tvrzení 9.32 roven

$$p_A(\lambda) = (-1)^2\lambda^2 - (3+5)\lambda + (3 \cdot 5 - 7 \cdot 4) = \lambda^2 - 8\lambda - 13 \quad .$$

▲

Poznámka. Charakteristický polynom chápeme jako *formální polynom*, tj. jako formální výraz tvaru $c_n\lambda^n + \cdots + c_1\lambda + c_0$, kde $c_i \in T$, nikoliv jako *polynomiální zobrazení*, tj. jako zobrazení $T \to T$ tohoto tvaru. Polynomy $c_n\lambda^n + \cdots + c_0$ a $d_n\lambda^n + \cdots + d_0$ tedy považujeme za různé kdykoliv $c_i \neq d_i$ pro nějaké i. Pro tělesa $\mathbf{T} = \mathbb{R}$ a $\mathbf{T} = \mathbb{C}$ je rozdíl zanedbatelný, protože koeficienty polynomu jsou jednoznačně určené příslušnou polynomiální funkcí. Ale například v tělese $\mathbf{T} = \mathbb{Z}_2$ jsou polynomy 0 a $\lambda + \lambda^2$ formálně různé, nicméně určují stejnou polynomiální funkci, protože po dosazení $\lambda = 0$ i $\lambda = 1$ vyjde v obou případech 0.

Z tohoto důvodu není definice 9.33 úplně formálně ukotvená, protože determinant vpravo je potřeba nad obecným tělesem chápat jako determinant matice, jejíž prvky jsou (konstantní nebo lineární) polynomy v proměnné λ. Takové matice jsme neuvažovali, vždy jsme dosud pracovali s maticemi nad tělesy. Podobný problém je také například v důkazu tvrzení 9.32. Čtenář, kterého tyto formální nedostatky trápí a neumí je zatím odstranit, ať vždy uvažuje jen reálná nebo komplexní čísla – nad těmito tělesy se nepřesností nedopouštíme.

Tvrzení 9.32 ukazuje, že charakteristický polynom jakékoliv matice A řádu n má stupeň právě n a pozorování 9.25 říká, že vlastní čísla matice A jsou jeho kořeny. Například charakteristický polynom matice A z příkladů 9.9 a 9.28 je

$$\det(A - \lambda I_2) = \det\begin{pmatrix} 3-\lambda & 0 \\ 1 & 2-\lambda \end{pmatrix} = (3-\lambda)(2-\lambda) = \lambda^2 - 5\lambda + 6 \quad .$$

Charakteristický polynom lineárního operátoru f na konečně dimenzionálním prostoru $\mathbf{V}$ definujeme jako charakteristický polynom matice $[f]_B^B$, kde B je nějaká báze prostoru $\mathbf{V}$. Musíme ovšem ověřit, že polynom nezávisí na volbě báze, jak jsme v konkrétní situaci viděli v příkladu 9.30.

Uvažujme tedy dvě různé báze B, C prostoru $\mathbf{V}$. Podle pravidel o počítání s maticemi zobrazení (viz tvrzení 6.18) je

$$[f]_B^B = R^{-1}[f]_C^C R \quad ,$$

kde R je matice přechodu od B k C. Matice svázané takovým vztahem nazýváme podobné.

Definice 9.35. Dvě čtvercové matice X, Y téhož řádu nad tělesem $\mathbf{T}$ se nazývají *podobné*, pokud existuje regulární matice R taková, že $Y = R^{-1}XR$.

Relace podobnosti matic je ekvivalence na množině všech čtvercových matic téhož řádu n nad tělesem $\mathbf{T}$, důkaz ponecháme jako cvičení. Podle diskuze předcházející definici 9.35 jsou matice $[f]_B^B$ a $[f]_C^C$ podobné.

Tvrzení 9.36. *Podobné matice mají stejný charakteristický polynom.*

Důkaz. Jsou-li X, Y dvě podobné matice téhož řádu nad tělesem $\mathbf{T}$, pak existuje regulární matice R taková, že $Y = R^{-1}XR$. Potom platí

$$\begin{aligned} \det(Y - \lambda I_n) &= \det(R^{-1}XR - \lambda I_n) = \det(R^{-1}XR - R^{-1}\lambda I_n R) \\ &= \det(R^{-1}(X - \lambda I_n)R) = \det(R)^{-1}\det(X - \lambda I_n)\det(R) \\ &= \det(X - \lambda I_n) \end{aligned}$$

podle věty o násobení determinantů a jejím důsledku pro determinant inverzní matice. ▲

To opravňuje definici charakteristického polynomu lineární operátoru na konečně generovaném prostoru.

DEFINICE 9.37. Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na konečně generovaném prostoru $\mathbf{V}$ dimenze n, pak *charakteristický polynom operátoru* f je polynom

$$p_f(\lambda) = \det\left([f]_B^B - \lambda I_n\right) \quad ,$$

kde B je libovolná báze prostoru $\mathbf{V}$.

Charakteristický polynom operátoru na (konečně generovaném prostoru) $\mathbf{V}$ je tedy roven charakteristickému polynomu matice $[f]_B^B$ pro jakoukoliv bázi B prostoru $\mathbf{V}$. Jeho kořeny jsou podle pozorování 9.26 vlastní čísla operátoru f.

PŘÍKLAD 9.38. V příkladu 9.19 jsme spočetli, že charakteristický polynom ortogonální projekce f na přímku LO $\left\{(1,2)^T\right\}$ je $p_f(\lambda) = \lambda^2 - \lambda$. Z druhého postupu nahlédněte, že stejně vyjde charakteristický polynom pro ortogonální projekci na libovolnou přímku, dokonce projekci na libovolnou přímku p ve směru přímky q, pokud $p \neq q$. ▲

9.2.4. Kořeny polynomů, algebraická násobnost. K určení vlastních čísel matice nebo operátoru na konečně generovaném prostoru potřebujeme najít kořeny charakteristického polynomu. Uvedeme několik pojmů a tvrzení (bez důkazů), které budeme o kořenech polynomů potřebovat. Důkazy se dozvíte v kurzu algebry nebo je najdete v jakékoliv úvodní knize o algebře.

Připomeňme, že polynom stupně n nad tělesem $\mathbf{T}$ je výraz

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \text{ kde } a_0, \ldots, a_n \in T,\ a_n \neq 0 \ .$$

Kořenem takového polynomu je prvek $t \in T$, pro který $p(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n = 0$. Nulovému polynomu $p(x) = 0$ předchozí definice nepřidělila stupeň, někdy se říká, že je stupně -1, jindy se stupeň nedefinuje.

Nyní směřujeme k pojmu násobnosti kořene. Řekneme, že polynom $p(x)$ dělí polynom $s(x)$ (oba polynomy jsou nad tělesem $\mathbf{T}$), pokud existuje polynom $q(x)$ (nad $\mathbf{T}$) takový, že $p(x)q(x) = s(x)$. Například reálný polynom $x - 1$ dělí polynom $x^2 - 1$, protože $(x-1)(x+1) = x^2 - 1$.

TVRZENÍ 9.39. *Nechť $p(x)$ je polynom nad $\mathbf{T}$. Prvek $t \in T$ je kořenem polynomu $p(x)$ právě tehdy, když polynom $x - t$ dělí polynom $p(x)$.*

Největší číslo l takové, že $(x-t)^l$ stále dělí polynom $p(x)$ nazýváme násobnost kořene t.

DEFINICE 9.40. Nechť $p(x)$ je polynom nad $\mathbf{T}$ a $t \in T$ je jeho kořen. *Násobnost kořene t* polynomu $p(x)$ definujeme jako největší přirozené číslo l takové, že polynom $(x-t)^l$ dělí polynom $p(x)$.

TVRZENÍ 9.41. *Nechť $p(x)$ je polynom nad $\mathbf{T}$, $t_1, \ldots, t_k \in T$ po dvou různé a $l_1, \ldots, l_k \in \mathbb{N}$. Pak následující tvrzení jsou ekvivalentní.*

(1) *Pro každé $i \in \{1, \ldots, k\}$ je t_i kořen násobnosti l_i.*
(2) *$p(x) = (x-t_1)^{l_1} \ldots (x-t_k)^{l_k} q(x)$ pro nějaký polynom $q(x)$ takový, že ani jeden z prvků $t_1, \ldots, t_k$ není jeho kořen.*

Implikaci (2) $\Rightarrow$ (1) můžeme použít k hledání násobnosti kořenů. Uhádneme nějaký kořen t polynomu $p(x)$ a polynom $p(x)$ vydělíme polynomem $x - t$. Dále pokračujeme stejným způsobem s výsledným polynomem. Proces ukončíme, když

získáme polynom, který již žádný kořen nemá. Nakonec získáme rozklad jako v části (2) a tvrzení nám dá informace o násobnostech.

Důsledkem tvrzení 9.41 je, že polynom stupně $n \geq 0$ má nejvýše n kořenů, i když počítáme každý tolikrát, kolik je jeho násobnost.

TVRZENÍ 9.42. *Polynom stupně n nad libovolným tělesem má nejvýše n kořenů včetně násobností.*

Obrat „včetně násobností“ budeme používat pro stručnost vyjadřování. Přesný význam je vysvětlený nad tvrzením, tj. pokud každý kořen počítáme tolikrát, kolik je jeho násobnost, vyjde nejvýše n.

PŘÍKLAD 9.43. Určíme kořeny a jejich násobnosti pro reálný polynom $p(x) = 2x^3 - 8x^2 + 10x - 4$.

Uhádneme kořen $t = 1$ a vydělíme polynom $p(x)$ polynomem $x - 1$.

$$q(x) = (2x^3 - 8x^2 + 10x - 4) : (x - 1) = 2x^2 - 6x + 4 \ .$$

Hledat kořeny reálného polynomu druhého stupně umíme, polynom $q(x)$ má kořeny 1 a 2. Polynom $q(x)$ lze proto zapsat

$$q(x) = 2(x - 1)(x - 2) \ .$$

Pro původní polynom máme

$$p(x) = (x - 1)q(x) = 2(x - 1)^2(x - 2) \ .$$

Tedy $p(x)$ má kořen 1 násobnosti 2 a kořen 2 násobnosti 1. ▲

PŘÍKLAD 9.44. Určíme kořeny a násobnosti kořenů reálného polynomu $p(x) = x^4 + x^2$.

Ihned vidíme, že x^2 dělí polynom $p(x)$. Máme

$$p(x) = x^2(x^2 + 1) \ ,$$

Polynom x^2+1 již žádný reálný kořen nemá, tedy $p(x)$ má jediný kořen 0 násobnosti 2.

Chápeme-li ovšem $p(x)$ jako polynom nad komplexními čísly, pak $x^2 + 1$ má dva kořeny i a $-i$ a polynom $p(x)$ lze psát

$$p(x) = x^2(x + i)(x - i)$$

Nad komplexními čísly tedy máme kořen 0 násobnosti 2 a kořeny i a $-i$ násobnosti 1. ▲

PŘÍKLAD 9.45. Určíme kořeny polynomu $p(x) = x^4+2x^3+x^2+2x$ nad tělesem $\mathbb{Z}_3$.

Vidíme, že $t = 0$ je kořen. Dosazením zjistíme, že $t = 1$ je kořenem a $t = 2$ kořenem není. K určení násobností vydělíme polynom $p(x)$ polynomem $x(x - 1) = x^2 - x = x^2 + 2x$.

$$(x^4 + 2x^3 + x^2 + 2x) : (x^2 + 2x) = x^2 + 1 \ .$$

Takže

$$p(x) = x(x + 2)(x^2 + 1) \ .$$

Dosazením prvků tělesa $\mathbb{Z}_3$ do polynomu $x^2 + 1$ zjistíme, že $x^2 + 1$ žádné kořeny v $\mathbb{Z}_3$ nemá, takže oba kořeny 0 i 1 mají násobnost 1. ▲

Ze základní věty algebry (věta 1.9) lze odvodit, že nad komplexními čísly je kořenů vždy maximální možný počet (opět musíme počítat i s násobnostmi).

VĚTA 9.46. *Každý polynom stupně $n \geq 1$ nad tělesem $\mathbb{C}$ lze napsat jako součin lineárních polynomů (tj. polynomů stupně 1).*

Speciálně, každý polynom stupně $n \geq 0$ nad tělesem $\mathbb{C}$ má právě n kořenů včetně násobností.

(Na okraj poznamenejme, že každé těleso lze rozšířit do většího tělesa, kde platí obdoba předchozí věty.)

Ještě uvedeme jeden pozitivní výsledek pro polynomy nad reálnými čísly, tentokrát výjimečně i s náznakem důkazu.

TVRZENÍ 9.47. *Polynom lichého stupně nad tělesem $\mathbb{R}$ má alespoň jeden kořen.*

DŮKAZ. Připomeňme, že je-li komplexní číslo z kořenem reálného polynomu $p(x)$, pak je jeho kořenem také číslo $\overline{z}$ komplexně sdružené se z (viz věta 1.12). Kořeny polynomu $p(x)$ tak můžeme uspořádat do dvojic komplexně sdružených kořenů, protože lze ověřit, že je-li kořen z k-násobný, pak je k-násobný i kořen $\overline{z}$. Protože ale všech kořenů (spolu s násobnostmi) je lichý počet, existuje aspoň jeden kořen z, pro který platí $z = \overline{z}$, tj. aspoň jeden reálný kořen.

Alternativně lze tvrzení dokázat analyticky, bez použití komplexních čísel. Je-li koeficent u x^n kladný, pak pro $x \to \infty$ je $p(x) \to \infty$ a pro $x \to -\infty$ je $p(x) \to -\infty$. Ze spojitosti funkce $p(x)$ pak vidíme, že nutně existuje číslo z, splňující $p(z) = 0$. (Je-li koefcient u x^n záporný, důkaz je obdobný.) ▲

Nyní se vrátíme k vlastním číslům. Ty lze spočítat jako kořeny charakteristického polynomu, jejich násobnosti jsou důležitou informací, proto si zaslouží samostatný pojem.

DEFINICE 9.48. Nechť f je lineární operátor na konečně generovaném prostoru a λ je jeho vlastní číslo. *Algebraickou násobností* vlastního čísla λ rozumíme jeho násobnost jako kořene charakteristického polynomu operátoru f.

DEFINICE 9.49. Nechť A je čtvercová matice a λ je její vlastní číslo. *Algebraickou násobností* vlastního čísla λ rozumíme jeho násobnost jako kořene charakteristického polynomu matice A.

PŘÍKLAD 9.50. Najdeme vlastní čísla a jejich algebraické násobnosti pro lineární operátor $f : \mathbb{R}^3 \to \mathbb{R}^3$ definovaný předpisem

$$f\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -y+z \\ -3x-2y+3z \\ -2x-2y+3z \end{pmatrix} .$$

Matice operátoru f vzhledem ke kanonické bázi je

$$A = [f]_K^K = \begin{pmatrix} 0 & -1 & 1 \\ -3 & -2 & 3 \\ -2 & -2 & 3 \end{pmatrix} .$$

Charakteristický polynom operátoru f se rovná

$$\det(A-\lambda I_3) = \det\begin{pmatrix} 0-\lambda & -1 & 1 \\ -3 & -2-\lambda & 3 \\ -2 & -2 & 3-\lambda \end{pmatrix} = -\lambda^3+\lambda^2+\lambda-1 = -(\lambda-1)^2(\lambda+1) .$$

Operátor má tedy 2 různá vlastní čísla: vlastní číslo 1 algebraické násobnosti 2 a vlastní číslo -1 algebraické násobnosti 1. (Takže dohromady máme 3 vlastní čísla včetně násobností.) ▲

Zformulujeme důsledky tvrzení 9.42, věty 9.46 a tvrzení 9.47 pro vlastní čísla operátorů.

DŮSLEDEK 9.51.

- *Každý lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném prostoru dimenze n nad tělesem $\mathbf{T}$ má nejvýše n vlastních čísel včetně násobností.*
- *Každý lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném prostoru dimenze n nad tělesem $\mathbb{C}$ má právě n vlastních čísel včetně násobností.*
- *Každý lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném vektorovém prostoru liché dimenze nad $\mathbb{R}$ má aspoň jedno (reálné) vlastní číslo.*

V řeči matic:

Důsledek 9.52.

- *Každá čtvercová matice řádu n nad tělesem $\mathbf{T}$ má nejvýše n vlastních čísel včetně algebraických násobností.*
- *Každá čtvercová matice řádu n nad tělesem $\mathbb{C}$ má právě n vlastních čísel včetně algebraických násobností.*
- *Každá čtvercová matice lichého řádu nad tělesem $\mathbb{R}$ má alespoň jedno reálné vlastní číslo.*

9.3. Diagonalizovatelné operátory

9.3.1. Definice diagonalizovatelnosti. Má-li operátor f (resp. matice A) „dostatek“ vlastních vektorů, můžeme diskrétní dynamický systém $\mathbf{x}_k = f(\mathbf{x}_{k-1})$ (resp. $\mathbf{x}_k = A\mathbf{x}_{k-1}$) snadno vyřešit. K ilustraci poslouží opět operátor z příkladů 9.9 a 9.28.

Důležitou roli v této části budou hrát diagonální matice, proto si pro ně zavedeme speciální označení. Diagonální matici $D = (d_{ij})$ řádu n budeme zapisovat $\operatorname{diag}(d_{11}, d_{22}, \cdots, d_{nn})$. Diagonální matice umíme snadno umocnit, neboť platí

$$\operatorname{diag}(t_1, t_2, \ldots, t_n)^k = \operatorname{diag}(t_1^k, t_2^k, \ldots, t_n^k)$$

pro každý exponent $k = 0, 1, 2, \ldots$.

Příklad 9.53. Uvažujme operátor f_A na $\mathbb{R}^2$ určený maticí

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

V příkladu 9.28 jsme vypočítali, že vlastní čísla tohoto operátoru jsou 2 a 3 a příslušné podprostory vlastních vektorů jsou

$$M_2 = \mathrm{LO}\left\{\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right\}, \quad M_3 = \mathrm{LO}\left\{\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right\} .$$

Vektory $\mathbf{v}_1 = (0,1)^T$, $\mathbf{v}_2 = (1,1)^T$ tvoří lineárně nezávislou posloupnost $B = (\mathbf{v}_1, \mathbf{v}_2)$, tedy bázi prostoru $\mathbb{R}^2$. (To, že posloupnost je lineárně nezávislá, není náhoda – viz věta 9.62.)

Platí $f_A(\mathbf{v}_1) = 2\mathbf{v}_1$ a $f_A(\mathbf{v}_2) = 3\mathbf{v}_2$. Z toho vidíme, že matice operátoru f_A vzhledem k bázi B je

$$[f_A]_B^B = \operatorname{diag}(2,3) = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} .$$

Diagonální matice ale mocnit umíme! Pro libovolné přirozené k proto umíme vypočítat matici operátoru $(f_A)^k$ vzhledem k bázi B:

$$[(f_A)^k]_B^B = ([f_A]_B^B)^k = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}^k = \operatorname{diag}(2^k, 3^k) = \begin{pmatrix} 2^k & 0 \\ 0 & 3^k \end{pmatrix} .$$

Nyní můžeme odpovědět na řadu otázek o operátoru f_A a matici A.

• **Řešení diskrétního dynamického systému $\mathbf{x}_k = f_A(\mathbf{x}_{k-1})$ „v bázi B“.** Platí

$$[\mathbf{x}_k]_B = [(f_A)^k(\mathbf{x}_0)]_B = [(f_A)^k]_B^B\,[\mathbf{x}_0]_B = \begin{pmatrix} 2^k & 0 \\ 0 & 3^k \end{pmatrix} [\mathbf{x}_0]_B \ .$$

Jsou-li tedy souřadnice $[\mathbf{x}_0]_B$ počátečního stavu $\mathbf{x}_0$ vzhledem k bázi B rovny

$$[\mathbf{x}_0]_B = \begin{pmatrix} r \\ s \end{pmatrix} \ ,$$

pak souřadnice stavu $\mathbf{x}_k$ v bázi B jsou

$$[\mathbf{x}_k]_B = \begin{pmatrix} 2^k & 0 \\ 0 & 3^k \end{pmatrix} \begin{pmatrix} r \\ s \end{pmatrix} = \begin{pmatrix} r2^k \\ s3^k \end{pmatrix} \ .$$

• **Kvalitativní chování diskrétního dynamického systému $\mathbf{x}_k = f_A(\mathbf{x}_{k-1})$.** Pokud $r \neq 0$ a $s \neq 0$, pak se pro $k \to \infty$ budou obě souřadnice vzhledem k B v absolutní hodnotě blížit nekonečnu. Přitom první složka bude pro velká k zanedbatelná vzhledem ke složce druhé.

• **Řešení diskrétního dynamického systému $\mathbf{x}_k = f_A(\mathbf{x}_{k-1})$ „v kanonické bázi“.** Z matice $[(f_A)^k]_B^B$ můžeme určit matici $(f_A)^k$ vzhledem ke kanonickým bázím pomocí matic přechodu (opakujeme výpočet v tvrzení 6.18):

$$\begin{aligned}[(f_A)^k]_K^K &= [\mathrm{id}]_K^B\,[(f_A)^k]_B^B\,[\mathrm{id}]_B^K = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2^k & 0 \\ 0 & 3^k \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2^k & 0 \\ 0 & 3^k \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3^k & 0 \\ 3^k - 2^k & 2^k \end{pmatrix}\end{aligned}$$

Z toho dostáváme

$$\mathbf{x}_k = (f_A)^k(\mathbf{x}_0) = [(f_A)^k]_K^K\,\mathbf{x}_0 = \begin{pmatrix} 3^k & 0 \\ 3^k - 2^k & 2^k \end{pmatrix} \mathbf{x}_0 \ .$$

Tedy pokud $\mathbf{x}_0 = (a, b)^T$, pak

$$\mathbf{x}_k = (f_A)^k(\mathbf{x}_0) = \begin{pmatrix} 3^k a \\ (3^k - 2^k)a + 2^k b \end{pmatrix} \ .$$

• **Výpočet k-té mocniny A^k matice A pro $k \geq 1$.** Protože $[(f_A)^k]_K^K = [f_{A^k}]_K^K = A^k$ máme z předchozího bodu

$$A^k = \begin{pmatrix} 3^k & 0 \\ 3^k - 2^k & 2^k \end{pmatrix} \ .$$

▲

Příklad nás vede k definici diagonalizovatelného operátoru.

Definice 9.54. Lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném prostoru $\mathbf{V}$ nazýváme *diagonalizovatelný*, pokud má vzhledem k nějaké bázi diagonální matici.

Ekvivalentně můžeme diagonalizovatelnost charakterizovat pomocí podobnosti matice operátoru (vzhledem k libovolné bázi) s diagonální maticí.

Tvrzení 9.55. *Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na konečně generovaném prostoru $\mathbf{V}$ dimenze n nad tělesem $\mathbf{T}$ a C báze prostoru $\mathbf{V}$, pak operátor f je diagonalizovatelný právě tehdy, když je matice $[f]_C^C$ podobná diagonální matici.*

Důkaz. Je-li operátor f diagonalizovatelný, pak existuje báze B prostoru $\mathbf{V}$ taková, že $[f]_B^B$ je diagonální matice. Podle tvrzení 6.18 jsou matice $[f]_C^C$ a $[f]_B^B$ podobné.

Naopak, je-li matice $[f]_C^C$ podobná diagonální matici D, pak existuje regulární matice $R = (\mathbf{r}_1|\mathbf{r}_2|\cdots|\mathbf{r}_n)$ taková, že $D = R^{-1}[f]_C^C\,R$. Protože je matice R regulární,

je posloupnost sloupcových vektorů $(\mathbf{r}_1, \mathbf{r}_2, \dots, \mathbf{r}_n)$ lineárně nezávislá a proto báze v $\mathbf{T}^n$. Zvolíme vektory $\mathbf{v}_i \in \mathbf{V}$ tak, aby platilo $[\mathbf{v}_i]_C = \mathbf{r}_i$ pro každé $i = 1, 2, \dots, n$. Posloupnost $B = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ je pak báze prostoru $\mathbf{V}$ a platí pro ni $[\mathrm{id}]_C^B = R$. Opět podle tvrzení 6.18 pak platí $[f]_B^B = R^{-1}[f]_C^C R = D$. ▲

Tvrzení 9.56. *Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na konečně generovaném prostoru $\mathbf{V}$ a je-li $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ báze prostoru $\mathbf{V}$, pak $[f]_B^B = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$ platí právě tehdy, když pro každé $i \in \{1, 2, \dots, n\}$ je $\mathbf{v}_i$ vlastní vektor příslušný vlastnímu číslu λ_i.*

Důkaz. Rovnost $[f]_B^B = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$ platí právě když pro každé $i \in \{1, \dots, n\}$ se i-tý sloupec matice $[f]_B^B$ rovná i-tému sloupci matice $\mathrm{diag}(\lambda_1, \dots, \lambda_n)$, tj. právě když $[f(\mathbf{v}_i)]_B = \lambda_i \mathbf{e}_i$ (použili jsme definici matice lineárního zobrazení).

Rovnost $[f(\mathbf{v}_i)]_B = \lambda_i \mathbf{e}_i$ je ekvivalentní vztahu $f(\mathbf{v}_i) = \lambda_i \mathbf{v}_i$ podle definice souřadnic prvku vzhledem k bázi. Protože $\mathbf{v}_i \neq \mathbf{o}$, vztah $f(\mathbf{v}_i) = \lambda_i \mathbf{v}_i$ je ekvivalentní tomu, že $\mathbf{v}_i$ je vlastní vektor příslušný vlastnímu číslu λ_i. ▲

Důsledek 9.57. *Lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném prostoru $\mathbf{V}$ je diagonalizovatelný právě tehdy, když existuje báze prostoru $\mathbf{V}$ tvořená vlastními vektory operátoru f.*

Přeformulujeme si definici a tvrzení o diagonalizovatelnosti operátorů pro matice.

Definice 9.58. Čtvercová matice A řádu n nad tělesem $\mathbf{T}$ se nazývá *diagonalizovatelná*, pokud je operátor $f_A : \mathbf{T}^n \to \mathbf{T}^n$ diagonalizovatelný.

Použitím tvrzení 9.55 na kanonickou bázi $C = K_n$ dostaneme následující maticovou verzi.

Tvrzení 9.59. *Čtvercová matice A řádu n nad tělesem $\mathbf{T}$ je diagonalizovatelná právě tehdy, když je podobná diagonální matici.*

Pro maticovou formulaci tvrzení 9.56 si opět připomeneme, že pro čtvercovou matici A řádu n nad $\mathbf{T}$ a bázi $B = (\mathbf{v}_1, \dots\ \mathbf{v}_n)$ prostoru $\mathbf{T}^n$ platí

$$[f_A]_B^B = [\mathrm{id}]_B^K\, [f_A]_K^K\, [\mathrm{id}]_K^B = R^{-1}AR, \qquad \text{kde } R = [\mathrm{id}]_K^B = (\mathbf{v}_1 | \dots | \mathbf{v}_n)\ .$$

Tvrzení 9.60. *Je-li A čtvercová matice řádu n nad tělesem $\mathbf{T}$, $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ báze prostoru $\mathbf{T}^n$ a $R = [\mathrm{id}]_K^B = (\mathbf{v}_1 | \dots | \mathbf{v}_n)$, pak matice $[f_A]_B^B = R^{-1}AR$ se rovná diagonální matici $\mathrm{diag}(\lambda_1, \dots, \lambda_n)$ právě tehdy, když pro každé $i \in \{1, 2, \dots, n\}$ je $\mathbf{v}_i$ vlastní vektor příslušný vlastnímu číslu λ_i.*

Důsledek 9.61. *Čtvercová matice A řádu n nad tělesem $\mathbf{T}$ je diagonalizovatelná právě tehdy, když existuje báze prostoru $\mathbf{T}^n$ tvořená vlastními vektory matice A.*

V situaci, kdy $[f]_B^B = [\mathrm{id}]_B^K\, [f_A]_K^K\, [\mathrm{id}]_K^B = R^{-1}AR = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$, umíme matici A umocnit stejně jako v příkladu 9.53:

$$\begin{aligned} A^k &= [(f_A)^k]_K^K = [\mathrm{id}]_K^B\, [(f_A)^k]_B^B\, [\mathrm{id}]_B^K = R\,([f_A]_B^B)^k\, R^{-1} \\ &= R\ \mathrm{diag}(\lambda_1, \dots, \lambda_n)^k\, R^{-1} = R\ \mathrm{diag}(\lambda_1^k, \dots, \lambda_n^k)\, R^{-1}\ . \end{aligned}$$

Výpočet mocniny A^k můžeme nahlédnout také algebraicky. Označíme $D = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$ a vztah $R^{-1}AR = D$ přepíšeme na $A = RDR^{-1}$. Pak

$$\begin{aligned} A^k &= \underbrace{(RDR^{-1})(RDR^{-1})\dots(RDR^{-1})}_{k\times} = R\underbrace{DD\cdots D}_{k\times}R^{-1} = RD^kR^{-1} \\ &= R\ \mathrm{diag}(\lambda_1^k, \dots, \lambda_n^k)\, R^{-1}\ . \end{aligned}$$

9.3.2. Lineární nezávislost vlastních vektorů. Chceme nalézt nutné a postačující podmínky pro to, aby byl lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném prostoru $\mathbf{V}$ diagonalizovatelný. Základem je následující věta, která platí zcela obecně, není nutné předpokládat, že prostor $\mathbf{V}$ má konečnou dimenzi.

VĚTA 9.62. *Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor a $(\mathbf{v_1}, \mathbf{v}_2, \dots, \mathbf{v}_k)$ posloupnost nenulových vlastních vektorů operátoru f příslušných navzájem různým vlastním číslům $\lambda_1, \dots, \lambda_k$, pak je posloupnost $(\mathbf{v_1}, \mathbf{v}_2, \dots, \mathbf{v}_k)$ lineárně nezávislá.*

DŮKAZ. Použijeme indukci podle k. Je-li $k = 1$, tvrzení platí, protože $\mathbf{v}_1 \neq \mathbf{o}$. Předpokládejme, že $k > 1$ a tvrzení platí pro $k-1$, tj. že posloupnost $(\mathbf{v_1}, \dots, \mathbf{v}_{k-1})$ je lineárně nezávislá. Uvažujme skaláry $a_1, \dots, a_k \in \mathbf{T}$ takové, že platí

$$\mathbf{o} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_{k-1}\mathbf{v}_{k-1} + a_k\mathbf{v}_k \ .$$

Aplikujeme na obě strany operátor $(f - \lambda_k \operatorname{id}_V)$ a upravíme. V prvních dvou úpravách používáme linearitu operátoru $(f - \lambda_k \operatorname{id}_V)$.

$$(f - \lambda_k \operatorname{id}_V)(a_1\mathbf{v}_1 + \cdots + a_{k-1}\mathbf{v}_{k-1} + a_k\mathbf{v}_k) = (f - \lambda_k \operatorname{id}_V)(\mathbf{o})$$

$$(f - \lambda_k \operatorname{id}_V)(a_1\mathbf{v}_1) + \cdots + (f - \lambda_k \operatorname{id}_V)(a_{k-1}\mathbf{v}_{k-1}) + (f - \lambda_k \operatorname{id}_V)(a_k\mathbf{v}_k) = \mathbf{o}$$

$$a_1(f - \lambda_k \operatorname{id}_V)(\mathbf{v}_1) + \cdots + a_{k-1}(f - \lambda_k \operatorname{id}_V)(\mathbf{v}_{k-1}) + a_k(f - \lambda_k \operatorname{id}_V)(\mathbf{v}_k) = \mathbf{o} \ .$$

K poslední úpravě využijeme toho, že pro každé $i = 1, 2, \dots, k$ platí

$$(f - \lambda_k \operatorname{id}_V)(\mathbf{v}_i) = f(\mathbf{v}_i) - (\lambda_k \operatorname{id}_V)(\mathbf{v}_i) = \lambda_i\mathbf{v}_i - \lambda_k\mathbf{v}_i = (\lambda_i - \lambda_k)\mathbf{v}_i \ ,$$

a dostaneme

$$\mathbf{o} = a_1(\lambda_1 - \lambda_k)\mathbf{v}_1 + \cdots + a_{k-1}(\lambda_{k-1} - \lambda_k)\mathbf{v}_{k-1} \ .$$

Posloupnost vektorů $(\mathbf{v_1}, \dots, \mathbf{v}_{k-1})$ je lineárně nezávislá podle indukčního předpokladu. Odtud plyne

$$a_1(\lambda_1 - \lambda_k) = a_2(\lambda_2 - \lambda_k) = \cdots = a_{k-1}(\lambda_{k-1} - \lambda_k) = 0 \ .$$

Protože vlastní čísla $\lambda_1, \dots, \lambda_{k-1}, \lambda_k$ jsou navzájem různá, vyplývá odtud, že $a_1 = a_2 = \cdots = a_{k-1} = 0$. Po dosazení do rovnosti

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_{k-1}\mathbf{v}_{k-1} + a_k\mathbf{v}_k = \mathbf{o}$$

dostaneme $a_k\mathbf{v}_k = \mathbf{o}$ a tedy také $a_k = 0$, protože $\mathbf{v}_k \neq \mathbf{o}$. Tím je dokázáno, že posloupnost $(\mathbf{v_1}, \dots, \mathbf{v}_{k-1}, \mathbf{v}_k)$ je lineárně nezávislá. ▲

DŮSLEDEK 9.63. *Má-li lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na vektorovém prostoru $\mathbf{V}$ dimenze n nad tělesem $\mathbf{T}$ celkem n navzájem různých vlastních čísel, pak je diagonalizovatelný.*

DŮKAZ. Má-li operátor f celkem n navzájem různých vlastních čísel $\lambda_1, \dots, \lambda_n$, existuje pro každé $i = 1, \dots, n$ nenulový vlastní vektor $\mathbf{v}_i$ příslušný λ_i. Podle předchozí věty je posloupnost vlastních vektorů $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ lineárně nezávislá a tedy je to báze prostoru $\mathbf{V}$. Operátor f má tak bázi složenou z vlastních vektorů operátoru f, je proto diagonalizovatelný podle důsledku 9.57. ▲

DŮSLEDEK 9.64. *Má-li matice A řádu n nad tělesem $\mathbf{T}$ celkem n navzájem různých vlastních čísel, pak je diagonalizovatelná.*

Operátor v příkladu 9.53 a operátor v motivačním příkladu o Fibonacciho posloupnosti 9.2 splňují předpoklad důsledku 9.63.

PŘÍKLAD 9.65. Ještě jednou spočítáme, jak vypadá k-tý prvek Fibonacciho posloupnosti. Najdeme vlastní čísla a vlastní vektory matice C. Charakteristický

polynom matice C je (podle tvrzení 9.32 o koeficientech charakteristického polynomu) roven

$$p_C(\lambda) = \lambda^2 - \lambda - 1$$

Vlastní čísla matice C, neboli kořeny rovnice $p_C(\lambda) = 0$, jsou

$$\lambda_1 = \frac{1+\sqrt{5}}{2}, \quad \lambda_2 = \frac{1-\sqrt{5}}{2} = 1 - \lambda_1 \ .$$

Všechny vlastní vektory příslušné vlastnímu číslu λ_1 jsou právě všechna řešení homogenní soustavy s maticí

$$\begin{pmatrix} 0-\lambda_1 & 1 \\ 1 & 1-\lambda_1 \end{pmatrix} ,$$

což jsou všechny vektory v $M_{\lambda_1} = \mathrm{LO}\left\{(1, 1/2+\sqrt{5}/2)^T\right\} = \mathrm{LO}\left\{(1,\lambda_1)^T\right\}$. Podobně jsou všechny vlastní vektory příslušné vlastnímu číslu $\lambda_2 = 1 - \lambda_1$ právě vektory z lineárního obalu vektoru $(1,\lambda_2)^T$.

Posloupnost

$$B = (\mathbf{v}_1, \mathbf{v}_2) = \left(\begin{pmatrix} 1 \\ \lambda_1 \end{pmatrix}, \begin{pmatrix} 1 \\ \lambda_2 \end{pmatrix} \right)$$

je (i podle věty 9.62) lineárně nezávislá, takže je bází $\mathbb{R}^2$, a platí

$$[f_C]_B^B = \mathrm{diag}(\lambda_1, \lambda_2), \quad [(f_C)^k]_B^B = \mathrm{diag}(\lambda_1^k, \lambda_2^k) \ .$$

Chceme znát $C^k(a_0,a_1)^T = (f_C)^k(a_0,a_1)^T$. Teď máme více možností, jak výpočet dokončit. Můžeme přejít ke kanonické bázi (tj. spočítat $[(f_C)^k]_K^K = C^k$), nebo pracovat přímo v bázi B. Zvolíme druhý přístup.

Vyjádříme vektor $(a_0,a_1)^T = (0,1)^T$ vzhledem k bázi B. Vyjde

$$\left[\begin{pmatrix} 0 \\ 1 \end{pmatrix} \right]_B = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \ .$$

Odtud dostáváme pro každé celé číslo $k \geq 0$

$$\left[\begin{pmatrix} a_k \\ a_{k+1} \end{pmatrix} \right]_B = [(f_C)^k]_B^B \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix} \right]_B = \begin{pmatrix} \lambda_1^k & 0 \\ 0 & \lambda_2^k \end{pmatrix} \frac{1}{\sqrt{5}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} \lambda_1^k \\ -\lambda_2^k \end{pmatrix} \ .$$

Z toho vyplývá

$$\begin{pmatrix} a_k \\ a_{k+1} \end{pmatrix} = \frac{1}{\sqrt{5}} \left(\lambda_1^k \begin{pmatrix} 1 \\ \lambda_1 \end{pmatrix} - \lambda_2^k \begin{pmatrix} 1 \\ \lambda_2 \end{pmatrix} \right) = \frac{1}{\sqrt{5}} \begin{pmatrix} \lambda_1^k - \lambda_2^k \\ \lambda_1^{k+1} - \lambda_2^{k+1} \end{pmatrix} \ .$$

Srovnáním prvních složek dostáváme

$$a_k = \frac{\lambda_1^k}{\sqrt{5}} - \frac{\lambda_2^k}{\sqrt{5}} \ .$$

Všimněme si také, že $|\lambda_2^k| < 1$, druhý sčítanec se proto pro $k \to \infty$ blíží 0, takže

$$a_k \approx \lambda_1^k/\sqrt{5} = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^k \ .$$

▲

K vzorci pro k-tý člen Fibonacciho posloupnosti se lze dopočítat rychleji, jak vyplyne z následující diskuze. Uvažujme diskrétní lineární dynamický systém $\mathbf{x}_{k+1} = A\mathbf{x}_k$, kde A je diagonalizovatelná matice nad libovolným tělesem. Matici A lze psát ve tvaru $A = R\,\mathrm{diag}(\lambda_1,\ldots,\lambda_n)R^{-1}$, kde λ_1, ..., λ_n jsou vlastní čísla, a platí

$$\mathbf{x}_k = A^k\mathbf{x}_0 = R\,\mathrm{diag}(\lambda_1^k,\ldots,\lambda_n^k)R^{-1}\mathbf{x}_0 \ .$$

Z uvedeného vztahu vyplývá, že všechny složky vektoru $\mathbf{x}_k$ jsou výrazy tvaru $c_1\lambda_1^k + \cdots + c_n\lambda_n^k$ pro vhodné konstantní skaláry $c_1, \ldots, c_k \in T$. Skutečně, označíme-li $(d_1, \ldots, d_n)^T = R^{-1}\mathbf{x}_0$, pak

$$\operatorname{diag}(\lambda_1^k, \ldots, \lambda_n^k)R^{-1}\mathbf{x}_0 = (d_1\lambda_1^k, d_2\lambda_2^k, \ldots, d_n\lambda_n^k)^T$$

a i-tá složka výsledného vektoru je potom $r_{i1}d_1\lambda_1^k + r_{i2}d_2\lambda_2^k + \cdots + r_{in}d_n\lambda_n^k$.

Příklad 9.66. Efektivněji spočítáme vzorec pro k-tý člen Fibonacciho posloupnosti z příkladu 9.65.

Protože vlastní čísla matice C jsou $\lambda_{1,2} = (1 \pm \sqrt{5})/2$, víme, že k-tý člen lze zapsat ve tvaru

$$a_k = c_1\lambda_1^k + c_2\lambda_2^k \ .$$

Dosazením $k = 0, 1$ získáme

$$\begin{aligned} 0 = a_0 &= c_1\lambda_1^0 + c_2\lambda_2^0 = c_1 + c_2 \\ 1 = a_1 &= c_1\lambda_1^1 + c_2\lambda_2^1 = c_1\lambda_1 + c_2\lambda_2 \end{aligned}$$

Vyřešením této soustavy lineárních rovnic o dvou neznámých získáme $c_1 = 1/\sqrt{5}$ a $c_2 = -1/\sqrt{5}$ a tím i odvozený vzorec. ▲

9.3.3. Geometrická násobnost, charakterizace diagonalizovatelných operátorů. Pokud chceme operátor f na konečně generovaném prostoru dimenze n diagonalizovat, musíme najít n-prvkovou lineárně nezávislou posloupnost B složenou z vlastních vektorů operátoru f. Každý z vektorů v B musí ležet v podprostoru $\mathbf{M}_\lambda$ vlastních vektorů příslušných nějakému vlastnímu číslu λ. Z něho může báze B obsahovat nanejvýš $\dim \mathbf{M}_\lambda$ prvků. Této dimenzi říkáme geometrická násobnost vlastního čísla λ.

Definice 9.67. *Geometrickou násobností* vlastního čísla λ operátoru f na konečně generovaném prostoru (nebo čtvercové matice A) rozumíme dimenzi podprostoru $\mathbf{M}_\lambda$ vlastních vektorů operátoru f (nebo matice A) příslušných vlastnímu číslu λ.

Geometrická násobnost každého vlastního čísla λ operátoru f je aspoň 1 (jinak by λ nebylo vlastní číslo). V tvrzení 9.69 dokážeme, že je menší nebo rovná algebraické násobnosti λ. K důkazu budeme potřebovat následující tvrzení o determinantech.

Tvrzení 9.68. *Pro čtvercovou blokovou matici*

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

se čtvercovými diagonálními bloky B, D platí

$$\det A = (\det B)\,(\det D) \ .$$

Důkaz. Označíme n řád matice $A = (a_{ij})$ a $k < n$ řád matice B. Důkaz uděláme indukcí podle k. Je-li $k = 1$, je $B = (a_{11})$ a všechny ostatní prvky v prvním sloupci jsou 0. Rozvineme $\det A$ podle prvního sloupce a dostaneme

$$\det A = a_{11} \det M_{11} = (\det B)\,(\det D) \ .$$

Nyní předpokládáme, že $k > 1$. Indukční předpoklad je, že determinant blokově horní trojúhelníkové matice se dvěma diagonálními bloky se rovná součinu determinantů diagonálních bloků kdykoliv má diagonální blok vlevo nahoře řád $k - 1$. Opět rozvineme $\det A$ podle prvního sloupce, tentokrát $a_{i1} = 0$ pro každé $i > k$. Dostaneme

$$\det A = (-1)^{1+1}a_{11} \det M_{11} + (-1)^{2+1}a_{21} \det M_{21} + \cdots + (-1)^{k+1}a_{k1} \det M_{k1} \ ,$$

kde M_{i1} je minor matice A vzniklý vynecháním prvního sloupce a i-tého řádku. Pro každé $i = 1, 2, \ldots, k$ je minor

$$M_{i1} = \begin{pmatrix} B_{i1} & C_i \\ 0 & D \end{pmatrix} ,$$

kde B_{i1} je minor v diagonálním bloku B vzniklý vynechnáním i-tého řádku a prvního sloupce, a C_i je matice, kterou dostaneme z bloku C vynecháním i-tého řádku. Minor M_{i1} je blokově horní trojúhelníková matice a podle indukčního předpokladu platí

$$\det M_{i1} = (\det B_{i1})\,(\det D) \ .$$

Dostáváme tak

$$\begin{aligned}\det A =&(-1)^{1+1}a_{11}\det M_{11} + (-1)^{2+1}a_{21}\det M_{21} + \cdots + (-1)^{k+1}a_{k1}\det M_{k1}\\ =&(-1)^{1+1}a_{11}(\det B_{11})\,(\det D) + \cdots + (-1)^{k+1}a_{k1}(\det B_{k1})\,(\det D)\\ =&\Big((-1)^{1+1}a_{11}(\det B_{11}) + \cdots + (-1)^{k+1}a_{k1}(\det B_{k1})\Big)\,(\det D)\\ =&(\det B)\,(\det D) \ ,\end{aligned}$$

podle věty o rozvoji determinantu podle sloupce použité na diagonální blok B. ▲

TVRZENÍ 9.69. *Pro každé vlastní číslo μ lineárního operátoru $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném prostoru $\mathbf{V}$ (čtvercové matice A) nad tělesem $\mathbf{T}$ platí, že geometrická násobnost μ je menší nebo rovná algebraické násobnosti μ.*

DŮKAZ. Buď k geometrická násobnost vlastního čísla μ operátoru f. Zvolíme nějakou bázi $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ podprostoru $\mathbf{M}_\mu$ vlastních vektorů příslušných μ a doplníme ji vektory $\mathbf{v}_{k+1}, \ldots, \mathbf{v}_n$ na bázi $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ celého prostoru $\mathbf{V}$.

Protože pro každé $i = 1, \ldots, k$ platí $[f(\mathbf{v}_i)]_B = [\mu\mathbf{v}_i]_B = \mu\mathbf{e}_i$, matice $[f]_B^B$ má blokově diagonální tvar

$$\begin{pmatrix} \mu I_k & C \\ 0 & D \end{pmatrix} ,$$

kde C je vhodný blok typu $k \times (n-k)$ a D vhodný čtvercový blok řádu $n-k$. Charakteristický polynom $p_f(\lambda)$ operátoru f se tedy rovná determinantu matice

$$[f]_B^B - \lambda I_n = \begin{pmatrix} (\mu-\lambda)I_k & C \\ 0 & D - \lambda I_{n-k} \end{pmatrix} .$$

Determinant této blokově horní trojúhelníkové matice se podle předchozího tvrzení rovná součinu determinantů diagonálních bloků. Proto

$$p_f(\lambda) = \det\left((\mu-\lambda)I_k\right)\det(D - \lambda I_{n-k}) = (\mu-\lambda)^k \det(D - \lambda I_{n-k}) \ .$$

Číslo μ je tedy aspoň k-násobným kořenem charakteristického polynomu operátoru f, jeho algebraická násobnost je proto aspoň k. ▲

Příkladem kdy nastane rovnost, je jednotková matice I_2, která má jediné vlastní číslo 1, které má geometrickou i algebraickou násobnost 2. Dále samozřejmě rovnost algebraické a geometrické násobnosti platí pro každé vlastní číslo s algebraickou násobností 1. V jistém smyslu typický případ, kdy je nerovnost ostrá, ukazuje následující příklad.

PŘÍKLAD 9.70. Reálná matice

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

má charakteristický polynom $\det A - \lambda I_2 = (\lambda-3)^2$ a tedy jediné vlastní číslo $\lambda = 3$ algebraické násobnosti 2. Podprostor vlastních vektorů příslušných vlastnímu číslu $\lambda = 3$ je

$$M_3 = \operatorname{Ker}(A - 3I_2) = \operatorname{Ker}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \mathrm{LO}\left\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right\} .$$

geometrická násobnost vlastního čísla $\lambda = 3$ je proto 1.

Tato matice není diagonalizovatelná, protože z M_3 zřejmě nelze vybrat dvoučlennou lineárně nezávislou posloupnost. ▲

Nediagonalizovatelnost operátoru nebo matice může mít dvě příčiny – nedostatek vlastních čísel (jako rotace o $\pi/2$ v příkladu 9.31) nebo nedostatek vlastních vektorů (jako v předchozím příkladu). Tím se dostáváme k charakterizaci diagonalizovatelných operátorů.

VĚTA 9.71. *Buď $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na konečně generovaném vektorovém prostoru $\mathbf{V}$ dimenze n (resp. buď A čtvercová matice řádu n) nad tělesem $\mathbf{T}$. Pak jsou následující tvrzení jsou ekvivalentní.*

(1) *Operátor f je diagonalizovatelný (resp. matice A je diagonalizovatelná).*
(2) *Operátor f (resp. matice A) má*
- *n vlastních čísel včetně algebraických násobností a*
- *geometrická násobnost každého vlastního čísla operátoru f (resp. matice A) je rovná jeho algebraické násobnosti.*

DŮKAZ. Označme $\lambda_1, \dots, \lambda_k$ všechna (navzájem různá) vlastní čísla operátoru f, $l_1, \dots, l_k$ jejich algebraické násobnosti a $m_1, \dots, m_k$ jejich geometrické násobnosti.

(1) $\Rightarrow$ (2). Předpokládáme, že je f diagonalizovatelný. Existuje tedy báze $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ prostoru $\mathbf{V}$ složená z vlastních vektorů operátoru f. Každý z vektorů v B leží v jednom z podprostorů $\mathbf{M}_{\lambda_1}$, ..., $\mathbf{M}_{\lambda_k}$, přičemž z každého podprostoru $\mathbf{M}_{\lambda_i}$ může v bázi B ležet nejvýše $\dim(\mathbf{M}_{\lambda_i}) = m_i$ vektorů (protože pouze nejvýše tolik vektorů může tvořit lineárně nezávislou posloupnost v $\mathbf{M}_{\lambda_i}$). Z toho vyplývá nerovnost $n \le m_1 + \dots + m_k$. Podle tvrzení 9.69 je geometrická násobnost menší nebo rovná algebraické násobnosti, tedy $m_i \le l_i$ (pro každé $i \in \{1, \dots, k\}$). Součet algebraických násobností je přitom nejvýše n (viz první bod důsledku 9.51). Dohromady máme

$$n \le m_1 + \dots + m_k \le l_1 + \dots + l_k \le n \quad \text{a} \quad m_i \le l_i \quad \text{pro každé} \quad i = 1, 2, \dots, k \ .$$

To znamená, že $l_1 + \dots + l_k = n$ a současně $m_i = l_i$ pro každé $i \in \{1, 2 \dots, k\}$, jak jsme chtěli dokázat.

(2) $\Rightarrow$ (1). Předpokládejme naopak, že podmínky na násobnosti jsou splněné. Pro každé $i \in \{1, \dots, k\}$ má $\mathbf{M}_{\lambda_i}$ dimenzi l_i, vezmeme jeho libovolnou bázi

$$B_i = (\mathbf{v}_1^i, \mathbf{v}_2^i, \dots, \mathbf{v}_{l_i}^i) \ .$$

Ukážeme, že posloupnost

$$B = (\mathbf{v}_1^1, \mathbf{v}_2^1, \dots, \mathbf{v}_{l_1}^1, \mathbf{v}_1^2, \mathbf{v}_2^2, \dots, \mathbf{v}_{l_2}^2, \dots, \mathbf{v}_1^k, \mathbf{v}_2^k, \dots, \mathbf{v}_{l_k}^k)$$

vytvořená ze všech vektorů všech bází podprostorů $\mathbf{M}_{\lambda_i}$ tvoří bázi prostoru $\mathbf{V}$.

Počet prvků této posloupnosti je $l_1 + l_2 + \dots + l_k = n = \dim \mathbf{V}$, stačí proto ukázat, že B je lineárně nezávislá posloupnost. Předpokládejme tedy, že pro nějaké skaláry a_j^i, $i = 1, \dots, k$ a $j = 1, \dots, l_i$, platí

$$a_1^1 \mathbf{v}_1^1 + a_2^1 \mathbf{v}_2^1 + \dots + a_{l_1}^1 \mathbf{v}_{l_1}^1 + \dots + a_1^k \mathbf{v}_1^k + a_2^k \mathbf{v}_2^k + \dots + a_{l_k}^k \mathbf{v}_{l_k}^k = \mathbf{o} \ .$$

Pro každé $i = 1, 2, \dots, k$ je vektor

$$\mathbf{w}_i = a_1^i \mathbf{v}_1^i + a_2^i \mathbf{v}_2^i + \dots + a_{l_i}^i \mathbf{v}_{l_i}^i$$

vlastní vektor operátoru f příslušný vlastnímu číslu λ_i. Dále platí

$$\mathbf{w}_1 + \mathbf{w}_2 + \dots + \mathbf{w}_k = \mathbf{o}.$$

Pokud by některý z vektorů $\mathbf{w}_i$ byl nenulový, vynechali bychom z poslední rovnosti všechny nulové vektory na levé straně a zůstal by nám součet, tj. lineární

kombinace s koeficienty 1,

$$\mathbf{w}_{i_1} + \mathbf{w}_{i_2} + \cdots + \mathbf{w}_{i_l} = \mathbf{o}$$

nenulových vlastních vektorů příslušných různým vlastním číslům $\lambda_{i_1}, \lambda_{i_2}, \ldots, \lambda_{i_l}$. To ale není možné podle věty 9.62 o lineární nezávislosti posloupnosti nenulových vlastních vektorů příslušných různým vlastním číslům.

Pro každé $i = 1, 2, \ldots, k$ tedy platí $\mathbf{w}_i = \mathbf{o}$, čili

$$\mathbf{o} = a_1^i \mathbf{v}_1^i + a_2^i \mathbf{v}_2^i + \cdots + a_{l_i}^i \mathbf{v}_{l_i}^i \ .$$

Posloupnost vektorů $B_i = (\mathbf{v}_1^i, \ldots, \mathbf{v}_{l_i}^i)$ je ale lineárně nezávislá neboť tvoří bázi $\mathbf{M}_{\lambda_i}$. Dostáváme tak, že $a_1^i = a_2^i = \cdots = a_{l_i}^i = 0$ pro každé $i = 1, 2, \ldots, k$. Posloupnost B je tedy lineárně nezávislá a tvoří proto bázi prostoru $\mathbf{V}$ složenou z vlastních vektorů operátoru f. ▲

Z důkazu vidíme, že v případě diagonalizovatelných operátorů bude v nalezené bázi B počet vlastních vektorů příslušných vlastnímu číslu λ roven algebraické (= geometrické) násobnosti λ. Proto $[f]_B^B$ bude mít na diagonále každé vlastní číslo tolikrát, kolik je jeho algebraická násobnost.

Rovněž si všimněte, že podmínku (2) lze ekvivalentně vyjádřit tak, že součet geometrických násobností všech vlastních čísel je n.

Příklad 9.72. V příkladu 9.50 jsme spočítali vlastní čísla a jejich algebraické násobnosti pro operátor $f : \mathbb{R}^3 \to \mathbb{R}^3$ definovaný předpisem

$$f\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -y + z \\ -3x - 2y + 3z \\ -2x - 2y + 3z \end{pmatrix} \ .$$

Zjistíme je-li diagonalizovatelný, a pokud ano, najdeme bázi v $\mathbb{R}^3$ složenou z vlastních vektorů operátoru f.

Operátor f je roven f_A pro matici

$$A = [f]_K^K = \begin{pmatrix} 0 & -1 & 1 \\ -3 & -2 & 3 \\ -2 & -2 & 3 \end{pmatrix} \ .$$

Charakteristický polynom operátoru f vyšel $-(\lambda - 1)^2(\lambda + 1)$, takže operátor f má vlastní číslo $\lambda_1 = 1$ algebraické násobnosti 2 a vlastní číslo $\lambda_2 = -1$ algebraické násobnosti 1. Splňuje tedy první podmínku pro diagonalizovatelnost. Zbývá ověřit rovnost algebraické a geometrické násobnosti obou vlastních čísel $\lambda_1 = 1$ a $\lambda_2 = -1$.

Algebraická násobnost vlastního čísla $\lambda_1 = 1$ je 2. Jeho geometrická násobnost se rovná dimenzi jádra matice

$$A - \lambda_1 I_3 = A - I_3 = \begin{pmatrix} -1 & -1 & 1 \\ -3 & -3 & 3 \\ -2 & -2 & 2 \end{pmatrix} \ .$$

Hodnost této matice se rovná 1, dimenze jádra je proto 2. Geometrická násobnost vlastního čísla $\lambda_1 = 1$ je rovná jeho algebraické násobnosti.

Algebraická násobnost vlastního čísla $\lambda_2 = -1$ je 1 a rovná se tak jeho geometrické násobnosti, protože ta je aspoň 1 pro jakékoliv vlastní číslo. Operátor f je tedy diagonalizovatelný.

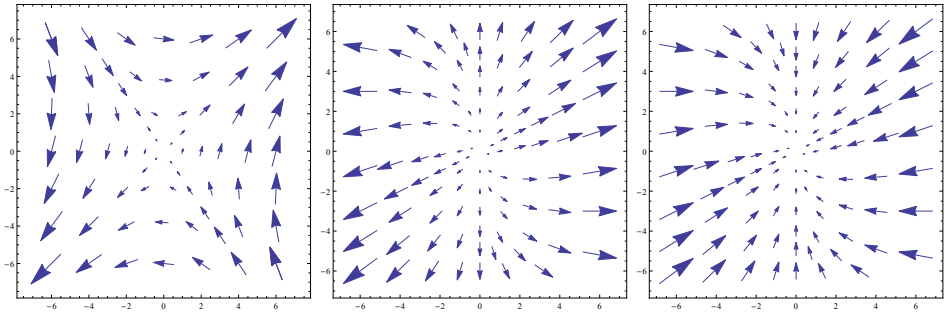
Najdeme ještě bázi $\mathbb{R}^3$, vzhledem ke které je matice operátoru f diagonální. Bázi jádra matice $A - \lambda_1 I_3 = A - I_3$, které má dimenzi 2, můžeme zvolit například $(1, 0, 1)^T$, $(0, 1, 1)^T$. Bázi jádra matice

$$A - \lambda_2 I_3 = A + I_3 = \begin{pmatrix} 1 & -1 & 1 \\ -3 & -1 & 3 \\ -2 & -2 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & 1 \\ 0 & -4 & 6 \end{pmatrix}$$

můžeme zvolit například $(1,3,2)^T$. Posloupnost $B = ((1,0,1)^T, (0,1,1)^T, (1,3,2)^T)$ tak tvoří bázi prostoru $\mathbb{R}^3$ tvořenou vlastními vektory operátoru f a platí $[f]_B^B = \operatorname{diag}(1,1,-1)$. ▲

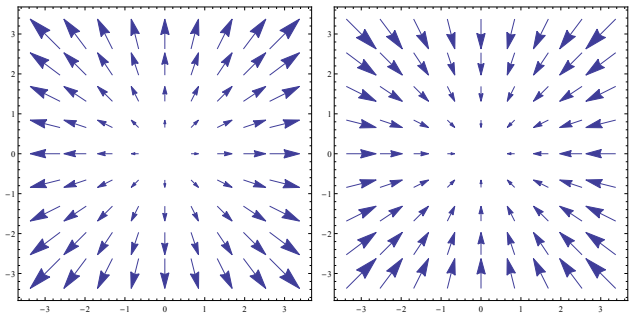
9.3.4. Lineární operátory na reálném vektorovém prostoru dimenze 2. Probereme možnosti, které mohou nastat pro diagonalizovatelný lineární operátor f na vektorovém prostoru $\mathbf{V}$ nad $\mathbb{R}$ dimenze 2.

• Operátor f má dvě různá vlastní čísla λ_1, λ_2. Pak je diagonalizovatelný. Pro představu o vývoji diskrétního dynamického systému $\mathbf{x}_{k+1} = f(\mathbf{x}_k)$ se podívejte na následující obrázek. Stejně jako v příkladu 9.12 vedou šipky z bodu $\mathbf{x}$ do bodu $f(\mathbf{x})$.



Obrázek 9.7. Dvě různá vlastní čísla. Vlevo $\lambda_1 > 1 > \lambda_2 > 0$, uprostřed $\lambda_1, \lambda_2 > 1$, vpravo $0 < \lambda_1, \lambda_2 < 1$

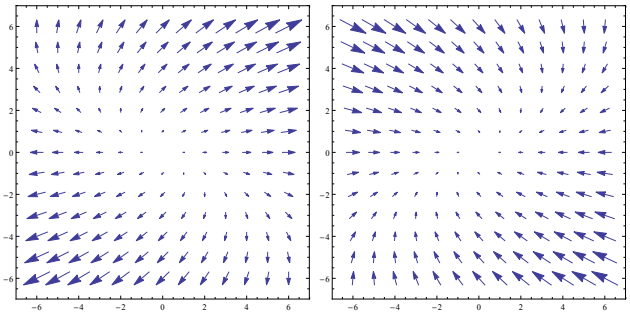
• Operátor f má jedno vlastní číslo algebraické násobnosti 2 a geometrické násobnosti 2. Pak je diagonalizovatelný, dokonce $\mathbf{M}_\lambda$ se rovná $\mathbf{V}$, tj. $f(\mathbf{x}) = \lambda\mathbf{x}$ pro každé $\mathbf{x}$. Vývoj diskrétního dynamického systému $\mathbf{x}_{k+1} = f(\mathbf{x}_k)$ si můžeme představit pomocí dalšího obrázku.



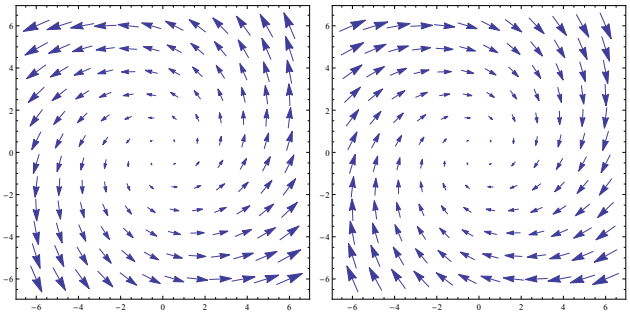
Obrázek 9.8. Jedno vlastní číslo algebraické násobnosti 2 a geometrické násobnosti 2. Vlevo $\lambda > 1$, vpravo $1 > \lambda > 0$.

• Operátor f má jedno vlastní číslo λ algebraické násobnosti 2 a geometrické násobnosti 1. Pak není diagonalizovatelný. Takovými operátory se budeme nyní zabývat v části o Jordanovu tvaru. Ilustrace je na obrázku 9.9.
• Operátor f nemá žádné vlastní číslo. Pak není diagonalizovatelný, ale můžeme si pomoci komplexními čísly, jak je diskutováno hned v následujícím odstavci. Příklady vývoje dynamického systému $\mathbf{x}_{k+1} = f_A(\mathbf{x}_k)$ jsou zobrazeny na obrázku 9.10.

9.3.5. Operátory na prostorech nad $\mathbb{R}$, které jsou „diagonalizovatelné nad $\mathbb{C}$“. Rozebereme situaci, kdy reálná matice A řádu n není diagonalizovatelná, ale stejná matice, chápaná jako matice nad $\mathbb{C}$, již diagonalizovatelná je. Podrobněji rozebereme případ $n = 2$. Diskuzi budeme provádět pouze pro matice (nebo



Obrázek 9.9. Jedno vlastní číslo algebrické násobnosti 2 a geometrické násobnosti 1. Vlevo $\lambda > 1$, vpravo $1 > \lambda > 0$.



Obrázek 9.10. Žádné reálné vlastní číslo.

operátory f_A), abychom nemuseli používat pojem komplexního rozšíření reálného vektorového prostoru a operátoru na něm.

Charakteristický polynom $p_A(\lambda)$ má v tom případě reálné koeficienty a spolu s každým komplexním vlastním číslem λ má matice A také komplexně sdružené vlastní číslo $\overline{\lambda}$. Následující jednoduché tvrzení ukazuje, že také komplexní vlastní vektory matice A můžeme sdružit do párů. Pro komplexní matici $A = (a_{ij})$ označíme $\overline{A} = (\overline{a_{ij}})$ matici, ve které každý prvek a_{ij} matice A nahradíme číslem $\overline{a_{ij}}$ komplexně sdruženým k a_{ij}. (Poněkud bizarní alternativní definice by byla $\overline{A} = (A^*)^T$.) Matice A má všechny prvky reálné právě když $\overline{A} = A$.

Tvrzení 9.73. *Je-li $\mathbf{x} \in \mathbb{C}^n$ vlastní vektor reálné matice $A = (a_{ij})$ příslušný vlastnímu číslu λ, pak $\overline{\mathbf{x}}$ je vlastní vektor matice A příslušný vlastnímu číslu $\overline{\lambda}$.*

Důkaz. Je-li $\mathbf{x} = (x_1, x_2, \dots, x_n)^T$ vlastní vektor reálné matice A příslušný vlastnímu číslu λ, platí $A\mathbf{x} = \lambda\mathbf{x}$. To znamená, že pro každé $i = 1, 2, \dots, n$ platí

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = \lambda x_i \ .$$

Rovnají se tedy také čísla komplexně sdružená k oběma stranám, tj.

$$\overline{a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n} = \overline{\lambda x_i}$$

a tedy také

$$\overline{a_{i1}}\ \overline{x_1} + \overline{a_{i2}}\ \overline{x_2} + \cdots + \overline{a_{in}}\ \overline{x_n} = \overline{\lambda}\ \overline{x_i} \ .$$

Protože A je reálná matice, platí $\overline{a_{ij}} = a_{ij}$ pro každé $i, j = 1, 2, \dots, n$ a tedy

$$a_{i1}\overline{x_1} + a_{i2}\overline{x_2} + \cdots + a_{in}\overline{x_n} = \overline{\lambda}\overline{x_i} \ .$$

pro každé $i = 1, 2, \dots, n$, což dokazuje rovnost $A\overline{\mathbf{x}} = \overline{\lambda}\overline{\mathbf{x}}$. ▲

Na konkrétním příkladu ukážeme přímočarý, ale nepříliš efektivní postup pro mocnění reálné matice, která nemá žádné reálné vlastní číslo.

PŘÍKLAD 9.74. Najdeme vzorec pro k-tou mocninu reálné matice

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

Charakteristický polynom matice A je

$$p_A(\lambda) = \lambda^2 - 2\lambda + 2 .$$

Tento polynom nemá reálné kořeny. Budeme proto považovat A za matici nad $\mathbb{C}$. Nyní má $p_A(\lambda)$ dva komplexně sdružené kořeny $\lambda = 1+i$, $\overline{\lambda} = 1-i$, matice je tedy nad $\mathbb{C}$ diagonalizovatelná.

Vlastní vektory příslušné vlastnímu číslu λ tvoří podprostor

$$M_{1+i} = \operatorname{Ker}(A - (1+i)I_2) = \operatorname{Ker}\begin{pmatrix} -i & -1 \\ 1 & -i \end{pmatrix} = \operatorname{LO}\left\{\begin{pmatrix} 1 \\ -i \end{pmatrix}\right\} .$$

Protože A je reálná matice, platí podle předchozího tvrzení 9.73, že $\mathbf{v}$ je vlastní vektor matice A příslušný komplexnímu λ právě tehdy, když je $\overline{\mathbf{v}}$ vlastní vektor matice A příslušný vlastnímu číslu $\overline{\lambda}$. Proto bez počítání víme, že

$$M_{1-i} = \operatorname{LO}\left\{\begin{pmatrix} 1 \\ i \end{pmatrix}\right\} .$$

Bázi v $\mathbb{C}^2$ z vlastních vektorů matice A zvolíme například

$$B = \left(\begin{pmatrix} 1 \\ -i \end{pmatrix}, \begin{pmatrix} 1 \\ i \end{pmatrix}\right) .$$

Pak

$$\begin{aligned} A^k =& [(f_A)^k]_K^K = [\mathrm{id}]_K^B\, [(f_A)^k]_B^B\, [\mathrm{id}]_B^K \\ =& \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix} \begin{pmatrix} (1+i)^k & 0 \\ 0 & (1-i)^k \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix}^{-1} . \end{aligned}$$

Vyjde

$$A^k = \frac{1}{2}\begin{pmatrix} (1+i)^k + (1-i)^k & i(1+i)^k - i(1-i)^k \\ -i(1+i)^k + i(1-i)^k & (1+i)^k + (1-i)^k \end{pmatrix} .$$

To je vcelku komplikovaný výraz, navíc obsahuje imaginární čísla, i když výsledek musí zřejmě být reálná matice.

Proto je v tomto případě lepší počítat s goniometrickým tvarem komplexních čísel. Je $1+i = \sqrt{2}e^{i\pi/4} = \sqrt{2}(\cos(\pi/4) + i\sin(\pi/4))$ a $1-i = \sqrt{2}e^{-i\pi/4} = \sqrt{2}(\cos(\pi/4) - i\sin(\pi/4))$. Dosazením a využitím Moivreovy věty vyjde daleko přijatelnější výsledek

$$\begin{aligned} A^k =& \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix} \begin{pmatrix} (1+i)^k & 0 \\ 0 & (1-i)^k \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix}^{-1} \\ =& \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix} \begin{pmatrix} (\sqrt{2})^k e^{ik\pi/4} & 0 \\ 0 & (\sqrt{2})^k e^{-ik\pi/4} \end{pmatrix} \frac{1}{2i} \begin{pmatrix} i & -1 \\ i & -i \end{pmatrix} \\ =& \sqrt{2}^k \begin{pmatrix} \cos(k\pi/4) & -\sin(k\pi/4) \\ \sin(k\pi/4) & \cos(k\pi/4) \end{pmatrix} . \end{aligned}$$

Stejného výsledku bychom docílili, kdybychom si hned na začátku všimli, že

$$A = \sqrt{2}\begin{pmatrix} \cos(\pi/4) & -\sin(\pi/4) \\ \sin(\pi/4) & \cos(\pi/4) \end{pmatrix} .$$

Tedy že A je matice složení rotace o $\pi/4$ a stejnolehlosti s koeficientem $\sqrt{2}$. Mocninu A^k pak vidíme geometricky okamžitě. ▲

Nyní budeme uvažovat obecnou reálnou matici A řádu 2, která nemá žádné reálné vlastní číslo. Zároveň budeme matici A chápat jako matici nad $\mathbb{C}$. Charakteristický polynom matice A má tedy dva různé komplexně sdružené kořeny λ, $\overline{\lambda}$, takže operátor $f_A : \mathbb{C}^2 \to \mathbb{C}^2$ má dvě různá komplexní vlastní čísla λ, $\overline{\lambda}$. Jako operátor $f_A : \mathbb{R}^2 \to \mathbb{R}^2$ diagonalizovatelný není (nemá žádné reálné vlastní číslo), jako operátor $f_A : \mathbb{C}^2 \to \mathbb{C}^2$ diagonalizovatelný je (dvě různá vlastní čísla). Vlastní čísla si vyjádříme v goniometrickém tvaru:

$$\lambda = re^{i\varphi} = r(\cos\varphi + i\sin\varphi), \quad \overline{\lambda} = re^{-i\varphi} = r(\cos\varphi - i\sin\varphi) \ .$$

Ukážeme, že existuje báze B prostoru $\mathbb{R}^2$ (!!) taková, že

$$[f_A]_B^B = r\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \ ,$$

tj. „vzhledem k bázi B“ se operátor $f_A : \mathbb{R}^2 \to \mathbb{R}^2$ rovná rotaci o φ složené se stejnolehlostí s koeficientem r. (Ve skutečnosti můžeme dokonce nalézt ortogonální bázi B, vzhledem ke které má operátor uvedenou matici, nemůžeme ale obecně požadovat ortonormální bázi. Výpočet je složitější, nebudeme jej provádět nyní, ale až v příští kapitole.)

Označme $\mathbf{v} \in \mathbb{C}^2$ nějaký nenulový vlastní vektor operátoru $f_A : \mathbb{C}^2 \to \mathbb{C}^2$ příslušný vlastnímu číslu λ. Podle tvrzení 9.73 víme, že $\overline{\mathbf{v}}$ je vlastní vektor operátoru $f_A : \mathbb{C}^2 \to \mathbb{C}^2$ příslušný vlastnímu číslu $\overline{\lambda}$.

Posloupnost vektorů $C = (\mathbf{v}, \overline{\mathbf{v}})$ je báze $\mathbb{C}^2$ a vzhledem k bázi C máme

$$[f_A]_C^C = \operatorname{diag}(\lambda, \overline{\lambda}) \ .$$

Označíme

$$\mathbf{w}_1 = \mathbf{v} + \overline{\mathbf{v}}, \quad \mathbf{w}_2 = i(\mathbf{v} - \overline{\mathbf{v}}) \ .$$

Vektory $\mathbf{w}_1, \mathbf{w}_2$ jsou reálné vektory, vektor $\mathbf{w}_1$ je dvojnásobek reálné části vektoru $\mathbf{v}$, vektor $\mathbf{w}_2$ je (-2)-násobek jeho imaginární části. Z definice vektorů $\mathbf{w}_1, \mathbf{w}_2$ plyne $[\mathbf{w}_1]_C = (1,1)^T$, $[\mathbf{w}_2]_C = (i,-i)^T$. Z toho vidíme, že $B = (\mathbf{w}_1, \mathbf{w}_2)$ je lineárně nezávislá posloupnost (v $\mathbb{C}^2$ i v $\mathbb{R}^2$) a tvoří tedy bázi prostoru $\mathbb{C}^2$ i $\mathbb{R}^2$. Vzhledem k této bázi máme

$$\begin{aligned} [f_A]_B^B &= [\mathrm{id}]_B^C\,[f_A]_C^C\,[\mathrm{id}]_C^B \\ &= \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}^{-1} \begin{pmatrix} r(\cos\varphi + i\sin\varphi) & 0 \\ 0 & r(\cos\varphi - i\sin\varphi) \end{pmatrix} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \end{aligned}$$

Výpočtem získáme

$$[f]_B^B = r\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \ ,$$

což jsme chtěli ukázat. Dokázali jsme tak následující tvrzení.

Tvrzení 9.75. *Je-li A reálná matice řádu 2, která nemá reálná vlastní čísla, a $\lambda = r(\cos\varphi + i\sin\varphi)$ je její komplexní vlastní číslo s nenulovým vlastním vektorem $\mathbf{v}$, pak platí*

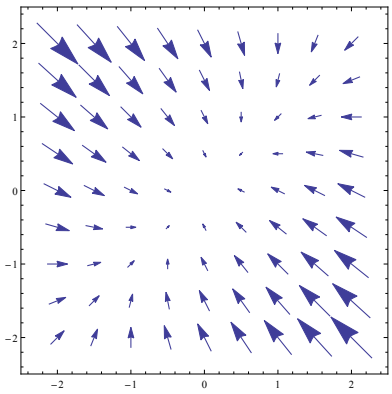
(1) *vektory $\mathbf{w}_1 = \mathbf{v} + \overline{\mathbf{v}}$ a $\mathbf{w}_2 = i(\mathbf{v} - \overline{\mathbf{v}})$ tvoří bázi $B = (\mathbf{w}_1, \mathbf{w}_2)$ prostoru $\mathbb{R}^2$,*
(2) *lineární zobrazení $f_A : \mathbb{R}^2 \to \mathbb{R}^2$ určené maticí A má vzhledem k bázi B matici*

$$[f_A]_B^B = r\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \ .$$

(To je matice složení rotace o úhel φ se stejnolehlostí s koeficientem $r > 0$.)

Na obrázku 9.10 je znázorněn vývoj dynamického systému $\mathbf{x}_{k+1} = f_A(\mathbf{x}_k)$ v této situaci, vlevo pro $|\lambda| > 1$, vpravo pro $1 > |\lambda|$, obojí v případě kdy B je ortonormální báze.

9.3.6. Vývoj reálného spojitého dynamického systému s diagonalizovatelnou maticí. Uvažujme spojitý dynamický systém $\mathbf{x}'(t) = A\mathbf{x}(t)$, kde A je reálná matice řádu n. Vektor $\mathbf{x}(t) \in \mathbb{R}^n$ může například udávat polohu pohybujícího se objektu v čase t a rovnice $\mathbf{x}'(t) = A\mathbf{x}(t)$ pak říká, že vektor rychlosti tohoto objektu je v bodě $\mathbf{x}(t)$ roven $A\mathbf{x}(t)$. Dobrou představu o řešení si můžeme udělat tak, že si do několika bodů $\mathbf{x}$ nakreslíme šipku z bodu $\mathbf{x}$ do bodu $\mathbf{x} + A\mathbf{x}$, neboli vektor $A\mathbf{x}$ s počátečním bodem $\mathbf{x}$, jako na následujícím obrázku.



OBRÁZEK 9.11. K příkladu 9.76. Šipky jsou pro přehlednost zkráceny.

Pokud je matice A diagonalizovatelná, můžeme soustavu vyřešit následujícím způsobem. V prostoru $\mathbb{R}^n$ existuje báze $B = (\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n)$ tvořená vlastními vektory matice A, přičemž vektor $\mathbf{u}_i$ je příslušný vlastnímu číslu λ_i matice A. Matice $R = (\mathbf{u}_1|\mathbf{u}_2|\cdots|\mathbf{u}_n)$ je regulární a rovná se matici přechodu $[\mathrm{id}]_K^B$ od báze B ke kanonické bázi K. Platí pro ni

$$R^{-1}AR = D = \mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n) \ .$$

Úpravou dostaneme $A = RDR^{-1}$ a dosadíme do rovnice $\mathbf{x}'(t) = A\mathbf{x}(t)$. Dostaneme tak

$$\begin{aligned} \mathbf{x}'(t) &= RDR^{-1}\mathbf{x}(t) \\ R^{-1}\mathbf{x}'(t) &= DR^{-1}\mathbf{x}(t) \end{aligned}$$

Položíme $\mathbf{y}(t) = R^{-1}\mathbf{x}(t)$. Snadno se pak ověří, že $\mathbf{y}'(t) = R^{-1}\mathbf{x}'(t)$. Stačí si uvědomit, že každá složka $y_j(t)$ vektoru $\mathbf{y}(t)$ je lineární kombinací funkcí $x_i(t)$ a tedy derivace $y_j'(t)$ je lineární kombinací derivací $x_i'(t)$ se stejnými koeficienty. Dosazením dostáváme

$$\mathbf{y}'(t) = D\mathbf{y}(t)$$

Tuto soustavu vyřešíme užitím příkladu 9.22 o řešení diferenciální rovnice $f'(t) = \lambda f(t)$. Původní funkce $\mathbf{x}(t)$ pak dopočteme ze vztahu $\mathbf{x}(t) = R\mathbf{y}(t)$.

PŘÍKLAD 9.76. Vyřešíme soustavu

$$\begin{pmatrix} x_1'(t) \\ x_2'(t) \end{pmatrix} = A \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix}$$

s počáteční podmínkou $x_1(0) = 5, x_2(0) = 7$. Charakteristický polynom matice A je $p_A(\lambda) = \lambda^2 + 4\lambda + 3$, který má dva různé reálné kořeny $\lambda_1 = -1$ a $\lambda_2 = -3$. Vlastní vektory příslušné vlastnímu číslu $\lambda_1 = -1$ tvoří lineární obal $\mathrm{LO}\left\{(1,1)^T\right\}$. Vlastní vektory příslušné vlastnímu číslu $\lambda_2 = -3$ tvoří linerání obal $\mathrm{LO}\left\{(1,-1)^T\right\}$. Položíme $B = ((1,1)^T, (1,-1)^T)$. Pak

$$R = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

a

$$D = R^{-1}AR = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \ .$$

Původní soustavu si přepíšeme do tvaru

$$R^{-1} \begin{pmatrix} x_1'(t) \\ x_2'(t) \end{pmatrix} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} R^{-1} \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix} \ .$$

Označíme

$$\begin{pmatrix} y_1(t) \\ y_2(t) \end{pmatrix} = R^{-1} \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix} .$$

Obě funkce $y_i(t)$ jsou lineární kombinace funkcí $x_1(t), x_2(t)$ s konstantními koeficienty v i-tém řádku matice R^{-1}. Platí proto

$$\begin{pmatrix} y_1'(t) \\ y_2'(t) \end{pmatrix} = R^{-1} \begin{pmatrix} x_1'(t) \\ x_2'(t) \end{pmatrix} .$$

Dvojice funkcí $y_1(t), y_2(t)$ tak splňuje soustavu lineárních diferenciálních rovnic

$$\begin{pmatrix} y_1'(t) \\ y_2'(t) \end{pmatrix} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \begin{pmatrix} y_1(t) \\ y_2(t) \end{pmatrix} = \begin{pmatrix} \lambda_1 y_1(t) \\ \lambda_2 y_2(t) \end{pmatrix} .$$

Tu už umíme řešit: $y_1(t) = y_1(0)e^{-t}$ a $y_2(t) = y_2(0)e^{-3t}$, kde

$$\begin{pmatrix} y_1(0) \\ y_2(0) \end{pmatrix} = R^{-1} \begin{pmatrix} x_1(0) \\ x_2(0) \end{pmatrix} .$$

Spočítáme původní funkce:

$$\begin{aligned}
\begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix} &= R \begin{pmatrix} y_1(t) \\ y_2(t) \end{pmatrix} = R \begin{pmatrix} y_1(0)e^{\lambda_1 t} \\ y_2(0)e^{\lambda_2 t} \end{pmatrix} = R \begin{pmatrix} e^{\lambda_1 t} & 0 \\ 0 & e^{\lambda_2 t} \end{pmatrix} \begin{pmatrix} y_1(0) \\ y_2(0) \end{pmatrix} \\
&= R \begin{pmatrix} e^{\lambda_1 t} & 0 \\ 0 & e^{\lambda_2 t} \end{pmatrix} R^{-1} \begin{pmatrix} x_1(0) \\ x_2(0) \end{pmatrix} \\
&= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} e^{\lambda_1 t} & 0 \\ 0 & e^{\lambda_2 t} \end{pmatrix} \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 5 \\ 7 \end{pmatrix} \\
&= \begin{pmatrix} 6e^{-t} - e^{-3t} \\ 6e^{-t} + e^{-3t} \end{pmatrix} .
\end{aligned}$$

▲

Z postupu při řešení předchozího příkladu můžeme nahlédnout, že pro obecnou diagonalizovatelnou matici A můžeme řešení spojitého dynamického systému $\mathbf{x}'(t) = A\mathbf{x}(t)$ vyjádřit ve tvaru řešením soustavy

$$\mathbf{x}(t) = R\,\mathrm{diag}(e^{\lambda_1 t}, \dots, e^{\lambda_n t})R^{-1}\mathbf{x}(0) ,$$

kde $A = R\ \mathrm{diag}(\lambda_1, \dots, \lambda_n)\, R^{-1}$.

Pro zajímavost uveďme, že matice $R\,\mathrm{diag}(e^{\lambda_1 t}, \dots, e^{\lambda_n t})R^{-1}$ je rovna tzv. exponenciále matice tA a značí se e^{tA}. To dává smysl, protože „dosadíme-li“ matici tA do Taylorovy řady funkce e^x máme

$$\begin{aligned}
& I_n + tA + t^2\frac{A^2}{2!} + t^3\frac{A^3}{3!} + \dots + t^k\frac{A^k}{k!} + \dots \\
= \quad & I_n + tRDR^{-1} + t^2\frac{RD^2R^{-1}}{2!} + t^3\frac{RD^3R^{-1}}{3!} + \dots + t^k\frac{RD^kR^{-1}}{k!} + \dots \\
= \quad & R\left(I_n + tD + \frac{(tD)^2}{2!} + \frac{(tD)^3}{3!} + \dots + \frac{(tD)^k}{k!} + \dots\right)R^{-1} \\
= \quad & R\,\mathrm{diag}(e^{\lambda_1 t}, \dots, e^{\lambda_n t})R^{-1} .
\end{aligned}$$

Řešení soustavy $\mathbf{x}'(t) = A\mathbf{x}(t)$ pak můžeme psát ve tvaru

$$\mathbf{x}(t) = e^{tA}\mathbf{x}(0) ,$$

zcela analogicky k vyjádření $f(t) = e^{t\lambda}f(0)$ jako řešení diferenciální rovnice $f' = \lambda f$.

Příklad 9.77. Vyřešíme ještě spojitý dynamický systém z příkladu 9.6 popisující přechod substance přes buněčnou blánu. Ten vede k soustavě

$$\begin{aligned}
u_1'(t) &= -ru_1(t) + su_2(t) , \\
u_2'(t) &= ru_1(t) - su_2(t) .
\end{aligned}$$

s počáteční podmínkou $u_1(0) = 1$, $u_2(0) = 0$. Matice soustavy

$$A = \begin{pmatrix} -r & s \\ r & -s \end{pmatrix}$$

má charakteristický polynom $p(\lambda) = \lambda^2 + (r+s)\lambda$ a tudíž dvě různá vlastní čísla $\lambda_1 = 0$ a $\lambda_2 = -(r+s)$, odtud plyne její diagonalizovatelnost.

Vlastní vektory příslušné vlastnímu číslu $\lambda_1 = 0$ tvoří jádro matice

$$A - 0I_2 = \begin{pmatrix} -r & s \\ r & -s \end{pmatrix} ,$$

který se rovná lineárnímu obalu $\mathrm{LO}\left\{(s,r)^T\right\}$.

Vlastní vektory příslušné vlastnímu číslu $\lambda_2 = -(r+s)$ tvoří jádro matice

$$A + (r+s)I_2 = \begin{pmatrix} s & s \\ r & r \end{pmatrix} ,$$

který se rovná lineárnímu obalu $\mathrm{LO}\left\{(1,-1)^T\right\}$. Zvolíme bázi $B = ((s,r)^T, (1,-1)^T))$. Pak

$$R = [\mathrm{id}]_K^B = \begin{pmatrix} s & 1 \\ r & -1 \end{pmatrix}, \quad R^{-1} = \frac{-1}{r+s}\begin{pmatrix} -1 & -1 \\ -r & s \end{pmatrix} .$$

Soustava má řešení

$$\begin{aligned} \begin{pmatrix} u_1(t) \\ u_2(t) \end{pmatrix} &= \begin{pmatrix} s & 1 \\ r & -1 \end{pmatrix}\begin{pmatrix} e^{0t} & 0 \\ 0 & e^{-(r+s)t} \end{pmatrix}\frac{-1}{r+s}\begin{pmatrix} -1 & -1 \\ -r & s \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \frac{1}{r+s}\begin{pmatrix} s + re^{-(r+s)t} \\ r - re^{-(r+s)t} \end{pmatrix} . \end{aligned}$$

Vidíme, že pro $t \to \infty$ hodnota $u_1(t)$ konverguje k $\frac{s}{r+s}$ a hodnota $u_2(t)$ konverguje k $\frac{r}{r+s}$. ▲

V následujícím příkladu si ukážeme, jak se vyvíjí spojitý dynamický systém $\mathbf{x}'(t) = A\mathbf{x}(t)$ v dimenzi 2 v případě, že reálná matice A nemá žádné reálné vlastní číslo.

Příklad 9.78. Spočítáme vlastní kmity pružiny se závažím. V příkladu 9.5 jsme odvodili, že vlastní kmity jsou popsané spojitým dynamickým systémem

$$\mathbf{x}'(t) = \begin{pmatrix} x_1'(t) \\ x_2'(t) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -\frac{k}{m} & 0 \end{pmatrix}\begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -\frac{k}{m} & 0 \end{pmatrix}\mathbf{x}(t) ,$$

kde k označuje koeficient pružnosti pružiny a m hmotnost závaží. Proto $k/m > 0$ existuje jednoznačně určené reálné číslo $\omega > 0$, pro které platí $k/m = \omega^2$. Řešíme tedy spojitý dynamický systém s maticí

$$A = \begin{pmatrix} 0 & 1 \\ -\omega^2 & 0 \end{pmatrix}$$

s libovolným počátečním stavem $\mathbf{x}(0) = (p_1, p_2)^T$. Charakteristický polynom matice A je $p_A\lambda = \lambda^2 + \omega^2$ a má imaginární kořeny $\lambda_{1,2} = \pm\, i\,\omega$. Matice A je tedy diagonalizovatelná pouze nad $\mathbb{C}$, nikoliv nad $\mathbb{R}$. Množina všech vlastních vektorů matice A příslušných vlastnímu číslu $\lambda = i\omega$ se rovná

$$M_{i\omega} = \mathrm{Ker}\begin{pmatrix} -i\omega & 1 \\ -\omega^2 & -i\omega \end{pmatrix} = \mathrm{LO}\left\{\begin{pmatrix} 1 \\ i\omega \end{pmatrix}\right\}$$

a podle tvrzení 9.73 je

$$M_{-i\omega} = \mathrm{LO}\left\{\begin{pmatrix} 1 \\ -i\omega \end{pmatrix}\right\} .$$

Pro matici

$$R = \begin{pmatrix} 1 & 1 \\ i\omega & -i\omega \end{pmatrix}$$

pak platí

$$R^{-1}AR = \begin{pmatrix} i\omega & 0 \\ 0 & -i\omega \end{pmatrix} .$$

Dynamický systém $\mathbf{x}'(t) = A\mathbf{x}(t)$ upravíme do tvaru

$$R^{-1}\mathbf{x}'(t) = \begin{pmatrix} i\omega & 0 \\ 0 & -i\omega \end{pmatrix} R^{-1}\mathbf{x}(t) .$$

a vyřešíme pro nový neznámý vektor $\mathbf{y}(t) = (y_1(t), y_2(t))^T = R^{-1}\mathbf{x}(t)$ s novým počátečním stavem $\mathbf{y}_0 = (y_1(0), y_2(0))^T = R^{-1}\mathbf{x}_0$. Spojitý dynamický systém

$$\begin{pmatrix} y_1'(t) \\ y_2'(t) \end{pmatrix} = \begin{pmatrix} i\omega & 0 \\ 0 & -i\omega \end{pmatrix}\begin{pmatrix} y_1(t) \\ y_2(t) \end{pmatrix}$$

se rozpadá na dva komplexní spojité dynamické systémy

$$\begin{aligned} y_1'(t) &= (i\omega)y_1(t) \\ y_2'(t) &= (-i\omega)y_2(t) \end{aligned}$$

v dimenzi 1 a v závěru úvodní motivační části 9.1 jsme si ukázali, že má řešení

$$\begin{aligned} y_1(t) &= y_1(0)e^{i\omega t} \\ y_2(t) &= y_2(0)e^{-i\omega t} , \end{aligned}$$

což můžeme přepsat do tvaru

$$\begin{pmatrix} y_1(t) \\ y_2(t) \end{pmatrix} = \begin{pmatrix} e^{i\omega t} & 0 \\ 0 & e^{-i\omega t} \end{pmatrix} \begin{pmatrix} y_1(0) \\ y_2(0) \end{pmatrix} .$$

Spočteme ještě matici

$$R^{-1} = \frac{1}{2\omega} \begin{pmatrix} \omega & -i \\ \omega & i \end{pmatrix}$$

a vyjádříme řešení původního spojitého dynamického systému $\mathbf{x}'(t) = A\mathbf{x}(t)$ s počáteční podmínkou $\mathbf{x}(0) = (p_1, p_2)^T$ ve tvaru

$$\mathbf{x}(t) = R\mathbf{y}(t) = \begin{pmatrix} 1\omega & 1 \\ i\omega & -i\omega \end{pmatrix} \begin{pmatrix} e^{i\omega t} & 0 \\ 0 & e^{-i\omega t} \end{pmatrix} \frac{1}{2\omega} \begin{pmatrix} \omega & -i \\ \omega & i \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} .$$

Po delším počítání s využitím Eulerovy formule $e^{i\omega t} = \cos(\omega t) + i\sin(\omega t)$ dostaneme výsledek

$$\begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix} = \begin{pmatrix} p_1\cos(\omega t) + (1/\omega)p_2\sin(\omega t) \\ -\omega p_1\sin(\omega t) + p_2\cos(\omega t) \end{pmatrix} .$$

Abychom pochopili trajektorii bodu $(x_1(t), x_2(t))^T$ v rovině $\mathbb{R}^2$, vynásobíme první složku $x_1(t)$ číslem ω a spočteme součet čtverců

$$\begin{aligned} (\omega x_1(t))^2 + (x_2(t))^2 &= (\omega p_1\cos(\omega t) + p_2\sin(\omega t))^2 + (-\omega p_1\sin(\omega t) + p_2\cos(\omega t))^2 \\ &= \omega^2 p_1^2\cos^2(\omega t) + p_2^2\sin^2(\omega t) + 2\omega p_1 p_2\cos(\omega t)\sin(\omega t) \\ &+ \omega^2 p_1^2\sin^2(\omega t) + p_2^2\cos^2(\omega t) - 2\omega p_1 p_2\cos(\omega t)\sin(\omega t) \\ &= \omega^2 p_1^2 + p_2^2 . \end{aligned}$$

Vidíme tedy, že bod $(x_1(t), x_2(t))^T$ se pohybuje po elipse se středem v počátku a poloosami délky $\sqrt{\omega^2 p_1^2 + p_2^2}/\omega$ ve směru osy x_1 a délky $\sqrt{\omega^2 p_1^2 + p_2^2}$ ve směru osy x_2.

Ve speciálním případě, kdy $\omega = 1$, se bod $(x_1, x_2)^T$ pohybuje po kružnici se středem v počátku o poloměru $\sqrt{p_1^2 + p_2^2}$ s konstantní úhlovou rychlostí $-\omega = -1$, tj. po směru hodinových ručiček. Směr pohybu a fázový posun zjistíme nejsnáze pomocí komplexních čísel. Použijeme goniometrický tvar $p_1 + ip_2 = re^{i\varphi}$ pro počáteční podmínku a spočteme

$$\begin{aligned} x_1(t) + ix_2(t) &= p_1\cos t + p_2\sin t - ip_1\sin t + ip_2\cos t = (p_1 + ip_2)(\cos t - i\sin t) \\ &= r\,e^{i\varphi}e^{-it} = r\,e^{i(-t+\varphi)} . \end{aligned}$$

Spočítali jsme tak, že fázový posun se rovná φ. ▲

9.4. Jordanův kanonický tvar

Jak jsme dokázali ve větě 9.71, lineární operátor na prostoru dimenze n může být nediagonalizovatelný ze dvou důvodů – součet algebraických násobností vlastních čísel je menší než n nebo geometrická násobnost nějakého vlastního čísla je menší než jeho algebraická násobnost. První příčinu lze obejít tím, že pracujeme ve větším tělese (například místo $\mathbb{R}$ v $\mathbb{C}$). Druhá příčina takto obejít nejde, musíme slevit z požadavku diagonalizovatelnosti. Naštěstí lze v případě splnění první podmínky na algebraické násobnosti vždy najít bázi, vzhledem ke které má operátor „téměř“ diagonální matici, přesněji tzv. matici v Jordanově tvaru. Mocninu takové matice stále lze explicitně vypočítat, tedy lze také spočítat libovolnou mocninu příslušného operátoru.

9.4.1. Nediagonalizovatelné operátory v dimenzi 2. V odstavci 9.3.4 jsme probrali možnosti, jaké mohou nastat pro operátory na reálném vektorovém prostoru dimenze 2. Zbyl jediný případ, který nyní podrobně rozebereme. Diskuze také snad poslouží k orientaci v obecnějších pojmech a tvrzeních.

Uvažujme tedy operátor f na vektorovém prostoru $\mathbf{V}$ dimenze 2 nad tělesem $\mathbf{T}$, který má jedno vlastní číslo λ algebraické násobnosti 2 a geometrické násobnosti

1. Ukážeme, že v takovém případě existuje báze $B = (\mathbf{u}, \mathbf{v})$ prostoru $\mathbf{V}$, vzhledem ke které má operátor f matici

$$[f]_B^B = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} .$$

To je nejjednodušší příklad matice v tzv. Jordanově tvaru, která není diagonální. Takovou matici umíme umocnit, platí totiž

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

Když takovou bázi B najdeme, budeme umět spočítat $[f^m]_B^B = ([f]_B^B)^m$ a tím pádem například vyřešit diskrétní dynamický systém $\mathbf{x}_m = f(\mathbf{x}_{m-1})$. Obecně je Jordanův tvar a mocnění rozebráno v odstavci 9.4.2.

Hledání báze B začneme přeformulováním podmínky na matici $[f]_B^B$. Podle definice matice f vzhledem k B a B potřebujeme, aby platilo

$$[f(\mathbf{u})]_B = \begin{pmatrix} \lambda \\ 0 \end{pmatrix}, \quad [f(\mathbf{v})]_B = \begin{pmatrix} 1 \\ \lambda \end{pmatrix} .$$

Podle definice souřadnic vzhledem k bázi tedy chceme, aby

$$f(\mathbf{u}) = \lambda\mathbf{u}, \quad f(\mathbf{v}) = \mathbf{u} + \lambda\mathbf{v} .$$

Označíme-li g operátor $f - \lambda\,\mathrm{id}_V$ můžeme tyto podmínky zapsat

$$g(\mathbf{u}) = \mathbf{o}, \quad g(\mathbf{v}) = \mathbf{u} ,$$

schematicky

$$\mathbf{v} \xmapsto{\;g\;} \mathbf{u} \xmapsto{\;g\;} \mathbf{o} .$$

Potřebujeme tedy, aby $\mathbf{u}$ byl vlastní vektor operátoru f příslušný vlastnímu číslu λ a aby $g(\mathbf{v}) = \mathbf{u}$. Obecně je toto přeformulování provedeno v odstavci 9.4.3.

Dále ukážeme, že kdykoliv máme vektory $\mathbf{u}, \mathbf{v}$ splňující podmínky $g(\mathbf{v}) = \mathbf{u}$, $g(\mathbf{u}) = \mathbf{o}$ a vektor $\mathbf{u}$ je nenulový, pak $B = (\mathbf{u}, \mathbf{v})$ je lineárně nezávislá posloupnost, tedy báze $\mathbf{V}$. Skutečně, je-li

$$a\mathbf{v} + b\mathbf{u} = \mathbf{o} ,$$

pak aplikací operátoru g na obě strany dostaneme

$$\begin{aligned} g(a\mathbf{v} + b\mathbf{u}) &= g(\mathbf{o}) \\ ag(\mathbf{v}) + bg(\mathbf{u}) &= \mathbf{o} \\ a\mathbf{u} &= \mathbf{o} . \end{aligned}$$

Protože je $\mathbf{u}$ nenulový vektor, plyne odsud $a = 0$. Dosazením do původního vztahu získáme $b\mathbf{u} = \mathbf{o}$, takže i $b = 0$. Obecné tvrzení je dokázáno v odstavci 9.4.4

V odstavci 9.4.5 probereme, jak takové vektory obecně hledat za předpokladu, že existují (v odstavcích 9.4.6, 9.4.7, 9.4.8, 9.4.9 ukážeme postup na řadě příkladů). Důkaz, že skutečně existují, využívá pojem invariantního podprostoru diskutovaného v odstavci 9.4.10, samotný důkaz je pak obsažen v odstavci 9.4.11.

V našem případě označme $\mathbf{W} = \operatorname{Im} g$. Tento prostor je invariantní ve smyslu, že $g(\mathbf{x}) \in W$ kdykoliv $\mathbf{x} \in W$. Skutečně, $g(\mathbf{x})$ leží v $\operatorname{Im} g$ pro jakýkoliv vektor $\mathbf{x}$ ve V, nejen pro vektory z W.

Podprostor $\operatorname{Ker} g \leq \mathbf{V}$ je tvořen všemi vlastními vektory operátoru f příslušnými vlastnímu číslu λ. Protože geometrická násobnost vlastního čísla λ je podle předpokladu 1, je $\dim \operatorname{Ker} g = 1$. Podle věty o dimenzi jádra a obrazu je $\dim(\operatorname{Im} g) = \dim \mathbf{W} = 1$. Vezmeme libovolný nenulový vektor $\mathbf{u} \in W$. Protože $\mathbf{W}$ má dimenzi 1, je vektor $g(\mathbf{u}) \in W$ násobkem vektoru $\mathbf{u}$, tj. $g(\mathbf{u}) = a\mathbf{u}$ pro nějaký skalár $a \in T$. Pak ale $(f - \lambda\,\mathrm{id}_V)\mathbf{u} = a\mathbf{u}$, takže $f(\mathbf{u}) = (\lambda + a)\mathbf{u}$. Protože f má jediné vlastní číslo λ, musí být nutně $a = 0$, platí tedy $g(\mathbf{u}) = \mathbf{o}$. Vektor $\mathbf{u}$ leží ve

$W = \operatorname{Im} g$, existuje proto vektor $\mathbf{v} \in V$ takový, že $g(\mathbf{v}) = \mathbf{u}$, a důkaz je hotov – nalezli jsme vektory $\mathbf{u}, \mathbf{v} \in V$ takové, že $g(\mathbf{v}) = \mathbf{u}$, $g(\mathbf{u}) = \mathbf{o}$ a $\mathbf{u} \neq \mathbf{o}$, což znamená, že pro bázi $B = (\mathbf{u}, \mathbf{v})$ v prostoru $\mathbf{V}$ platí

$$[f]_B^B = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} .$$

9.4.2. Matice v Jordanově tvaru. Matice v Jordanově tvaru je blokově diagonální matice, jejíž bloky tvoří Jordanovy buňky. Jordanova buňka je matice, která má všechny diagonální prvky rovny nějakému $\lambda \in T$ a všechny prvky o jednu pozici nad diagonálou rovny 1.

Definice 9.79. *Jordanova buňka* řádu $k \geq 1$ nad tělesem $\mathbf{T}$ příslušná prvku $\lambda \in T$ je čtvercová matice

$$J_{\lambda,k} = \begin{pmatrix} \lambda & 1 & 0 & & 0 & 0 \\ 0 & \lambda & 1 & \dots & 0 & 0 \\ 0 & 0 & \lambda & & 0 & 0 \\ & \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda \end{pmatrix} .$$

Příklad 9.80. Reálné matice

$$\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix}, \quad (4)$$

jsou Jordanovy buňky $J_{2,2}$, $J_{0,2}$, $J_{3,3}$, $J_{4,1}$ (příslušné po řadě číslům $2, 0, 3, 4$). ▲

Definice 9.81. Matice J nad tělesem $\mathbf{T}$ je v *Jordanově kanonickém tvaru* (nebo stručněji v *Jordanově tvaru*), pokud J je blokově diagonální matice, jejíž každý diagonální blok je Jordanova buňka (nějakého řádu příslušná nějakému číslu), tj.

$$J = \operatorname{diag}(J_{\lambda_1,k_1}, \dots, J_{\lambda_s,k_s}) = \begin{pmatrix} J_{\lambda_1,k_1} & 0 & \dots & 0 \\ 0 & J_{\lambda_2,k_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_{\lambda_s,k_s} \end{pmatrix} ,$$

kde $\lambda_1, \dots, \lambda_s \in T$ a $k_1, \dots, k_s$ jsou kladná celá čísla. (Nuly v matici v tomto případě značí nulové matice vhodných typů.)

Příklad 9.82. Diagonální matice $\operatorname{diag}(\lambda_1, \dots, \lambda_n)$ je v Jordanově tvaru. Je složená z Jordanových buněk $J_{\lambda_1,1}$, ..., $J_{\lambda_n,1}$ řádu 1. ▲

Příklad 9.83. Matice

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

je v Jordanově tvaru. Je složená z Jordanových buněk $J_{0,2}$, $J_{0,1}$, $J_{2,3}$. ▲

Nyní najdeme vzorec pro mocninu Jordanovy matice. Matici

$$J = \begin{pmatrix} J_1 & 0 & \dots & 0 \\ 0 & J_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_s \end{pmatrix}$$

v blokově diagonálním tvaru můžeme mocnit po diagonálních blocích:

$$J^m = \begin{pmatrix} J_1 & 0 & \dots & 0 \\ 0 & J_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_s \end{pmatrix}^m = \begin{pmatrix} J_1^m & 0 & \dots & 0 \\ 0 & J_2^m & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_s^m \end{pmatrix} .$$

Stačí se proto zaměřit pouze na mocnění Jordanových buněk.

Jednoduchý je speciální případ Jordanových buněk příslušných prvku 0.

Tvrzení 9.84. *Pro libovolná přirozená čísla $m < k$ platí*

$$J_{0,k}^m = (\underbrace{\mathbf{o}|\cdots|\mathbf{o}}_{m\times}|\mathbf{e}_1|\mathbf{e}_2|\cdots|\mathbf{e}_{k-m})$$

Pro $m \geq k$ je $J_{0,k}^m = 0$.

Důkaz. Indukcí podle $m < k$, případ $m = 1$ je zjevný, neboť $J_{0,k} = (\mathbf{o}|\mathbf{e}_1|\mathbf{e}_2|\cdots|\mathbf{e}_{k-1})$. Platí-li tvrzení pro nějaké m menší než k, máme ze sloupcového pohledu na násobení

$$\begin{aligned} J_{0,k}^{m+1} &= J_{0,k}^m J_{0,k} = (\underbrace{\mathbf{o}|\dots|\mathbf{o}}_{m\times}|\mathbf{e}_1|\mathbf{e}_2|\dots|\mathbf{e}_{k-m})(\mathbf{o}|\mathbf{e}_1|\mathbf{e}_2|\dots|\mathbf{e}_{k-1}) \\ &= (\underbrace{\mathbf{o}|\dots|\mathbf{o}}_{(m+1)\times}|\mathbf{e}_1|\dots|\mathbf{e}_{k-(m+1)}) \ . \end{aligned}$$

Pro $m \geq k$ je indukční krok zřejmý, neboť $J_{0,k}^m = 0$. ▲

Příklad 9.85.

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

▲

Jordanovu buňku $J_{\lambda,k}$ můžeme rozepsat

$$J_{\lambda,k} = \lambda I_k + J_{0,k}$$

Pokud dvě čtvercové matice A, B komutují, tj. platí-li $AB = BA$, pak pro ně platí obdoba binomické věty (cvičení)

$$(A+B)^m = \binom{m}{0}A^m + \binom{m}{1}A^{m-1}B + \binom{m}{2}A^{m-2}B^2 + \dots + \binom{m}{m}B^m \ .$$

Použitím na matice λI_k a $J_{0,k}$ dostaneme vzorec v následujícím tvrzení. Používáme konvenci, že binomické číslo $\binom{m}{j} = 0$ pokud $m < j$. Dále pro $i \in \{0, 1, \dots\}$ a prvek t v tělese $\mathbf{T}$ definujeme it jako $\underbrace{t + t + \dots + t}_{i\times}$.

Tvrzení 9.86. *Buď $\lambda \neq 0$ a buďte k, m kladná přirozená čísla. Potom pro mocniny Jordanovy buňky platí*

$$J_{\lambda,k}^m = \begin{pmatrix} \lambda^m & \binom{m}{1}\lambda^{m-1} & \binom{m}{2}\lambda^{m-2} & \dots & \binom{m}{k-1}\lambda^{m-k+1} \\ 0 & \lambda^m & \binom{m}{1}\lambda^{m-1} & \dots & \binom{m}{k-2}\lambda^{m-k+2} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda^m & \binom{m}{1}\lambda^{m-1} \\ 0 & 0 & \dots & 0 & \lambda^m \end{pmatrix} .$$

Důkaz. Jeden z možných výpočtů byl naznačen před tvrzením, ukážeme alternativní důkaz.

Pro ℓ záporné položme $\binom{m}{\ell} = 0$. Lze se snadno přesvědčit, že toto zobecnění kombinačních čísel zachovává platnost vzorečku $\binom{m}{\ell} + \binom{m}{\ell-1} = \binom{m+1}{\ell}$ pro všechna $\ell \in \mathbb{Z}$.

Tvrdíme, že prvek na místě (i,j) v mocnině $J^m_{\lambda,k}$ lze zapsat jako $\binom{m}{j-i}\lambda^{m-(j-i)}$. K důkazu lze použít indukci podle m, případ $m = 1$ je zjevný. Pokud formulka platí pro $m \geq 1$, spočítáme $J^{m+1}_{\lambda,k} = J_{\lambda,k}J^m_{\lambda,k}$. Obě matice, které násobíme, jsou horní trojúhelníkové, součin je proto také horní trojúhelníkový. Zbývá spočítat prvky na místě (i,j) v součinu $J_{\lambda,k}J^m_{\lambda,k}$ pro $i \leq j$. Prvek na místě (i,j) v matici $J^m_{\lambda,k}$ se podle indukčního předpokladu rovná $\binom{m}{j-i}\lambda^{m-(j-i)}$. Prvek na místě (i,j) v matici $J_{\lambda,k}J^m_{\lambda,k}$ se pak rovná

$$\begin{aligned}
& \lambda\binom{m}{j-i}\lambda^{m-(j-i)} + 1\binom{m}{j-(i+1)}\lambda^{m-(j-i-1)} \\
= \; & \binom{m}{j-i}\lambda^{m+1-(j-i)} + \binom{m}{j-i-1}\lambda^{m+1-(j-i)} \\
= \; & \binom{m+1}{j-i}\lambda^{m+1-(j-i)} \;,
\end{aligned}$$

kde jsme na poslední řádce použili vztah $\binom{m}{\ell} + \binom{m}{\ell-1} = \binom{m+1}{\ell}$. ▲

9.4.3. Operátory s Jordanovým tvarem. Chceme zjistit, zda daný operátor f na konečně generovaném prostoru má vzhledem k nějaké bázi B matici v Jordanově tvaru, jak takovou bázi najít, a z jakých buněk se matice $[f]^B_B$ skládá.

Formulujeme obdobu definice 9.54 diagonalizovatelnosti. Pojem „jordanizovatelnost“ se nepoužívá, raději říkáme, že pro operátor existuje Jordanův kanonický tvar.

Definice 9.87. Říkáme, že pro lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném prostoru $\mathbf{V}$ *existuje Jordanův kanonický tvar*, pokud má vzhledem k nějaké bázi matici v Jordanově kanonickém tvaru.

Odvodíme obdobu tvrzení 9.56. Nejprve pro samotné buňky. Kdy má operátor $f : \mathbf{V} \to \mathbf{V}$ vzhledem k nějaké bázi $B = (\mathbf{v}_1, \dots, \mathbf{v}_k)$ matici $[f]^B_B = J_{\lambda,k}$? Podle definice matice operátoru musí platit (a stačí)

$$[f(\mathbf{v}_1)]_B = \begin{pmatrix} \lambda \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad [f(\mathbf{v}_2)]_B = \begin{pmatrix} 1 \\ \lambda \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, [f(\mathbf{v}_k)]_B = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ \lambda \end{pmatrix} \;,$$

neboli

$$f(\mathbf{v}_1) = \lambda\mathbf{v}_1,\; f(\mathbf{v}_2) = \lambda\mathbf{v}_2 + \mathbf{v}_1,\; f(\mathbf{v}_3) = \lambda\mathbf{v}_3 + \mathbf{v}_2,\; \dots, f(\mathbf{v}_k) = \lambda\mathbf{v}_k + \mathbf{v}_{k-1} \;.$$

Úpravou (podobně jako v části 9.2.2) dostaneme ekvivalentně

$$\begin{aligned}
& (f - \lambda\,\mathrm{id}_V)(\mathbf{v}_1) = \mathbf{o},\; (f - \lambda\,\mathrm{id}_V)(\mathbf{v}_2) = \mathbf{v}_1,\; (f - \lambda\,\mathrm{id}_V)(\mathbf{v}_3) = \mathbf{v}_2,\; \dots, \\
& (f - \lambda\,\mathrm{id}_V)(\mathbf{v}_k) = \mathbf{v}_{k-1} \;,
\end{aligned}$$

schematicky

$$\mathbf{v}_k \xmapsto{f-\lambda\,\mathrm{id}_V} \mathbf{v}_{k-1} \xmapsto{f-\lambda\,\mathrm{id}_V} \dots \xmapsto{f-\lambda\,\mathrm{id}_V} \mathbf{v}_3 \xmapsto{f-\lambda\,\mathrm{id}_V} \mathbf{v}_2 \xmapsto{f-\lambda\,\mathrm{id}_V} \mathbf{v}_1 \xmapsto{f-\lambda\,\mathrm{id}_V} \mathbf{o} \;.$$

Vidíme, že v tom případě je λ vlastní číslo operátoru f, a že $\mathbf{v}_1$ je vlastní vektor příslušný λ. Posloupnosti $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ budeme říkat Jordanův řetízek, vektorům $\mathbf{v}_2, \dots, \mathbf{v}_k$ se někdy říká *zobecněné vlastní vektory* příslušné vlastnímu číslu λ.

Definice 9.88. Je-li f lineární operátor na vektorovém prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ a λ vlastní číslo operátoru f, pak posloupnost $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ vektorů z $\mathbf{V}$ nazýváme *Jordanův řetízek operátoru f délky k příslušný vlastnímu číslu λ s počátkem $\mathbf{v}_1$*, pokud platí

$$(f - \lambda\,\mathrm{id}_V)(\mathbf{v}_1) = \mathbf{o},\ (f - \lambda\,\mathrm{id}_V)(\mathbf{v}_2) = \mathbf{v}_1,\ (f - \lambda\,\mathrm{id}_V)(\mathbf{v}_3) = \mathbf{v}_2,\ \dots,$$
$$(f - \lambda\,\mathrm{id}_V)(\mathbf{v}_k) = \mathbf{v}_{k-1}\ .$$

Před definicí jsme odvodili následující tvrzení.

Tvrzení 9.89. *Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na konečně generovaném prostoru $\mathbf{V}$ a $B = (\mathbf{v}_1, \dots, \mathbf{v}_k)$ báze prostoru $\mathbf{V}$, pak $[f]_B^B = J_{\lambda,k}$ právě tehdy, když $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ je Jordanův řetízek operátoru f příslušný vlastnímu číslu λ s počátkem $\mathbf{v}_1$.*

Snadno se tvrzení zobecní na obecné matice v Jordanově tvaru. Budeme říkat, že posloupnost vektorů B je *spojením* posloupností

$$B_1 = (\mathbf{v}_1^1, \dots, \mathbf{v}_{k_1}^1), B_2 = (\mathbf{v}_1^2, \dots, \mathbf{v}_{k_2}^2), \dots, B_s = (\mathbf{v}_1^s, \dots, \mathbf{v}_{k_s}^s)\ ,$$

pokud

$$B = (\mathbf{v}_1^1, \dots, \mathbf{v}_{k_1}^1, \mathbf{v}_1^2, \dots, \mathbf{v}_{k_2}^2, \dots, \mathbf{v}_1^s, \dots, \mathbf{v}_{k_s}^s)\ .$$

Budeme také používat zápis

$$B = B_1, \dots, B_s\ .$$

Tvrzení 9.90. *Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na konečně generovaném prostoru $\mathbf{V}$ a B báze prostoru $\mathbf{V}$, pak $[f]_B^B = \mathrm{diag}(J_{\lambda_1,k_1}, \dots, J_{\lambda_s,k_s})$ platí právě tehdy, když B je spojením posloupností $B_1, \dots, B_s$, kde pro každé $i \in \{1, \dots, s\}$ je B_i Jordanův řetízek operátoru f délky k_i příslušný vlastnímu číslu λ_i s počátkem $\mathbf{v}_1^i$.*

Důsledek 9.91. *Pro lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném prostoru $\mathbf{V}$ existuje Jordanův tvar právě tehdy, když existuje báze prostoru $\mathbf{V}$ vzniklá spojením Jordanových řetízků operátoru f.*

Nakonec formulujeme obdobu tvrzení 9.55. Důkaz je stejný.

Tvrzení 9.92. *Nechť $f : \mathbf{V} \to \mathbf{V}$ je lineární operátor na konečně generovaném prostoru $\mathbf{V}$ a C je báze prostoru $\mathbf{V}$. Pak pro operátor f existuje Jordanův tvar právě tehdy, když je matice $[f]_C^C$ podobná matici v Jordanově tvaru.*

Maticové verze definic a tvrzení přenecháme k rozmyšlení čtenáři.

9.4.4. Lineární nezávislost zobecněných vlastních vektorů. Chceme-li najít bázi, vzhledem ke které má operátor na prostoru dimenze n matici v Jordanově tvaru, musíme najít Jordanovy řetízky celkové délky n, tak aby jejich spojení byla lineárně nezávislá posloupnost. Následující věta, která zobecňuje větu 9.62 o lineární nezávislosti vlastních vektorů příslušných různým vlastním číslům, říká že stačí zaručit, aby pro každé vlastní číslo λ tvořily počáteční vektory řetízků příslušných vlastnímu číslu λ lineárně nezávislou posloupnost.

Věta 9.93. *Předpokládáme, že $f : \mathbf{V} \to \mathbf{V}$ je lineární operátor a $B_1, \dots, B_s$ jsou Jordanovy řetízky operátoru f příslušné vlastním číslům $\lambda_1, \dots, \lambda_s$. Předpokládejme dále, že pro každé $\lambda \in \{\lambda_1, \dots, \lambda_s\}$ je posloupnost počátečních vektorů těch řetízků z $B_1, \dots, B_s$, které přísluší vlastnímu číslu λ, lineárně nezávislá. Pak spojení $B = B_1, \dots, B_s$ je lineárně nezávislá posloupnost.*

Důkaz. Použijeme indukci podle celkového počtu k vektorů v řetízcích $B_1, \dots, B_s$. Pro $k = 1$ je tvrzení zřejmé, neboť v tom případě máme jediný řetízek délky 1 a jeho počáteční vektor je nenulový.

Předpokládáme nyní, že součet délek řetízků $B_1, B_2, \dots, B_s$ je $k > 1$. Indukční předpoklad je, že kdykoliv máme nějaké Jordanovy řetízky $C_1, C_2, \dots, C_t$ operátoru f o celkové délce menší než k a takové, že počáteční vektory těch řetízků mezi $C_1, C_2, \dots, C_t$, které přísluší stejnému vlastnímu číslu, tvoří lineárně nezávislou posloupnost, pak je spojení řetízků $C_1, C_2, \dots, C_t$ lineárně nezávislá posloupnost.

Označíme r počet řetízků příslušných vlastnímu číslu λ_1 a uspořádáme si řetízky tak, že všechny řetízky příslušející vlastnímu číslu λ_1 jsou na začátku, tj. řetízky $B_1, \dots, B_r$ přísluší vlastnímu číslu λ_1 a zbylé přísluší jiným vlastním číslům. Označme pro $i = 1, \dots, s$

$$B_i = (\mathbf{v}_1^i, \mathbf{v}_2^i, \dots, \mathbf{v}_{k_i}^i) \ .$$

Uvažujme skaláry $a_j^i \in T$ ($i \in \{1, \dots, s\}$, $j \in \{1, \dots, k_i\}$) takové, že

$$\begin{aligned} \mathbf{o} = {} & a_1^1\mathbf{v}_1^1 + a_2^1\mathbf{v}_2^1 + \dots + a_{k_1}^1\mathbf{v}_{k_1}^1 \\ & + a_1^2\mathbf{v}_1^2 + a_2^2\mathbf{v}_2^2 + \dots + a_{k_2}^2\mathbf{v}_{k_2}^2 \\ & \vdots \\ & + a_1^s\mathbf{v}_1^s + a_2^s\mathbf{v}_2^s + \dots + a_{k_s}^s\mathbf{v}_{k_s}^s \ . \end{aligned} \tag{2}$$

Potřebujeme ukázat, že všechny skaláry a_j^i jsou nulové.

Aplikujeme na obě strany operátor $f - \lambda_1 \operatorname{id}_V$. Využitím linearity, podobně jako v důkazu věty 9.62, získáme

$$\begin{aligned} \mathbf{o} = {} & a_1^1(f - \lambda_1 \operatorname{id}_V)(\mathbf{v}_1^1) + a_2^1(f - \lambda_1 \operatorname{id}_V)(\mathbf{v}_2^1) + \dots + a_{k_1}^1(f - \lambda_1 \operatorname{id}_V)(\mathbf{v}_{k_1}^1) \\ & + a_1^2(f - \lambda_1 \operatorname{id}_V)(\mathbf{v}_1^2) + a_2^2(f - \lambda_1 \operatorname{id}_V)(\mathbf{v}_2^2) + \dots + a_{k_2}^2(f - \lambda_1 \operatorname{id}_V)(\mathbf{v}_{k_2}^2) \\ & \vdots \\ & + a_1^s(f - \lambda_1 \operatorname{id}_V)(\mathbf{v}_1^s) + a_2^s(f - \lambda_1 \operatorname{id}_V)(\mathbf{v}_2^s) + \dots + a_{k_s}^s(f - \lambda_1 \operatorname{id})(\mathbf{v}_{k_s}^s) \ . \end{aligned} \tag{3}$$

Definujeme pro pohodlí $\mathbf{v}_0^i = \mathbf{o}$. Z definice Jordanova řetízku platí pro $i \in \{1, \dots, r\}$, $j \in \{1, \dots, k_i\}$ vztah

$$(f - \lambda_1 \operatorname{id}_V)(\mathbf{v}_j^i) = \mathbf{v}_{j-1}^i \ .$$

Pro $i > r$, $j \in \{1, \dots, k_i\}$ máme

$$\begin{aligned} (f - \lambda_1 \operatorname{id}_V)(\mathbf{v}_j^i) &= f(\mathbf{v}_j^i) - \lambda_1\mathbf{v}_j^i \\ &= f(\mathbf{v}_j^i) - \lambda_i\mathbf{v}_j^i + \lambda_i\mathbf{v}_j^i - \lambda_1\mathbf{v}_j^i \\ &= (f - \lambda_i \operatorname{id}_V)(\mathbf{v}_j^i) + (\lambda_i - \lambda_1)\mathbf{v}_j^i \\ &= \mathbf{v}_{j-1}^i + (\lambda_i - \lambda_1)\mathbf{v}_j^i \ . \end{aligned}$$

Důležité je pro nás pouze to, že výraz je lineární kombinací vektorů v řetízku B^i. Dosazením do (3) tedy získáme

$$\begin{aligned} \mathbf{o} = {} & a_2^1\mathbf{v}_1^1 + a_3^1\mathbf{v}_2^1 + \dots + a_{k_1}^1\mathbf{v}_{k_1-1}^1 \\ & \vdots \\ & + a_2^r\mathbf{v}_1^r + a_3^r\mathbf{v}_2^r + \dots + a_{k_1}^r\mathbf{v}_{k_r-1}^r \\ & + b_1^{r+1}\mathbf{v}_1^{r+1} + b_2^{r+1}\mathbf{v}_2^{r+1} + \dots + b_{k_{r+1}}^{r+1}\mathbf{v}_{k_{r+1}}^{r+1} \\ & + b_1^s\mathbf{v}_1^s + b_2^s\mathbf{v}_2^s + \dots + b_{k_s}^s\mathbf{v}_{k_s}^s \ , \end{aligned}$$

kde b^i_j jsou skaláry, které pochází ze součtu lineárních kombinací vektorů v řetízku B^i z výrazů pro $(f - \lambda_1 \operatorname{id}_V)(\mathbf{v}^i_j)$.

Tento výraz je lineární kombinací vektorů v řetízcích $B'_1, B'_2 \dots, B'_r, B_{r+1}, \dots, B_s$, kde řetízek B'_i vznikne z B_i odebráním posledního vektoru v řetízku B_i, může tak vzniknout i prázdný řetízek, pokud měl některý z řetízků B_i pro $i = 1, 2, \dots, r$ délku 1. Počáteční vektory v řetízcích $B'_1, B'_2 \dots, B'_r, B_{r+1}, \dots, B_s$ jsou podposloupností počátečních vektorů v řetízcích $B_1, B_2, \dots, B_s$ a ty z nich, které jsou příslušné stejnému vlastnímu číslu λ, proto tvoří lineárně nezávislou posloupnost podle předpokladu věty. Celková délka řetízků $B'_1, B'_2 \dots, B'_r, B_{r+1}, \dots, B_s$ je o $r \geq 1$ menší než celková délka řetízků $B_1, B_2, \dots, B_s$, a tedy je menší než k. Z indukčního předpokladu proto vyplývá, že všechny koeficienty v poslední lineární kombinaci jsou nutně nulové, tj. speciálně

$$a^1_2 = a^1_3 \cdots = a^1_{k_1} = a^2_2 = \cdots a^2_{k_2} = \cdots = a^r_2 = \cdots = a^r_{k_r} = 0 \ .$$

Aplikací operátorů $(f - \lambda \operatorname{id}_V)$ na rovnost (2) pro další vlastní čísla λ obdobně získáme

$$a^i_j = 0 \qquad \text{kdykoliv } i \in \{1, \dots s\}, j \in \{2, \dots, k_i\}.$$

Po dosazení do (2) nyní zbývají na pravé straně potenciálně nenulové koefcienty jen u počátků řetízků:

$$\mathbf{o} = a^1_1 \mathbf{v}^1_1 + a^2_1 \mathbf{v}^2_1 + \cdots + a^s_1 \mathbf{v}^s_1 \ . \tag{4}$$

Seskupíme členy odpovídající stejným vlastním číslům a příslušnou část součtu odpovídající vlastnímu číslu λ označíme $\mathbf{w}_\lambda$, tj.

$$\mathbf{w}_\lambda = \sum_{i : \mathbf{v}^i_1 \in M_\lambda} a^i_1 \mathbf{v}^i_1 \ . \tag{5}$$

Protože $\mathbf{w}_\lambda$ je vlastní vektor příslušný vlastnímu číslu λ a součet těchto vektorů je podle (4) nulový, jsou tyto vektory všechny nutně nulové díky větě 9.62 o lineární nezávislosti nenulových vlastních vektorů příslušných různým vlastním číslům. Z (5) a z předpokladu lineární nezávislosti počátků řetízků $B_1, B_2, \dots, B_r$ příslušných stejnému vlastnímu číslu získáme konečně i

$$a^1_1 = a^2_1 = \cdots = a^s_1 = 0 \ .$$

▲

9.4.5. Výpočet řetízků. Uvažujme operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném prostoru $\mathbf{V}$ dimenze n a bázi $B = B_1, \dots, B_s$ složenou ze Jordanových řetízků $B_1, \dots, B_s$ délek $k_1, \dots, k_s$ příslušných vlastním číslům $\lambda_1, \dots, \lambda_s$. Pro přehlednost si je uspořádáme tak, aby řetízky příslušné stejným číslům byly pohromadě. Řekněme, že prvních r odpovídá stejnému vlastnímu číslu λ, tj. $\lambda = \lambda_1 = \lambda_2 = \cdots = \lambda_r$ a $\lambda_i \neq \lambda$ pro $i > r$. Označme $B_i = (\mathbf{v}^i_1, \mathbf{v}^i_2, \dots, \mathbf{v}^i_{k_i})$ pro $i \in \{1, \dots, s\}$. Schematicky:

$$\begin{array}{l}
\mathbf{v}^1_{k_1} \xmapsto{f-\lambda \operatorname{id}_V} \mathbf{v}^1_{k_1-1} \longmapsto \cdots \longmapsto \mathbf{v}^1_2 \xmapsto{f-\lambda \operatorname{id}_V} \mathbf{v}^1_1 \xmapsto{f-\lambda \operatorname{id}_V} \mathbf{o} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots \\
\mathbf{v}^r_{k_r} \xmapsto{f-\lambda \operatorname{id}_V} \mathbf{v}^r_{k_r-1} \longmapsto \cdots \longmapsto \mathbf{v}^r_2 \xmapsto{f-\lambda \operatorname{id}_V} \mathbf{v}^r_1 \xmapsto{f-\lambda \operatorname{id}_V} \mathbf{o} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots \\
\mathbf{v}^s_{k_s} \xmapsto{f-\lambda_s \operatorname{id}_V} \mathbf{v}^s_{k_s-1} \longmapsto \cdots \longmapsto \mathbf{v}^s_2 \xmapsto{f-\lambda_s \operatorname{id}_V} \mathbf{v}^s_1 \xmapsto{f-\lambda_s \operatorname{id}_V} \mathbf{o}
\end{array}$$

a

$$[f]^B_B = J = \operatorname{diag}(J_{\lambda_1,k_1}, J_{\lambda_2,k_2}, \dots, J_{\lambda_s,k_s}) \ .$$

Za této situace spočítáme charakteristický polynom operátoru f, vlastní čísla a vektory, geometrické násobnosti a navíc jádra a obrazy operátorů $(f - \lambda_i \operatorname{id}_V)^l$ pro $l = 1, 2, \ldots$. (Zaměříme se na vlastní číslo $\lambda_1 = \cdots = \lambda_r$, přičemž výsledky přirozeně budou platit pro všechna další vlastní čísla.) Tyto poznatky nám pak umožní hledat Jordanovy řetízky i v situaci, kdy je předem neznáme.

Charakteristický polynom $p_f(\lambda)$ operátoru f je roven determinantu matice $J - \lambda I_n$. Tato matice je horní trojúhelníková a na diagonále má postupně k_1-krát výraz $(\lambda_1 - \lambda)$, k_2-krát výraz $(\lambda_2 - \lambda)$, atd. Charakteristický polynom je proto roven

$$(\lambda_1 - \lambda)^{k_1}(\lambda_2 - \lambda)^{k_2} \ldots (\lambda_s - \lambda)^{k_s} \quad .$$

Důsledkem je, že operátor f má n vlastních čísel včetně násobností a algebraická násobnost vlastního čísla λ_1 je rovna součtu délek Jordanových řetízků příslušných vlastnímu číslu λ_1 (to jest $k_1 + k_2 + \cdots + k_r$).

Dále vypočítáme jádro a obraz operátoru $f - \lambda_1 \operatorname{id}_V$. (Pro představu je dobré sledovat výpočet na konkrétní situaci, viz např. příklad 9.94). Jeho matice $[f - \lambda_1 \operatorname{id}_V]_B^B$ vzhledem k bázi B je

$$J - \lambda_1 I_n = \operatorname{diag}(J_{0,k_1}, \ldots, J_{0,k_r}, J_{\lambda_{r+1}-\lambda_1,k_{r+1}}, \ldots, J_{\lambda_s-\lambda_1,k_s})$$

Tato matice má nulové řádky, které odpovídají pozici koncových vektorů řetízků $B_1, \ldots, B_r$ v bázi B. Vynecháme-li je, dostaneme matici v řádkově odstupňovaném tvaru s $(n-r)$ nenulovými řádky. Dimenze jádra matice $J - \lambda_1 I_n$ je r a také vidíme, že množina všech řešení homogenní soustavy rovnic s maticí $J - \lambda_1 I_n$ je $\operatorname{Ker}(J - \lambda_1 I_n) = \operatorname{LO}\{\mathbf{e}_{i_1}, \ldots, \mathbf{e}_{i_r}\}$, kde indexy $i_1, \ldots, i_r$ odpovídají pozicím počátečních vektorů řetízků $B_1, \ldots, B_r$ v bázi B, tj. $i_1 = 1$, $i_2 = 1 + k_1$, $i_3 = 1 + k_1 + k_2$, ..., $i_r = 1 + k_1 + \cdots + k_{r-1}$. Je tedy

$$[\operatorname{Ker}(f - \lambda_1 \operatorname{id}_V)]_B = \operatorname{Ker}(J - \lambda_1 I_n) = \operatorname{LO}\{\mathbf{e}_{i_1}, \ldots, \mathbf{e}_{i_r}\} \quad ,$$

takže

$$\operatorname{Ker}(f - \lambda_1 \operatorname{id}_V) = \operatorname{LO}\left\{\mathbf{v}_1^1, \mathbf{v}_1^2, \ldots, \mathbf{v}_1^r\right\} \quad .$$

Geometrická násobnost r vlastního čísla λ_1 je tedy rovná počtu řetízků příslušných vlastnímu číslu λ_1 a jádro operátoru $(f - \lambda_1 \operatorname{id}_V)$ je rovno lineárnímu obalu počátečních vektorů těchto řetízků.

Přejdeme k výpočtu obrazu (tj. oboru hodnot) $\operatorname{Im}(f - \lambda_1 \operatorname{id}_V)$ operátoru $f - \lambda_1 \operatorname{id}_V$. Obor hodnot matice $J - \lambda_1 I_n = [f - \lambda_1 \operatorname{id}_V]_B^B$ se rovná lineárnímu obalu sloupcových vektorů. Sloupce odpovídající pozicím počátečních vektorů řetízků $B_1, \ldots, B_r$ jsou nulové a zbylé sloupce příslušné kterékoliv z buněk J_{0,k_i} pro $i = 1, 2, \ldots, r$ obsahují vektory kanonické báze. Ostatní buňky (příslušné vlastním číslům různým od λ_1) jsou horní trojúhelníkové matice s nenulovými prvky na hlavní diagonále, můžeme je tedy elementárními sloupcovými úpravami (které nemění obraz) převést na jednotkové matice. Obraz matice $J - \lambda_1 I_n$ je tedy roven lineárnímu obalu těch vektorů kanonické báze, které neodpovídají pozicím koncových vektorů řetízků $B_1, \ldots, B_r$. Protože $[\operatorname{Im}(f - \lambda_1 \operatorname{id}_V)]_B = \operatorname{Im}(J - \lambda_1 I_n)$, je obraz operátoru $f - \lambda_1 \operatorname{id}_V$ roven lineárnímu obalu všech vektorů v B kromě koncových vektorů řetízků $B_1, \ldots, B_r$. Můžeme si představovat, že umažeme jeden vektor z konce každého řetízku příslušného vlastnímu číslu λ_1.

PŘÍKLAD 9.94. Pro $\lambda = \lambda_1 = \lambda_2 = \lambda_3 = 7$, $\lambda_4 = 9$, $k_1 = 1$, $k_2 = 2$, $k_3 = 3$, $k_4 = 2$ máme řetízky

$$\begin{array}{ccccccc}
 & & & & \mathbf{v}_1^1 & \xmapsto{f-7\,\mathrm{id}_V} & \mathbf{o} \\
 & & & \mathbf{v}_2^2 & \xmapsto{f-7\,\mathrm{id}_V} & \mathbf{v}_1^2 & \xmapsto{f-7\,\mathrm{id}_V} \mathbf{o} \\
\mathbf{v}_3^3 & \xmapsto{f-7\,\mathrm{id}_V} & \mathbf{v}_2^3 & \xmapsto{f-7\,\mathrm{id}_V} & \mathbf{v}_1^3 & \xmapsto{f-7\,\mathrm{id}_V} & \mathbf{o} \\
 & & \mathbf{v}_2^4 & \xmapsto{f-9\,\mathrm{id}_V} & \mathbf{v}_1^4 & \xmapsto{f-9\,\mathrm{id}_V} & \mathbf{o}
\end{array}$$

Operátor f má charakteristický polynom $p_f(\lambda) = (7-\lambda)^6(9-\lambda)^2$, vlastní číslo 7 algebraické násobnosti 6 a vlastní číslo 9 algebraické násobnosti 2.

Matice operátoru $f - 7\,\mathrm{id}_V$ vzhledem k B je

$$J-7I_8 = \begin{pmatrix} 7&0&0&0&0&0&0&0\\ 0&7&1&0&0&0&0&0\\ 0&0&7&0&0&0&0&0\\ 0&0&0&7&1&0&0&0\\ 0&0&0&0&7&1&0&0\\ 0&0&0&0&0&7&0&0\\ 0&0&0&0&0&0&9&1\\ 0&0&0&0&0&0&0&9 \end{pmatrix} -7I_8 = \begin{pmatrix} 0&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&2&1\\ 0&0&0&0&0&0&0&2 \end{pmatrix} .$$

Jádro matice $J - 7I_8$ je

$$\mathrm{Ker}\begin{pmatrix} 0&0&1&0&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&2&1\\ 0&0&0&0&0&0&0&2 \end{pmatrix} = \mathrm{LO}\,\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_4\}$$

a tudíž jádro operátoru $f - 7\,\mathrm{id}_V$ je $\mathrm{Ker}\,(f - 7\,\mathrm{id}_V) = \mathrm{LO}\,\{\mathbf{v}_1^1, \mathbf{v}_1^2, \mathbf{v}_1^3\}$ (lineární obal počátečních vektorů příslušných vlastnímu číslu 7), jeho dimenze je 3 a je rovná geometrické násobnost vlastního čísla 7, která udává počet řetízků příslušných tomuto vlastnímu číslu.

Obraz matice $J - 7I_8$ je

$$\mathrm{Im}\begin{pmatrix} 0&0&0&0&0\\ 1&0&0&0&0\\ 0&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&0&0\\ 0&0&0&2&1\\ 0&0&0&0&2 \end{pmatrix} = \mathrm{Im}\begin{pmatrix} 0&0&0&0&0\\ 1&0&0&0&0\\ 0&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1 \end{pmatrix} = \mathrm{LO}\,\{\mathbf{e}_2, \mathbf{e}_4, \mathbf{e}_5, \mathbf{e}_7, \mathbf{e}_8\}$$

a tudíž obraz operátoru $f - 7\,\mathrm{id}_V$ je $\mathrm{Im}\,(f - 7\,\mathrm{id}_V) = \mathrm{LO}\,\{\mathbf{v}_1^2, \mathbf{v}_1^3, \mathbf{v}_2^3, \mathbf{v}_1^4, \mathbf{v}_2^4\}$ (lineární obal všech vektorů v řetízcích kromě koncových vektorů příslušných vlastnímu číslu 7). ▲

Nakonec obecněji vypočteme jádro a obraz operátoru $(f - \lambda_1\,\mathrm{id}_V)^l$ pro $l \geq 2$. Jeho matice vzhledem k B je

$$(J - \lambda_1 I_n)^l = \mathrm{diag}(J^l_{0,k_1}, \ldots, J^l_{0,k_r}, J^l_{\lambda_{r+1}-\lambda_1,k_{r+1}}, \ldots, J^l_{\lambda_s-\lambda_1,k_s}) \ .$$

Tvar prvních r diagonálních buněk jsme spočítali v tvrzení 9.84, tvar ostatních v tvrzení 9.86, ten ale teď nebudeme potřebovat, stačí vědět, že v případě buněk

příslušných vlastním číslům různým od λ_1 vyjdou regulární matice (horní trojúhelníkové s nenulovými prvky na hlavní diagonále).

Matice $(J - \lambda_1 I_n)^l$ má nulové řádky odpovídající pozici l koncových prvků řetízků $B_1, \dots, B_r$ v bázi B (pokud má některý z těchto řetízků délku nejvýše l, pak uvažujeme všechny jeho prvky). Vynecháme-li je, dostaneme matici v řádkově odstupňovaném tvaru a jádro $\operatorname{Ker}(J-\lambda_1 I_n)^l$ matice $(J-\lambda_1 I_n)^l$ je rovno lineárnímu obalu $\operatorname{LO}\{\mathbf{e}_{i_1}, \dots, \}$, kde indexy $i_1, \dots,$ odpovídají pozicím l počátečních vektorů řetízků $B_1, \dots, B_r$ v bázi B. To znamená, že

$$\operatorname{Ker}(f - \lambda_1 \operatorname{id}_V)^l = \operatorname{LO}\left\{\mathbf{v}_1^1, \dots, \mathbf{v}_l^1, \mathbf{v}_1^2, \dots, \mathbf{v}_l^2, \dots, \mathbf{v}_1^r, \dots, \mathbf{v}_l^r\right\} \ .$$

(Pro řetízky B_i délky menší než l nejsou vektory $\mathbf{v}_{k_i+1}^i, \dots, \mathbf{v}_l^i$ definované.) Jádro operátoru $(f - \lambda_1 \operatorname{id}_V)^l$ se rovná lineárnímu obalu l počátečních vektorů z každého řetízku příslušného vlastnímu číslu λ_1 (z řetízků délky menší než l bereme všechny vektory.)

Z toho také vyplývá důležité pozorování – počet řetízků příslušných vlastnímu číslu λ, které mají délku aspoň l, se rovná

$$\dim \operatorname{Ker}(f - \lambda_1 \operatorname{id}_V)^l - \dim \operatorname{Ker}(f - \lambda_1 \operatorname{id}_V)^{l-1} \ .$$

Obraz operátoru $(f - \lambda_1 \operatorname{id}_V)^l$ také spočteme obdobně jako v případu $l = 1$.

Příklad 9.95. Vrátíme se k příkladu 9.94. Operátory $(f - 7\operatorname{id})^2$, $(f - 7\operatorname{id})^3$ mají vzhledem k B matici

$$(J-7I_8)^2 = \begin{pmatrix} 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&4&4\\ 0&0&0&0&0&0&0&4 \end{pmatrix}, (J-7I_8)^3 = \begin{pmatrix} 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&8&12\\ 0&0&0&0&0&0&0&8 \end{pmatrix} .$$

Jádra jsou

$$\operatorname{Ker}(J-7I_8)^2 = \operatorname{LO}\{\mathbf{e}_1, \dots, \mathbf{e}_5\}\,,\ \operatorname{Ker}(J-7I_8)^3 = \operatorname{Ker}(J-7I_8)^4 = \dots = \operatorname{LO}\{\mathbf{e}_1, \dots, \mathbf{e}_6\}$$

a proto

$$\operatorname{Ker}(f-7\operatorname{id})^2 = \operatorname{LO}\left\{\mathbf{v}_1^1, \mathbf{v}_1^2, \mathbf{v}_2^2, \mathbf{v}_1^3, \mathbf{v}_2^3\right\}\,,\ \operatorname{Ker}(f-7\operatorname{id})^3 = \operatorname{LO}\left\{\mathbf{v}_1^1, \mathbf{v}_1^2, \mathbf{v}_2^2, \mathbf{v}_1^3, \mathbf{v}_2^3, \mathbf{v}_3^3\right\} \ .$$

Obrazy jsou

$$\operatorname{Im}(J - 7I_8)^2 = \operatorname{LO}\{\mathbf{e}_4, \mathbf{e}_7, \mathbf{e}_8\}\,,\ \operatorname{Im}(J - 7I_8)^3 = \operatorname{Im}(J - 7I_8)^4 = \dots = \operatorname{LO}\{\mathbf{e}_7, \mathbf{e}_8\}$$

a proto

$$\operatorname{Im}(f - 7\operatorname{id})^2 = \operatorname{LO}\left\{\mathbf{v}_1^3, \mathbf{v}_1^4, \mathbf{v}_2^4\right\}\,,\ \operatorname{Im}(f - 7\operatorname{id})^3 = \operatorname{LO}\left\{\mathbf{v}_1^4, \mathbf{v}_2^4\right\} \ .$$

▲

Shrneme získané poznatky.

Tvrzení 9.96. *Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na prostoru $\mathbf{V}$ dimenze n a B báze vzniklá spojením Jordanových řetízků operátoru f, pak platí*

(1) *operátor f má n vlastních čísel včetně násobností,*
(2) *pro libovolné vlastní číslo λ operátoru f je jeho algebraická násobnost rovna součtu délek Jordanových řetízků v B příslušných vlastnímu číslu λ,*
(3) *pro libovolné vlastní číslo λ operátoru f a libovolné $l \in \mathbb{N}$ je jádro operátoru $(f - \lambda \operatorname{id}_V)^l$ rovno lineárnímu obalu l počátečních vektorů z každého řetízku v B příslušného vlastnímu číslu λ (z řetízků délky menší než l bereme všechny vektory),*

(4) *pro libovolné vlastní číslo λ operátoru f a libovolné $l \in \mathbb{N}$ je obraz operátoru $(f - \lambda\,\mathrm{id}_V)^l$, roven lineárnímu obalu všech vektorů v B kromě l koncových vektorů z řetízků příslušných vlastnímu číslu λ (z řetízků příslušných vlastnímu číslu λ délky menší než l nebereme žádný vektor).*

Speciálně pro libovolné vlastní číslo λ operátoru f platí

(5) *geometrická násobnost vlastního čísla λ se rovná počtu řetízků v B příslušných vlastnímu číslu λ a prostor $M_\lambda = \mathrm{Ker}\,(f - \lambda\,\mathrm{id}_V)$ je roven lineárnímu obalu počátečních vektorů těchto řetízků,*

(6) *počet řetízků příslušných vlastnímu číslu λ délky alespoň l je roven*

$$z_l = \dim \mathrm{Ker}\,(f - \lambda\,\mathrm{id}_V)^l - \dim \mathrm{Ker}\,(f - \lambda\,\mathrm{id}_V)^{l-1} \ ,$$

(aby měl výraz smysl i pro $l = 1$ definujeme $(f - \lambda\,\mathrm{id}_V)^0 = \mathrm{id}_V$),

(7) *počet řetízků příslušných vlastnímu číslu λ délky právě l je $z_l - z_{l+1}$.*

Z prvního bodu vyplývá nutná podmínka pro existenci Jordanova kanonického tvaru – operátor musí mít dostatek vlastních čísel (včetně násobností). Tato podmínka je i dostačující podle následující veledůležité věty.

VĚTA 9.97 (o Jordanově kanonickém tvaru). *Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na konečně generovaném vektorovém prostoru $\mathbf{V}$ dimenze n (resp. A čtvercová matice řádu n), pak jsou následující tvrzení ekvivalentní.*

(1) *Pro operátor f (resp. matici A) existuje Jordanův kanonický tvar.*

(2) *Operátor f (resp. matice A) má n vlastních čísel včetně algebraických násobností.*

DŮSLEDEK 9.98. *Pro každý operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném prostoru $\mathbf{V}$ nad tělesem komplexních čísel $\mathbb{C}$ existuje Jordanův kanonický tvar.*

Důkaz chybějící implikace odložíme na později. Poznamenejme, že Jordanův tvar operátoru je určen jednoznačně v tom smyslu, že jsou-li matice $[f]_B^B$ a $[f]_C^C$ obě v Jordanově tvaru, pak se mohou lišit pouze pořadím Jordanových buněk. To vyplývá z tvrzení 9.96, protože matice je určena vlastními čísly λ operátoru, jejich algebraickou násobností, a dimenzemi podprostorů $\mathrm{Ker}\,(f - \lambda\,\mathrm{id}_V)^l$. Těmto číselným charakteristikám operátoru f říkáme *algebraické invarianty operátoru f*.

Algoritmus pro hledání Jordanova tvaru je možné odvodit z tvrzení 9.96. Obecná diskuze by byla dost nepřehledná, proto ukážeme postup na konktétních příkladech.

9.4.6. Jordanův tvar v dimenzi 2. Jediný případ, kdy má operátor f na prostoru dimenze 2 dvě vlastní čísla včetně násobností a není diagonalizovatelný, je případ kdy f má vlastní číslo λ algebraické násobnosti 2 a geometrické násobnosti 1. V tom případě máme jeden Jordanův řetízek délky 2.

PŘÍKLAD 9.99. Uvažujme operátor f_A na $\mathbb{R}^2$ určený maticí

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

Charakteristický polynom je $p_A(\lambda) = \lambda^2 + 2\lambda + 1 = (\lambda+1)^2$. Operátor f_A má vlastní číslo -1 algebraické násobnosti 2, existuje pro něj proto Jordanův kanonický tvar.

Spočítáme $M_{-1} = \mathrm{Ker}\,(f_A + \mathrm{id})$.

$$M_{-1} = \mathrm{Ker} \begin{pmatrix} 2 & -1 \\ 4 & -2 \end{pmatrix} = \mathrm{LO}\left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\} \ .$$

Geometrická násobnost vlastního čísla -1 je 1. Operátor není diagonalizovatelný a budeme proto hledat Jordanův řetízek délky 2

$$\mathbf{v}_2 \xmapsto{f_A + \mathrm{id}} \mathbf{v}_1 \xmapsto{f_A + \mathrm{id}} \mathbf{o} \ .$$

Vektor $\mathbf{v}_1$ zvolíme jako libovolný nenulový vlastní vektor, například $\mathbf{v}_1 = (1,2)^T$.

Podle tvrzení 9.96 je $\operatorname{Im}(f_A + \mathrm{id}) = \operatorname{Ker}(f_A + \mathrm{id}) = \mathrm{LO}\{\mathbf{v}_1\}$, takže speciálně $\mathbf{v}_1 \in \operatorname{Im}(f_A + \mathrm{id})$, proto můžeme vždy počáteční vektor $\mathbf{v}_1$ doplnit vektorem $\mathbf{v}_2$ tak, aby platilo $(f_A + \mathrm{id})(\mathbf{v}_2) = \mathbf{v}_1$. Pro takový vektor $\mathbf{v}_2$ platí

$$(A + \mathrm{id})\mathbf{v}_2 = \mathbf{v}_1, \quad \begin{pmatrix} 2 & -1 \\ 4 & -2 \end{pmatrix} \mathbf{v}_2 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \quad \text{zvolíme např. } \mathbf{v}_2 = \begin{pmatrix} 0 \\ -1 \end{pmatrix}$$

Podle věty 9.93 o lineární nezávislosti zobecněných vlastních vektorů je $B = (\mathbf{v}_1, \mathbf{v}_2)$ báze (v takto malém případě to vidíme okamžitě, ve větších dimenzích už to tak zřejmé není). Matice operátoru f_A vzhledem k bázi B je

$$[f_A]_B^B = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$$

▲

9.4.7. Jordanův tvar v dimenzi 3. Pro nediagonalizovatelný operátor na prostoru dimenze 3 s třemi vlastními čísly včetně násobností můžou nastat následující možnosti.

(1) Operátor f má dvě různá vlastní čísla λ_1, λ_2, kde λ_1 má algebraickou (i geometrickou) násobnost 1 a λ_2 má algebraickou násobnost 2, zatímco geometrickou násobnost 1. V tom případě máme jeden řetízek délky 1 příslušný λ_1 a jeden řetízek délky 2 příslušný λ_2:

$$\begin{array}{ccccc} & & \mathbf{v}_1^1 & \xmapsto{f-\lambda_1 \mathrm{id}_V} & \mathbf{o} \\ \mathbf{v}_2^2 & \xmapsto{f-\lambda_2 \mathrm{id}_V} & \mathbf{v}_1^2 & \xmapsto{f-\lambda_2 \mathrm{id}_V} & \mathbf{o} \ . \end{array}$$

(2) Operátor f má vlastní číslo λ algebraické násobnosti 3 a geometrické násobnosti 2. Pak máme dva řetízky příslušné vlastnímu číslu λ a tím pádem nutně jeden z nich má délku 1 a druhý má délku 2:

$$\begin{array}{ccccc} & & \mathbf{v}_1^1 & \xmapsto{f-\lambda \mathrm{id}_V} & \mathbf{o} \\ \mathbf{v}_2^2 & \xmapsto{f-\lambda \mathrm{id}_V} & \mathbf{v}_1^2 & \xmapsto{f-\lambda \mathrm{id}_V} & \mathbf{o} \ . \end{array}$$

(3) Operátor f má vlastní číslo λ algebraické násobnosti 3 a geometrické násobnosti 1. Pak máme jeden řetízek délky 3:

$$\mathbf{v}_3 \xmapsto{f-\lambda \mathrm{id}_V} \mathbf{v}_2 \xmapsto{f-\lambda \mathrm{id}_V} \mathbf{v}_1 \xmapsto{f-\lambda \mathrm{id}_V} \mathbf{o} \ .$$

PŘÍKLAD 9.100. Uvažujme operátor $f_A : \mathbb{R}^3 \to \mathbb{R}^3$ určený maticí

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

Charakteristický polynom operátoru f_A je $p_A(\lambda) = -\lambda^3 + \lambda^2 + \lambda - 1 = -(\lambda - 1)^2(\lambda + 1)$. Vlastní čísla operátoru A jsou 1 (algebraická násobnost je 2) a -1 (s algebraickou násobností 1), existuje pro něj Jordanův tvar. Příslušné prostory vlastních vektorů jsou

$$M_1 = \operatorname{Ker}(f_A - \mathrm{id}) = \operatorname{Ker} \begin{pmatrix} -2 & 0 & 1 \\ 0 & -2 & 0 \\ -4 & 0 & 2 \end{pmatrix} = \mathrm{LO}\left\{ \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix} \right\},$$

$$M_{-1} = \operatorname{Ker}(f_A + \mathrm{id}) = \mathrm{LO}\left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\} \ .$$

Geometrická násobnost vlastního čísla 1 je 1, takže operátor není diagonalizovatelný a Jordanovy řetízky budou tvaru

$$\begin{array}{ccccc} & & \mathbf{v}_1^1 & \xmapsto{f_A+\mathrm{id}} & \mathbf{o} \\ \mathbf{v}_2^2 & \xmapsto{f_A-\mathrm{id}} & \mathbf{v}_1^2 & \xmapsto{f_A-\mathrm{id}} & \mathbf{o} \end{array}$$

Za vektor $\mathbf{v}_1^1$ zvolíme libovolný nenulový vektor z M_{-1}, např. $\mathbf{v}_1^1 = (0,1,0)^T$. Za vektor $\mathbf{v}_1^2$ zvolíme libovolný nenulový vektor z M_1, např. $\mathbf{v}_1^2 = (1,0,2)^T$, protože (podobně jako v příkladu 9.99) z tvrzení 9.96 plyne, že $\mathbf{v}_1^2 \in \operatorname{Im}(f_A - \mathrm{id})$, takže řetízek můžeme doplnit. Řešením soustavy

$$(A - I_3)\mathbf{v}_2^2 = \mathbf{v}_1^1, \quad \text{tj.} \begin{pmatrix} -2 & 0 & 1 \\ 0 & -1 & 0 \\ -4 & 0 & 2 \end{pmatrix} \mathbf{v}_2^2 = \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}$$

najdeme například vektor $\mathbf{v}_2^2 = (0,0,1)^T$. Podle věty 9.93 je $B = (\mathbf{v}_1^1, \mathbf{v}_1^2, \mathbf{v}_2^2)$ bází prostoru $\mathbb{R}^3$. Matice operátoru f_A vzhledem k B je

$$[f_A]_B^B = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} .$$

▲

Příklad 9.101. Uvažujme operátor $f_A : \mathbb{R}^3 \to \mathbb{R}^3$ určený maticí

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

Charakteristický polynom operátoru f_A vyjde $p_A(\lambda) = -\lambda^3$. Operátor f_A má vlastní číslo 0 algebraické násobnosti 3, existuje pro něj Jordanův tvar. Prostor vlastních vektorů příslušných nule je

$$M_0 = \operatorname{Ker}(f_A - 0\,\mathrm{id}) = \operatorname{Ker} f_A = \operatorname{Ker} A = \mathrm{LO}\left\{ \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} \right\} .$$

Geometrická násobnost vlastního čísla 0 je 2, proto operátor není diagonalizovatelný, budeme mít dva Jordanovy řetízky tvaru

$$\begin{array}{ccccc} & & \mathbf{v}_1^1 & \xmapsto{f_A} & \mathbf{o} \\ \mathbf{v}_2^2 & \xmapsto{f_A} & \mathbf{v}_1^2 & \xmapsto{f_A} & \mathbf{o} \end{array} .$$

Podle tvrzení 9.96 je $\operatorname{Im} f_A = \mathrm{LO}\left\{\mathbf{v}_1^2\right\}$ a $\operatorname{Ker} f_A = \mathrm{LO}\left\{\mathbf{v}_1^1, \mathbf{v}_1^2\right\}$. Při hledání vektorů v řetízku postupujeme od počátku nejdelšího řetízku. Vektor $\mathbf{v}_1^2$ zvolíme v $\operatorname{Im} f_A$, např. $\mathbf{v}_1^2 = (2,0,1)^T$. Pak je $\mathbf{v}_1^2 \in \operatorname{Ker} f_A$. Doplníme $\mathbf{v}_1^2$ na bázi $(\mathbf{v}_1^2, \mathbf{v}_1^1)$ prostoru $\operatorname{Ker} f_A$, třeba vektorem $\mathbf{v}_1^1 = (-1,1,0)^T$. Nakonec najdeme $\mathbf{v}_2^2$ tak, aby $f_A(\mathbf{v}_2^2) = \mathbf{v}_1^2$. To musí jít, protože $\mathbf{v}_1^2 \in \operatorname{Im} f_A$. Řešením rovnice $A\mathbf{v}_2^2 = \mathbf{v}_1^2$ je například vektor $\mathbf{v}_2^2 = (1,0,0)^T$.

Počátky řetízků tvoří lineárně nezávislou posloupnost (tak jsme je zvolili), takže podle věty 9.93 je $B = (\mathbf{v}_1^1, \mathbf{v}_1^2, \mathbf{v}_2^2)$ báze prostoru $\mathbb{R}^3$. Matice operátoru f_A vzhledem k B je

$$[f_A]_B^B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} .$$

▲

PŘÍKLAD 9.102. Uvažujme operátor $f_A : \mathbb{R}^3 \to \mathbb{R}^3$ určený maticí

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

Charakteristický polynom operátoru f_A je $p_A(\lambda) = -(\lambda+1)^3$, máme jedno vlastní číslo -1 algebraické násobnosti 3.

$$M_{-1} = \operatorname{Ker}(f_A + \mathrm{id}) = \operatorname{Ker}(A + I_3) = \mathrm{LO}\left\{ \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix} \right\} .$$

Geometrická násobnost vlastního čísla -1 je 1. Operátor f_A není diagonalizovatelný, existuje pro něj Jordanův tvar a příslušná báze B bude obsahovat jeden řetízek

$$\mathbf{v}_3 \xmapsto{f_A+\mathrm{id}} \mathbf{v}_2 \xmapsto{f_A+\mathrm{id}} \mathbf{v}_1 \xmapsto{f_A+\mathrm{id}} \mathbf{o} .$$

Podle tvrzení 9.96 je $\operatorname{Ker}(f_A+\mathrm{id}) = \operatorname{Im}(f_A+\mathrm{id})^2 = \mathrm{LO}\{\mathbf{v}_1\}$, takže za počátek můžeme zvolit libovolný nenulový vektor v tomto prostoru, například $\mathbf{v}_1 = (0,2,1)^T$. Vektor $\mathbf{v}_2$ musíme zvolit tak, aby $(f_A + \mathrm{id})(\mathbf{v}_2) = \mathbf{v}_1$ a aby ležel v $\operatorname{Im}(f_A + \mathrm{id})$, abychom pak mohli nalézt vektor $\mathbf{v}_3$. První podmínka je

$$(A + \mathrm{id})\mathbf{v}_2 = \mathbf{v}_1, \quad \begin{pmatrix} 0 & 0 & 0 \\ 1 & 2 & -4 \\ 1 & 1 & -2 \end{pmatrix} \mathbf{v}_2 = \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}$$

Řešením soustavy je $(0,1,0)^T + \mathrm{LO}\left\{(0,2,1)^T\right\} = (0,1,0)^T + \operatorname{Ker}(A+\mathrm{id})$. Některý z takových vektorů leží v $\operatorname{Im}(f_A+\mathrm{id})$, protože ale $\operatorname{Ker}(f_A+\mathrm{id}) \subseteq \operatorname{Im}(f_A+\mathrm{id})$ (viz opět tvrzení 9.96), každý z těchto vektorů leží v $\operatorname{Im}(f_A + \mathrm{id})$. Druhá podmínka je splněná v tomto případě automaticky a můžeme zvolit třeba $\mathbf{v}_2 = (0,1,0)^T$. (Pokud bychom měli více řetízků, neplatilo by $\operatorname{Ker}(f - \lambda\,\mathrm{id}) \subseteq \operatorname{Im}(f - \lambda\,\mathrm{id})$, takže volba by nemohla být libovolná.) Nakonec najdeme vektor $\mathbf{v}_3$, aby $(f_A+\mathrm{id})\mathbf{v}_3 = \mathbf{v}_2$. Můžeme vzít například $\mathbf{v}_3 = (-1,1,0)^T$.

Podle věty 9.93 je $B = (\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ báze prostoru $\mathbb{R}^3$. Matice operátoru f_A vzhledem k B je

$$[f_A]_B^B = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix} .$$

▲

9.4.8. Jordanův tvar ve vyšších dimenzích. Do dimenze 3 je možné o počtu a délkách řetízků rozhodnout pouze z algebraických a geometrických násobností. Stejně je tomu v dimenzi 4 kromě případu, že má operátor vlastní číslo λ algebraické násobnosti 4 a geometrické násobnosti 2. Pak má bázi ze dvou Jordanových řetízků, nevíme ale, jsou-li oba délky 2, nebo jeden z nich délky 1 a druhý délky 3.

PŘÍKLAD 9.103. Uvažujme operátor $f_A : \mathbb{R}^4 \to \mathbb{R}^4$ pro matici

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

Výpočtem charakteristického polynomu zjistíme, že f_A má jediné vlastní číslo 0 algebraické násobnosti 4. Prostor vlastních vektorů příslušných vlastnímu číslu 0 je

$$M_0 = \mathrm{LO}\left\{\begin{pmatrix}0\\1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\0\\1\\0\end{pmatrix}\right\} .$$

Geometrická násobnost nuly je 2, takže hledaná báze B, vzhledem ke které je $[f]_B^B$ v Jordanově tvaru, bude spojením dvou řetízků příslušných vlastnímu číslu 0. Nevíme, ale budou-li jejich délky $1, 3$ nebo $2, 2$. Vypočteme proto ještě jádro operátoru $(f_A - 0\,\mathrm{id})^2$.

$$\mathrm{Ker}\,(f_A - 0\,\mathrm{id})^2 = \mathrm{Ker}\,A^2 = \mathrm{Ker}\,0_{4\times 4} = \mathbb{R}^4 \ .$$

Dimenze jádra operátoru $(f_A + 0\,\mathrm{id})^2$ je o 2 vyšší než dimenze jádra operátoru $(f_A + 0\,\mathrm{id})$, takže podle tvrzení 9.96 budou v B právě 2 řetízky délky alespoň 2. Tím pádem je B spojením řetízků

$$\begin{aligned}\mathbf{v}_2^1 &\xmapsto{f_A} \mathbf{v}_1^1 \xmapsto{f_A} \mathbf{o}\\ \mathbf{v}_2^2 &\xmapsto{f_A} \mathbf{v}_1^2 \xmapsto{f_A} \mathbf{o}\ .\end{aligned}$$

Protože (opět podle tvrzení 9.96) je $\mathrm{Im}\,f_A = \mathrm{Ker}\,f_A = \mathrm{LO}\left\{\mathbf{v}_1^1, \mathbf{v}_1^2\right\}$, můžeme za $\mathbf{v}_1^1, \mathbf{v}_1^2$ zvolit libovolnou bázi $\mathrm{Ker}\,f_A$, například $\mathbf{v}_1^1 = (0,1,0,1)$, $\mathbf{v}_1^2 = (1,0,1,0)$, a pak nalézt vektory $\mathbf{v}_2^1$ a $\mathbf{v}_2^2$ tak, aby $f_A(\mathbf{v}_2^1) = \mathbf{v}_1^1$ a $f_A(\mathbf{v}_2^2) = \mathbf{v}_1^2$, třeba $\mathbf{v}_2^1 = (0,1,0,0)^T$ a $\mathbf{v}_2^2 = (1,0,0,0)^T$. Pak $B = (\mathbf{v}_1^1, \mathbf{v}_2^1, \mathbf{v}_1^2, \mathbf{v}_2^2)$ je podle věty 9.93 báze prostoru $\mathbf{R}^4$ a platí

$$[f]_B^B = \begin{pmatrix}0&1&0&0\\0&0&0&0\\0&0&0&1\\0&0&0&0\end{pmatrix} .$$

▲

Příklad 9.104. Uvažujme operátor $f_A : \mathbb{R}^4 \to \mathbb{R}^4$ pro matici

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

Charakteristický polynom vyjde $p_A(\lambda) = (\lambda - 4)^4$, operátor f_A má vlastní číslo 4 algebraické násobnosti 4.

$$M_4 = \mathrm{Ker}\,(f_A - 4\,\mathrm{id}) = \mathrm{Ker}\,(A - 4I_4) = \mathrm{Ker}\begin{pmatrix}1&0&0&-1\\1&0&0&-1\\0&1&-1&0\\0&1&-1&0\end{pmatrix} = \mathrm{LO}\left\{\begin{pmatrix}1\\0\\0\\1\end{pmatrix}, \begin{pmatrix}0\\1\\1\\0\end{pmatrix}\right\} .$$

Geometrická násobnost vlastního čísla 4 je 2. Operátor bude mít dva řetízky. Abychom zjistili jejich délky, spočítáme $\mathrm{Ker}\,(f_A - 4\,\mathrm{id})^2$.

$$\mathrm{Ker}\,(f_A - 4\,\mathrm{id})^2 = \mathrm{Ker}\begin{pmatrix}1&-1&1&-1\\1&-1&1&-1\\1&-1&1&-1\\1&-1&1&-1\end{pmatrix} = \mathrm{LO}\left\{\begin{pmatrix}1\\0\\0\\1\end{pmatrix}, \begin{pmatrix}-1\\0\\1\\0\end{pmatrix}, \begin{pmatrix}1\\1\\0\\0\end{pmatrix}\right\} .$$

Dimenze je o 1 vyšší než dimenze $\operatorname{Ker}(A - 4I_4)$, takže počet řetízků délky alespoň 2 je 1. Hledaná báze B je tedy spojením řetízku délky 1 a řetízku délky 3.

$$\begin{array}{ccccccc} & & & & \mathbf{v}_1^1 & \xmapsto{f_A - 4\,\mathrm{id}} & \mathbf{o} \\ \mathbf{v}_3^2 & \xmapsto{f_A - 4\,\mathrm{id}} & \mathbf{v}_2^2 & \xmapsto{f_A - 4\,\mathrm{id}} & \mathbf{v}_1^2 & \xmapsto{f_A - 4\,\mathrm{id}} & \mathbf{o}\ . \end{array}$$

Protože $\operatorname{Im}(f - 4\,\mathrm{id})^2 = \mathrm{LO}\left\{\mathbf{v}_1^2\right\}$, zvolíme vektor $\mathbf{v}_1^2$ v tomto prostoru, např. $\mathbf{v}_1^2 = (1,1,1,1)^T$. Je $\operatorname{Ker}(f - 4\,\mathrm{id}) = \mathrm{LO}\left\{\mathbf{v}_1^1, \mathbf{v}_1^2\right\}$, doplníme vektor $\mathbf{v}_1^2$ na bázi prostoru $\operatorname{Ker}(f - 4\,\mathrm{id})$, například vektorem $\mathbf{v}_1^1 = (1,0,0,1)^T$.

Vektor $\mathbf{v}_2^2$ musíme zvolit tak, aby $(f_A - 4\,\mathrm{id})(\mathbf{v}_2^2) = \mathbf{v}_1^2$ a aby $\mathbf{v}_2^2 \in \operatorname{Im}(f_A - 4\,\mathrm{id})$ (druhou podmínku již nemůžeme ignorovat jako v předcházejícím příkladu). Množina všech řešení soustavy $(A - 4I_4)\mathbf{v}_2^2 = (1,1,1,1)^T$ je

$$\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \mathrm{LO}\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right\}\ .$$

Obraz operátoru $f_A - 4\,\mathrm{id}$ je lineární obal sloupců matice $A - 4I_4$, který se rovná $\mathrm{LO}\left\{(1,1,0,0)^T, (0,0,1,1)^T\right\}$. Oběma podmínkám vyhovuje například vektor $\mathbf{v}_2^2 = (1,1,0,0)^T$. Nyní už stačí vzít libovolný vektor $\mathbf{v}_3^2$ tak, aby platilo $(f_A - 4\,\mathrm{id})\mathbf{v}_3^2 = \mathbf{v}_2^2$, např. $\mathbf{v}_3^2 = (1,0,0,0)^T$.

Podle věty 9.93 je $B = (\mathbf{v}_1^1, \mathbf{v}_1^2, \mathbf{v}_2^2, \mathbf{v}_3^2)$ báze. Vzhledem k B má operátor f matici

$$[f]_B^B = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 1 & 0 \\ 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 4 \end{pmatrix}$$

▲

Na příkladu si rozmyslíme postup v ještě vyšší dimenzi.

PŘÍKLAD 9.105. Operátor $f : \mathbf{V} \to \mathbf{V}$ na prostoru $\mathbf{V}$ dimenze 15 splňuje následující podmínky.

(1) f má vlastní číslo 31 algebraické násobnosti 11 a vlastní číslo 47 algebraické násobnosti 4,
(2) $\dim \operatorname{Ker}(f - 31\,\mathrm{id}) = 4$, $\dim \operatorname{Ker}(f - 47\,\mathrm{id}) = 2$,
(3) $\dim \operatorname{Ker}(f - 31\,\mathrm{id})^2 = 7$, $\dim \operatorname{Ker}(f - 47\,\mathrm{id})^2 = 3$,
(4) $\dim \operatorname{Ker}(f - 31\,\mathrm{id})^3 = 9$,
(5) $\dim \operatorname{Ker}(f - 31\,\mathrm{id})^4 = 11$.

Rozmyslíme si, že existuje báze B, pro které je $[f]_B^B$ v Jordanově tvaru, z jakých bloků se $[f]_B^B$ skládá a jak bychom takovou bázi hledali.

Z první podmínky vidíme, že pro f existuje Jordanův kanonický tvar, celkový počet vektorů v řetízcích příslušným vlastnímu číslu 31 je 11 a celkový počet vektorů v řetízcích příslušných vlastnímu číslu 47 je 4.

Zaměříme se nejprve na vlastní číslo 47 a příslušné řetízky. Z druhé podmínky vyplývá, že řetízky jsou 2, takže zbývají dvě možnosti: délky 1, 3, nebo délky 2,2. Ze třetí podmínky máme $\dim \operatorname{Ker}(f - 47\,\mathrm{id})^2 - \dim \operatorname{Ker}(f - 47\,\mathrm{id}) = 1$, takže máme právě jeden řetízek délky alespoň 2, což vylučuje první možnost. Řetízky příslušné vlastnímu číslu 47 tedy budou

$$\begin{array}{ccccccc} & & & & \mathbf{v}_1^1 & \xmapsto{f - 47\,\mathrm{id}} & \mathbf{o} \\ \mathbf{v}_3^2 & \xmapsto{f - 47\,\mathrm{id}} & \mathbf{v}_2^2 & \xmapsto{f - 47\,\mathrm{id}} & \mathbf{v}_1^2 & \xmapsto{f - 47\,\mathrm{id}} & \mathbf{o} \end{array}$$

Počet řetízků pro vlastní číslo 31 je podle druhé podmínky 4. Ze třetí podmínky máme $\dim \operatorname{Ker}(f-31\,\mathrm{id})^2 - \dim \operatorname{Ker}(f-31\,\mathrm{id}) = 3$, takže tři řetízky mají délku alespoň 2. Možnosti délek jsou $1+2+2+6$, $1+2+3+5$, $1+2+4+4$, $1+3+3+4$. Z předposlední podmínky víme, že počet řetízků délky alespoň 3 je 2 (protože $\dim \operatorname{Ker}(f-31\,\mathrm{id})^3 - \dim \operatorname{Ker}(f-31\,\mathrm{id})^2 = 2$). Zbývají dvě možnosti $1+2+3+5$ a $1+2+4+4$, první možnost vylučuje poslední podmínka. Řetízky příslušné vlastnímu číslu 31 jsou

$$\begin{array}{ccccccccc}
 & & & & & & \mathbf{v}_1^3 & \xmapsto{f-31\,\mathrm{id}} & \mathbf{o} \\
 & & & & \mathbf{v}_2^4 & \xmapsto{f-31\,\mathrm{id}} & \mathbf{v}_1^4 & \xmapsto{f-31\,\mathrm{id}} & \mathbf{o} \\
\mathbf{v}_4^5 & \xmapsto{f-31\,\mathrm{id}} & \mathbf{v}_3^5 & \xmapsto{f-31\,\mathrm{id}} & \mathbf{v}_2^5 & \xmapsto{f-31\,\mathrm{id}} & \mathbf{v}_1^5 & \xmapsto{f-31\,\mathrm{id}} & \mathbf{o} \\
\mathbf{v}_4^6 & \xmapsto{f-31\,\mathrm{id}} & \mathbf{v}_3^6 & \xmapsto{f-31\,\mathrm{id}} & \mathbf{v}_2^6 & \xmapsto{f-31\,\mathrm{id}} & \mathbf{v}_1^6 & \xmapsto{f-31\,\mathrm{id}} & \mathbf{o}
\end{array}$$

Vzhledem k bázi B složené z těchto řetízků bude

$$[f]_B^B = \operatorname{diag}(J_{47,1}, J_{47,3}, J_{31,1}, J_{31,2}, J_{31,4}, J_{31,4}) \ .$$

Řetízky bychom opět hledali od počátků. Zaměříme se na vlastní číslo 31. Protože $\operatorname{Im}(f-31\,\mathrm{id})^3 \cap \operatorname{Ker}(f-31\,\mathrm{id}) = \mathrm{LO}\left\{\mathbf{v}_1^5, \mathbf{v}_1^6\right\}$, vektory $\mathbf{v}_1^5, \mathbf{v}_1^6$ bychom zvolili tak, aby tvořili bázi tohoto průniku. Tyto dva vektory bychom doplnili vektorem $\mathbf{v}_1^4$ do báze prostoru $\operatorname{Ker}(f-31\,\mathrm{id}) \cap \operatorname{Im}(f-31\,\mathrm{id})$. A vektory $\mathbf{v}_1^4, \mathbf{v}_1^5, \mathbf{v}_1^6$ doplnili vektorem $\mathbf{v}_1^3$ do báze prostoru $\operatorname{Ker}(f-31\,\mathrm{id})$. Pak bychom pro každý počáteční vektor postupně doplnili zbylé vektory do řetízku. Rozmyslíme si třetí z řetízků. Vektor $\mathbf{v}_2^5$ bychom zvolili tak, aby $(f-31\,\mathrm{id})(\mathbf{v}_2^5) = \mathbf{v}_1^5$ a zároveň $\mathbf{v}_2^5 \in \operatorname{Im}(f-31\,\mathrm{id})^2$ (druhá podmínka je nutná, abychom mohli pokračovat). Dále vektor $\mathbf{v}_3^5$ bychom zvolili tak, aby $(f-31\,\mathrm{id})(\mathbf{v}_3^5) = \mathbf{v}_2^5$ a $\mathbf{v}_3^5 \in \operatorname{Im}(f-31\,\mathrm{id})$. Konečně vektor $\mathbf{v}_4^5$ bychom zvolili tak, aby $(f-31\,\mathrm{id})(\mathbf{v}_4^5) = \mathbf{v}_3^5$.

Podobně bychom posupovali pro další řetízky a druhé vlastní číslo 47. ▲

9.4.9. Řešení spojitého dynamického systému. V odstavci 9.3.6 jsme ukázali, jak vyřešit spojitý dynamický systém $\mathbf{x}'(t) = A\mathbf{x}(t)$ v případě, že A je diagonalizovatelná matice. Řešení spočívalo v tom, že jsme původní soustavu převedli na soustavu $\mathbf{y}'(t) = D\mathbf{y}(t)$, kde D je diagonální matice, a takovou soustavu již umíme řešit. Stejný postup lze použít pro matici podobnou matici v Jordanově tvaru, získáme soustavu $\mathbf{y}'(t) = J\mathbf{y}(t)$, kde J je v Jordanově tvaru.

Zopakujeme tento postup. Předpokládejme, že pro f_A existuje Jordanův kanonický tvar. Pak umíme najít matici J v Jordanově tvaru a regulární matici R takovou, že $J = R^{-1}AR$. (Připomeňme, že R je matice přechodu od báze B tvořené spojením Jordanových řetízků matice A ke kanonické bázi a $J = [f_A]_B^B$.) Úpravou dostaneme $A = RJR^{-1}$ a rovnici můžeme ekvivalentně přepsat

$$\begin{aligned}
\mathbf{x}'(t) &= RJR^{-1}\mathbf{x}(t) \\
R^{-1}\mathbf{x}'(t) &= JR^{-1}\mathbf{x}(t) \ .
\end{aligned}$$

Definujeme $\mathbf{y}(t) = R^{-1}\mathbf{x}(t)$ a dostaneme

$$\mathbf{y}'(t) = J\mathbf{y}(t) \ .$$

Původní funkce $\mathbf{x}(t)$ dopočteme ze vztahu $\mathbf{x}(t) = R\mathbf{y}(t)$.

Stačí tedy umět řešit spojité dynamické systémy tvaru $\mathbf{y}'(t) = J\mathbf{y}(t)$, kde J je matice v Jordanově kanonickém tvaru. Pro diagonální matici J jsme v 9.3.6 ukázali, že řešením

$$\begin{pmatrix} y_1'(t) \\ y_2'(t) \\ \vdots \\ y_n'(t) \end{pmatrix} = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ & & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix} \begin{pmatrix} y_1(t) \\ y_2(t) \\ \vdots \\ y_n(t) \end{pmatrix} \ .$$

funkce

$$\begin{pmatrix} y_1(t) \\ y_2(t) \\ \vdots \\ y_n(t) \end{pmatrix} = \begin{pmatrix} y_1(0)e^{\lambda_1 t} \\ y_2(0)e^{\lambda_2 t} \\ \vdots \\ y_n(0)e^{\lambda_n t} \end{pmatrix} = \begin{pmatrix} e^{\lambda_1 t} & 0 & \dots & 0 \\ 0 & e^{\lambda_2 t} & \dots & 0 \\ & & \ddots & \vdots \\ 0 & 0 & \dots & e^{\lambda_n t} \end{pmatrix} \begin{pmatrix} y_1(0) \\ y_2(0) \\ \vdots \\ y_n(0) \end{pmatrix} .$$

Ukážeme si řešení v případě Jordanovy buňky řádu 2

$$\begin{pmatrix} y_1'(t) \\ y_2'(t) \end{pmatrix} = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} y_1(t) \\ y_2(t) \end{pmatrix} .$$

Řešíme tedy spojitý dynamický systém

$$\begin{aligned} y_1'(t) &= \lambda y_1(t) + y_2(t) \\ y_2'(t) &= \lambda y_2(t) \ . \end{aligned}$$

(V řeči operátorů, $y_2(t)$ je vlastním vektorem operátoru derivování, $y_1(t)$ je zobecněným vlastním vektorem.) Z druhé rovnice máme $y_2(t) = y_2(0)e^{\lambda t}$. Dosazením do první rovnice dostáváme

$$y_1'(t) = \lambda y_1(t) + y_2(0)e^{\lambda t} \ ,$$

což přepíšeme do tvaru

$$y_1'(t) - \lambda y_1(t) = y_2(0)e^{\lambda t} \ .$$

Funkci $y_1(t)$ najdeme pomocí následujícího triku – napíšeme si ji jako součin $y_1(t) = u(t)v(t)$ dvou jiných funkcí. Po dosazení do předchozí rovnosti a použití vzorečku pro derivaci součinu dvou funkcí dostaneme

$$u'(t)v(t) + u(t)v'(t) - \lambda u(t)v(t) = y_2(0)e^{\lambda t}$$

neboli

$$u'(t)v(t) + u(t)(v'(t) - \lambda v(t)) = y_2(0)e^{\lambda t} \ .$$

Funkci $v(t)$ zvolíme tak, aby byla závorka na levé straně rovná 0, tj. tak aby platilo $v'(t) = \lambda v(t)$ pro každé $t \in \mathbb{R}$. Jednou z možností je zvolit $v(t) = e^{\lambda t}$. Tím se poslední rovnice redukuje na

$$u'(t)e^{\lambda t} = y_2(0)e^{\lambda t}$$

a tedy

$$u'(t) = y_2(0) \ .$$

Pro libovolnou konstantu d funkce $u(t) = y_2(0)t + d$ splňuje poslední rovnici, takže

$$y_1(t) = u(t)v(t) = (y_2(0)t + d)e^{\lambda t} = y_2(0)te^{\lambda t} + de^{\lambda t}.$$

Dosazením $t = 0$ vyjde $y_1(0) = d$. Dostali jsem tak, že musí platit

$$y_1(t) = y_2(0)te^{\lambda t} + y_1(0)e^{\lambda t} \ .$$

Řešením spojitého dynamického systému

$$\begin{aligned} y_1'(t) &= \lambda y_1(t) + y_2(t) \\ y_2'(t) &= \lambda y_2(t) \end{aligned}$$

jsou tedy funkce

$$\begin{pmatrix} y_1(t) \\ y_2(t) \end{pmatrix} = \begin{pmatrix} y_2(0)te^{\lambda t} + y_1(0)e^{\lambda t} \\ y_2(0)e^{\lambda t} \end{pmatrix} = \begin{pmatrix} e^{\lambda t} & te^{\lambda t} \\ 0 & e^{\lambda t} \end{pmatrix} \begin{pmatrix} y_1(0) \\ y_2(0) \end{pmatrix} .$$

Uvedeným postupem jsme našli všechna možná řešení $(y_1(t), y_2(t))^T$. Jednoznačnost funkce $y_2(t) = y_2(0)e^{\lambda t}$ jsme si ukázali už v tvrzení 9.7. Pokud jde o jednoznačnost funkce $y_1(t)$, můžeme se o ní přesvědčit také přímo podobně jako v tvrzení 9.7. Stačí spočítat, že pro každou funkci $f(t)$ splňující rovnost $f'(t) = \lambda f(t) + y_2(0)e^{\lambda t}$ a $f(0) = y_1(0)$ je derivace funkce $(f(t) - y_2(0)te^{\lambda t})e^{-\lambda t}$ rovná 0.

Příklad 9.106. Vyřešíme spojitý dynamický systém

$$\begin{pmatrix} x_1'(t) \\ x_2'(t) \end{pmatrix} = A \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 4 & -3 \end{pmatrix} \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix}$$

s počáteční podmínkou $x_1(0) = 3, x_2(0) = 4$. V příkladu 9.99 jsme vypočetli, že vzhledem k bázi $B = ((1,2)^T, (0,-1)^T)$ je $[f]_B^B = J_{-1,2}$, tj. platí

$$A = RAR^{-1}, \text{ kde } J = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \text{ a } R = [\mathrm{id}]_K^B = \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} .$$

Původní soustavu si přepíšeme do tvaru

$$\begin{pmatrix} x_1'(t) \\ x_2'(t) \end{pmatrix} = R \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} R^{-1} \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix} .$$

a poté

$$R^{-1} \begin{pmatrix} x_1'(t) \\ x_2'(t) \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} R^{-1} \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix} .$$

Označíme-li

$$\begin{pmatrix} y_1(t) \\ y_2(t) \end{pmatrix} = R^{-1} \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix} ,$$

platí

$$\begin{pmatrix} y_1'(t) \\ y_2'(t) \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} y_1(t) \\ y_2(t) \end{pmatrix} .$$

Řešením je

$$\begin{pmatrix} y_1(t) \\ y_2(t) \end{pmatrix} = \begin{pmatrix} e^{-t} & te^{-t} \\ 0 & e^{-t} \end{pmatrix} \begin{pmatrix} y_1(0) \\ y_2(0) \end{pmatrix} ,$$

takže

$$\begin{aligned} \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix} &= R \begin{pmatrix} y_1(t) \\ y_2(t) \end{pmatrix} = R \begin{pmatrix} e^{-t} & te^{-t} \\ 0 & e^{-t} \end{pmatrix} \begin{pmatrix} y_1(0) \\ y_2(0) \end{pmatrix} \\ &= R \begin{pmatrix} e^{-t} & te^{-t} \\ 0 & e^{-t} \end{pmatrix} R^{-1} \begin{pmatrix} x_1(0) \\ x_2(0) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} e^{-t} & te^{-t} \\ 0 & e^{-t} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \\ &= \begin{pmatrix} 3e^{-t} + 2te^{-t} \\ 4e^{-t} + 4te^{-t} \end{pmatrix} . \end{aligned}$$

▲

Příklad 9.107. Tři chemikálie E, F, G spolu reagují podle schématu

$$E \longrightarrow F \longrightarrow G .$$

To znamená, že E se při reakci mění na F a F se mění na G. Rychlost přeměny je přímo úměrná koncentraci, pro jednoduchost bude v naší reakci koeficient úměrnosti rovný 1. Na začátku, v čase $t = 0$, bude přítomná pouze chemikálie E. Zajímá nás, jak se budou koncentrace všech tří chemikálií vyvíjet v čase.

Označme $\mathbf{x}(t) = (x_E(t), x_F(t), x_G(t))^T$ vektor koncentrací v čase t. Z popisu reakce vyplývá, že koncentrace splňují

$$\begin{aligned} x_E'(t) &= -x_E(t) \\ x_F'(t) &= x_E(t) - x_F(t) \\ x_G'(t) &= x_F(t) . \end{aligned}$$

Navíc víme, že $\mathbf{x}(0) = (1, 0, 0)^T$. Maticově zapsáno máme

$$\mathbf{x}'(t) = A\mathbf{x}(t), \quad \text{kde } A = \begin{pmatrix} -1 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \ \mathbf{x}(0) = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} .$$

Nyní již stačí aplikovat probraný postup. Zjistíme, že matice A se rovná

$$A = RJR^{-1}, \text{ kde } R = \begin{pmatrix} 0 & -1 & 0 \\ -1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \ J = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} .$$

(R je matice přechodu od báze B tvořené spojením Jordanových řetízků ke kanonické bázi a $J = [f_A]_B^B$.) Označíme $\mathbf{y}(t) = R^{-1}\mathbf{x}(t)$ a původní soustavu přepíšeme do tvaru

$$\mathbf{y}'(t) = J\mathbf{y}(t) = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \mathbf{y}(t) .$$

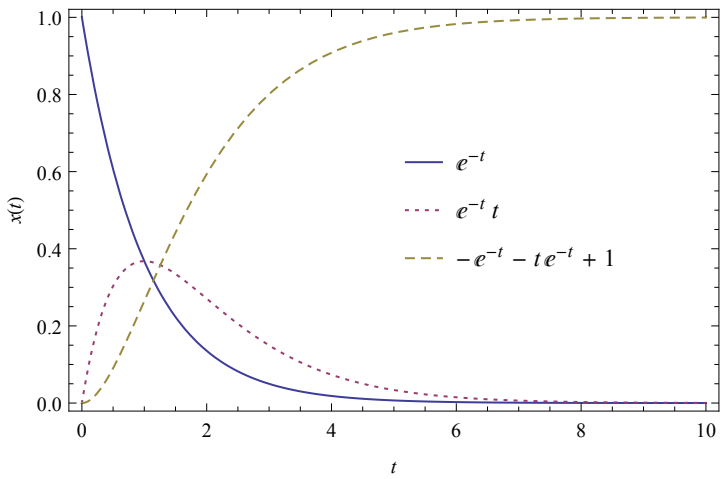
Podle předchozího příkladu dostáváme řešení

$$\mathbf{y}(t) = \begin{pmatrix} e^{-t} & te^{-t} & 0 \\ 0 & e^{-t} & 0 \\ 0 & 0 & e^{0t} \end{pmatrix} \mathbf{y}(0) .$$

Z toho

$$\mathbf{x}(t) = R \begin{pmatrix} e^{-t} & te^{-t} & 0 \\ 0 & e^{-t} & 0 \\ 0 & 0 & e^{0t} \end{pmatrix} R^{-1}\mathbf{x}(0) = \begin{pmatrix} e^{-t} \\ te^{-t} \\ -e^{-t} - te^{-t} + 1 \end{pmatrix} .$$

Koncentrace chemikálií E, F, G v čase t tedy bude $x_E(t) = e^{-t}$, $x_F(t) = te^{-t}$, $x_G(t) = -e^{-t} - te^{-t} + 1$.



Obrázek 9.12. Grafy průběhu koncentrací jednotlivých chemikálií.

▲

Poznamenejme, že obecněji pro Jordanovu buňku $J_{\lambda,n}$ jsou řešením spojitého dynamického systému $\mathbf{y}'(t) = J_{\lambda,n}\mathbf{y}(t)$ funkce

$$\begin{pmatrix} y_1(t) \\ y_2(t) \\ \vdots \\ y_{n-1}(t) \\ y_n(t) \end{pmatrix} = \begin{pmatrix} e^{\lambda t} & \frac{t}{1!}e^{\lambda t} & \frac{t^2}{2!}e^{\lambda t} & \dots & \frac{t^{n-1}}{(n-1)!}e^{\lambda t} \\ 0 & e^{\lambda t} & \frac{t}{1!}e^{\lambda t} & \dots & \frac{t^{n-2}}{(n-2)!}e^{\lambda t} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & e^{\lambda t} & \frac{t}{1!}e^{\lambda t} \\ 0 & 0 & \dots & 0 & e^{\lambda t} \end{pmatrix} \begin{pmatrix} y_1(0) \\ y_2(0) \\ \vdots \\ y_{n-1}(0) \\ y_n(0) \end{pmatrix} .$$

Stačí k tomu použít indukci podle n a v indukčním kroku stejný trik jako v případě Jordanovy buňky řádu 2.

9.4.10. Invariantní podprostory. Invariantní podprostory operátoru f jsou podprostory, které operátor f zachovává v následujícím smyslu.

Definice 9.108. Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na vektorovém prostoru $\mathbf{V}$, pak podprostor $\mathbf{W} \leq \mathbf{V}$ nazýváme *invariantní podprostor operátoru* f, pokud platí pro každý vektor $\mathbf{x} \in W$, že také $f(\mathbf{x}) \in W$.

Invariantní podprostor čtvercové matice A definujeme jako invariantní podprostor operátoru f_A určeného maticí A.

Příklad 9.109. Každý operátor má dva triviální invariantní podprostory $\{\mathbf{o}\}$ a $\mathbf{V}$.

Z geometrického náhledu vidíme, že rotace v $\mathbb{R}^2$ o úhel α, který není násobkem π, má pouze triviální invariantní podprostory.

Osová souměrnost v $\mathbb{R}^2$ podle přímky LO $\{\mathbf{v}\}$ má kromě triviálních podprostorů ještě dva invariantní podprostory: LO $\{\mathbf{v}\}$ a $\mathbf{v}^\perp$ (ortogonální doplněk je vzhledem ke standardnímu skalárnímu součinu.)

Pro rotaci v $\mathbb{R}^3$ kolem přímky LO $\{\mathbf{p}\}$ jsou LO $\{\mathbf{p}\}$ a $\mathbf{p}^\perp$ invariantní podprostory. Rotace o π má ještě další invariantní podprostory.

Každý podprostor prostoru $\mathbf{V}$ je invariantním podprostorem operátoru id a také operátoru $\lambda\,\mathrm{id}$ pro libolný skalár λ. ▲

Tvrzení 9.110. *Pro každý lineární operátor $f : \mathbf{V} \to \mathbf{V}$ jsou následující podprostory $\mathbf{V}$ invariantní podprostory operátoru f:*

(1) $\mathrm{Ker}\,(f)$,
(2) $\mathrm{Im}\,(f)$,
(3) *podprostor* LO $\{\mathbf{u}\}$ *generovaný libovolným nenulovým vlastním vektorem* $\mathbf{u}$ *operátoru f,*
(4) *obecněji, podprostor* LO $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ *generovaný Jordanovým řetízkem* $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ *operátoru f příslušným vlastnímu číslu λ.*

Důkaz. Body (1) a (2) jsou triviální. Bod (3) je speciálním případem bodu (4).

Pro důkaz (4) uvažujme libovolný vektor $\mathbf{x} = a_1\mathbf{v}_1 + \cdots + a_k\mathbf{v}_k$. Jeho obraz je po úpravě

$$f(\mathbf{x}) = a_1 f(\mathbf{v}_1) + a_2 f(\mathbf{v}_2) + \cdots + a_k f(\mathbf{v}_k) = a_1\lambda\mathbf{v}_1 + a_2(\lambda\mathbf{v}_2 + \mathbf{v}_1) + \cdots + a_k(\lambda\mathbf{v}_k + \mathbf{v}_{k-1}) \ .$$

Výraz na pravé straně jde vyjádřit jako lineární kombinaci vektorů $\mathbf{v}_1, \ldots, \mathbf{v}_k$, takže skutečně $f(\mathbf{x}) \in \mathrm{LO}\,\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$. ▲

Další invariantní podprostory můžeme získat průniky a součty invariantních podprostorů.

Tvrzení 9.111. *Jsou-li $\mathbf{U}$ a $\mathbf{W}$ dva invariantní podprostory operátoru $f : \mathbf{V} \to \mathbf{V}$, pak jsou podprostory $\mathbf{U} \cap \mathbf{W}$ a $\mathbf{U} + \mathbf{W}$ rovněž invariantními podprostory operátoru f.*

Důkaz. Je-li $\mathbf{x} \in U \cap W$, pak $f(\mathbf{x}) \in U$, protože $\mathbf{U}$ je invariatní, a $f(\mathbf{x}) \in W$, protože $\mathbf{W}$ je invariantní. Z toho plyne $f(\mathbf{x}) \in U \cap W$.

Je-li $\mathbf{x} \in U + W$, pak existují vektory $\mathbf{u} \in U$, $\mathbf{w} \in W$ takové, že $\mathbf{x} = \mathbf{u} + \mathbf{w}$. Z invariance U a W víme, že $f(\mathbf{u}) \in U$ a $f(\mathbf{w}) \in W$, proto $f(\mathbf{x}) = f(\mathbf{u} + \mathbf{w}) = f(\mathbf{u}) + f(\mathbf{w}) \in U + W$. ▲

Z předchozích dvou tvrzení vyplývá, že lineární obal spojení libovolného počtu Jordanových řetízků nějakého operátoru je jeho invariantním podprostorem.

Je-li $\mathbf{W}$ invariantní podprostor operátoru f, pak zúžení $g = f|_W$ operátoru f na podprostor $\mathbf{W}$ je lineární operátor na prostoru $\mathbf{W}$. Je zřejmé, že každé vlastní číslo operátoru $g = f|_W$ je vlastním číslem operátoru f a každý vlastní vektor operátoru g je také vlastním vektorem operátoru f (příslušný stejnému vlastnímu číslu). Dokážeme silnější tvrzení. Metodu důkazu jsme použili už v důkazu věty o tom, že geometrická násobnost libovolného vlastního čísla operátoru f je nejvýše rovná jeho algebraické násobnosti.

Tvrzení 9.112. *Buď $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na konečně dimenzionálním prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ a $\mathbf{W} \leq \mathbf{V}$ invariantní podprostor operátoru f. Potom charakteristický polynom zúžení $g = f|_W$ operátoru f na podprostor $\mathbf{W}$ dělí charakteristický polynom operátoru f.*

Důkaz. Zvolme nějakou bázi $C = (\mathbf{v}_1, \ldots, \mathbf{v}_k)$ podprostoru $\mathbf{W}$ a doplňme ji na bázi $B = (\mathbf{v}_1, \ldots, \mathbf{v}_k, \mathbf{v}_{k+1}, \ldots, \mathbf{v}_n)$ prostoru $\mathbf{V}$. Pro každý vektor $\mathbf{v}_j$, $j = 1, \ldots, k$ platí $f(\mathbf{v}_j) \in W$, neboť $\mathbf{W}$ je invariantní podprostor operátoru f. Vyjádření $[f(\mathbf{v}_j)]_B$ vektoru $f(\mathbf{v}_j)$ v bázi B proto bude mít složky $k+1, \ldots, n$ nulové a vektor tvořený

prvními k složkami bude rovný $[g(\mathbf{v}_j)]_C$. Matice $[f]_B^B$ operátoru f vzhledem k bázi B má potom blokový tvar

$$[f]_B^B = \begin{pmatrix} A & E \\ 0 & F \end{pmatrix} ,$$

kde $A = [g]_C^C$, F je nějaká čtvercová matice řádu $n-k$ a E je matice typu $k \times (n-k)$. Potom

$$[f]_B^B - \lambda I_n = \begin{pmatrix} A - \lambda I_k & E \\ 0 & F - \lambda I_{n-k} \end{pmatrix} ,$$

$p_f(\lambda) = \det([f]_B^B - \lambda I_n) = \det(A - \lambda I_k)\det(F - \lambda I_{n-k})$ a $p_g(\lambda) = \det([g]_C^C - \lambda I_n) = \det(A - \lambda I_k)$. Takže $p_g(\lambda)$ skutečně dělí $p_f(\lambda)$. ▲

Formulujeme důležitý důsledek.

Důsledek 9.113. *Nechť $f : \mathbf{V} \to \mathbf{V}$ je operátor na prostoru $\mathbf{V}$ dimenze n a $\mathbf{W}$ je invariantní podprostor operátoru f dimenze k. Pokud má operátor f právě n vlastních čísel včetně násobností, pak má operátor $g = f|_W : \mathbf{W} \to \mathbf{W}$ právě k vlastních čísel včetně násobností.*

Důkaz. Bez důkazu použijeme tvrzení, které dokážete v kurzu algebry – pokud se polynom rozkládá na lineární faktory, pak se na lineární faktory rozkládá i libovolný jeho dělitel.

Pokud má operátor f právě n vlastních čísel včetně násobností, pak se jeho charakteristický polynom $p_f(\lambda)$ rozkládá na lineární faktory. Polynom $p_g(\lambda)$ podle předchozího tvrzení dělí polynom $p_f(\lambda)$, z toho vyplývá, že se $p_g(\lambda)$ rovněž rozkládá na lineární faktory, operátor g má tedy k vlastních čísel včetně násobností. ▲

Příklad 9.114. Uvažujme operátor $f = f_A : \mathbb{R}^3 \to \mathbb{R}^3$ určený maticí

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

Ukážeme, že $\mathbf{W} = \mathrm{LO}\{\mathbf{u}, \mathbf{v}\} = \mathrm{LO}\left\{(0,1,0)^T, (1,1,2)^T\right\}$ je jeho invariatní podprostor. Platí $f(\mathbf{u}) = (0,-1,0)^T$ a $f(\mathbf{v}) = (1,-1,2)^T$. Obrazy obou generátorů jsou lineární kombinace vektorů $\mathbf{u}, \mathbf{v}$:

$$f(\mathbf{u}) = -\mathbf{u}, \quad f(\mathbf{v}) = -2\mathbf{u} + \mathbf{v} \ .$$

Z toho vyplývá, že každý vektor z W se zobrazí do W: Je-li totiž $\mathbf{x} = a\mathbf{u} + b\mathbf{v}$, pak $f(\mathbf{x}) = af(\mathbf{u}) + bf(\mathbf{v})$. Podprostor $\mathbf{W}$ je tedy invariantní podprostor operátoru f. (Operátor f_A je shodný s operátorem v příkladu 9.100, podprostor $\mathbf{W}$ je rovný lineárnímu obalu vlastních vektorů.)

Podívejme se ještě na operátor $g = f|_W$. Jeho matice vzhledem k bázi $C = (\mathbf{u}, \mathbf{v})$ je

$$[g]_C^C = \begin{pmatrix} -1 & -2 \\ 0 & 1 \end{pmatrix}$$

Charakteristický polynom operátoru g je $p_g(\lambda) = (\lambda - 1)(\lambda + 1)$ a příslušné vlastní podprostory jsou

$$[M_1]_C = \mathrm{LO}\left\{\begin{pmatrix} -1 \\ 1 \end{pmatrix}\right\}, \quad [M_{-1}]_C = \mathrm{LO}\left\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right\} ,$$

neboli

$$M_1 = \mathrm{LO}\{-u + v\} = \mathrm{LO}\left\{(1,0,2)^T\right\}, \quad M_{-1} = \mathrm{LO}\{u\} = \mathrm{LO}\left\{(0,1,0)^T\right\}$$

Matice operátoru g vzhledem k bázi $D = ((1,0,2)^T, (0,1,0)^T)$ je

$$[g]_D^D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} .$$

Geometricky, operátor g je reflexe podle přímky LO $\{(1,0,2)^T\}$ ve směru přímky LO $\{(0,1,0)^T\}$. To nám dává představu, jak operátor f „vypadá“ v rovině $\mathbf{W}$.

Pro ilustraci předchozího tvrzení ještě uveďme, že $p_f(\lambda) = -(\lambda-1)^2(\lambda+1)$. Polynom $p_g(\lambda)$ skutečně dělí polynom $p_f(\lambda)$. ▲

Na závěr si ještě všimneme, že množina operátorů, pro které je daný podprostor $\mathbf{W}$ prostoru $\mathbf{V}$ invariantní, je uzavřená na sčítání a násobení skalárem.

TVRZENÍ 9.115. *Nechť $\mathbf{V}$ je vektorový prostor, $\mathbf{W}$ jeho podprostor, f, g lineární operátory na $\mathbf{V}$ a $t \in T$. Pak platí:*

(1) *Je-li $\mathbf{W}$ invariantní podprostor operátorů f i g, pak je $\mathbf{W}$ invariantní podprostor operátoru $f+g$.*
(2) *Je-li $\mathbf{W}$ invariantní podprostor operátoru f, pak je $\mathbf{W}$ invariantní podprostor operátoru tf.*

DŮKAZ. (1). Je-li $\mathbf{x} \in W$ a $f(\mathbf{x}) \in W$, $g(\mathbf{x}) \in W$, pak $(f+g)(\mathbf{x}) = f(\mathbf{x}) + g(\mathbf{x}) \in W$.

(2). Je-li $\mathbf{x} \in W$ a $f(\mathbf{x}) \in W$, pak $(tf)(\mathbf{x}) = t(f(\mathbf{x})) \in W$. ▲

Například, je-li $\mathbf{W}$ invariatní podprostor operátoru f, pak je také invariantním podprostorem operátoru $f - \lambda\,\mathrm{id}$ pro libovolné $\lambda \in T$.

9.4.11. Důkaz věty o Jordanově kanonickém tvaru. Nyní dokážeme chybějící implikaci ve větě 9.97 o Jordanově kanonickém tvaru. Předpokládejme, že $\mathbf{V}$ je konečně generovaný prostor dimenze n a $f : \mathbf{V} \to \mathbf{V}$ je lineární operátor, který má n vlastních čísel včetně algebraických násobností. Chceme dokázat, že pro operátor f existuje Jordanův kanonický tvar.

Větu dokážeme tak, že najdeme bázi $\mathbf{V}$, která je spojením Jordanových řetízků operátoru $\mathbf{V}$. Postupovat budeme indukcí podle dimenze n.

Je-li $n = 1$, matice f vzhledem k jakékoliv bázi B prostoru $\mathbf{V}$ má řád 1 a je tedy Jordanovo buňkou a báze B je tvořena jedním Jordanovým řetízkem délky 1. Předpokládejme, že $n > 1$ a že tvrzení platí pro všechna menší n.

Označme λ libovolné vlastní číslo operátoru f a pro přehlednost označme $g = f - \lambda\,\mathrm{id}$. Pak $\dim(\operatorname{Ker} g) > 0$ (protože prostor $\operatorname{Ker} g$ je tvořen vlastními vektory operátoru f příslušnými vlastnímu číslu λ) a podle věty o dimenzi jádra a obrazu je $\dim(\operatorname{Im} g) = n - \dim(\operatorname{Ker} g) < n$.

Podprostor $\operatorname{Im} g$ je podle tvrzení 9.110 invariantním podprostorem operátoru g, takže také operátoru $f = g + \lambda\,\mathrm{id}$ (viz tvrzení 9.115). Charakteristický polynom zúžení h operátoru f na $\operatorname{Im} g$ dělí charakteristický polynom operátoru f, a ten má n vlastních čísel včetně násobností. Operátor h má podle důsledku 9.113 $\dim \operatorname{Im} g$ vlastních čísel včetně násobností, takže na něj můžeme použít indukční předpoklad. Existuje tedy báze C prostoru $\operatorname{Im} g$, která je složením Jordanových řetízků operátoru h (ty jsou samořejmě rovněž Jordanovými řetízky operátoru f). Jordanovy řetízky příslušné vlastnímu číslu λ označíme podle schématu

$$\begin{array}{ccccccccc}
\mathbf{v}^1_{k_1} & \xmapsto{g} & \dots & \xmapsto{g} & \mathbf{v}^1_2 & \xmapsto{g} & \mathbf{v}^1_1 & \xmapsto{g} & \mathbf{o} \\
 & & & & & & & & \vdots \\
\mathbf{v}^r_{k_r} & \xmapsto{g} & \dots & \xmapsto{g} & \mathbf{v}^r_2 & \xmapsto{g} & \mathbf{v}^r_1 & \xmapsto{g} & \mathbf{o}
\end{array}$$

(V bázi C mohou být ještě řetízky příslušné jiným vlastním číslům.) Počáteční vektory $\mathbf{v}^1_1$, ..., $\mathbf{v}^r_1$ tvoří lineárně nezávislou posloupnost v $\operatorname{Ker} g$, doplníme tyto vektory na bázi $(\mathbf{v}^1_1, \dots, \mathbf{v}^s_1)$ prostoru $\operatorname{Ker} g$. Pro každé $i = 1, \dots, r$ leží koncový vektor $\mathbf{v}^i_{k_i}$ v prostoru $\operatorname{Im} g$, existují proto vektory $\mathbf{v}^i_{k_i+1}$ takové,

že $g(\mathbf{v}^i_{k_i+1}) = \mathbf{v}^i_{k_i}$. Tím nám vznikne soubor řetízků

$$\begin{array}{ccccccccccc}
\mathbf{v}^1_{k_1+1} & \xmapsto{g} & \mathbf{v}^1_{k_1} & \xmapsto{g} & \dots & \xmapsto{g} & \mathbf{v}^1_2 & \xmapsto{g} & \mathbf{v}^1_1 & \xmapsto{g} & \mathbf{o} \\
 & & & & & & & & & & \vdots \\
\mathbf{v}^r_{k_r+1} & \xmapsto{g} & \mathbf{v}^r_{k_r} & \xmapsto{g} & \dots & \xmapsto{g} & \mathbf{v}^r_2 & \xmapsto{g} & \mathbf{v}^r_1 & \xmapsto{g} & \mathbf{o} \\
 & & & & & & & & \mathbf{v}^{r+1}_1 & \xmapsto{g} & \mathbf{o} \\
 & & & & & & & & & & \vdots \\
 & & & & & & & & \mathbf{v}^s_1 & \xmapsto{g} & \mathbf{o}
\end{array}$$

plus řetízky v bázi C, které přísluší jiným vlastním číslům. Zkonstruovali jsme novou posloupnost B, která je spojením Jordanových řetízků operátoru f. Zbývá ukázat, že B je báze.

Podle věty 9.93 je B lineárně nezávislá, protože počáteční vektory příslušné vlastnímu číslu λ tvoří z konstrukce lineárně nezávislou posloupnost a pro jiná vlastní čísla jsme nic nezměnili. Nyní stačí spočítat, že počet vektorů v B je n. V bázi C je $\dim \operatorname{Im} g$ vektorů k nim jsme doplnili $\dim \operatorname{Ker} g - r$ vektorů z $\operatorname{Ker} g$ a poté jsme k existujícím řetízkům doplnili r vektorů, ke každému z r řetízků jeden. Dohromady je v B $\dim \operatorname{Im} g + (\dim \operatorname{Ker} g - r) + r = \dim \operatorname{Im} g + \dim \operatorname{Ker} g = n$ vektorů. Tím je důkaz ukončen.

9.4.12. Cayleyho-Hamiltonova věta. Uvažujme čtvercovou matici A řádu n nad tělesem $\mathbf{T}$ (nebo operátor f na prostoru $\mathbf{V}$ dimenze n). Posloupnost matic

$$(I_n, A, A^2, A^3, \dots, A^{n^2})$$

(resp. operátorů $(\mathrm{id}, f, f^2, \dots, f^{n^2})$) je lineárně závislá posloupnost v prostoru $\mathbf{T}^{n\times n}$ (resp. $\operatorname{Hom}(\mathbf{V}, \mathbf{V})$), protože tento prostor má dimenzi n^2. Existují proto skaláry $a_0, a_1, \dots$ takové, že

$$a_0 I_n + a_1 A + a_2 A^2 + \dots + a_{n^2} A^{n^2} = 0_{n\times n}$$

(resp. $a_0 \,\mathrm{id} + a_1 f + \dots + a_{n^2} f^{n^2} = 0$). Cayleyho-Hamiltonova věta říká, že taková závislost existuje mnohem dříve – stačí prvních $n+1$ členů posloupnosti, přičemž za koeficienty lze vzít koeficenty charakteristického polynomu matice A (resp. polynomu f). Zhruba řečeno, každá matice (resp. každý operátor) je „kořenem“ svého charakteristického polynomu.

Definujeme dosazení matice (operátoru) do polynomu.

Definice 9.116. Nechť $\mathbf{T}$ je těleso, $p(t) = a_0 + a_1 t + a_2 t^2 + \dots + a_n t^n$ polynom s koeficienty $a_0, \dots, a_n$ v $\mathbf{T}$, A čtvercová matice řádu k nad $\mathbf{T}$ a f lineární operátor na prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$. *Dosazením matice A do polynomu $p(t)$* rozumíme matici

$$p(A) = a_0 I_k + a_1 A + a_2 A^2 + \dots + a_n A^n \ .$$

Dosazením operátoru f do polynomu $p(t)$ rozumíme operátor

$$p(f) = a_0 \,\mathrm{id}_V + a_1 f + a_2 f^2 + \dots + a_n f^n \ .$$

Příklad 9.117. Je-li f operátor na $\mathbf{V}$, pak dosazením operátoru f do polynomu $p(t) = t - 3$ je operátor $p(f) = f - 3\,\mathrm{id}$. ▲

Příklad 9.118. Uvažujme reálnou matici

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

Její charakteristický polynom je

$$p_A(\lambda) = \lambda^2 - 5\lambda - 2 \ .$$

Dosazením matice A do tohoto polynomu získáme matici

$$p_A(A) = A^2 - 5A - 2I_2 = \begin{pmatrix} 7 & 15 \\ 10 & 22 \end{pmatrix} + \begin{pmatrix} -5 & -15 \\ -10 & -20 \end{pmatrix} + \begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix} = 0_{2\times 2} \ .$$

▲

Před důkazem Cayleyho-Hamiltonovy věty si všimneme, že dosazování do součinu polynomů lze provádět po jednotlivých činitelích. Je-li $p(t) = p_1(t)p_2(t)\dots p_i(t)$, pak $p(A) = p_1(A)p_2(A)\dots p_i(A)$. Důvodem je, že při roznásobení maticového výrazu $p_1(A)\dots p_i(A)$ je koeficient u A^j stejný jako koeficient u t^j při roznásobování výrazu $p_1(t)p_2(t)\dots p_i(t)$ (pro každé $j \in \{0,\dots,i\}$). Podobně pro operátory $p(f) = p_1(f)p_2(f)\dots p_i(f)$.

VĚTA 9.119 (Cayleyho-Hamiltonova věta). *Je-li f lineární operátor na konečně generovaném prostoru $\mathbf{V}$ dimenze n nad tělesem $\mathbf{T}$ (resp. je-li A čtvercová matice řádu n nad $\mathbf{T}$), pak $p_f(f) = 0$ (resp. $p_A(A) = 0$).*

DŮKAZ. Dokážeme si operátorovou verzi, maticovou přenecháme čtenáři. Větu dokážeme pouze v případě, že f má n vlastních čísel včetně násobností. V případě, že tomu tak není, je nutné napřed rozšířit těleso $\mathbf{T}$ do většího tělesa tak, aby v tom větším tělese měl charakteristický polynom dostatek kořenů. To lze udělat vždy a bude to v kursu algebry ve druhém ročníku.

Označme $\lambda_1,\dots,\lambda_m$ vlastní čísla operátoru f a $l_1,\dots,l_m$ jejich násobnosti. Podle předpokladu je $l_1 + \dots + l_m = n$ a charakteristický polynom je proto

$$p_f(\lambda) = (-1)^n(\lambda-\lambda_1)^{l_1}(\lambda-\lambda_2)^{l_2}\cdots(\lambda-\lambda_m)^{l_m} \ .$$

Podle věty 9.97 o Jordanově kanonickém tvaru existuje báze B taková, že $J = [f]_B^B$ je v Jordanově tvaru. Podle pozorování nad větou platí

$$p_f(f) = (-1)^n(f-\lambda_1\,\mathrm{id})^{l_1}(f-\lambda_2\,\mathrm{id})^{l_2}\cdots(f-\lambda_m\,\mathrm{id})^{l_m}$$

a tedy

$$\begin{aligned}[p_f(f)]_B^B &= [(-1)^n(f-\lambda_1\,\mathrm{id})^{l_1}(f-\lambda_2\,\mathrm{id})\cdots(f-\lambda_m\,\mathrm{id})^{l_m}]_B^B \\ &= (-1)^n([f-\lambda_1\,\mathrm{id}]_B^B)^{l_1}\cdots([f-\lambda_m\,\mathrm{id}]_B^B)^{l_m} \\ &= (-1)^n(J-\lambda_1 I_n)^{l_1}\cdots(J-\lambda_m I_n)^{l_m} \ .\end{aligned}$$

Matice v součinu jsou blokově diagonální (bloky odpovídají Jordanovým buňkám matice J), můžeme je násobit po blocích. Uvažujme libovolný blok K. Ten odpovídá nějaké Jordanově buňce $J_{\lambda_i,k}$, přičemž k je nejvýše l_i, protože velikost žádné buňky příslušné vlastnímu číslu λ_i nemůže být větší než jeho algebraická násobnost (viz tvrzení 9.96). Pak je ale $(J-\lambda_i I_n)^{l_i} = J_{0,k_i}^{l_i}$ nulová matice podle tvrzení 9.84, takže v celém součinu bude blok K nulový. Dokázali jsme, že $[p_f(f)]_B^B = 0_{n\times n}$, takže $p_f(f) = 0$. ▲

PŘÍKLAD 9.120. Ukážeme si použití Cayleyho-Hamiltonovy věty v teorii řízení. Diskrétní dynamický systém $\mathbf{x}_{k+1} = A\mathbf{x}_k$ dimenze n nad tělesem $\mathbf{T}$ s počáteční podmínkou $\mathbf{x}_0 = \mathbf{o}$ má řešení $\mathbf{x}_k = \mathbf{o}$ pro každé k, systém zůstává stále v počátečním stavu.

Přidáme si k němu možnost lineárního „řízení“

$$\mathbf{x}_{k+1} = A\mathbf{x}_k + B\mathbf{u}_k \ ,$$

kde $B = (\mathbf{b}_1|\mathbf{b}_2|\cdots,\mathbf{b}_n)$ je matice stejného řádu jako A. Můžeme si ji představit jako „joystick“ nebo „knipl“, kterým systém uvedeme do pohybu a pak jej řídíme volbou vstupů $\mathbf{u}_0,\mathbf{u}_1,\dots,\mathbf{u}_k,\dots$. Chceme vědět, jakých stavů $\mathbf{x}_k$ můžeme dosáhnout v čase k.

Pro $k = 1$ dostáváme

$$\mathbf{x}_1 = A\mathbf{x}_0 + B\mathbf{u}_0 = B\mathbf{u}_0 \in \operatorname{Im} B$$

a protože vstup $\mathbf{u}_0$ můžeme zvolit libovolně, tvoří možné stavy v čase $k = 1$ sloupcový prostor $\operatorname{Im} B$ „řídící“ matice B.

Pro $k = 2$ dostáváme

$$\mathbf{x}_2 = A\mathbf{x}_1 + B\mathbf{u}_1 = AB\mathbf{u}_0 + B\mathbf{u}_1 \in \operatorname{Im}(AB|B)$$

a protože vstupy $\mathbf{u}_0,\mathbf{u}_1 \in \mathbf{T}^n$ můžeme volit libovolně, tvoří možné stavy v čase $k = 2$ celý sloupcový prostor $\operatorname{Im}(AB|B)$ matice $(AB|B)$ typu $n\times(2n)$.

Jednoduchou indukcí podle k odvodíme, že v čase k tvoří možné stavy $\mathbf{x}_k$ sloupcový prostor

$$\operatorname{Im}(A^{k-1}B|A^{k-2}B|\cdots|AB|B)$$

matice $(A^{k-1}B|A^{k-2}B|\cdots|AB|B)$ typu $n \times (nk)$.

Porovnáme množiny možných stavů v časech $k = n$ a $k = n+1$, tj. sloupcové prostory

$$\operatorname{Im}(A^{n-1}B|A^{n-2}B|\cdots|AB|B), \quad \operatorname{Im}(A^nB|A^{n-1}B|A^{n-2}B|\cdots|AB|B) \ .$$

Zřejmě platí

$$\operatorname{Im}(A^{n-1}B|A^{n-2}B|\cdots|AB|B) \subseteq \operatorname{Im}(A^nB|A^{n-1}B|\cdots|AB|B) \ ,$$

protože každý sloupec matice vlevo je mezi sloupci matice vpravo. Podle Cayleyho-Hamiltonovy věty můžeme matici A^n vyjádřit jako lineární kombinaci

$$A^n = c_{n-1}A^{n-1} + \cdots + c_1A + c_0I_n$$

pro nějaké koeficienty c_i, které se rovnají $+/-$ koeficientům charakteristického polynomu matice A, protože koeficient u λ^n v charakteristickém polynomu $p_A(\lambda)$ je $(-1)^n$. V každém případě koeficienty c_i leží v $\mathbf{T}$. Poslední rovnost přenásobíme zprava maticí B a dostaneme

$$A^nB = c_{n-1}A^{n-1}B + \cdots + c_1AB + c_0B \ .$$

Každý sloupec $A^n\mathbf{b}_j$ matice A^nB, tj. každý nový sloupec matice $(A^nB|A^{n-1}B|A^{n-2}B|\cdots|AB|B)$ se tedy rovná lineární kombinaci

$$A^n\mathbf{b}_j = c_{n-1}A^{n-1}\mathbf{b}_j + \cdots + c_1A\mathbf{b}_j + c_0\mathbf{b}_j$$

nějakých sloupců v matici $(A^{n-1}B|A^{n-2}B|\cdots|AB|B)$. Každý nový sloupec matice $(A^nB|A^{n-1}B|\cdots|AB|B)$ proto už leží ve sloupcovém prostoru matice $\operatorname{Im}(A^{n-1}B|A^{n-2}B|\cdots|AB|B)$.

Dostali jsme tak, že každého možného stavu $\mathbf{x}_{n+1}$ už můžeme dosáhnout po $k = n$ krocích, rovná se nějakému z možných stavů $\mathbf{x}_n$.

▲

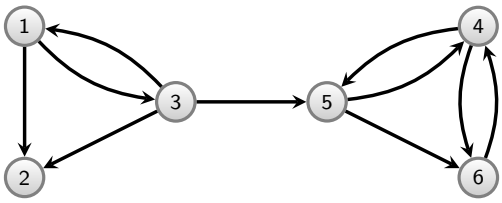
9.5. Google

Ukážeme si jednu moderní aplikaci vlastních čísel a vlastních vektorů. Myšlenku uspořádání webových stránek podle důležitosti si napřed předvedeme na jednoduchém příkladu. Poté odvodíme obecnou formulaci problému.

Představme si malou síť šesti webových stránek, které na sebe odkazují. Odkazy si zapíšeme do matice $A = (a_{ij})$, kde $a_{ij} = 1$ právě když stránka j odkazuje na stránku i. Naše síť je zadána maticí

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

Protože $a_{21} = 1$, stránka 1 odkazuje na stránku 2. Dále $a_{23} = 1$, také stránka 3 odkazuje na stránku 2. Žádná jiná stránka na stránku 2 neodkazuje. Takto si můžeme nakreslit graf sítě.



Obrázek 9.13. Google

Z vrcholu j vede šipka do i právě když stránka j odkazuje na stránku i. Matice A je tak maticí incidence grafu sítě. Z prvního semestru víme, že prvek na místě (i, j) v mocnině A^k říká, kolik orientovaných cest délky k vede z vrcholu j do vrcholu i.

Základní myšlenka vyhledávače Google spočívá v tom, že měří důležitost stránky pravděpodobností, s jakou se na stránku dostaneme náhodným klikáním. Důležitosti stránky se dopracujeme tak, že

na začátku přiřadíme všem stránkám stejnou důležitost $1/6$. Počáteční aproximací vektoru důležitosti stránek tak bude vektor $\mathbf{r}_0 = (1/6, 1/6, 1/6, 1/6, 1/6, 1/6)^T$, i-tá složka je důležitost i-té stránky.

Nyní musíme matici incidence webu upravit tak, aby její hodnoty říkaly, s jakou pravděpodobností klikneme na link ze stránky j na stránku i. Pokud ze stránky j vede více odkazů, řekněme k, pak na každý z nich klikneme s pravděpodobností $1/k$. Matici A si upravíme tak, že každou jednotku v j-tém sloupci nahradíme číslem $1/k$, kde k je počet prvků rovných 1 v j-tém sloupci matice A. Dostaneme tak matici

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

Všechny prvky matice H jsou nezáporné a součet každého sloupce se rovná buď 1 nebo 0. Druhá možnost nastane v případě, že z příslušné stránky nevede žádný odkaz. Jako třeba ze stránky s pdf souborem těchto přednášek.

První iteraci vektoru důležitosti stránek v naší síti pak získáme jako $\mathbf{r}_1 = H\mathbf{r}_0$. Složka i tohoto vektoru říká, s jakou pravděpodobností se na stránku i dostaneme z náhodně vybrané stránky po jednom kliknutí. Platí

$$\mathbf{r}_1 = H\mathbf{r}_0 = \begin{pmatrix} 0 & 0 & 1/3 & 0 & 0 & 0 \\ 1/2 & 0 & 1/3 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/2 & 1 \\ 0 & 0 & 1/3 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 1/2 & 1/2 & 0 \end{pmatrix} \begin{pmatrix} 1/6 \\ 1/6 \\ 1/6 \\ 1/6 \\ 1/6 \\ 1/6 \end{pmatrix} = \begin{pmatrix} 1/18 \\ 5/36 \\ 1/12 \\ 1/4 \\ 5/36 \\ 1/6 \end{pmatrix}.$$

Druhou iteraci vektoru důležitosti $\mathbf{r}_2$ dostaneme jako $H\mathbf{r}_1$. Můžeme ji slovně popsat tak, že uvádí, s jakou pravděpodobností se na i-tou stránku dostaneme jedním kliknutím z nějaké stránky, přičemž počáteční stránky volíme s pravděpodobnostmi danými vektorem $\mathbf{r}_1$. Stránka je tedy tím „důležitější“, čím „důležitější“ stránky na ni odkazují. Vyjde

$$\mathbf{r}_2 = H\mathbf{r}_1 = \begin{pmatrix} 0 & 0 & 1/3 & 0 & 0 & 0 \\ 1/2 & 0 & 1/3 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/2 & 1 \\ 0 & 0 & 1/3 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 1/2 & 1/2 & 0 \end{pmatrix} \begin{pmatrix} 1/18 \\ 5/36 \\ 1/12 \\ 1/4 \\ 5/36 \\ 1/6 \end{pmatrix} = \begin{pmatrix} 1/36 \\ 1/18 \\ 1/36 \\ 17/72 \\ 11/72 \\ 14/72 \end{pmatrix}.$$

Hledání vektoru důležitosti jednotlivých stránek tak vede na diferenční rovnici $\mathbf{r}_k = H\mathbf{r}_{k-1}$, která jak víme má řešení $\mathbf{r}_k = H^k\mathbf{r}_0$. Tento vektor můžeme interpretovat tak, že udává, s jakou pravděpodobností se dostaneme na danou stránku po k náhodných kliknutích.

Pro porovnávání důležitosti všech webových stránek bychom museli uvažovat matici celého webu, tedy matici řádu n, kde n je číslo v současnosti větší než třicet miliard. Každá iterace navíc vyžaduje spočítat součin matice tohoto řádu s jedním n-složkovým vektorem, počet aritmetických operací je tak řádu n^2. To všechno se zdá být zhola nemožné. Nicméně matice H je velmi řídká, naprostá většina jejích prvků se rovná 0. Pro ty jsou vypracované efektivní metody ukládání. Dále v každém sloupci matice H je v průměru 10 odkazů na jiné stránky, aspoň tak je jejich počet odhadován. Takže součin matice s vektorem vyžaduje pouze $10n$ operací. A to už je v současnosti výpočetně zvládnutelné.

Popsaná diferenční rovnice vyvolává řadu důležitých otázek:

- Konverguje posloupnost vektorů $\mathbf{r}_k$ k nějakému vektoru nebo je celý proces nestabilní?
- Může se stát, že posloupnost vektorů osciluje kolem několika různých limitních vektorů?
- Za jakých podmínek na matici H proces konverguje k jedinému vektoru?
- Pokud konverguje, dává výsledný limitní vektor dobrou míru důležitosti jednotlivých webových stránek?
- Závisí konvergence na počáteční aproximaci $\mathbf{r}_0$?
- Pokud proces konverguje, kolik iterací musíme provést, abychom dostali dobrou aproximaci limitního vektoru?

Už při prvním hraní si s naším malým příkladem zjistíme jeden problém tohoto přístupu. Díky tomu, že v našem příkladu ze stránky 2 nevede žádný odkaz, důležitost této stránky se nijak neprojeví na důležitosti jiných stránek. Na druhou stranu při každé iteraci do sebe nasaje něco z důležitosti jiných stránek a celková suma důležitostí všech stránek se postupně snižuje. Stránkou 2 tak důležitost „odtéká“. Mnohem závažnější je skutečnost, že klastr stránek 4,5,6 odkazuje pouze na stránky 4,5,6, a žádná z nich neodkazuje na žádnou ze stránek 1,2,3, zatímco stránka 3 odkazuje na stránku 5 z tohoto

klastru. Klastr stránek 4,5,6 tak bude akumulovat důležitost stránek z celé sítě. Skutečně, již třináctá iterace $\mathbf{r}_{13}$ má první tři složky zanedbatelně malé a zbylé tři složky v poměru $(2/3) : (1/3) : (1/5)$.

Problém se stránkami, ze kterých nevede žádný odkaz, vyřešíme předpokladem, že z takové stránky můžeme náhodně přeskočit na jakoukoliv jinou stránku, na všechny se stejnou pravděpodobností. V našem malém příkladu je takovou stránkou stránka 2, nulový sloupec v matici H nahradíme sloupcem ze samých hodnot $1/6$. Dostaneme tak matici

$$S = \begin{pmatrix} 0 & 1/6 & 1/3 & 0 & 0 & 0 \\ 1/2 & 1/6 & 1/3 & 0 & 0 & 0 \\ 1/2 & 1/6 & 0 & 0 & 0 & 0 \\ 0 & 1/6 & 0 & 0 & 1/2 & 1 \\ 0 & 1/6 & 1/3 & 1/2 & 0 & 0 \\ 0 & 1/6 & 0 & 1/2 & 1/2 & 0 \end{pmatrix} .$$

V obecném případě bychom matici H nahradili maticí

$$S = H + \frac{1}{n}\mathbf{e}\mathbf{a}^T,$$

kde $\mathbf{e}$ je sloupcový vektor se všemi složkami rovnými 1 a $\mathbf{a}$ je vektor, jehož j-tá složka je rovna 1, pokud z j-té stránky nevede žádný odkaz, a rovná se 0, pokud z j-té stránky nějaký odkaz na jinou stránku vede. Matice S je markovovská matice, to znamená, že její prvky jsou nezáporné a každý sloupec má součet rovný 1. O takových maticích už víme, že číslo 1 je jejich vlastním číslem.

Problém klastru stránek, které akumulují důležitost všech ostatních stránek, touto úpravou nevyřešíme. V našem příkladu bude pořád platit, že mezi klastrem stránek 1,2,3 a klastrem stránek 4,5,6 vedou odkazy pouze jednosměrně, ze stránek 1,2,3 na stránky 4,5,6. Naše brouzdání po webu upravíme ještě jedním způsobem. Zvolíme si nějaké číslo $\alpha \in (1/2, 1)$. Toto číslo je pravděpodobnost, se kterou volíme následující krok při prohlížení webu tak, že klikneme na nějaký odkaz. Pravděpodobnost $1 - \alpha$ je pak pravděpodobnost, že skočíme náhodně na jakoukoliv jinou stránku webu. Dostaneme tak další matici

$$G = \alpha S + \frac{1}{n}(1-\alpha)\mathbf{e}\mathbf{e}^T \ .$$

Tato **Google matice** je matice, kterou zakladatelé firmy Google Larry Page a Sergey Brin uvedli ve svém prvním článku o jejich algoritmu PageRank na porovnávání důležitosti webových stránek. Všimněme si, že všechny prvky matice G jsou kladné a součet prvků v každém sloupci zůstává rovný 1.

Náš malý příklad vede při volbě $\alpha = 0,9$ na matici

$$G = 0,9 \cdot S + 0,1 \cdot \frac{1}{6}\mathbf{e}\mathbf{e}^T = \begin{pmatrix} 1/60 & 1/6 & 19/60 & 1/60 & 1/60 & 1/60 \\ 7/15 & 1/6 & 19/60 & 1/60 & 1/60 & 1/60 \\ 7/15 & 1/6 & 1/60 & 1/60 & 1/60 & 1/60 \\ 1/60 & 1/6 & 1/60 & 1/60 & 7/15 & 11/12 \\ 1/60 & 1/6 & 19/60 & 7/15 & 1/60 & 1/60 \\ 1/60 & 1/6 & 1/60 & 7/15 & 7/15 & 1/60 \end{pmatrix} .$$

Diferenční rovnice $\mathbf{r}_k = G\mathbf{r}_{k-1}$ s počátečním vektorem $\mathbf{r}_0$ má pak řešení $\mathbf{r}_k = G^k\mathbf{r}_0$, které konverguje k jednoznačně určenému vektoru

$$\mathbf{r} = \begin{pmatrix} 0,03721 \\ 0,05396 \\ 0,04151 \\ 0,3751 \\ 0,206 \\ 0,2862 \end{pmatrix} .$$

Tento limitní vektor interpretujeme tak, že náhodný brouzdal po webu řídící se našimi pravidly stráví v průměru $3,721\%$ času na stránce 1, $5,396\%$ času na stránce 2, $37,51\%$ času na stránce 4, atd.

Vlastnosti vlastních čísel matice G plynou z **Perronovy věty**, kterou dokázal již v roce 1907 německý matematik Oskar Perron. Uvedeme si bez důkazu její důsledky pro Google matici G.

VĚTA 9.121. *Pro Google matici G platí*

(1) *Číslo 1 je vlastním číslem matice G,*
(2) *geometrická i algebraická násobnost vlastního čísla 1 se rovná jedné,*
(3) *existuje vlastní vektor $\mathbf{r}$ příslušný vlastnímu číslu 1, který má všechny složky kladné,*
(4) *pro jakékoliv jiné vlastní číslo λ matice G platí $|\lambda| < 1$.*

Pokud kladný vlastní vektor $\mathbf{r}$ splňuje navíc podmínku $\|\mathbf{r}\| = 1$, nazývá se *Perronův vektor* matice G. První vlastnost jsme si už ukázali dříve, protože matice G je markovovská (tj. nezáporná a součet každého sloupce se rovná 1) a 1 je proto vlastní číslo G. Můžeme si také ověřit, že z dalších uvedených vlastností matice G plyne konvergence vektorů $\mathbf{r}_k = G^k\mathbf{r}_0$. Pokud si matici G převedeme do Jordanova kanonického tvaru $J = R^{-1}GR$ pomocí nějaké regulární matice R, můžeme předpokládat, že první

Jordanova buňka $J_1 = J_{1,1}$ odpovídá vlastnímu číslu 1 a Perronův vektor $\mathbf{r}$ je prvním sloupcem matice R, jejíž sloupce tvoří bázi $B = (\mathbf{r} = \mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n)$ aritmetického prostoru $\mathbb{R}^n$ složenou ze Jordanových řetízků. Potom pro matici $J = \operatorname{diag}(J_1, J_2, \ldots, J_s)$ platí

$$\mathbf{r}_k = RJ^kR^{-1}\mathbf{r}_0 = R\operatorname{diag}(J_1^k, J_2^k, \ldots, J_s^k)R^{-1}\mathbf{r}_0 \ .$$

Protože $|\lambda| < 1$ pro jakékoliv vlastní číslo matice G různé od 1, platí $J_i^k \to O$ pro jakoukoliv Jordanovu buňku různou od J_1. Matice J^k tak konverguje k matici, která má na místě $(1,1)$ prvek 1 a všechny ostatní prvky nulové. Odtud plyne, že posloupnost vektorů

$$\mathbf{r}_k = RJ^kR^{-1}\mathbf{r}_0 = R\operatorname{diag}(J_1^k, J_2^k, \ldots, J_s^k)R^{-1}\mathbf{r}_0$$

konverguje k nějakému skalárnímu násobku vektoru $\mathbf{r}$. Protože začínáme s vektorem $\mathbf{r}_0$, který má součet složek rovný 1, a násobíme jej markovovskou maticí, každý vektor $\mathbf{r}_k$ má součet složek rovný 1 a tedy jej má rovný 1 i limita posloupnosti vektorů $\mathbf{r}_k$. Posloupnost vektorů $\mathbf{r}_k$ tak komverguje k nějakému kladnému násobku Perronova vektoru $\mathbf{r}$, který má všechny složky kladné.

Tento výpočet ukazuje, že vhodný násobek Perronova vektoru odpovídá na všechny otázky spojené s řešením diferenční rovnice $\mathbf{r}_k = G^k\mathbf{r}_{k-1}$ s výjimkou rychlosti konvergence. Rychlost konvergence posloupnosti $\mathbf{r}_k$ závisí na tom, jak rychle konvergují k O mocniny Jordanovy buňky příslušné vlastním číslům $\lambda \neq 1$. Nejpomaleji z nich konvergují buňky odpovídající vlastnímu číslu $\lambda \neq 1$, který má co největší absolutní hodnotu $|\lambda|$. Rychlost konvergence tak závisí nejvíce na $|\lambda_2|$, kde λ_2 je druhé největší (pokud jde o absolutní hodnotu) vlastní číslo matice G.

Pokud jde o volbu parametru α, autoři algoritmu uvádějí $\alpha = 0,85$. Na volbě α závisí rychlost konvergence a numerická stabilita výpočtů. Z odhadů absolutní hodnoty druhého největšího vlastního čísla matice G vyplývá, že při této volbě α stačí k přesnosti na tři desetinná místa zhruba 50 iterací, tj. stačí spočítat vektor $\mathbf{r}_{50}$. Rychlost konvergence výpočtu také závisí na volbě počátečního vektoru $\mathbf{r}_0$. Otázka volby $\mathbf{r}_0$ je teoreticky podrobně zkoumána, žádné definitivní výsledky zatím nejsou. Firma Google uvádí, že každý výpočet začíná vždy od stejného počátečního vektoru $\mathbf{r}_0 = (1/n)\mathbf{e}$. Zatím se nepodařilo najít způsob, jak využít předchozích masivních výpočtů při výpočtu nové aktualizace vektoru důležitosti stránek.

Uvedené použití Jordanova kanonického tvaru pro důkaz konvergence posloupnosti vektorů $\mathbf{r}_k$ dobře ilustruje význam teoretických výsledků. Při vlastním výpočtu iterací $\mathbf{r}_k = G\mathbf{r}_{k-1}$ jej nepotřebujeme, součin počítáme přímo. Jordanův kanonický tvar nám umožňuje dokázat, že uvedený numerický postup vede k očekávanému výsledku.

Poslední poznámka se týká rychlosti násobení matice s vektorem. Matice G už není řídká, všechny její prvky jsou nenulové. Její tvar je

$$G = \alpha S + (1-\alpha)\frac{1}{n}\mathbf{e}\mathbf{e}^T = \alpha H + \alpha\frac{1}{n}\mathbf{e}\mathbf{a}^T + (1-\alpha)\frac{1}{n}\mathbf{e}\mathbf{e}^T \ .$$

Matice H je řídká, s naprostou většinou prvků rovných 0. Matice G se od ní liší přičtením dvou matic s hodností rovnou 1. Násobíme-li maticí G libovolný vektor $\mathbf{x}$, počítáme

$$G\mathbf{x} = (\alpha S + (1-\alpha)\frac{1}{n}\mathbf{e}\mathbf{e}^T)\mathbf{x} = \alpha H\mathbf{x} + \alpha\frac{1}{n}\mathbf{e}\mathbf{a}^T\mathbf{x} + (1-\alpha)\frac{1}{n}\mathbf{e}\mathbf{e}^T\mathbf{x} \ .$$

Člen $\alpha\mathbf{e}\mathbf{a}^T\mathbf{x}$ vyžaduje pouze výpočet standardního skalárního součinu $\mathbf{a}^T\mathbf{x}$, což je n násobení, doplněného o jedno další násobení $\alpha(\mathbf{a}^T\mathbf{x})$. Stejný počet násobení vyžaduje výpočet třetího členu. Celá složitost výpočtu $G\mathbf{x}$ tak závisí na složitosti výpočtu součinu velmi řídké matice H s vektorem $\mathbf{x}$.

Tento tvar matice G tak stále umožňuje řadu optimalizací výpočtů vytvořených pro počítání s řídkými maticemi.

Označíme-li $E = \frac{1}{n}\mathbf{e}\mathbf{e}^T$ matici, jejíž všechny prvky jsou rovné $1/n$, můžeme rovnici definující vektor $\mathbf{r}$ napsat ve tvaru

$$(\alpha S + (1-\alpha)E)\mathbf{r} = \mathbf{r} \ .$$

Její jednoduchost a elegance vede některé autory k názoru, že by měla být zařazena do příštího vydání knihy *It Must Be Beautiful: Great Equations of Modern Science*, jejíž první vydání vyšlo v roce 2002.

Cvičení

1. Dokažte, že relace podobnosti matic je ekvivalence na množině všech čtvercových matic téhož řádu n nad tělesem $\mathbf{T}$.

2. Nechť $\mathbf{V}$ je vektorový prostor dimenze n nad tělesem T, $B = (\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n)$ je báze $\mathbf{V}$, $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na $\mathbf{V}$ a $R = (r_{ij})$ regulární matice řádu n nad $\mathbf{T}$. Najděte bázi $C = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ ve $\mathbf{V}$, pro kterou platí

$$[f]_C^C = R^{-1}[f]_B^B R.$$

3. Dokažte, že číslo 0 je vlastní číslo lineárního operátoru $f : \mathbf{V} \to \mathbf{V}$ právě když $\mathrm{Ker}\,(f) \neq \{\mathbf{o}\}$.

4. Dokažte, že jediné vlastní číslo jednotkové matice I_n je 1.

5. Dokaže, že je-li λ vlastní číslo matice A, je λ^2 vlastní číslo matice A^2.

6. Dokažte, že je-li A regulární matice a λ vlastní číslo A, pak λ^{-1} je vlastní číslo inverzní matice A^{-1}.

7. Nechť $\mathbf{V}$ je konečně generovaný prostor nad $\mathbf{T}$, $C = (\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n)$ je báze $\mathbf{V}$ a matice $[f]_C^C$ je podobná matici A. Dokažte, že existuje báze D ve $\mathbf{V}$, pro kterou platí $A = [f]_D^D$.

8. Spočítejte vlastní čísla a vlastní vektory matice ortogonální projekce na přímku určenou nenulovým vektorem $(a, b)^T \in \mathbb{R}^2$.

9. Najděte matici osové souměrnosti určené přímkou – lineárním obalem nenulového vektoru $(a, b)^T \in \mathbb{R}^2$ vzhledem ke kanonické bázi $\mathbb{R}^2$ a spočítejte její vlastní čísla a vlastní vektory.

10. Dokažte, že rotace kolem počátku souřadnic o úhel φ má reálná vlastní čísla právě když φ je násobkem π.

11. Spočítejte vlastní čísla a vlastní vektory projekce na obecnou přímku v $\mathbb{R}^3$. Napřed odhadněte výsledek z geometrického významu vlastních čísel a vektorů.

12. Jaké kořeny má v tělese $\mathbb{Z}_2$ polynom $x^2 + 1$? Jaké kořeny má v tělesech $\mathbb{Z}_3$ a $\mathbb{Z}_5$?

Shrnutí deváté kapitoly

(1) Je-li $\mathbf{V}$ vektorový prostor nad tělesem $\mathbf{T}$, $f : \mathbf{V} \to \mathbf{V}$ lineární zobrazení, a $\mathbf{x}_0 \in \mathbf{V}$, pak *diskrétní lineární dynamický systém* je definovaný rovností $\mathbf{x}_k = f(\mathbf{x}_{k-1})$ pro každé $k \in \mathbb{N}$ a *počátečním stavem* $\mathbf{x}_0$. Prvek $\mathbf{x}_k \in \mathbf{V}$ nazýváme *stav systému* v čase k. Má-li prostor $\mathbf{V}$ konečnou dimenzi n, říkáme také, že dynamický systém má dimenzi n.

(2) Vývoj diskrétního lineárního dynamického systému je popsán vztahem $\mathbf{x}_k = f^k(\mathbf{x}_0)$ pro každé $k \geq 0$. Speciálně, je-li $\dim \mathbf{V} = 1$ a $f(x) = ax$ pro každé $x \in \mathbf{T}$, pak stav diskrétního lineárního dynamického systému $\mathbf{x}_k = f(\mathbf{x}_{k-1})$ v čase k se rovná $x_k = a^k\, x_0$ pro každé $k \geq 0$.

(3) Je-li $\mathbf{V} = \mathbb{R}^n$ (nebo $\mathbf{V} = \mathbb{C}^n$) a $\mathbf{x}(t) = (x_1(t), x_2(t), \ldots, x_n(t))^T \in \mathbf{V}$ pro každé $t \in \mathbb{R}$, pak definujeme derivaci $\mathbf{x}'(t)$ stavového vektoru $\mathbf{x}(t)$ jako vektor $\mathbf{x}'(t) = (x_1'(t), x_2'(t), \ldots, x_n'(t))^T$.

(4) Spojitý lineární dynamický systém je definovaný rovností $\mathbf{x}'(t) = f(\mathbf{x}(\mathbf{t}))$ pro každé $t \in \mathbb{R}$ a počátečním stavem $\mathbf{x}(0) \in \mathbb{R}^n$ (nebo $\mathbf{x}(0) \in \mathbb{C}^n$).

(5) Je-li $n = 1$, pak v čase t se stav spojitého lineárního dynamického systému $x'(t) = ax(t)$ s počátečním stavem $x(0) \in \mathbb{R}$ (nebo $x(0) \in \mathbb{C}^n$) rovná $x(t) = x(0)\, e^{at}$.

(6) Příklady diskrétních lineárních dynamických systémů - úročení, Fibonacciho posloupnost. Příklady spojitých lineárních dynamických systémů - rozpad radioaktivních jader, vlastní kmity pružiny, přechod substance přes buněčnou bránu.

(7) Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na vektorovém prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$, pak skalár $\lambda \in T$ nazýváme *vlastní číslo* operátoru f, pokud existuje nenulový vektor $\mathbf{x} \in V$, pro který platí

$$f(\mathbf{x}) = \lambda \mathbf{x} \ .$$

Je-li λ vlastní číslo operátoru f, pak libovolný prvek $\mathbf{x} \in V$, pro který platí $f(\mathbf{x}) = \lambda \mathbf{x}$, nazýváme *vlastní vektor* operátoru f *příslušný vlastnímu číslu* λ.

(8) Je-li A čtvercová matice řádu n nad tělesem $\mathbf{T}$, pak skalár $\lambda \in \mathbf{T}$ nazýváme *vlastní číslo* matice A, pokud existuje nenulový vektor $\mathbf{x} \in T^n$ takový, že

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

Je-li λ vlastní číslo matice A, pak libovolný vektor $\mathbf{x} \in T^n$, pro který platí $A\mathbf{x} = \lambda \mathbf{x}$, nazýváme *vlastní vektor* matice A *příslušný vlastnímu číslu* λ.

(9) Operátor $f : \mathbf{V} \to \mathbf{V}$ má vlastní číslo 0 právě tehdy, když f není prostý. Čtvercová matice A má vlastní číslo 0 právě tehdy, když A je singulární.

(10) Geometrický význam vlastních čísel a vektorů v případě jednoduchých geometrických zobrazení v $\mathbb{R}^2$.

(11) Nechť f je lineární operátor na prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$. Pak $\lambda \in T$ je vlastním číslem operátoru f právě tehdy, když operátor $(f - \lambda\, \mathrm{id}_V)$ není prostý.

Je-li λ vlastním číslem operátoru f, pak množina M_λ všech vlastních vektorů operátoru f příslušných vlastnímu číslu λ je podprostorem $\mathbf{V}$ a platí

$$M_\lambda = \mathrm{Ker}\,(f - \lambda\, \mathrm{id}_V) \ .$$

(12) Je-li A čtvercová matice řádu n nad tělesem $\mathbf{T}$, pak $\lambda \in T$ je vlastním číslem matice A právě tehdy, když je matice $A - \lambda I_n$ singulární.

Je-li λ vlastním číslem matice f, pak množina M_λ všech vlastních vektorů matice A příslušných vlastnímu číslu λ je podprostorem $\mathbf{T}^n$ a

platí

$$M_\lambda = \operatorname{Ker}(A - \lambda I_n) \ .$$

(13) Je-li A čtvercová matice řádu n nad tělesem $\mathbf{T}$, pak $\lambda \in T$ je vlastním číslem matice A právě tehdy, když $\det(A - \lambda I_n) = 0$.

Je-li f lineární operátor na konečně generovaném prostoru $\mathbf{V}$ dimenze n nad tělesem $\mathbf{T}$ a B je báze $\mathbf{V}$, pak $\lambda \in T$ je vlastním číslem operátoru f právě když je λ vlastní číslo matice $[f]_B^B$ vzhledem k bázím B a B, což nastává právě když $\det\left([f]_B^B - \lambda I_n\right) = 0$.

(14) Pro každou matici $A = (a_{ij})$ řádu n nad libovolným tělesem $\mathbf{T}$ platí
  (a) $\det(A - \lambda I_n)$ je polynom stupně n s koeficienty v $\mathbf{T}$,
  (b) koeficient u λ^n se rovná $(-1)^n$,
  (c) koeficient u λ^{n-1} se rovná $(-1)^{n-1}(a_{11} + a_{22} + \cdots + a_{nn})$,
  (d) absolutní člen se rovná $\det A$.

(15) Je-li A čtvercová matice řádu n nad tělesem $\mathbf{T}$, pak *charakteristický polynom matice* A je polynom

$$p_A(\lambda) = \det(A - \lambda I_n) \ .$$

(16) Dvě čtvercové matice X, Y téhož řádu nad tělesem $\mathbf{T}$ se nazývají *podobné*, pokud existuje regulární matice R taková, že $Y = R^{-1}XR$.

(17) Podobné matice mají stejný charakteristický polynom.

(18) Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na konečně generovaném prostoru $\mathbf{V}$ dimenze n, pak *charakteristický polynom operátoru* f je polynom

$$p_f(\lambda) = \det\left([f]_B^B - \lambda I_n\right) \ ,$$

kde B je libovolná báze prostoru $\mathbf{V}$.

(19) Nechť $p(x)$ je polynom nad $\mathbf{T}$. Prvek $t \in T$ je kořenem polynomu $p(x)$ právě tehdy, když polynom $x - t$ dělí polynom $p(x)$.

(20) Nechť $p(x)$ je polynom nad $\mathbf{T}$ a $t \in T$ je jeho kořen. *Násobnost kořene* t polynomu $p(x)$ definujeme jako největší přirozené číslo l takové, že polynom $(x - t)^l$ dělí polynom $p(x)$.

(21) Nechť $p(x)$ je polynom nad $\mathbf{T}$, $t_1, \ldots, t_k \in T$ po dvou různé a $l_1, \ldots, l_k \in \mathbb{N}$. Pak následující tvrzení jsou ekvivalentní.
  (1) Pro každé $i \in \{1, \ldots, k\}$ je t_i kořen násobnosti l_i.
  (2) $p(x) = (x - t_1)^{l_1} \ldots (x - t_k)^{l_k} q(x)$ pro nějaký polynom $q(x)$ takový, že ani jeden z prvků $t_1, \ldots, t_k$ není kořen.

(22) Polynom stupně n nad libovolným tělesem má nejvýše n kořenů včetně násobností.

(23) Každý polynom stupně $n \geq 1$ nad tělesem $\mathbb{C}$ lze napsat jako součin lineárních polynomů (tj. polynomů stupně 1).

Speciálně, každý polynom stupně $n \geq 0$ nad tělesem $\mathbb{C}$ má právě n kořenů včetně násobností.

Polynom lichého stupně nad tělesem $\mathbb{R}$ má alespoň jeden kořen.

(24) Nechť f je lineární operátor na konečně generovaném prostoru a λ je jeho vlastní číslo. *Algebraickou násobností* vlastního čísla λ rozumíme jeho násobnost jako kořene charakteristického polynomu operátoru f. Nechť A je čtvercová matice a λ je její vlastní číslo.

Algebraickou násobností vlastního čísla λ rozumíme jeho násobnost jako kořene charakteristického polynomu matice A.

(25)
- Každý lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném prostoru dimenze n nad tělesem $\mathbf{T}$ má nejvýše n vlastních čísel včetně násobností.

- Lineární operátor $f : \mathbf{V} \to \mathbf{V}$ má právě n vlastních čísel včetně násobností právě tehdy, když je jeho charakteristický polynom součinem lineárních polynomů.
- Každý lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném prostoru dimenze n nad tělesem $\mathbb{C}$ má právě n vlastních čísel včetně násobností.
- Každý lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném vektorovém prostoru liché dimenze nad $\mathbb{R}$ má aspoň jedno (reálné) vlastní číslo.

(26)
- Každá čtvercová matice řádu n nad tělesem $\mathbf{T}$ má nejvýše n vlastních čísel včetně algebraických násobností.
- Čtvecová matice řádu n nad tělesem $\mathbf{T}$ má právě n vlastních čísel včetně násobností právě tehdy, když je její charakteristický polynom součinem lineárních polynomů.
- Každá čtvercová matice řádu n nad tělesem $\mathbb{C}$ má právě n vlastních čísel včetně algebraických násobností.
- Každá čtvercová matice lichého řádu nad tělesem $\mathbb{R}$ má alespoň jedno reálné vlastní číslo.

(27) Lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném prostoru $\mathbf{V}$ nazýváme *diagonalizovatelný*, pokud má vzhledem k nějaké bázi diagonální matici.

(28) Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na konečně generovaném prostoru $\mathbf{V}$ a je-li $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ báze prostoru $\mathbf{V}$, pak $[f]_B^B = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$ platí právě tehdy, když pro každé $i \in \{1, 2, \dots, n\}$ je $\mathbf{v}_i$ vlastní vektor příslušný vlastnímu číslu λ_i.

(29) Lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném prostoru $\mathbf{V}$ je diagonalizovatelný právě tehdy, když existuje báze prostoru $\mathbf{V}$ tvořená vlastními vektory operátoru f.

(30) Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na konečně generovaném prostoru $\mathbf{V}$ dimenze n nad tělesem $\mathbf{T}$ a C báze prostoru $\mathbf{V}$, pak operátor f je diagonalizovatelný právě tehdy, když je matice $[f]_C^C$ podobná diagonální matici.

(31) Čtvercová matice A řádu n nad tělesem $\mathbf{T}$ se nazývá *diagonalizovatelná*, pokud je operátor $f_A : \mathbf{T}^n \to \mathbf{T}^n$ diagonalizovatelný.

(32) Je-li A čtvercová matice řádu n nad tělesem $\mathbf{T}$, $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ báze prostoru $\mathbf{T}^n$ a $R = [\mathrm{id}]_K^B = (\mathbf{v}_1 | \dots | \mathbf{v}_n)$, pak matice $[f_A]_B^B = R^{-1}AR$ se rovná diagonální matici $\operatorname{diag}(\lambda_1, \dots, \lambda_n)$ právě tehdy, když pro každé $i \in \{1, 2, \dots, n\}$ je $\mathbf{v}_i$ vlastní vektor příslušný vlastnímu číslu λ_i.

(33) Čtvercová matice A řádu n nad tělesem $\mathbf{T}$ je diagonalizovatelná právě tehdy, když existuje báze prostoru $\mathbf{T}^n$ tvořená vlastními vektory matice A.

(34) Čtvercová matice A řádu n nad tělesem $\mathbf{T}$ je diagonalizovatelná právě tehdy, když je podobná diagonální matici.

(35) Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor a $(\mathbf{v_1}, \mathbf{v}_2, \dots, \mathbf{v}_k)$ posloupnost nenulových vlastních vektorů operátoru f příslušných navzájem různým vlastním číslům $\lambda_1, \dots, \lambda_k$, pak je posloupnost $(\mathbf{v_1}, \mathbf{v}_2, \dots, \mathbf{v}_k)$ lineárně nezávislá.

(36) Má-li lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na vektorovém prostoru $\mathbf{V}$ dimenze n nad tělesem $\mathbf{T}$ celkem n navzájem různých vlastních čísel, pak je diagonalizovatelný.

(37) Má-li matice A řádu n nad tělesem $\mathbf{T}$ celkem n navzájem různých vlastních čísel, pak je diagonalizovatelná.

(38) Celé odvození vztahu pro k-tý člen Fibonacciho posloupnosti.

(39) *Geometrickou násobností* vlastního čísla λ operátoru f na konečně generovaném prostoru (nebo čtvercové matice A) rozumíme dimenzi podprostoru $\mathbf{M}_\lambda$ vlastních vektorů operátoru f (nebo matice A) příslušných vlastnímu číslu λ.

(40) Pro čtvercovou blokovou matici

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

se čtvercovými diagonálními bloky B, D platí

$$\det A = (\det B)\,(\det D)\ .$$

(41) Pro každé vlastní číslo λ lineárního operátoru $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném prostoru $\mathbf{V}$ (čtvercové matice A) nad tělesem $\mathbf{T}$ platí, že geometrická násobnost λ je menší nebo rovná algebraické násobnosti λ.

(42) Buď $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na konečně generovaném vektorovém prostoru $\mathbf{V}$ dimenze n (resp. buď A je čtvercová matice řádu n) nad tělesem $\mathbf{T}$. Pak jsou následující tvrzení jsou ekvivalentní.

(a) Operátor f je diagonalizovatelný (resp. matice A je diagonalizovatelná).

(b) Operátor f (resp. matice A) má
- n vlastních čísel včetně algebraických násobností a
- geometrická násobnost každého vlastního čísla operátoru f (resp. matice A) je rovná jeho algebraické násobnosti.

(43) Je-li $\mathbf{x} \in \mathbb{C}^n$ vlastní vektor reálné matice $A = (a_{ij})$ příslušný vlastnímu číslu λ, pak $\overline{\mathbf{x}}$ je vlastní vektor matice A příslušný vlastnímu číslu $\overline{\lambda}$.

(44) Je-li A reálná matice řádu 2, která nemá reálná vlastní čísla, a $\lambda = r(\cos\varphi + i\sin\varphi)$ je komplexní vlastní číslo s nenulovým vlastním vektorem $\mathbf{v}$, pak platí

(a) vektory $\mathbf{w}_1 = \mathbf{v} + \overline{\mathbf{v}}$ a $\mathbf{w}_2 = i(\mathbf{v} - \overline{\mathbf{v}})$ tvoří bázi $B = (\mathbf{w}_1, \mathbf{w}_2)$ prostoru $\mathbb{R}^2$,

(b) lineární zobrazení $f_A : \mathbb{R}^2 \to \mathbb{R}^2$ určené maticí A má vzhledem k bázi B matici

$$[f_A]_B^B = r \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$$

a je tedy složením rotace o úhel φ se stejnolehlostí s koeficientem $r > 0$

(45) Vývoj spojitého lineárního dynamického systému s diagonalizovatelnou maticí.

(46) *Jordanova buňka* řádu $k \geq 1$ nad tělesem $\mathbf{T}$ příslušná prvku $\lambda \in T$ je čtvercová matice

$$J_{\lambda,k} = \begin{pmatrix} \lambda & 1 & 0 & & 0 & 0 \\ 0 & \lambda & 1 & \dots & 0 & 0 \\ 0 & 0 & \lambda & & 0 & 0 \\ & \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda \end{pmatrix}\ .$$

(47) Matice J nad tělesem $\mathbf{T}$ je v *Jordanově kanonickém tvaru* (nebo stručněji v *Jordanově tvaru*), pokud J je blokově diagonální matice, jejíž každý diagonální blok je Jordanova buňka (nějakého řádu příslušná nějakému

číslu), tj.

$$J = \operatorname{diag}(J_{\lambda_1,k_1}, \dots, J_{\lambda_s,k_s}) = \begin{pmatrix} J_{\lambda_1,k_1} & 0 & \dots & 0 \\ 0 & J_{\lambda_2,k_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_{\lambda_s,k_s} \end{pmatrix},$$

kde $\lambda_1, \dots, \lambda_s \in T$ a $k_1, \dots, k_s$ jsou kladná celá čísla.

(48) Pro libovolná přirozená čísla $m < k$ platí

$$J^m_{0,k} = (\underbrace{\mathbf{o}|\dots|\mathbf{o}}_{m\times}|\mathbf{e}_1|\mathbf{e}_2|\mathbf{e}_{k-m})$$

Pro $m \geq k$ je $J^m_{0,k} = 0$.

(49) Je-li $J = J_{\lambda,k}$ Jordanova buňka, pak pro každé kladné m platí

$$J^m_{\lambda,k} = \begin{pmatrix} \lambda^m & \binom{m}{1}\lambda^{m-1} & \binom{m}{2}\lambda^{m-2} & \dots & \binom{m}{k-1}\lambda^{m-k+1} \\ 0 & \lambda^m & \binom{m}{1}\lambda^{m-1} & \dots & \binom{m}{k-2}\lambda^{m-k+2} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda^m & \binom{m}{1}\lambda^{m-1} \\ 0 & 0 & \dots & 0 & \lambda^m \end{pmatrix}.$$

(50) Říkáme, že pro lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném prostoru $\mathbf{V}$ *existuje Jordanův kanonický tvar*, pokud má vzhledem k nějaké bázi matici v Jordanově kanonickém tvaru.

(51) Je-li f lineární operátor na vektorovém prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ a λ vlastní číslo operátoru f, pak posloupnost $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ vektorů z $\mathbf{V}$ nazýváme *Jordanův řetízek operátoru f délky k příslušný vlastnímu číslu λ s počátkem* $\mathbf{v}_1$, pokud platí

$$(f - \lambda\,\mathrm{id}_V)(\mathbf{v}_1) = \mathbf{o},\ (f - \lambda\,\mathrm{id}_V)(\mathbf{v}_2) = \mathbf{v}_1,\ (f - \lambda\,\mathrm{id}_V)(\mathbf{v}_3) = \mathbf{v}_2,\ \dots,$$
$$(f - \lambda\,\mathrm{id}_V)(\mathbf{v}_k) = \mathbf{v}_{k-1}\ .$$

(52) Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na konečně generovaném prostoru $\mathbf{V}$ a $B = (\mathbf{v}_1, \dots, \mathbf{v}_k)$ báze prostoru $\mathbf{V}$, pak $[f]^B_B = J_{\lambda,k}$ právě tehdy, když $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ je Jordanův řetízek operátoru f příslušný vlastnímu číslu λ s počátkem $\mathbf{v}_1$.

(53) Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na konečně generovaném prostoru $\mathbf{V}$ a B báze prostoru $\mathbf{V}$, pak $[f]^B_B = \operatorname{diag}(J_{\lambda_1,k_1}, \dots, J_{\lambda_s,k_s})$ platí právě tehdy, když B je spojením posloupností $B_1, \dots, B_s$, kde pro každé $i \in \{1, \dots, s\}$ je B_i Jordanův řetízek operátoru f délky k_i příslušný vlastnímu číslu λ_i s počátkem $\mathbf{v}^i_1$.

(54) Pro lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně generovaném prostoru $\mathbf{V}$ existuje Jordanův tvar právě tehdy, když existuje báze prostoru $\mathbf{V}$ vzniklá spojením Jordanových řetízků operátoru f.

(55) Nechť $f : \mathbf{V} \to \mathbf{V}$ je lineární operátor na konečně generovaném prostoru $\mathbf{V}$ a C je báze prostoru $\mathbf{V}$. Pak pro operátor f existuje Jordanův tvar právě tehdy, když je matice $[f]^C_C$ podobná matici v Jordanově tvaru.

(56) Předpokládáme, že $f : \mathbf{V} \to \mathbf{V}$ lineární operátor a $B_1, \dots, B_s$ jsou Jordanovy řetízky operátoru f příslušné vlastním číslům $\lambda_1, \dots, \lambda_s$. Předpokládejme dále, že pro každé $\lambda \in \{\lambda_1, \dots, \lambda_s\}$ je posloupnost počátečních vektorů těch řetízků z $B_1, \dots, B_s$, které přísluší vlastnímu číslu λ, lineárně nezávislá. Pak spojení $B = B_1, \dots, B_s$ je lineárně nezávislá posloupnost.

(57) Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na prostoru $\mathbf{V}$ dimenze n a B báze vzniklá spojením Jordanových řetízků operátoru f, pak platí
  (a) operátor f má n vlastních čísel včetně násobností,
  (b) pro libovolné vlastní číslo λ operátoru f je jeho algebraická násobnost rovna součtu délek Jordanových řetízků v B příslušných vlastnímu číslu λ,
  (c) pro libovolné vlastní číslo λ operátoru f a libovolné $l \in \mathbb{N}$ je jádro operátoru $(f - \lambda\,\mathrm{id}_V)^l$ rovno lineárnímu obalu l počátečních vektorů z každého řetízku v B příslušného vlastnímu číslu λ (z řetízků délky menší než l bereme všechny vektory),
  (d) pro libovolné vlastní číslo λ operátoru f a libovolné $l \in \mathbb{N}$ je obraz operátoru $(f - \lambda\,\mathrm{id}_V)^l$, roven lineárnímu obalu všech vektorů v B kromě l koncových vektorů z řetízků příslušných vlastnímu číslu λ (z řetízků příslušných vlastnímu číslu λ délky menší než l nebereme žádný vektor).

  Speciálně pro libovolné vlastní číslo λ operátoru f platí
  (5) geometrická násobnost vlastního čísla λ se rovná počtu řetízků v B příslušných vlastnímu číslu λ a prostor $M_\lambda = \mathrm{Ker}\,(f - \lambda\,\mathrm{id}_V)$ je roven lineárnímu obalu počátečních vektorů těchto řetízků,
  (6) počet řetízků příslušných vlastnímu číslu λ délky alespoň l je roven
  $$z_l = \dim \mathrm{Ker}\,(f - \lambda\,\mathrm{id}_V)^l - \dim \mathrm{Ker}\,(f - \lambda\,\mathrm{id}_V)^{l-1} \ ,$$
  (aby měl výraz smysl i pro $l = 1$ definujeme $(f - \lambda\,\mathrm{id}_V)^0 = \mathrm{id}_V$),
  (7) počet řetízků příslušných vlastnímu číslu λ délky právě l je $z_l - z_{l+1}$.

(58) Je-li $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na konečně generovaném vektorovém prostoru $\mathbf{V}$ dimenze n, pak jsou následující tvrzení ekvivalentní.
  (a) Pro operátor f existuje Jordanův kanonický tvar.
  (b) Operátor f (resp. matice A) má n vlastních čísel včetně algebraických násobností.

(59) Pro každý operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně dimenzionálním prostoru $\mathbf{V}$ nad tělesem komplexních čísel $\mathbb{C}$ existuje Jordanův kanonický tvar.

(60) Řešení spojitého lineárního dynamického systému s maticí rovnou Jordanově buňce řádu 2.

(61) Nechť $\mathbf{T}$ je těleso, $p(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n$ polynom s koeficienty $a_0, \ldots, a_n$ v $\mathbf{T}$, A čtvercová matice řádu k nad $\mathbf{T}$ a f lineární operátor na prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$. *Dosazením matice A do polynomu $p(t)$* rozumíme matici
$$p(A) = a_0 I_k + a_1 A + a_2 A^2 + \cdots + a_n A^n \ .$$
Dosazením operátoru f do polynomu $p(t)$ rozumíme operátor
$$p(f) = a_0\,\mathrm{id}_V + a_1 f + a_2 f^2 + \cdots + a_n f^n \ .$$

(62) Cayleyho-Hamiltonova věta. Je-li f lineární operátor na konečně generovaném prostoru $\mathbf{V}$ dimenze n nad tělesem $\mathbf{T}$ (resp. je-li A čtvercová matice řádu n nad $\mathbf{T}$), pak $p_f(f) = 0$ (resp. $p_A(A) = 0$).

KAPITOLA 10

Unitární diagonalizace

Cíl. *V této kapitole se zaměříme na operátory a lineární zobrazení mezi konečně generovanými reálnými a komplexními vektorovými prostory se skalárním součinem. Speciální typy operátorů, tzv. operátory normální, jdou ortogonálně (unitárně) diagonalizovat, tj. lze najít ortonormální bázi tvořenou vlastními vektory. Pro obecné lineární zobrazení najdeme ortonormální báze, vzhledem ke kterým má toto zobrazení obdélníkovou diagonální matici. Tomuto procesu se říká singulární rozklad.*

Má-li operátor f vzhledem k nějaké bázi diagonální matici, máme docela dobrou představu, co operátor "dělá". Víme-li například, že operátor f na prostoru $\mathbb{R}^2$ má vzhledem k bázi $B = (\mathbf{v}_1, \mathbf{v}_2)$ matici $D = \operatorname{diag}(1, 2)$, víme, že f zachovává vektor $\mathbf{v}_1$ a dvakrát prodlužuje vektor $\mathbf{v}_2$. Tím je díky linearitě operátor f zcela určen.

Informace, že matice f je vzhledem k bázi B prostoru $\mathbb{R}^2$ diagonální, ale není úplně uspokojivá. Jedním z důvodů je, že vektory báze B můžou být „téměř rovnoběžné", takže hrozí nebezpečí numerické nestability výpočtů, jak jsme viděli u soustav lineárních rovnic. Další důvod je, že nedokážeme zodpovědět na jemnější metrické otázky, jako například, jaký je obraz jednotkové kružnice. Z obrázku můžeme odhadovat, že jde o elipsu. Proč tomu tak je a jak přesně je elipsa umístěná? Obecně nejsou délky a směry poloos v jednoduchém vztahu s bází B a maticí D.

OBRAZEK - obraz jednotkove kruznice operatorem

Pokud ale najdeme v $\mathbb{R}^2$ ortonormální bázi $B = (\mathbf{v}_1, \mathbf{v}_2)$ (vzhledem ke standardnímu skalárnímu součinu) takovou, že $[f]_B^B = \operatorname{diag}(1, 2)$, pak vektory B jsou „maximálně nerovnoběžné" a také vidíme, že obraz jednotkové kružnice je elipsa s osami LO $\{\mathbf{v}_1\}$, LO $\{\mathbf{v}_2\}$, délkou poloosy 1 ve směru LO $\{\mathbf{v}_1\}$ a délkou poloosy 2 ve směru LO $\{\mathbf{v}_2\}$.

OBRAZEK - obraz jednotkove kruznice operatorem vzhledem k ortonormalni bazi

V prvních dvou oddílech této kapitoly se budeme zabývat otázkou, kdy pro operátor f na prostoru $\mathbf{V}$ se skalárním součinem existuje ortonormální báze B prostoru $\mathbf{V}$ taková, že $[f]_B^B$ je diagonální. Chceme tedy, aby matice operátoru byla co nejjednodušší (tak jako v kapitole o vlastních číslech), ale také, aby báze B byla co nejhezčí – ortonormální. Abychom mohli mluvit o kolmosti, musí být $\mathbf{V}$ lineární prostor se skalárním součinem. Z technických důvodů se **budeme věnovat pouze aritmetickým vektorovým prostorům $\mathbb{R}^n$ a $\mathbb{C}^n$ se standardním skalárním součinem**, operátory jsou tedy tvaru f_A pro nějakou čtvercovou reálnou nebo komplexní matici A.

Ve třetím a čtvrtém oddíle využijeme poznatky o unitární (ortogonální) diagonalizaci na obecné reálné nebo komplexní matice.

10.1. Unitární a ortogonální diagonalizovatelnost

10.1.1. Definice a základní vlastnosti.

DEFINICE 10.1. Říkáme, že komplexní (resp. reálná) čtvercová matice A řádu n je *unitárně diagonalizovatelná* (resp. *ortogonálně diagonalizovatelná*), pokud existuje ortonormální báze B prostoru $\mathbb{C}^n$ (resp. $\mathbb{R}^n$) taková, že $[f_A]_B^B$ je diagonální.

Připomeňme, že v $\mathbb{R}^n$ a $\mathbb{C}^n$ budeme v této kapitole vždy uvažovat standardní skalární součin. Takto také chápeme ortonormalitu v předchozí definici.

Definici unitární (ortogonální) diagonalizovatelnosti přeformulujeme podobně jako jsme v důsledku 9.61 a tvrzení 9.59 přeformulovali definici diagonalizovatelnosti. K obdobě důsledku 9.61 si stačí připomenout, že vztah $[f_A]_B^B = D = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$ platí právě tehdy, když B je tvořená vlastními vektory; λ_i jsou pak příslušná vlastní čísla. Obdoba tvrzení 9.59 o podobnosti je důsledkem vztahu

$$[f_A]_B^B = ([\mathrm{id}]_{K_n}^B)^{-1}[f_A]_{K_n}^{K_n}[\mathrm{id}]_{K_n}^B = ([\mathrm{id}]_{K_n}^B)^{-1}A[\mathrm{id}]_{K_n}^B.$$

Báze B je ortonormální právě když $[\mathrm{id}]_{K_n}^B$ je unitární (ortogonální). To vede k definici unitární (ortogonální) podobnosti.

DEFINICE 10.2. Dvě čtvercové matice X, Y téhož řádu nad tělesem $\mathbb{C}$ (resp. $\mathbb{R}$) se nazývají *unitárně (resp. ortogonálně) podobné*, pokud existuje unitární (resp. ortogonální) matice U taková, že $Y = U^{-1}XU$ (což je rovno U^*XU, protože U je unitární nebo ortogonální matice).

Dostáváme následující charakterizace unitární (ortogonální) diagonalizovatelnosti.

TVRZENÍ 10.3. *Nechť A je komplexní (resp. reálná) čtvercová matice řádu n. Pak následující tvrzení jsou ekvivalentní.*

(i) *Matice A je unitárně (resp. ortogonálně) diagonalizovatelná.*
(ii) *Aritmetický prostor $\mathbb{C}^n$ (resp. $\mathbb{R}^n$) má ortonormální bázi tvořenou vlastními vektory matice A.*
(iii) *Matice A je unitárně (resp. ortogonálně) podobná diagonální matici (přičemž na diagonále jsou vlastní čísla matice A, každé tolikrát kolik je jeho algebraická=geometrická násobnost).*

Následující tvrzení je obdobou věty 9.71, která charakterizujíce diagonalizovatelné operátory pomocí algebraických a geometrických násobností vlastních čísel.

VĚTA 10.4. *Je-li A komplexní (resp. reálná) čtvercová matice řádu n, pak jsou následující tvrzení ekvivalentní.*

(1) *Matice A je unitárně (resp. ortogonálně) diagonalizovatelná.*
(2) *Matice A*
   - *má n vlastních čísel včetně algebraických násobností,*
   - *geometrická násobnost každého vlastního čísla matice A se rovná jeho algebraické násobnosti a*
   - *pro libovolná dvě různá vlastní čísla λ_i, λ_j matice A platí $M_{\lambda_i} \perp M_{\lambda_j}$.*

DŮKAZ. Důkaz je podobný jako ve větě 9.71. Předpokládáme, že $\lambda_1, \dots, \lambda_k$ jsou všechna navzájem různá vlastní čísla operátoru f.

Pro důkaz (2) $\Rightarrow$ (1) vybereme v každém z prostorů $\mathbf{M}_{\lambda_i}$ ortonormální bázi B_i a spojení B bází $B_1, B_2, \cdots, B_k$ bude báze v $\mathbb{C}^n$ (resp. $\mathbb{R}^n$). Stejně jako v důkazu věty 9.71 k tomu stačí první dva z předpokladů na operátor f v bodě (2). Báze B je navíc ortonormální. Všechny prvky báze B mají normu 1, protože B_i je ortonormální báze v $\mathbf{M}_{\lambda_i}$, a z téhož důvodu jsou libovolné dva různé prvky B_i

kolmé. Je-li $i \neq j$, pak každý prvek $B_i \subseteq M_{\lambda_i}$ je kolmý na každý prvek $B_j \subseteq M_{\lambda_j}$ podle třetího z předpokladů.

Přepodkládejme naopak, že B je ortonormální báze příslušného aritmetického prostoru taková, že matice $[f_A]_B^B$ je diagonální. To znamená, že každý z prvků báze B je nenulový vlastní vektor matice A. Stejně jako v důkazu implikace (1) $\Rightarrow$ (2) ve větě 9.71 z toho vyplývá, že báze B je složená z bází prostorů M_{λ_1}, ..., M_{λ_k}. Protože všechny vektory v B jsou navzájem kolmé, jsou navzájem kolmé i podprostory $\mathbf{M}_{\lambda_i} = \mathrm{LO}\, B_i$ a $\mathbf{M}_{\lambda_j} = \mathrm{LO}\, B_j$ (viz tvrzení 8.40 o kolmosti lineárního obalu). ▲

Jinými slovy věta říká, že matice je unitárně (ortogonálně) diagonalizovatelná právě tehdy, když je diagonalizovatelná a vlastní vektory příslušné různým vlastním číslům jsou na sebe kolmé.

Na rozdíl od diagonalizovatelnosti, unitární (ortogonální) diagonalizovatelnost lze charakterizovat velmi jednoduchou rovností, kterou lze snadno ověřit bez znalosti vlastních čísel. To je obsahem spektrální věty pro normální matice dokázané v další části.

10.1.2. Hermitovsky sdružené matice. Důležitou roli v celé kapitole bude hrát hermitovské sdružování, v reálném případě transponování. Připomeňme, že matice hermitovsky sdružená k A je matice komplexně sdružená k A^T. Následující tvrzení shrnuje některé jednoduché vlastnosti sdružování, které budeme používat automaticky.

Tvrzení 10.5. *Nechť A, B jsou komplexní matice a $t \in \mathbb{C}$. Pak platí*

(1) $A^{**} = A$,
(2) *má-li $A + B$ smysl, pak* $(A + B)^* = A^* + B^*$,
(3) $(tA)^* = \bar{t}A^*$,
(4) *má-li AB smysl, pak* $(AB)^* = B^*A^*$,
(5) *je-li A regulární, pak je A^* regulární a platí* $(A^{-1})^* = (A^*)^{-1}$.

Další jednoduchý vztah, který budeme často využívat, ukazuje jeden z geometrických významů hermitovského sdružování: Je-li A komplexní matice typu $m \times n$ a $\mathbf{x} \in \mathbb{C}^m$, $\mathbf{y} \in \mathbb{C}^n$, pak

$$A^*\mathbf{x} \cdot \mathbf{y} = \mathbf{x} \cdot A\mathbf{y} \ ,$$

kde na levé straně značí $\cdot$ standardní skalární součin v $\mathbb{C}^n$, na pravé straně v $\mathbb{C}^m$. Formulku lze ověřit jednoduchým výpočtem

$$A^*\mathbf{x} \cdot \mathbf{y} = (A^*\mathbf{x})^*\mathbf{y} = \mathbf{x}^*A\mathbf{y} = \mathbf{x} \cdot A\mathbf{y} \ .$$

Tento vztah hermitovsky sdruženou matici k A charakterizuje ve smyslu, že A^* je jediná taková matice B, pro kterou platí formulka $B\mathbf{x} \cdot \mathbf{y} = \mathbf{x} \cdot A\mathbf{y}$, jak se přesvědčíme dosazením všech dvojic vektorů kanonické báze. Pro reálné matice a reálné aritmetické vektory můžeme hermitovské sdružování samozřejmě všude nahradit transponováním.

Pomocí vztahu $\langle f^*(\mathbf{x}), \mathbf{y} \rangle = \langle \mathbf{x}, f(\mathbf{y}) \rangle$ se obecně definuje sdružené lineární zobrazení. Na aritmetické prostory se standardním součinem jsme se v této kapitole omezili právě proto, abychom se vyhli abstraktní definici sdruženého zobrazení. Důkazy jsou ale podány tak, aby zobecnění šlo udělat přímočaře.

Důležitou vlastností hermitovsky sdružené matice ke čtvercové matici je, že její vlastní čísla jsou komplexně sdružená k vlastním číslům původní matice.

Tvrzení 10.6. *Nechť A je komplexní čtvercová matice řádu n. Pak $\lambda \in \mathbb{C}$ je vlastní číslo matice A právě tehdy, když je $\overline{\lambda}$ vlastní číslo matice A^*.*

Speciálně, reálná čtvercová matice A a transponovaná matice A^T mají stejná reálná vlastní čísla.

Důkaz. Díky vlastnosti $A^{**} = A$ stačí dokázat jednu implikaci. Předpokládejme, že λ je vlastní číslo matice A. Pak matice $A - \lambda I_n$ je singulární. Potom i $(A - \lambda I_n)^* = A^* - \overline{\lambda} I_n$ je singulární, tedy $\overline{\lambda}$ je vlastní číslo matice A^*.

Alternativně lze tvrzení dokázat pomocí toho, že charakteristický polynom matice A^* je komplexně sdružený polynom k charakteristickému polynomu matice A, viz cvičení. ▲

Tvrzení nedává žádnou informaci o příslušných vlastních vektorech, žádný jednoduchý vztah totiž obecně neplatí.

Příklad 10.7. Reálná matice

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

má vlastní čísla 1 a -2 a příslušné podprostory vlastních čísel $M_1 = \mathrm{LO}\left\{(-1,4)^T\right\}$, $M_{-2} = \mathrm{LO}\left\{(-1,1)^T\right\}$. Matice transponovaná má stejná vlastní čísla a $M_1 = \mathrm{LO}\left\{(1,1)^T\right\}$, $M_{-2} = \mathrm{LO}\left\{(4,1)^T\right\}$. ▲

10.1.3. Normální matice. Normální matice lze definovat jednoduchým, ale poněkud neprůhledným vztahem. Jak uvidíme, jsou to právě unitárně diagonalizovatelné komplexní matice. Vysvětlení názvu „normální“ uvidíme v tvrzení 10.11.

Definice 10.8. Komplexní nebo reálná čtvercová matice A se nazývá *normální*, pokud $A^*A = AA^*$ (v reálném případě můžeme psát $A^TA = AA^T$).

Příklady komplexních normálních matic jsou unitární matice a hermitovské matice, dále například diagonální matice a antihermitovské matice, tj. matice splňující $-A^* = A$. Příklady reálných normálních matic zahrnují všechny ortogonální, symetrické, diagonální a antisymetrické matice.

Příklad 10.9. Reálná matice

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

je normální, protože

$$A^TA = AA^T = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix} .$$

Matice A není symetrická, antisymetrická, ani ortogonální. ▲

Skalární násobek normální matice je rovněž normální a sdružená matice normální matici je normální (cvičení). Navíc libovolná matice unitárně podobná normální matici je rovněž normální. Součet ani součin normálních matic nemusí být normální, ale stačí, aby operátory komutovaly. Budeme potřebovat pouze následující speciální případy:

Tvrzení 10.10. *Je-li A normální komplexní matice řádu n, pak*

(i) *pro libovolné $t \in \mathbb{C}$ je matice $A - tI_n$ normální,*
(ii) *libovolná matice X unitárně podobná A je normální.*

Důkaz. Pro důkaz (i) spočítáme

$$\begin{aligned}(A - tI_n)^*(A - tI_n) &= (A^* - (tI_n)^*)(A - tI_n) = (A^* - \overline{t}I_n)(A - tI_n) \\ &= A^*A - tA^* - \overline{t}A + t\overline{t}I_n\end{aligned}$$

Stejně vyjde i $(A - tI_n)(A - tI_n)^*$.

Je-li $X = U^{-1}AU$, kde U je unitární, pak $U^{-1} = U^*$ a tudíž

$$XX^* = U^*AU(U^*AU)^* = U^*AUU^*A^*U^{**} = U^*AA^*U \ .$$

Protože $A^*A = AA^*$, stejně vychází X^*X. ▲

Normální operátory se vyznačují tím, že se normy f_A-obrazu a f_{A^*}-obrazu libovolného vektoru rovnají.

Tvrzení 10.11. *Nechť A je normální matice řádu n a $\mathbf{v} \in \mathbb{C}^n$. Pak platí*

$$\|A\mathbf{v}\| = \|A^*\mathbf{v}\| \ .$$

Důkaz. Protože norma je vždy nezáporné reálné číslo, stačí dokázat rovnost druhých mocnin norem.

$$\begin{aligned}\|A\mathbf{v}\|^2 &= A\mathbf{v} \cdot A\mathbf{v} = A^*A\mathbf{v} \cdot \mathbf{v} = AA^*\mathbf{v} \cdot \mathbf{v} \\ &= A^{**}A^*\mathbf{v} \cdot \mathbf{v} = A^*\mathbf{v} \cdot A^*\mathbf{v} = \|A^*\mathbf{v}\|^2\end{aligned}$$

▲

Pomocí polarizační identity lze dokázat (viz cvičení), že vlastnost v předchozím tvrzení normální matice charakterizuje. To vysvětluje jejich pojmenování.

Z tvrzení 10.6 víme, že λ je vlastní číslo čtvercové komplexní matice A právě tehdy, když je $\overline{\lambda}$ vlastní číslo matice A^*. Příslušné vlastní vektory ale nejsou obecně v jednoduchém vztahu. Pro normální matice je situace daleko přehlednější.

Tvrzení 10.12. *Nechť A je normální komplexní matice řádu n, $\lambda \in \mathbb{C}$ a $\mathbf{v} \in \mathbb{C}^n$. Pak $\mathbf{v}$ je vlastní vektor matice A příslušný vlastnímu číslu λ právě tehdy, když je $\mathbf{v}$ vlastní vektor matice A^* příslušný vlastnímu číslu $\overline{\lambda}$.*

Důkaz. Předpokládejme, že $\mathbf{v}$ je vlastní vektor matice A příslušný vlastnímu číslu λ. Z tvrzení 10.6 již víme, že $\overline{\lambda}$ je vlastní číslo matice A^*, zbývá dokázat, že $\mathbf{v}$ je příslušný vlastní vektor. Platí $(A - \lambda I_n)\mathbf{v} = \mathbf{o}$, tedy také $\|(A - \lambda I_n)\mathbf{v}\| = 0$. Protože A je normální, je podle tvrzení 10.10 normální také matice $A - \lambda I_n$. Z tvrzení 10.11 o normách vyplývá $\|(A - \lambda I_n)^*\mathbf{v}\| = \left\|(A^* - \overline{\lambda} I_n)\mathbf{v}\right\| = 0$. Z toho $(A^* - \overline{\lambda} I_n)\mathbf{v} = \mathbf{o}$, tedy $\mathbf{v}$ je skutečně vlastní vektor matice A^* příslušný vlastnímu číslu $\overline{\lambda}$.

Pro důkaz druhé implikace stačí připomenout, že A^* je normální operátor a $A^{**} = A$. ▲

10.2. Spektrální věty

V této části dokážeme slíbenou charakterizaci unitárně diagonalizovatelných matic jako matic normálních. Dále se budeme věnovat charakterizacím speciálních typů normálních matic, hlavní výsledky jsou schematicky znázorněné na obrázku zvlášť v komplexním a reálném případě. Nakonec využijeme poznatky k popisu všech ortogonálních operátorů $\mathbb{R}^2 \to \mathbb{R}^2$ a $\mathbb{R}^3 \to \mathbb{R}^3$.

OBRAZEK - vlevo komplexní, vpravo reálné

TODO: analogie ke komplexním číslům

10.2.1. Normální matice.

Věta 10.13 (Spektrální věta pro normální matice). *Nechť A je čtvercová komplexní matice. Pak následující tvrzení jsou ekvivalentní.*

(1) *Matice A je unitárně diagonalizovatelná.*
(2) *Matice A je normální.*

Důkaz. (1) $\Rightarrow$ (2). Je-li A unitárně diagonalizovatelná, pak je unitárně podobná diagonální matici $D = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$ (viz tvrzení 10.3). Diagonální matice je normální, protože $D^*D = DD^* = \operatorname{diag}(|\lambda_1|^2, \dots, |\lambda_n|^2)$. Ale každá matice unitárně podobná normální je normální podle tvrzení 10.10.

(2) $\Rightarrow$ (1). Tvrzení dokážeme indukcí podle řádu n matice A. Pro $n = 1$ tvrzení zřejmě platí. Předpokládejme, že A je normální a každá normální matice řádu $n-1$ je unitárně diagonalizovatelná.

Každá komplexní čtvercová matice má vlastní číslo λ_1 (viz důsledek 9.51). Vezmeme libovolný nenulový vlastní vektor příslušný vlastnímu číslu λ, znormujeme jej a označíme $\mathbf{v}_1$. Vektor $\mathbf{v}_1$ doplníme na ortonormální bázi $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ prostoru $\mathbb{C}^n$, což lze podle věty 8.70. Ukážeme, že matice $X = [f_A]_B^B$ je blokově diagonální tvaru

$$X = [f_A]_B^B = ([f_A(\mathbf{v}_1)]_B | \cdots | [f_A(\mathbf{v}_n)]_B) = \left(\begin{array}{c|cccc} \lambda & 0 & 0 & \dots & 0 \quad 0 \\ \hline 0 & & & & \\ 0 & & & Y & \\ 0 & & & & \end{array}\right) .$$

Pro první sloupec plyne tvrzení z volby $\mathbf{v}_1$, protože

$$[f_A(\mathbf{v}_1)]_B = [A\mathbf{v}_1]_B = [\lambda\mathbf{v}_1]_B = (\lambda, 0, \dots, 0)^T \ .$$

Podle tvrzení 8.48 o souřadnicích vzhledem k ortonormální bázi je první složka vektoru $[f_A(\mathbf{v}_i)]_B = [A\mathbf{v}_i]_B$ rovná $\mathbf{v}_1 \cdot A\mathbf{v}_i$. Pro $i > 1$ dostáváme užitím tvrzení 10.12 o vlastních vektorech normální matice a kolmosti vektorů $\mathbf{v}_1$ a $\mathbf{v}_i$

$$\mathbf{v}_1 \cdot A\mathbf{v}_i = A^*\mathbf{v}_1 \cdot \mathbf{v}_i = \overline{\lambda}\mathbf{v}_1 \cdot \mathbf{v}_i = \lambda(\mathbf{v}_1 \cdot \mathbf{v}_i) = 0 \ .$$

První složka i-tého sloupce matice $[f_A]_B^B$ je tedy pro $i > 1$ skutečně nulová.

Důkaz dokončíme maticovým výpočtem využitím indukčního předpokladu. Předně $X = [f_A]_B^B$ je unitárně podobná normální matici $A = [f_A]_K^K$:

$$X = U^*AU \ , \text{ kde } U = [\mathrm{id}]_K^B \ .$$

Speciálně, X je také normální matice (viz tvrzení 10.10). Platí proto

$$\left(\begin{array}{c|c} |\lambda|^2 & \mathbf{0} \\ \hline \mathbf{0} & Y^*Y \end{array}\right) = \left(\begin{array}{c|c} \overline{\lambda} & \mathbf{0} \\ \hline \mathbf{0} & Y^* \end{array}\right) \left(\begin{array}{c|c} \lambda & \mathbf{0} \\ \hline \mathbf{0} & Y \end{array}\right) = X^*X = XX^* = \left(\begin{array}{c|c} |\lambda|^2 & \mathbf{0} \\ \hline \mathbf{0} & YY^* \end{array}\right) \ ,$$

a tudíž Y je rovněž normální. Podle indukčního předpokladu je Y unitárně diagonalizovatelná, takže podle jedné z ekvivalentních formulací z tvrzení 10.3 existuje unitární matice V řádu $n-1$ taková, že V^*YV je diagonální. Položíme-li

$$W = \left(\begin{array}{c|c} 1 & \mathbf{0} \\ \hline \mathbf{0} & V \end{array}\right) \ ,$$

vidíme, že W je unitární, UW je rovněž unitární jakožto součin unitárních matic, a platí

$$\begin{aligned} (UW)^*A(UW) = W^*U^*AUW = W^*XW &= \left(\begin{array}{c|c} 1 & \mathbf{0} \\ \hline \mathbf{0} & V^* \end{array}\right) \left(\begin{array}{c|c} \lambda & \mathbf{0} \\ \hline \mathbf{0} & Y \end{array}\right) \left(\begin{array}{c|c} 1 & \mathbf{0} \\ \hline \mathbf{0} & V \end{array}\right) \\ &= \left(\begin{array}{c|c} \lambda & \mathbf{0} \\ \hline \mathbf{0} & V^*YV \end{array}\right) \end{aligned}$$

Výsledná matice je diagonální, matice A je tudíž unitárně podobná diagonální matici, takže je unitárně diagonalizovatelná opět podle tvrzení 10.3. ▲

Speciálně, normální reálná matice je unitárně diagonalizovatelná, **chápeme-li ji jako matici nad** $\mathbb{C}$. Není pravda, že je nutně ortogonálně diagonalizovatelná nad $\mathbb{R}$! Reálné matice, které jsou ortogonálně diagonalizovatelné, charakterizujeme v důsledku 10.16, jsou to přesně symetrické matice.

Pro danou normální matici by bylo neefektivní hledat ortonormální bázi vlastních vektorů postupem z důkazu spektrální věty. Je lepší postupovat obdobně jako u diagonalizace, podle důkazu věty 10.4, tj. v každém z prostorů vlastních vektorů najít **ortonormální** bázi, viz příklad 10.17.

Příklad 10.14. V příkladu 10.9 jsme viděli, že reálná matice

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

je normální. Její charakteristický polynom je

$$p_A(t) = -t^3 + 3t^2 - 3t + 2 = -(t-2)(t^2 - t + 1) \ .$$

Tento polynom má pouze jeden reálný kořen $\lambda = 2$ násobnosti 1, matice A tedy není ortogonálně diagonalizovatelná.

Chápejme nyní A jako matici nad $\mathbb{C}$. Podle spektrální věty je unitárně diagonalizovatelná. Má tři vlastní čísla

$$\lambda_1 = 2, \ \lambda_2 = \frac{1}{2} + \frac{\sqrt{3}}{2}i, \ \lambda_3 = \overline{\lambda_2} = \frac{1}{2} - \frac{\sqrt{3}}{2}i \ ,$$

prostory vlastních vektorů mají tedy dimenzi 1 a stačí v každém z nich zvolit jednotkový vektor.

$$\mathbf{v}_1 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \ \mathbf{v}_2 = \frac{1}{\sqrt{3}} \begin{pmatrix} \frac{-1+\sqrt{3}i}{2} \\ \frac{-1-\sqrt{3}i}{2} \\ 1 \end{pmatrix}, \mathbf{v}_3 = \overline{\mathbf{v}_2} = \frac{1}{\sqrt{3}} \begin{pmatrix} \frac{-1-\sqrt{3}i}{2} \\ \frac{-1+\sqrt{3}i}{2} \\ 1 \end{pmatrix}$$

Vzhledem k bázi $B = (\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ je matice operátoru $f_A : \mathbb{C}^3 \to \mathbb{C}^3$ rovná

$$[f_A]_B^B = \begin{pmatrix} 2 & 0 & 0 \\ 0 & \frac{1+\sqrt{3}i}{2} & 0 \\ 0 & 0 & \frac{1-\sqrt{3}i}{2} \end{pmatrix} \ .$$

To nám také dává maticový rozklad

$$A = [f_A]_K^K = [\mathrm{id}]_K^B [f_A]_B^B [\mathrm{id}]_B^K = [\mathrm{id}]_K^B [f_A]_B^B ([\mathrm{id}]_K^B)^{-1} = [\mathrm{id}]_K^B [f_A]_B^B ([\mathrm{id}]_K^B)^*$$

$$= \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & \frac{-1+\sqrt{3}i}{2} & \frac{-1-\sqrt{3}i}{2} \\ 1 & \frac{-1-\sqrt{3}i}{2} & \frac{-1+\sqrt{3}i}{2} \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 & 0 \\ 0 & \frac{1+\sqrt{3}i}{2} & 0 \\ 0 & 0 & \frac{1-\sqrt{3}i}{2} \end{pmatrix} \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \frac{-1-\sqrt{3}i}{2} & \frac{-1+\sqrt{3}i}{2} & 1 \\ \frac{-1+\sqrt{3}i}{2} & \frac{-1-\sqrt{3}i}{2} & 1 \end{pmatrix} \ .$$

▲

10.2.2. Hermitovské a symetrické matice. Připomeňme, že matice A se nazývá hermitovská, pokud $A^* = A$ (v reálném případě $A^T = A$). Hermitovské matice tvoří podtřídu normálních matic. Následující věta ukazuje, že jsou to ve skutečnosti právě ty normální matice, jejichž vlastní čísla jsou reálná.

Věta 10.15 (Spektrální věta pro hermitovské matice). *Nechť A je komplexní čtvercová matice. Pak následující tvrzení jsou ekvivalentní.*

(1) *Matice A je unitárně diagonalizovatelná a všechna její vlastní čísla jsou reálná.*
(2) *Matice A je hermitovská.*

Důkaz. (1) $\Rightarrow$ (2). Je-li A unitárně diagonalizovatelná a všechna její vlastní čísla jsou reálná, pak můžeme podle tvrzení 10.3 psát $A = UDU^*$, kde U je unitární a D je reálná diagonální. Reálná diagonální matice je zřejmě hermitovská, takže

$$A = UDU^* = UD^*U^* = (UDU^*)^* = A^* \ .$$

(2) $\Rightarrow$ (1). Protože každý hermitovský operátor je normální, stačí podle spektrální věty o normálních operátorech (věta 10.13) ukázat, že všechna vlastní čísla matice A jsou reálná. To nahlédneme z tvrzení 10.12 o vlastních vektorech normálních matic: Je-li $\lambda \in \mathbb{C}$ vlastní číslo matice A a $\mathbf{v}$ nenulový vlastní vektor příslušný λ, pak $\mathbf{v}$ je vlastní vektor operátoru $A^* = A$ příslušný vlastnímu číslu $\overline{\lambda}$. Jeden nenulový vektor nemůže příslušet více vlastním číslům, platí tedy $\lambda = \overline{\lambda}$, neboli $\lambda \in \mathbb{R}$. ▲

Důsledek 10.16 (Spektrální věta pro symetrické matice). *Nechť A je reálná čtvercová matice. Pak následující tvrzení jsou ekvivalentní.*

(1) *Matice A je ortogonálně diagonalizovatelná.*
(2) *Matice A je symetrická.*

Důkaz. Důkaz (1) $\Rightarrow$ (2) se udělá stejně jako v předchozí větě.

Pro důkaz opačné implikace předpokládejme, že A je reálná symetrická matice. Chápejme nyní A jako matici nad $\mathbb{C}$. Protože je A hermitovská, podle předchozí věty je unitárně diagonalizovatelná a všechna vlastní čísla jsou reálná. Z toho vyplývá (viz větu 10.4), že A má n reálných vlastních čísel včetně násobností, geometrická násobnost každého vlastního čísla je rovná jeho algebraické násobnosti a prostory M_λ jsou navzájem kolmé. Algebraická (geometrická) násobnost nad $\mathbb{C}$ je rovná algebraické (geometrické) násobnosti nad $\mathbb{R}$, takže chápeme-li A opět jako reálnou matici, bude splňovat podmínky z věty 10.4, a bude proto ortogonálně diagonalizovatelná. ▲

Příklad 10.17. Jako ilustraci spektrální věty pro reálné symetrické matice najdeme pro operátor f_A určený maticí

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

ortonormální bázi složenou z vlastních vektorů.

Operátor f_A má charakteristický polynom $p(\lambda) = (1-\lambda)(\lambda^2-1)$ a tedy vlastní čísla 1 a -1. Příslušné prostory vlastních vektorů jsou

$$\mathbf{M}_1 = \mathrm{LO}\left\{(1,1,0)^T, (0,0,1)^T\right\}, \mathbf{M}_{-1} = \mathrm{LO}\left\{(1,-1,0)^T\right\}$$

V prostoru $\mathbf{M}_1$ je ortonormální báze například $(\mathbf{v}_1, \mathbf{v}_2)$, kde

$$\mathbf{v_1} = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \quad \mathbf{v}_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad .$$

V prostoru $\mathbf{M}_{-1}$ tvoří ortonormální bázi například vektor

$$\mathbf{v}_3 = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \quad .$$

Báze $B = (\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ je ortonormální báze prostoru $\mathbf{V}$ a $[f_A]_B^B = \mathrm{diag}(1,1,-1)$.

Zapíšeme ještě výsledek maticově. Označme

$$Q = [\mathrm{id}]_K^B = \begin{pmatrix} \frac{\sqrt{2}}{2} & 0 & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & 0 & -\frac{\sqrt{2}}{2} \\ 0 & 1 & 0 \end{pmatrix} \quad .$$

Matice Q je ortogonální, takže $Q^{-1} = Q^T$ a můžeme psát

$$\mathrm{diag}(1,1,-1) = [f_A]_B^B = [\mathrm{id}]_B^K [f_A]_K^K [\mathrm{id}]_K^B = Q^{-1}AQ = Q^TAQ \quad ,$$

nebo ve formě rozkladu matice A

$$A = Q\,\mathrm{diag}(1,1,-1)Q^{-1} = Q\,\mathrm{diag}(1,1,-1)Q^T \ .$$

▲

10.2.3. Pozitivně (semi)definitní matice. Je-li A hermitovská matice řádu n, pak pro libovolný vektor $\mathbf{x} \in \mathbb{C}^n$ platí

$$\mathbf{x} \cdot A\mathbf{x} = A^*\mathbf{x} \cdot \mathbf{x} = A\mathbf{x} \cdot \mathbf{x} = \overline{\mathbf{x} \cdot A\mathbf{x}} \ .$$

Z toho plyne, že

$$\mathbf{x} \cdot A\mathbf{x} = \mathbf{x}^* A\mathbf{x}$$

je vždy reálné číslo. Pro $\mathbf{x} = \mathbf{o}$ je rovno 0. Ty matice, pro které je jinak toto číslo vždy kladné (resp. nezáporné) nazýváme pozitivně definitní (resp. semidefinitní).

Definice 10.18. Čtvercová matice A řádu n nad $\mathbb{C}$ (resp. $\mathbb{R}$) se nazývá

- *pozitivně definitní*, pokud je hermitovská (resp. symetrická) a pro všechna $\mathbf{o} \neq \mathbf{x} \in \mathbb{C}^n$ (resp. $\mathbf{o} \neq \mathbf{x} \in \mathbb{R}^n$) platí $\mathbf{x}^* A\mathbf{x} > 0$;
- *pozitivně semidefinitní*, pokud je hermitovská (resp. symetrická) a $\mathbf{x}^* A\mathbf{x} \geq 0$.

Všimněte si také geometrického významu nerovnosti $\mathbf{x}^* A\mathbf{x} = \mathbf{x} \cdot A\mathbf{x} > 0$. Říká, že vektor $\mathbf{x}$ a jeho obraz při zobrazení f_A svírají ostrý úhel.

Pozitivně definitní matice jsme již potkali v kapitole o skalárním součinu. Jsou to podle pozorování 8.21 právě ty matice A, pro které rovnost $\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}^* A\mathbf{v}$ definuje skalární součin na $\mathbb{C}^n$. Rovněž jsme si již uvědomili, že pozitivně definitní matice jsou regulární.

Pozitivně definitní matice lze ekvivalentně definovat tak, že jsou hermitovské (symetrické) a všechna vlastní čísla jsou kladná; podobně pro semidefinitnost. Z toho také vyplývají příslušné spektrální věty.

Tvrzení 10.19. *Nechť A je hermitovská (nebo symetrická) matice řádu n. Pak A je pozitivně definitní (resp. semidefinitní) právě tehdy, když jsou všechna vlastní čísla matice A kladná (resp. nezáporná).*

Důkaz. Dokážeme pouze verzi pro pozitivně definitní komplexní matice. Zbylá tvrzení se dokážou podobně.

Je-li A pozitivně definitní a λ je vlastní číslo matice A (to je nutně reálné), pak pro nenulový vlastní vektor $\mathbf{v}$ příslušný λ platí $0 < \mathbf{v} \cdot A\mathbf{v} = \mathbf{v} \cdot \lambda\mathbf{v} = \lambda \|\mathbf{v}\|^2$. Protože norma je kladná, plyne odsud $\lambda > 0$.

Jsou-li naopak všechna vlastní čísla matice A kladná, existuje podle spektrální věty pro hermitovské matice (věta 10.15) ortonormální báze B prostoru $\mathbb{C}^n$ taková, že $[f_A]_B^B = D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, kde λ_i jsou reálná vlastní čísla operátoru f, tj. $\lambda_i > 0$ pro všechna $i \in \{1, \ldots, n\}$. Pak užitím tvrzení 8.50 o skalárním součinu vzhledem k ortonormální bázi dostáváme pro libovolný vektor $\mathbf{x}$ vztah

$$\mathbf{x} \cdot A\mathbf{x} = [\mathbf{x}]_B \cdot [A\mathbf{x}]_B = ([\mathbf{x}]_B)^*[A\mathbf{x}]_B = ([\mathbf{x}]_B)^*[f_A]_B^B[\mathbf{x}]_B = ([\mathbf{x}]_B)^* D[\mathbf{x}]_B \ .$$

Označíme-li $[\mathbf{x}]_B = (x_1, \ldots, x_n)$ je výraz roven $\lambda_1|x_1|^2 + \cdots + \lambda_n|x_n|^2$, což je ostře větší než 0, kdykoliv $\mathbf{x} \neq 0$. ▲

Věta 10.20 (Spektrální věta pro pozitivně (semi)definitní matice). *Nechť A je komplexní čtvercová matice. Pak následující tvrzení jsou ekvivalentní.*

(1) *Matice A je unitárně diagonalizovatelná a všechna její vlastní čísla jsou kladná reálná (resp. nezáporná reálná).*
(2) *Matice A je pozitivně definitní (resp. semidefinitní).*

Důkaz. Věta je důsledkem spektrální věty pro hermitovské matice a předchozího tvrzení. ▲

Drobnou úpravu formulace spektrální věty pro reálný případ přenecháme čtenáři.

PŘÍKLAD 10.21. Reálná matice

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

není pozitivně definitní ani semidefinitní, protože má záporné vlastní číslo -1.

Reálná matice

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

má vlastní čísla 0 a 5, proto není pozitivně definitní. Matice A je pozitivně semidefinitní, protože je navíc ortogonálně diagonatlizovatelná.

Reálná matice

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$$

je pozitivně definitní. Pro libovolný nenulový vektor $(a, b) \in \mathbb{R}^2$ je proto číslo

$$(a, b)A \begin{pmatrix} a \\ b \end{pmatrix} = a^2 + 4ab + 5b^2$$

kladné. ▲

Aplikací spektrální věty dostaneme popis pozitivně definitních matic slíbený v kapitole o skalárním součinu: ukážeme, že všechny jsou tvaru A^*A.

To, že matice tvaru A^*A jsou pozitivně semidefinitní jsme již vlastně zdůvodnili v kapitole o skalárním součinu (mimo jiné je A^*A Gramova matice posloupnosti sloupcových vektorů matice A), odvození zopakujeme v důkazu následujícího tvrzení. Matice tvaru A^*DA, kde $D = \operatorname{diag}(d_1, \ldots, d_m)$, $d_i \geq 0$, lze psát ve tvaru

$$A^*DA = A^*\sqrt{D}\sqrt{D}A = A^*\sqrt{D}^*\sqrt{D}A = (\sqrt{D}A)^*(\sqrt{D}A) \ ,$$

kde $\sqrt{D}$ značí matici $\operatorname{diag}(\sqrt{d_1}, \ldots, \sqrt{d_m})$, jsou tedy také pozitivně semidefinitní.

TVRZENÍ 10.22. *Pro libovolnou komplexní matici A typu $m \times n$ je matice A^*A pozitivně semidefinitní. Je-li navíc A čtvercová regulární matice, pak A^*A je pozitivně definitní.*

Naopak, každou pozitivně semidefinitní komplexní matici B lze psát ve tvaru $B = A^*A$, kde A je čtvercová matice. V případě, že B je pozitivně definitní, je nutně A regulární.

DŮKAZ. Matice A^*A je hermitovská, protože $(A^*A)^* = A^*A^{**} = A^*A$. Pro libovolný vektor $\mathbf{x} \in \mathbb{C}^n$ platí $\mathbf{x}^*A^*A\mathbf{x} = (A\mathbf{x})^*(A\mathbf{x}) = \|A\mathbf{x}\|^2 \geq 0$, takže A^*A je pozitivně semidefinitní. Je-li navíc A regulární a $\mathbf{x} \neq \mathbf{o}$, pak $\|A\mathbf{x}\|^2 > 0$, a A je proto pozitivně definitní.

Naopak, nechť B je pozitivně semidefinitní komplexní matice. Podle spektrální věty a tvrzení 10.3 lze B psát ve tvaru $B = U^*DU$, kde U je unitární matice a D diagonální matice s nezápornými prvky na diagonále. Využitím obratu nad tvrzením dostáváme rozklad $B = (\sqrt{D}U)^*(\sqrt{D}U)$, takže stačí položit $A = \sqrt{D}U$. Je-li B pozitivně definitní, je $B = A^*A$ regulární. Pak je ale nutně i matice A regulární. ▲

10.2.4. Unitární a ortogonální matice. Další podtřídou normálních matic jsou matice unitární, v reálném případě ortogonální.

VĚTA 10.23 (Spektrální věta pro unitární matice). *Nechť A je komplexní čtvercová matice. Pak následující tvrzení jsou ekvivalentní.*

(1) *Matice A je unitárně diagonalizovatelná a pro všechna vlastní čísla $\lambda \in \mathbb{C}$ platí $|\lambda| = 1$.*
(2) *Matice A je unitární.*

Důkaz. (1) $\Rightarrow$ (2). Je-li A unitárně diagonalizovatelná a všechna její vlastní čísla jsou jednotková, pak můžeme podle tvrzení 10.3 psát $A = UDU^*$, kde U je unitární a D je diagonální s jednotkovými prvky na diagonále. Pak ale $D^*D = I_n$, takže platí

$$A^*A = (UDU^*)^*(UDU^*) = UD^*U^*UDU^* = UD^*DU^* = UU^* = I_n \ .$$

Matice A je tedy unitární.

(2) $\Rightarrow$ (1). Protože každá unitární matice je normální, stačí podle věty 10.13 ukázat, že pro všechna vlastní čísla λ matice A platí $|\lambda| = 1$. Vezmeme libovolný nenulový vlastní vektor $\mathbf{v}$ příslušný vlastnímu číslu λ. Protože f_A zachovává normu (viz bod (6) tvrzení 8.82 a bod (2) 8.88), platí $\|\mathbf{v}\| = \|A\mathbf{v}\| = \|\lambda\mathbf{v}\| = |\lambda|\,\|\mathbf{v}\|$. Z toho plyne $|\lambda| = 1$, jak jsme chtěli. ▲

Spektrální větu využijeme v následujících odstavcích k popisu ortogonálních operátorů na prostorech $\mathbb{R}^2$ a $\mathbb{R}^3$. Upozorňujeme, že pro ortogonální matice nemůžeme ve spektrální větě nahradit unitární diagonalizovatelnost ortogonální. Ne všechny ortogonální matice jsou totiž ortogonálně diagonalizovatelné, pouze ty symetrické. Při studiu ortogonálních matic nebo operátorů se proto většinou komplexním číslům nevyhneme.

10.2.5. Ortogonální operátory v dimenzi 2. Nechť $f : \mathbb{R}^2 \to \mathbb{R}^2$ je ortogonální operátor. Obrazy vektorů nějaké ortonormální báze (např. kanonické) jsou jednotkové a na sebe kolmé. Z toho lze geometricky nahlédnout, že f je buď rotace nebo reflexe (osová souměrnost). Toto pozorování teď dokážeme algebraicky, jako rozcvičku pro vyšší dimenze.

Označme si A matici f vzhledem ke kanonické bázi, tj. $f = f_A$. Někdy budeme A chápat jako komplexní matici a $f = f_A$ jako operátor na $\mathbb{C}^2$. Podle spektrální věty pro unitární matice pro všechna vlastní čísla matice A platí $|\lambda| = 1$. Protože má charakteristický polynom matice A reálné koeficienty, jsou obě vlastní čísla buď reálná nebo je tvoří dvojice komplexně sdružených čísel $\cos\varphi + i\sin\varphi = e^{i\varphi}$ a $\cos\varphi - i\sin\varphi = e^{-i\varphi}$. Označme $C = (\mathbf{v}_1, \mathbf{v}_2)$ nějakou ortonormální bázi prostoru $\mathbb{C}^2$ složenou z vlastních vektorů matice A.

Nejdříve probereme případ, kdy vlastní čísla matice A jsou reálná. Pak můžeme zvolit oba vlastní vektory $\mathbf{v}_1, \mathbf{v}_2$ reálné. Zde máme tři možnosti.

- Obě vlastní čísla se rovnají 1. Matice $[f]_C^C$ se pak rovná I_2 a operátor f se rovná identickému zobrazení.
- Obě vlastní čísla se rovnají -1. Matice $[f]_C^C$ se pak rovná $-I_2$ a operátor f se rovná středové symetrii – stejnolehlosti s koeficientem -1.
- Jedno vlastní číslo se rovná 1 a druhé -1. Matice $[f]_C^C$ se pak při vhodném uspořádání bázových vektorů rovná

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

  Zobrazení f je reflexe (osová souměrnost) vzhledem k přímce generované vektorem $\mathbf{v}_1$.

Zbývá případ komplexních vlastních čísel, která nejsou reálná. Označme $\mathbf{v} = (a + bi, c + di)$ vlastní vektor příslušný číslu $\lambda = \cos\varphi + i\sin\varphi$. V části 9.3.5 jsme ukázali, že $\overline{\mathbf{v}}$ je vlastní vektor příslušný vlastnímu číslu $\overline{\lambda}$ a vzhledem k bázi $C' = (\mathbf{w}_1, \mathbf{w}_2) = (\mathbf{v} + \overline{\mathbf{v}}, i(\mathbf{v} - \overline{\mathbf{v}})) = (2Re(\mathbf{v}), -2Im(\mathbf{v}))$ má operátor matici rovnou matici rotace o úhel φ.

Protože $\mathbf{v}$ a $\overline{\mathbf{v}}$ jsou na sebe kolmé, platí

$$\mathbf{v}^*\overline{\mathbf{v}} = (a - ib, c - id)\begin{pmatrix} a - ib \\ c - id \end{pmatrix} = a^2 - b^2 + c^2 - d^2 - 2i(ab + cd) = 0 \ .$$

Z imaginární části výrazu vidíme, že $ab + cd = 0$ a reálné vektory $\mathbf{w}_1 = 2Re\,\mathbf{v} = (2a, 2c)^T$ a $\mathbf{w}_2 = -2Im\,\mathbf{v} = (-2b, -2d)$ jsou na sebe kolmé. Z reálné části výrazu vidíme, že oba vektory $\mathbf{w}_1, \mathbf{w}_2$ mají stejnou normu $e = \sqrt{4a^2 + 4c^2} = \sqrt{4b^2 + 4d^2}$. Báze

$$B = (\mathbf{w}_1/e, \mathbf{w}_2/e)$$

je ortonormální báze prostoru $\mathbb{R}^2$. Protože vznikla vynásobením vektorů báze C' stejným skalárem je

$$[f]_B^B = [f]_{C'}^{C'} = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$$

a zobrazení f je tedy rotace.

Pokud vezmeme do úvahy, že středová symetrie je rotace o úhel π a identické zobrazení je rotace o úhel 0, dokázali jsme následující klasifikaci ortogonálních zobrazení v $\mathbb{R}^2$.

Tvrzení 10.24. *Každý ortogonální operátor f na $\mathbb{R}^2$ je buď rotace nebo reflexe. Rotace je to právě když* $\det[f]_B^B = 1$ *a reflexe je to právě když* $\det[f]_B^B = -1$*, kde B je libovolná báze $\mathbb{R}^2$.*

Protože složení dvou ortogonálních zobrazení je opět ortogonální zobrazení, dostáváme s použitím věty o součinu determinantů tento důsledek.

Důsledek 10.25. *Složení dvou rotací v $\mathbb{R}^2$ je opět rotace, složení dvou reflexí je rotace a složení rotace s reflexí (v libovolném pořadí) je opět nějaká reflexe.*

10.2.6. Ortogonální operátory v dimenzi 3. Rozšíříme klasifikaci ortogonálních zobrazení na aritmetické prostory dimenze 3.

Nechť $f : \mathbb{R}^3 \to \mathbb{R}^3$ je ortogonální operátor na prostoru $\mathbb{R}^3$ se standardním skalárním součinem a $A = [f]_K^K$ jeho matice vzhledem ke kanonické bázi v $\mathbb{R}^3$. Podobně jako v dimenzi 2 budeme A někdy chápat jako komplexní matici. Charakteristický polynom má všechna vlastní čísla rovná v absolutní hodnotě 1 a existuje ortonormální báze $C = (\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ prostoru $\mathbb{C}^3$ složená z vlastních vektorů matice A. Protože charakteristický polynom má reálné koeficienty, jsou buď všechna vlastní čísla reálná (rovná ± 1) a nebo je jedno reálné a zbylá dvě jsou komplexně sdružená čísla $e^{i\varphi}$ a $e^{-i\varphi}$ pro nějaký úhel φ.

Předpokládejme, že pouze jedno vlastní číslo je reálné. K němu příslušný vlastní vektor $\mathbf{v}_1$ můžeme proto také zvolit reálný. Chápeme-li A jako komplexní matici, podprostor $\mathbf{v}_1^\perp = \mathrm{LO}\{\mathbf{v}_2, \mathbf{v}_3\}$ prostoru $\mathbb{C}^3$ je invariantním podprostorem operátoru f_A, protože je lineárním obalem vlastních vektorů. Tím spíše je i $W = \mathbf{v}_1^\perp$ (tentokrát chápáno reálně) invariatním podprostorem v $\mathbb{R}^3$ operátoru f. Označme $g = f_{|W}$ zúžení f na tento podprostor dimenze 2.

Operátor g na prostoru $\mathbf{W}$ je zřejmě ortogonální. Podle tvrzení 9.112 charakteristický polynom operátoru g dělí charakteristický polynom operátoru f. Z toho vyplývá, že $p_g(\lambda)$ má komplexní vlastní čísla $e^{i\varphi}$ a $e^{-i\varphi}$. Z diskuze v dimenzi 2 nyní vyplývá (viz poznámku), že g má vzhledem k ortonormální bázi $(a\,Re\,\mathbf{v}_2, -a\,Im\,\mathbf{v}_2)$ tohoto podprostoru, kde $a = \|Re\,\mathbf{v}_2\|^{-1}$, matici

$$\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \ .$$

Poznámka. Zde se projevuje jedna z nevýhod práce s aritmetickými prostory místo abstraktních. Diskuzi v části 10.2.5 jsme prováděli pro operátory na $\mathbb{R}^2$, nyní

bychom ale potřebovali výsledek pro dvoudimenzionální podprostor $\mathbb{R}^3$, což není aritmetický prostor. Doplnit argument ale můžeme užitím libovolné ortonormální báze C prostoru $\mathbf{W}$. Potřebujeme ukázat, že vektory $Re\,\mathbf{v}_2$ a $Im\,\mathbf{v}_2$ jsou na sebe kolmé a mají stejnou normu. Víme, že $\mathbf{v}_2 \cdot \overline{\mathbf{v}_2} = 0$, takže také $[\mathbf{v}_2]_C \cdot [\overline{\mathbf{v}_2}]_C = [\mathbf{v}_2]_C \cdot \overline{[\mathbf{v}_2]_C} = 0$ podle tvrzení 8.50. Výpočet v části 10.2.5 ukazuje, že pak $[Re\,\mathbf{v}_2]_C$ a $[Im\,\mathbf{v}_2]_C$ jsou na sebe kolmé a mají stejnou normu, a tedy totéž platí pro $Re\,\mathbf{v}_2$ a $Im\,\mathbf{v}_2$, opět podle tvrzení 8.50. (V právě provedeném argumentu opět poněkud neformálně kombinujeme reálná a komplexní čísla, formální doladění ale již přenecháme čtenáři.)

Je-li reálné vlastní číslo rovné 1, má potom f vzhledem k ortonormální bázi $B = (\mathbf{v_1}, a\,Re\,\mathbf{v}_2, -a\,Im\,\mathbf{v}_2)$ prostoru $\mathbb{R}^3$ matici

$$[f]_B^B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{pmatrix} .$$

a jde tedy o rotaci kolem osy generované vektorem $\mathbf{v}_1$ o úhel φ.

Je-li jediné reálné vlastní číslo operátoru f rovné -1, platí

$$[f]_B^B = \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{pmatrix}$$

a zobrazení f je tedy složením rotace kolem osy generované $\mathbf{v}_1$ o úhel φ s reflexí (zrcadlením) určenou rovinou kolmou na vektor $\mathbf{v}_1$.

Jsou-li všechna vlastní čísla matice A reálná, můžeme zvolit ortonormální bázi $\mathbb{C}^3$ složenou z reálných vektorů a matice $[f]_B^B$ má (až na pořadí prvků na hlavní diagonále) jeden ze tvarů

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

V prvním případě jde o identické zobrazení (tj. rotaci o úhel 0), ve druhém případě jde o zrcadlení vzhledem k rovině $\mathrm{LO}\{\mathbf{v}_1, \mathbf{v}_2\} = \{\mathbf{v}_3\}^\perp$, ve třetím případě jde o rotaci kolem osy generované $\mathbf{v}_1$ o úhel π a ve čtvrtém případě jde o složení této rotace s reflexí (zrcadlením) určenou rovinou $\mathrm{LO}\{\mathbf{v}_2, \mathbf{v}_3\}$.

Platí proto následující tvrzení.

Tvrzení 10.26. *Každé ortogonální zobrazení v euklidovském prostoru $\mathbb{R}^3$ je buď rotace kolem nějaké osy, reflexe vzhledem k nějaké rovině a nebo složení rotace s reflexí. Rotace je to právě tehdy, když determinant matice tohoto zobrazení vzhledem k jakékoliv bázi je rovný* 1.

Důsledek 10.27. *Složení dvou rotací v $\mathbb{R}^3$ je zase rotace v $\mathbb{R}^3$, složení dvou reflexí je rotace (osa rotace je rovná průniku rovin reflexí).*

10.3. Singulární rozklad

Pro některé operátory určené čtvercovými komplexními nebo reálnými maticemi umíme najít ortonormální bázi, vzhledem ke které má daný operátor diagonální matici. V komplexním případě jsou to právě operátory určené normální maticí, v reálném případě symetrickou maticí. Když slevíme z požadavku, že báze pro vzory a obrazy jsou stejné, lze „unitárně diagonalizovat“ každou komplexní nebo reálnou matici, která ani nemusí být čtvercová. Navíc na diagonále budou v tomto diagonálním tvaru nezáporná reálná čísla.

10.3.1. Tři pohledy na singulární rozklad. Začneme příkladem, který ilustruje tři pohledy na tuto zobecněnou unitární diagonalizaci.

PŘÍKLAD 10.28. Uvažujme „zkosení“ $f_A : \mathbb{R}^2 \to \mathbb{R}^2$, kde

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

Budeme umět spočítat, že vzhledem k bázím B a C, kde

$$B = (\mathbf{v}_1, \mathbf{v}_2) \approx \left(\begin{pmatrix} 0{,}526 \\ 0{,}851 \end{pmatrix}, \begin{pmatrix} -0{,}851 \\ 0{,}526 \end{pmatrix} \right) ,$$

$$C = (\mathbf{u}_1, \mathbf{u}_2) \approx \left(\begin{pmatrix} 0{,}851 \\ 0{,}526 \end{pmatrix}, \begin{pmatrix} -0{,}526 \\ 0{,}851 \end{pmatrix} \right) ,$$

má f matici

$$[f_A]_C^B = \begin{pmatrix} \sigma_1 & 0 \\ 0 & \sigma_2 \end{pmatrix} \approx \begin{pmatrix} 1{,}618 & 0 \\ 0 & 0{,}618 \end{pmatrix} .$$

Z toho vidíme, že vektor $\mathbf{v}_1$ se při zobrazení f_A zobrazí na přibližně 1,618-násobek vektoru $\mathbf{u}_1$ a vektor $\mathbf{v}_2$ se zobrazí na přibližně 0,618-násobek vektoru $\mathbf{u}_2$. Obecněji, obraz vektoru $\mathbf{x}$ o souřadnicích $[\mathbf{x}]_B = (x_1, x_2)^T$ vzhledem k bázi B je vektor $A\mathbf{x}$ o souřadnicích $[A\mathbf{x}]_C \approx (1{,}618x_1, 0{,}618x_2)^T$ vzhledem k bázi C.

OBRAZEK

Z této informace například snadno určíme obraz jednotkového kruhu $O = \{\mathbf{x} : \|\mathbf{x}\| \leq 1\}$. Protože B je ortonormální báze, platí $\|\mathbf{x}\| = \|[\mathbf{x}]_B\|$. Vektor $\mathbf{x}$ proto leží v O právě tehdy, když jeho souřadnice $[\mathbf{x}]_B = (x_1, x_2)^T$ vzhledem k bázi B splňují $x_1^2 + x_2^2 \leq 1$. Obrazem vektoru $\mathbf{x}$ je vektor $A\mathbf{x}$ o souřadnicích $[A\mathbf{x}]_C = (y_1, y_2)^T \approx (1{,}618x_1, 0{,}618x_2)^T$. V obrazu kruhu O tedy budou právě ty body, jejichž souřadnice vzhledem k C splňují

$$\left(\frac{y_1}{1{,}618}\right)^2 + \left(\frac{y_2}{0{,}618}\right)^2 \leq 1$$

Z toho vidíme, že obrazem je elipsa s délkami poloos (přibližně) 1,618, 0,618. Směry poloos jsou určeny vektory $\mathbf{u}_1, \mathbf{u}_2$ báze C.

Užitečná je také maticová verze. Označíme-li $U = [\mathrm{id}]_K^C$ a $V = [\mathrm{id}]_K^B$, dostaneme z $[f_A]_C^B = D$ vztah $A = UDV^{-1}$. Protože V je ortogonální matice, platí $V^{-1} = V^T$, takže také můžeme psát $A = UDV^T$.

$$A = UDV^T \approx \begin{pmatrix} 0{,}851 & -0{,}526 \\ 0{,}526 & 0{,}851 \end{pmatrix} \begin{pmatrix} 1{,}618 & 0 \\ 0 & 0{,}618 \end{pmatrix} \begin{pmatrix} 0{,}526 & 0{,}851 \\ -0{,}851 & 0{,}526 \end{pmatrix}$$

Na tento rozklad se také můžeme dívat tak, že zobrazení f_A vyjadřujeme jako složení $f_A = f_U f_D f_{V^T}$, kde f_U a f_{V^T} jsou ortogonální zobrazení a f_D je zobrazení určené diagonální maticí. Zobrazení f_A je tak v našem případě složením zobrazení $f_{V^T} = f_{V^{-1}}$, což je rotace o přibližně $-58{,}28°$, zobrazení f_D, které natahuje vektory 1,618-krát ve směru první osy a zkracuje 0,618-krát ve směru druhé osy, a zobrazení f_U, což je rotace o přibližně $31{,}72°$. I z tohoto pohledu vidíme obraz jednotkového kruhu: Zobrazení $f_{V^T} = f_{V^{-1}}$ zobrazí O na O (přičemž vektor $\mathbf{v}_1$ se zobrazí na $\mathbf{e}_1$ a vektor $\mathbf{v}_2$ na $\mathbf{e}_2$). Zobrazení f_D kružnici deformuje ve směru souřadnicových os, čímž vznikne elipsa s osami LO $\{\mathbf{e}_1\}$, LO $\{\mathbf{e}_2\}$. Tuto elipsu zobrazení f_U otočí.

OBRAZEK

Použijeme-li pohled na násobení matic systémem “sloupec krát řádek”, můžeme vztah $A = (UD)V^T$ napsat ve tvaru *dyadického rozvoje*

$$A = \sigma_1 \mathbf{u}_1 \mathbf{v}_1^* + \sigma_2 \mathbf{u}_2 \mathbf{v}_2^* .$$

Matici A jsme vyjádřili jako součet matic hodností 1. Uvidíme, že první sčítanec

$$\sigma_1 \mathbf{u}_1 \mathbf{v}_1^* \approx \begin{pmatrix} 0{,}724 & 1{,}171 \\ 0{,}447 & 0{,}724 \end{pmatrix}$$

je vlastně v jistém smyslu nejlepší aproximace matice A maticí hodnosti 1. ▲

10.3.2. Singulární rozklad. Uvažujme obdélníkovou matici typu $m \times n$ nad $\mathbb{C}$ (resp. $\mathbb{R}$) a příslušné lineární zobrazení $f_A : \mathbb{C}^n \to \mathbb{C}^m$ (resp. $f_A : \mathbb{R}^n \to \mathbb{R}^m$). Chceme najít ortonormální bázi B prostoru $\mathbb{C}^n$ (resp. $\mathbb{R}^n$) a ortonormální bázi C prostoru $\mathbb{C}^m$ (resp. $\mathbb{R}^m$) tak, aby $[f_A]_C^B$ byla „diagonální“ s nezápornými reálnými čísly na diagonále.

Tato matice nemusí být čtvercová, pojem diagonální matice proto rozšíříme. Říkáme, že matice $D = (d_{ij})$ typu $m \times n$ je *obdélníková diagonální matice*, pokud $d_{ij} = 0$, kdykoliv $i \neq j$ (kde $i \in \{1, \dots, m\}$, $j \in \{1, \dots, n\}$). Obdélníkovou diagonální matici budeme zapisovat $D = \operatorname{diag}(d_{11}, \dots, d_{rr})$ nebo obšírněji

$$D = \operatorname{diag}_{m \times n}(d_{11}, \dots, d_{rr}) \ ,$$

chceme-li zvýraznit typ matice D. Budeme často vypisovat pouze nenulové prvky, tj. je-li $r < \min(m, n)$, rozumí se, že zbylé diagonální prvky jsou nulové.

Klíčové pozorování k nalezení bází B a C je následující. Pokud

$$[f_A]_C^B = D = \operatorname{diag}_{m \times n}(d_{11}, \dots, d_{rr}), \quad d_{ii} \in \mathbb{R} \ ,$$

pak matice lineárního zobrazení f_{A^*} vzhledem k bázím C a B je D^*, protože

$$\begin{aligned} [f_{A^*}]_B^C &= [\mathrm{id}]_B^{K_n} [f_{A^*}]_{K_n}^{K_m} [\mathrm{id}]_{K_m}^C = ([\mathrm{id}]_{K_n}^B)^* A^* ([\mathrm{id}]_C^{K_m})^* \\ &= ([\mathrm{id}]_C^{K_m} A [\mathrm{id}]_{K_n}^B)^* = ([f_A]_C^B)^* = D^* \ , \end{aligned}$$

kde ve druhé úpravě jsme využili $([\mathrm{id}]_K^B)^{-1} = ([\mathrm{id}]_K^B)^*$ a $([\mathrm{id}]_C^K)^{-1} = ([\mathrm{id}]_C^K)^*$, což platí, protože obě matice jsou unitární. Z toho vyplývá, že matice operátoru f_{A^*A} vzhledem k ortonormální bázi B je

$$[f_{A^*A}]_B^B = [f_{A^*} \circ f_A]_B^B = [f_{A^*}]_B^C [f_A]_C^B = D^* D = \operatorname{diag}_{n \times n}(d_{11}^2, \dots, d_{rr}^2) \ .$$

Všimněte si, že jsme vlastně unitárně zdiagonalizovali matici A^*A. Nyní vidíme, že prvky na diagonále matice $[f_A]_C^B$ jsou nutně druhé odmocniny vlastních čísel matice A^*A a báze B musí sestávat z vlastních vektorů této matice. Navíc ze vztahu $[f_A]_C^B = D$ vidíme, že obraz i-tého vektoru báze B při zobrazení f_A musí být d_{ii}-násobkem i-tého vektoru v bázi C (pro $i \leq \min(m, n)$). Tato pozorování dávají návod k důkazu věty o singulárním rozkladu.

Věta 10.29. *[o singulárním rozkladu] Nechť A je komplexní (resp. reálná) matice typu $m \times n$ hodnosti r. Pak existují ortonormální báze $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$, $C = (\mathbf{u}_1, \dots, \mathbf{u}_m)$ prostorů $\mathbb{C}^n$, $\mathbb{C}^m$ (resp. $\mathbb{R}^n$, $\mathbb{R}^m$) a reálná čísla $\sigma_1, \dots, \sigma_r > 0$ taková, že*

(i) *(singulární rozklad, geometrická verze) $[f_A]_C^B$ je obdélníková diagonální matice*

$$[f_A]_C^B = \operatorname{diag}_{m \times n}(\sigma_1, \dots, \sigma_r) \ ,$$

(ii) *(singulární rozklad, algebraická verze) platí*

$$A = UDV^{-1} = UDV^* \ ,$$

kde U, V jsou unitární (resp. ortogonální) matice

$$U = [\mathrm{id}]_{K_m}^C = (\mathbf{u}_1 | \dots | \mathbf{u}_m), \quad V = [\mathrm{id}]_{K_n}^B = (\mathbf{v}_1 | \dots | \mathbf{v}_n)$$

a $D = \operatorname{diag}_{m \times n}(\sigma_1, \dots, \sigma_r)$.

(iii) *(dyadický rozvoj) platí*

$$A = \sigma_1 \mathbf{u}_1 \mathbf{v}_1^* + \dots + \sigma_r \mathbf{u}_r \mathbf{v}_r^* \ .$$

Navíc v této situaci

(iv) $\sigma_1, \ldots, \sigma_r$ *jsou druhé odmocniny vlastních čísel matice* A^*A,

(v) *pro každé* $i \in \{1, \ldots, r\}$ *je* $\mathbf{v}_i$ *vlastní vektor matice* A^*A *příslušný vlastnímu číslu* σ_i^2,

(vi) $\operatorname{Ker} A = \operatorname{LO}\{\mathbf{v}_{r+1}, \ldots, \mathbf{v}_n\} = \operatorname{LO}\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}^\perp$,

(vii) $\operatorname{Im} A = \operatorname{LO}\{\mathbf{u}_1, \ldots, \mathbf{u}_r\} = \operatorname{LO}\{\mathbf{u}_{r+1}, \ldots, \mathbf{u}_m\}^\perp$.

Důkaz. Matice A^*A řádu n je podle tvrzení 10.22 pozitivně semidefinitní, takže podle spektrální věty pro hermitovské (resp. v reálném případě symetrické) operátory (věta 10.15 nebo důsledek 10.16) existuje ortonormální báze $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ prostoru $\mathbb{C}^n$ (resp. $\mathbb{R}^n$) složená z vlastních vektorů matice A^*A a $[f_{A^*A}]_B^B = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$, kde $\lambda_1, \ldots, \lambda_n$ jsou nezáporná reálná vlastní čísla matice A^*A. Vektory v bázi B uspořádáme tak, aby $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. Řekněme, že prvních r vektorů je nenulových; nakonec uvidíme, že r je hodnost A.

Podívejme se, jak vypadá $A\mathbf{v}_i$ pro $i > r$. Protože pro taková i je $\lambda_i = 0$, tak platí

$$A^\star A\mathbf{v}_i = \lambda_i \mathbf{v}_i = 0\mathbf{v}_i = \mathbf{o}.$$

Vynásobením $\mathbf{v}_i^\star$ zleva dostaneme

$$\mathbf{v}_i^\star A^\star A\mathbf{v}_i = \mathbf{v}_i^\star \mathbf{o} = 0.$$

Porovnáním s normou odvozenou ze standardního skalárního součinu dostáváme

$$0 = \mathbf{v}_i^\star A^\star A\mathbf{v}_i = (A\mathbf{v}_i) \cdot (A\mathbf{v}_i) = \|A\mathbf{v}_i\|^2.$$

Tedy $A\mathbf{v}_i$ má nulovou normu, což lze jen tak, že $A\mathbf{v}_i = \mathbf{o}$ kdykoli $i > r$. (Na okraj poznamenejme, že jsme právě našli $n - r$ lineárně nezávislých vektorů $\mathbf{v}_i$ v jádru A; hodnost A tedy bude nejvýše r.)

Pro $i \in \{1, \ldots, r\}$ označíme $\sigma_i = \sqrt{\lambda_i}$ a $\mathbf{u}_i = \sigma_i^{-1} A\mathbf{v}_i$. Pak pro libovolná $i, j \in \{1, \ldots, r\}$ platí

$$\begin{aligned}\mathbf{u}_i \cdot \mathbf{u}_j &= \sigma_i^{-1} A\mathbf{v}_i \cdot \sigma_j^{-1} A\mathbf{v}_j = \sigma_i^{-1}\sigma_j^{-1}(A\mathbf{v}_i \cdot A\mathbf{v}_j) \\ &= \sigma_i^{-1}\sigma_j^{-1}(A^*A\mathbf{v}_i \cdot \mathbf{v}_j) = \sigma_i^{-1}\sigma_j^{-1}\lambda_i(\mathbf{v}_i \cdot \mathbf{v}_j) \ .\end{aligned}$$

Z toho vyplývá, že pro $i \neq j$ jsou vektory $\mathbf{u}_i, \mathbf{u}_j$ na sebe kolmé a navíc $\mathbf{u}_i \cdot \mathbf{u}_i = \sigma_i^{-2}\lambda_i = 1$, takže každý z vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_r$ má jednotkovou normu. Můžeme tedy tuto posloupnost doplnit na ortonormální bázi $C = (\mathbf{u}_1, \ldots, \mathbf{u}_m)$ prostoru $\mathbf{C}^m$ (resp. $\mathbb{R}^m$).

Nyní pro $i \in \{1, \ldots, r\}$ je $A\mathbf{v}_i = \sigma_i \mathbf{u}_i$, neboli $[f_A(\mathbf{v}_i)]_C = \sigma_i \mathbf{e}_i$. Jak to bude pro $i > r$?

Tedy $[f_A(\mathbf{v}_i)]_C = \mathbf{o}$. Matice lineárního zobrazení f_A vzhledem k bázím B a C je tedy skutečně

$$[f_A]_C^B = D = \operatorname{diag}_{m\times n}(\sigma_1, \ldots, \sigma_r) \ .$$

Bod (ii) nyní plyne z výpočtu

$$A = [f]_K^K = [\mathrm{id}]_K^C [f]_C^B [\mathrm{id}]_B^K = UDV^{-1} = UDV^*$$

a výraz z bodu (iii) je součin $(UD)V^*$ rozepsaný systémem "sloupec krát řádek". Body (iv) a (v) plynou z diskuze před větou. Konečně, podle tvrzení 6.23 o výpočtu jádra a obrazu máme

$$[\operatorname{Ker} f_A]_B = \operatorname{Ker} D = \operatorname{LO}\{\mathbf{e}_{r+1}, \ldots, \mathbf{e}_n\}, \quad [\operatorname{Im} f_A]_C = \operatorname{Im} D = \operatorname{LO}\{\mathbf{e}_1, \ldots, \mathbf{e}_r\}$$

takže

$$\begin{aligned}\operatorname{Ker} A &= \operatorname{LO}\{\mathbf{v}_{r+1}, \ldots, \mathbf{v}_n\} = \operatorname{LO}\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}^\perp \\ \operatorname{Im} A &= \operatorname{LO}\{\mathbf{u}_1, \ldots, \mathbf{u}_r\} = \operatorname{LO}\{\mathbf{u}_{r+1}, \ldots, \mathbf{u}_m\}^\perp \ .\end{aligned}$$

Speciálně, hodnost matice A je $\dim \operatorname{Im} A = r$. ▲

Je zvykem vektory v bázích B a C uspořádat tak, že na diagonále matice $[f]_C^B$ jsou prvky uspořádány sestupně podle velikosti. Nenulové prvky na diagonále se nazývají singulární hodnoty matice A.

Definice 10.30. Nechť A je komplexní nebo reálná matice. Kladné reálné číslo σ nazýváme *singulární hodnota* matice A, pokud σ^2 je vlastní číslo matice A^*A.

Z pozorování nad větou 10.29 také vyplývá, že nenulová hodnota σ je na diagonále matice D tolikrát, kolik je násobnost σ^2 jako vlastního čísla matice A^*A.

Příklad 10.31. Spočítáme singulární rozklad matice zkosení $f_A : \mathbb{R}^2 \to \mathbb{R}^2$ diskutovaného v příkladu 10.28.

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

Postupujeme podle důkazu věty 10.29. Najdeme ortonormální bázi $B = (\mathbf{v}_1, \mathbf{v}_2)$ prostoru $\mathbb{R}^2$ se standardním skalárním součinem takovou, že matice operátoru $f_{A^*A} = f_{A^TA}$ vzhledem k B je diagonální.

Vlastní čísla matice

$$A^TA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

jsou $\lambda_{1,2} = (3 \pm \sqrt{5})/2$, singulární hodnoty jsou proto

$$\sigma_{1,2} = \sqrt{\frac{3 \pm \sqrt{5}}{2}}, \quad \sigma_1 \approx 1{,}618, \quad \sigma_2 \approx 0{,}618 \ .$$

Příslušné prostory vlastních vektorů matice A^TA jsou jednodimenzionální, vybereme v nich vektory jednotkové velikosti. Vyjde přibližně

$$\mathbf{v}_1 \approx \begin{pmatrix} 0{,}526 \\ 0{,}851 \end{pmatrix} \in M_{\lambda_1}, \quad \mathbf{v}_2 \approx \begin{pmatrix} -0{,}851 \\ 0{,}526 \end{pmatrix} \in M_{\lambda_2} \ .$$

Vektory $\mathbf{u}_1, \mathbf{u}_2$ vypočteme ze vzorce $\mathbf{u}_i = \sigma_i^{-1} A\mathbf{v}_i$.

$$\mathbf{u}_1 \approx \begin{pmatrix} 0{,}851 \\ 0{,}526 \end{pmatrix}, \quad \mathbf{u}_2 \approx \begin{pmatrix} -0{,}526 \\ 0{,}851 \end{pmatrix} \ .$$

Vzhledem k bázím $B = (\mathbf{v}_1, \mathbf{v}_2)$ a $C = (\mathbf{u}_1, \mathbf{u}_2)$ má f_A matici

$$D = [f_A]_C^B \approx \begin{pmatrix} 1{,}618 & 0 \\ 0 & 0{,}618 \end{pmatrix} \ .$$

▲

10.3.3. Interpretace geometrické verze. Rozmyslíme si podrobněji, co vztah $[f_A]_C^B = D = \mathrm{diag}_{m\times n}(\sigma_1, \dots, \sigma_r)$ říká o lineárním zobrazení f_A. Označme $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ a $C = (\mathbf{u}_1, \dots, \mathbf{u}_m)$. Podle definice matice lineárního zobrazení je $f_A(\mathbf{v}_1) = \sigma_1\mathbf{u}_1$, ..., $f_A(\mathbf{v}_r) = \sigma_r\mathbf{u}_r$. Pro zbylé vektory v bázi B je $f_A(\mathbf{v}_{r+1}) = \dots = f_A(\mathbf{v}_n) = \mathbf{o}$. Obecněji, obraz vektoru $\mathbf{x}$ spočítáme vzorcem $[f_A(\mathbf{x})]_C = [f_A]_C^B[\mathbf{x}]_B$, tedy obrazem vektoru $\mathbf{x}$, jehož souřadnice vzhledem k bázi B jsou

$$[\mathbf{x}]_B = (x_1, \dots, x_n)^T \ ,$$

je vektor $f_A(\mathbf{x})$, jehož souřadnice vzhledem k bázi C jsou

$$[f_A(\mathbf{x})]_C = D(x_1, \dots, x_n)^T = \underbrace{(\sigma_1 x_1, \dots, \sigma_r x_r, 0, \dots, 0)^T}_{m \text{ složek}}$$

Podobně jako v příkladu 10.28 z toho v případě reálných matic malých typů vidíme, že obrazem jednotkové koule v $\mathbb{R}^n$ je *zobecněný elipsoid* v $\mathbb{R}^m$ s poloosami $\sigma_1\mathbf{u}_1$, ..., $\sigma_r\mathbf{u}_r$ velikostí σ_1, ..., σ_r. Pokud $r = 1$ je zobecněný elipsoid úsečka, pro $r = 2$ elipsa (i s vnitřkem) a pro $r = 3$ elipsoid (opět s vnitřkem).

OBRAZEK

V některých situacích můžeme vektory $\mathbf{v}_1, \dots, \mathbf{v}_n$ interpretovat jako význačné směry v $\mathbb{C}^n$ ($\mathbb{R}^n$), vektory $\mathbf{u}_1$, ..., $\mathbf{u}_m$ jako význačné směry pro obrazy a čísla $\sigma_1, \dots, \sigma_r$ jako velikosti vlivů jednotlivých složek na výsledný vektor.

PŘÍKLAD 10.32. Předpokládejme $\dim \mathbf{V} = 5$, $\dim \mathbf{U} = 4$, $B = (\mathbf{v}_1, \dots, \mathbf{v}_5)$, $C = (\mathbf{u}_1, \dots, \mathbf{u}_4)$ a $[f]_C^B = \mathrm{diag}_{4\times 5}(10,\ 9,\ 0{,}1)$.

Vektor $\mathbf{x}$ s vyjádřením $[\mathbf{x}]_B = (x_1, x_2, x_3, x_4, x_5)^T$ se zobrazí na vektor $f(\mathbf{x})$ s vyjádřením $[f(\mathbf{x})]_C = (10x_1, 9x_2, 0{,}1x_3, 0)$, čili vektor $f(\mathbf{x}) = 10x_1\mathbf{u}_1 + 9x_2\mathbf{u}_2 + 0{,}1x_3\mathbf{u}_3$. To lze interpretovat tak, že největší vliv na $f(\mathbf{x})$ mají první dvě složky x_1, x_2 odpovídající vektorům $\mathbf{v}_1, \mathbf{v}_2$. Tyto složky se přibližně zdesetinásobí, $f(\mathbf{x})$ bude „blízko“ roviny $\mathrm{LO}\{\mathbf{u}_1, \mathbf{u}_2\}$ a bude mít přibližně desetkrát větší normu (pokud není třetí složka příliš velká). Vliv třetí složky x_3 je malý a další složky nemají na výsledek žádný vliv.

Jádrem f je prostor $\mathrm{Ker}\, f = \mathrm{LO}\{\mathbf{v}_4, \mathbf{v}_5\} = \mathrm{LO}\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}^\perp$ a obrazem f je prostor $\mathrm{LO}\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\} = \mathbf{u}_4^\perp$. ▲

10.3.4. Geometrická interpretace algebraické verze. Rozklad $A = UDV^T = UDV^{-1}$ můžeme geometricky interpretovat jako $f_A = f_U f_D f_{V^{-1}}$. V případě reálné čtvercové matice řádu n je tedy $f_A : \mathbb{R}^n \to \mathbb{R}^n$ složením pořadě ortogonálního zobrazení $f_{V^{-1}}$, zobrazení f_D, které natahuje nebo zkracuje souřadnicové osy a ortogonálního zobrazení f_U.

Pro zobrazení $f_A = f_U f_D f_{V^T} : \mathbb{R}^n \to \mathbb{R}^m$ sledujme postupně obraz n-dimenzionální koule $O = \{\mathbf{x} : \|\mathbf{x}\| \le 1\}$. Zobrazení f_{V^T} je ortogonální, proto zobrazí O opět na O, přičemž vektor $\mathbf{v}_i$ se zobrazí na $\mathbf{e}_i$. Zobrazení f_D pak kruh O natáhne nebo smrští ve směru souřadnicových os (případně ještě ubere nebo přidá složky pokud $m \ne n$), tím vznikne zobecněný elipsoid s poloosami $\sigma_1\mathbf{e}_1, \sigma_2\mathbf{e}_2, \dots$. Nakonec se na vzniklou množinu aplikuje zobrazení f_U, které vektor $\mathbf{e}_i$ zobrazí na vektor $\mathbf{u}_i$. Tím vznikne zobecněný elipsoid s polosami $\sigma_1\mathbf{u}_1, \sigma_2\mathbf{u}_2, \dots$ velikostí $\sigma_1, \sigma_2, \dots$.

10.3.5. Příklady.

PŘÍKLAD 10.33. Spočítáme singulární rozklad pro reálnou čtvercovou matici

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

Tato matice je normální, v příkladu 10.14 jsme ji unitárně diagonalizovali. V následujícím odstavci si rozmyslíme, jak spočítat singulární rozklad přímo z unitární diagonalizace, pokud nám nevadí komplexní aritmetické vektory v bázích B a C. Nyní ale budeme postupovat přímo podle důkazu věty 10.29. Najdeme ortonormální bázi $B = (\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ prostoru $\mathbb{R}^3$ se standardním skalárním součinem takovou, že matice operátoru f_{A^TA} vzhledem k B a B je diagonální. Matice

$$A^TA = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$$

má vlastní číslo $\lambda_1 = 4$ násobnosti 1 a vlastní číslo $\lambda_2 = \lambda_3 = 1$ násobnosti 2. Singulární hodnoty matice A jsou $\sigma_1 = 2$ a $\sigma_2 = \sigma_3 = 1$. Příslušné prostory vlastních vektorů jsou

$$M_4 = \mathrm{LO}\left\{\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}\right\} , \quad M_1 = \mathrm{LO}\left\{\begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}\right\},$$

V nich najdeme ortonormální báze. V prostoru M_1 je ortonormální báze třeba

$$(\mathbf{v}_2, \mathbf{v}_3) = \left(\frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ 1 \\ -2 \end{pmatrix} \right) ,$$

v prostoru M_4

$$\mathbf{v}_1 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} .$$

Vektory báze $C = (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ vypočteme ze vztahu $\mathbf{u}_i = \sigma_i^{-1} f_A(\mathbf{v}_i)$.

$$\mathbf{u}_1 = 2^{-1} A\mathbf{v}_1 = 2^{-1} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} .$$

$$\mathbf{u}_2 = A\mathbf{v}_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} , \quad \mathbf{u}_3 = A\mathbf{v}_3 = \frac{1}{\sqrt{6}} \begin{pmatrix} 2 \\ -1 \\ -1 \end{pmatrix} ,$$

Vzhledem k ortonormálním bázím B a C je

$$D = [f_A]_C^B = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} .$$

To nám dává rozklad ($U = [\mathrm{id}]_K^C$, $V = ([\mathrm{id}]_K^B)^T$)

$$A = UDV^T = \begin{pmatrix} \frac{1}{\sqrt{3}} & 0 & \frac{2}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} \end{pmatrix} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & -\frac{2}{\sqrt{6}} \end{pmatrix}$$

nebo také následující rozklad na matice hodnosti 1

$$A = 2\mathbf{u}_1\mathbf{v}_1^T + \mathbf{u}_2\mathbf{v}_2^T + \mathbf{u}_3\mathbf{v}_3^T = \frac{1}{3} \begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 2 \\ 2 & 2 & 2 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 0 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & -1 & 0 \end{pmatrix} + \frac{1}{6} \begin{pmatrix} 2 & 2 & -4 \\ -1 & -1 & 2 \\ -1 & -1 & 2 \end{pmatrix}$$

Obrazem jednotkové koule při zobrazení f_A je elipsoid s poloosami $2\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ velikostí $2, 1, 1$. Protože velikosti druhé a třetí poloosy jsou stejné, je tento elipsoid rotačně symetrický podle osy $\mathrm{LO}\{\mathbf{u}_1\}$.

OBRAZEK ▲

Příklad 10.34. Spočítáme singulární rozklad pro reálnou matici

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

Vlastní čísla matice

$$A^T A = \begin{pmatrix} 6 & 12 \\ 12 & 24 \end{pmatrix}$$

jsou 30 a 0, singulární hodnota matice A je tedy $\sigma_1 = \sqrt{30}$. Příslušné normované vlastní vektory jsou

$$\mathbf{v}_1 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \quad \mathbf{v}_2 = \frac{1}{\sqrt{5}} \begin{pmatrix} -2 \\ 1 \end{pmatrix} .$$

Vektor

$$\mathbf{u}_1 = \sigma_1^{-1} A\mathbf{v}_1 = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}$$

doplníme do ortonormální báze $\mathbb{R}^3$ například vektory

$$\mathbf{u}_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}, \quad \mathbf{u}_3 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} .$$

Vzhledem k bázím $B = (\mathbf{v}_1, \mathbf{v}_2)$ a $C = (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ máme

$$[f_A]_C^B = \begin{pmatrix} \sqrt{30} & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} ,$$

což nám dává rozklady $A = \sigma_1 \mathbf{u}_1 \mathbf{v}_1^*$ a

$$A = \begin{pmatrix} \frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{3}} \\ \frac{2}{\sqrt{6}} & 0 & -\frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{3}} \end{pmatrix} \begin{pmatrix} \sqrt{30} & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{5}} & \frac{2}{\sqrt{5}} \\ -\frac{2}{\sqrt{5}} & \frac{1}{\sqrt{5}} \end{pmatrix}$$

Obrazem jednotkového kruhu při zobrazení f_A je úsečka spojující $-\sqrt{30}\mathbf{u}_1$ a $\sqrt{30}\mathbf{u}_1$.

OBRAZEK ▲

10.3.6. Singulární rozklad unitárně diagonalizovatelných matic. Jaká je souvislost unitární nebo ortogonální diagonalizace matic a singulárního rozkladu? Uvažujme normální matici A řádu n a ortonormální bázi $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ prostoru $\mathbb{C}^n$ ($\mathbb{R}^n$) takovou, že $[f_A]_B^B = D' = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$. Vektory v B si uspořádáme tak, aby $\lambda_1, \dots, \lambda_r \neq 0$ a $\lambda_{r+1} = \dots = \lambda_n = 0$.

Jsou-li $\lambda_1, \dots, \lambda_n$ nezáporná reálná čísla, což nastane právě když A je pozitivně semidefinitní, pak máme přímo singulární rozklad, kde $C = B$ a $D = D'$. V obecném případě si nejprve rozmyslíme, jaké jsou singulární hodnoty matice A, a pak nalezneme příslušnou bázi C.

Singulární hodnoty matice A jsou druhé odmocniny nenulových vlastních čísel matice A^*A, které můžeme spočítat jako (nenulová) vlastní čísla matice

$$[f_{A^*A}]_B^B = (D')^* D' = \operatorname{diag}(|\lambda_1|^2, \dots, |\lambda_n|^2) .$$

Proto platí:

Pozorování 10.35. *Singulární hodnoty normální matice jsou rovny absolutním hodnotám jejích nenulových vlastních čísel.*

Proto definujeme

$$D = \operatorname{diag}_{n\times n}(|\lambda_1|, \dots, |\lambda_n|) .$$

Pro $i \leq r$ položíme $\mathbf{u}_i = (\lambda_i/|\lambda_i|)\mathbf{v}_i$. Posloupnost $(\mathbf{u}_1, \dots, \mathbf{u}_r)$ je ortonormální, protože vznikla vynásobením vektorů $\mathbf{v}_1, \dots, \mathbf{v}_r$ komplexními čísly s absolutní hodnotou 1. Tyto vektory doplníme na ortonormální bázi $(\mathbf{u}_1, \dots, \mathbf{u}_n)$. Protože pro $i \leq r$ je $f_A(\mathbf{v}_i) = \lambda_i \mathbf{v}_i = |\lambda_i|\mathbf{u}_i$ a pro $i > r$ je $f_A(\mathbf{v}_i) = \mathbf{o} = \lambda_i \mathbf{u}_i$, platí

$$[f_A]_C^B = D$$

a nalezli jsme singulární rozklad.

Příklad 10.36. Vrátíme se k normální matici z příkladu 10.33. Budeme ji chápat jako komplexní matici a spočítáme její singulární rozklad.

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

V příkladu 10.14 jsme spočítali, že A má vlastní čísla

$$\lambda_1 = 2,\ \lambda_2 = \frac{1}{2} + \frac{\sqrt{3}}{2}i,\ \lambda_3 = \overline{\lambda_2} = \frac{1}{2} - \frac{\sqrt{3}}{2}i ,$$

a ortonormální báze tvořená příslušnými vlastními vektory je $B = (\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$, kde

$$\mathbf{v}_1 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix},\ \mathbf{v}_2 = \frac{1}{\sqrt{3}}\begin{pmatrix} \frac{-1+\sqrt{3}i}{2} \\ \frac{-1-\sqrt{3}i}{2} \\ 1 \end{pmatrix}, \mathbf{v}_3 = \overline{\mathbf{v}_2} = \frac{1}{\sqrt{3}}\begin{pmatrix} \frac{-1-\sqrt{3}i}{2} \\ \frac{-1+\sqrt{3}i}{2} \\ 1 \end{pmatrix}$$

Singulární hodnoty matice A jsou proto

$$\sigma_1 = |\lambda_1| = 2,\ \sigma_2 = |\lambda_2| = 1,\ \sigma_3 = |\lambda_3| = 1$$

a vektory v bázi $C = (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ vypočteme ze vztahu $\mathbf{u}_i = (\lambda_i/\sigma_i)\mathbf{v}_i$.

$$\mathbf{u}_1 = \frac{\lambda_1}{\sigma_1}\mathbf{v}_1 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix},\ \mathbf{u}_2 = \frac{\lambda_2}{\sigma_2}\mathbf{v}_2 = \frac{1}{\sqrt{3}}\begin{pmatrix} -1 \\ \frac{1-\sqrt{3}i}{2} \\ \frac{1+\sqrt{3}i}{2} \end{pmatrix},\ \mathbf{u}_3 = \frac{\lambda_3}{\sigma_3}\mathbf{v}_3 = \frac{1}{\sqrt{3}}\begin{pmatrix} -1 \\ \frac{1+\sqrt{3}i}{2} \\ \frac{1-\sqrt{3}i}{2} \end{pmatrix}.$$

Vyšel nám singulární rozklad komplexní matice A. Tento postup ale nemůžeme použít, chceme-li singulární rozklad A jakožto reálné matice. Ten jsme našli v příkladu 10.33. ▲

10.4. Použití singulárního rozkladu

10.4.1. Spektrální norma. Singulární rozklad matice A nám umožňuje odpovědět na otázku, jaký nejvýše (nejméně) může být podíl $\|A\mathbf{x}\| / \|\mathbf{x}\|$ pro $\mathbf{x} \neq \mathbf{o}$. Jinými slovy, jak nejvíc se může změnit délka vektoru při zobrazení f_A. Pro které vektory se tohoto maxima (minima) nabývá?

Nejprve si všimneme, že

$$\frac{\|A\mathbf{x}\|}{\|\mathbf{x}\|} = \left\| A\left(\frac{\mathbf{x}}{\|\mathbf{x}\|}\right)\right\| \ ,$$

takže se stačí zabývat otázkou, jaká je největší, nebo nejmenší hodnota $\|A\mathbf{x}\|$ pro vektory $\mathbf{x}$ jednotkové velikosti (tj. pro vektory na jednotkové sféře). Geometricky je v případě reálných matic malých typů odpověď patrná z diskuze o obrazu jednotkové koule. Ukážeme algebraické odvození v obecném případě.

Nechť B, C jsou ortonormální báze takové, že $[f]_C^B = \mathrm{diag}_{m\times n}(\sigma_1, \dots, \sigma_r)$, $\sigma_1 \geq \dots \geq \sigma_r > 0$. Označme $[\mathbf{x}]_B = (x_1, \dots, x_n)^T$. Protože $\|\mathbf{x}\| = 1$ a B je ortonormální, je $\|[\mathbf{x}]_B\| = 1$, čili

$$|x_1|^2 + |x_2|^2 + \dots + |x_n|^2 = 1 \ .$$

Norma vektoru $f(\mathbf{x})$ je potom

$$\|f(\mathbf{x})\| = \|[f(\mathbf{x})]_C\| = \left\|(\sigma_1 x_1, \dots, \sigma_r x_r, 0, \dots, 0)^T\right\| = \sqrt{\sigma_1^2|x_1|^2 + \dots + \sigma_r^2|x_r|^2} \ .$$

Protože $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_r > 0$ je tento výraz menší nebo roven

$$\sqrt{\sigma_1^2(|x_1|^2 + \dots + |x_n|^2)} = \sigma_1 \ ,$$

přičemž rovnost nastává právě tehdy, když $|x_i| = 0$ pro každé i takové, že $\sigma_i < \sigma_1$, neboli právě pro vektory $\mathbf{x}$ v lineárním obalu vektorů báze B příslušných singulární hodnotě σ_1, neboli právě pro vlastní vektory matice A^*A příslušné vlastnímu číslu σ_1^2. Odvodili jsme následující tvrzení

Tvrzení 10.37. *Nechť A je komplexní (resp. reálná) matice typu $m \times n$. Pak pro libovolný vektor $\mathbf{o} \neq \mathbf{x} \in \mathbb{C}^n$ (resp. $\mathbf{o} \neq \mathbf{x} \in \mathbb{R}^n$) platí*

$$\frac{\|A\mathbf{x}\|}{\|\mathbf{x}\|} \leq \sigma_1 \ ,$$

kde σ_1 je největší singulární hodnota matice A. Rovnost nastává právě tehdy, když $\mathbf{x}$ je nenulový vlastní vektor matice A^*A příslušný vlastnímu číslu σ_1^2.

Maximu výrazu $\|A\mathbf{x}\| \,/\, \|\mathbf{x}\|$ se také říká *spektrální norma* matice A. Je rovná největší singulární hodnotě. Budeme ji značit resp. $\|A\|$. Podle definice je

$$\|A\mathbf{x}\| \leq \|A\| \, \|\mathbf{x}\| \quad .$$

Obdobné tvrzení lze odvodit pro minima, viz cvičení.

PŘÍKLAD 10.38. Matice

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

z příkladů 10.33, 10.36 má spektrální normu $\|A\| = 2$, tj. pro libovolný vektor $\mathbf{x} \in \mathbb{C}^3$ platí

$$\frac{\|A\mathbf{x}\|}{\|\mathbf{x}\|} \leq 2 \quad .$$

Rovnost nastává právě tehdy, když $\mathbf{o} \neq \mathbf{x} \in M_4 = \mathrm{LO}\{\mathbf{v}_1\} = \mathrm{LO}\left\{(1,1,1)^T\right\}$ (značení přebíráme z příkladu 10.33). ▲

PŘÍKLAD 10.39. Pro matici

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

z příkladu 10.34 platí

$$\frac{\|A\mathbf{x}\|}{\|\mathbf{x}\|} \leq \sqrt{30} \quad .$$

Rovnost nastává pro $\mathbf{o} \neq \mathbf{x} \in \mathrm{LO}\{\mathbf{v}_1\} = \mathrm{LO}\left\{(1,2)^T\right\}$. Spektrální norma matice A je $\|A\| = \sqrt{30}$. ▲

10.4.2. Numerická stabilita řešení soustavy lineárních rovnic s regulární maticí. Uvažujme soustavu $A\mathbf{x} = \mathbf{b}$, kde A je reálná regulární matice, jejíž řešení je, jak víme, $\mathbf{x} = A^{-1}\mathbf{b}$.

Řekněme, že vektor $\mathbf{b}$ získáme měřením, které je zatíženo chybou $\delta\mathbf{b}$ (výraz $\delta\mathbf{b}$ chápejte jako označení vektoru, nikoliv jako součin). Ve skutečnosti tedy neznámé hodnoty $\mathbf{x}$ budou zatížené chybou $\delta\mathbf{x}$, kde

$$A(\mathbf{x} + \delta\mathbf{x}) = \mathbf{b} + \delta\mathbf{b} \ , \ \text{tj. } \delta\mathbf{x} = A^{-1}\delta\mathbf{b} \ .$$

Velikost chyby bude

$$\|\delta\mathbf{x}\| = \left\|A^{-1}\delta\mathbf{b}\right\| \leq \left\|A^{-1}\right\| \|\delta\mathbf{b}\| \quad .$$

(Přičemž rovnost může nastat.) Pokud je spektrální norma $\left\|A^{-1}\right\|$ vysoká, např. 10^6, velikost chyby neznámých hodnot může být až 10^6-krát větší než velikost chyby naměřených hodnot. To je neuspokojivé a je nejspíše potřeba změnit model. Všimněte si, že norma $\left\|A^{-1}\right\|$ je rovná převrácené hodnotě nejmenší singulární hodnoty matice A (cvičení).

V praxi nás spíše bude zajímat odhad na velikost relativní chyby $\|\delta\mathbf{x}\| \,/\, \|\mathbf{x}\|$ neznámých hodnot v závislosti na velikosti relativní chyby $\|\delta\mathbf{b}\| \,/\, \|\mathbf{b}\|$ měření. K tomu si všimneme

$$\|\mathbf{b}\| = \|A\mathbf{x}\| \leq \|A\| \, \|\mathbf{x}\| \quad ,$$

takže

$$\frac{\|\delta\mathbf{x}\|}{\|\mathbf{x}\|} \leq \left\|A^{-1}\right\| \|\delta\mathbf{b}\| \frac{1}{\|\mathbf{x}\|} \leq \left\|A^{-1}\right\| \|\delta\mathbf{b}\| \frac{\|A\|}{\|\mathbf{b}\|} = \|A\| \left\|A^{-1}\right\| \frac{\|\delta\mathbf{b}\|}{\|\mathbf{b}\|} \quad .$$

Číslu $\|A\| \left\|A^{-1}\right\|$ se říká *číslo podmíněnosti matice* A, je rovno podílu největší a nejmenší singulární hodnoty. Relativní chybu řešení lze tedy odhadnout relativní chybou měření krát číslo podmíněnosti.

PŘÍKLAD 10.40. Číslo podmíněnosti matice

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

z příkladu 10.33 je $2/1 = 2$. Relativní chyba řešení soustavy $A\mathbf{x} = \mathbf{b}$ bude tedy nejvýše dvakrát větší než relativní chyba měření pravé strany. ▲

10.4.3. Aproximace maticí nižší hodnosti. Uvažujme komplexní nebo reálnou matici A typu $m \times n$ hodnosti r. Chceme najít matici $\hat{A}$ stejného typu nad stejným tělesem dané hodnosti $s < r$, která co nejlépe aproximuje A ve smyslu, že spektrální norma $\left\|A - \hat{A}\right\|$ je co nejmenší. To se nám může hodit při komprimaci dat nebo při zjednodušování matematických modelů.

Nechť $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$, C jsou ortonormální báze $\mathbb{C}^n$ a $\mathbb{C}^m$ (resp. $\mathbb{R}^n$ a $\mathbb{R}^m$) takové, že $[f_A]_C^B = \operatorname{diag}_{m\times n}(\sigma_1, \dots, \sigma_r)$, kde $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_r > 0$. Ukážeme, že hledaná nejlepší aproximace $\hat{A}$ matice A je určená vztahem

$$[f_{\hat{A}}]_C^B = \operatorname{diag}_{m\times n}(\sigma_1, \dots, \sigma_s) \ .$$

Při této volbě je

$$[f_{A-\hat{A}}]_C^B = \operatorname{diag}_{m\times n}(0, \dots, 0, \sigma_{s+1}, \dots, \sigma_r) \ .$$

To znamená, že největší singulární číslo matice $A - \hat{A}$ je σ_{s+1}, takže

$$\left\|A - \hat{A}\right\| = \sigma_{s+1} \ .$$

Zbývá ukázat, že lepší normy nelze dosáhnout. Předpokládejme, že Q je matice stejného typu jako A nad stejným tělesem, jejíž hodnost je nejvýše s. Protože $\dim \operatorname{LO}\{\mathbf{v}_1, \dots, \mathbf{v}_{s+1}\} = s + 1$ a $\dim \operatorname{Ker} Q = n - \dim \operatorname{Im} Q \geq n - s$, plyne z věty o dimenzi součtu a průniku, že se tyto dva prostory protínají. Uvažujme libovolný nenulový vektor $\mathbf{x}$ v jejich průniku a označme $[\mathbf{x}]_B = (x_1, \dots, x_n)$, tj. $Q\mathbf{x} = \mathbf{o}$ a $x_{s+2} = \dots = x_n = 0$. Pak

$$\begin{aligned}\|A - Q\| &\geq \frac{\|(A-Q)(\mathbf{x})\|}{\|\mathbf{x}\|} = \frac{\|A\mathbf{x}\|}{\|\mathbf{x}\|} = \frac{\|[A\mathbf{x}]_C\|}{\|[\mathbf{x}]_B\|} = \frac{\left\|(\sigma_1 x_1, \dots, \sigma_{s+1} x_{s+1}, 0, \dots, 0)^T\right\|}{\|(x_1, \dots, x_{s+1}, 0, \dots, 0)^T\|} \\ &\geq \frac{\left\|(\sigma_{s+1} x_1, \dots, \sigma_{s+1} x_{s+1}, 0, \dots, 0)^T\right\|}{\|(x_1, \dots, x_{s+1}, 0, \dots, 0)^T\|} = \sigma_{s+1} \ ,\end{aligned}$$

Tedy norma je skutečně alespoň σ_{s+1}.

V maticovém pohledu můžeme výsledek formulovat následujícím způsobem. Je-li singulární rozklad matice A roven

$$A = UDV^* = U \operatorname{diag}_{m\times n}(\sigma_1, \dots, \sigma_r) V^* = \sigma_1 \mathbf{u}_1 \mathbf{v}_1^* + \dots + \sigma_r \mathbf{u}_r \mathbf{v}_r^* \ ,$$

kde $\sigma_1 \geq \dots \geq \sigma_r$, pak nejlepší aproximace $\hat{A}$ matice A maticí hodnosti s je

$$\hat{A} = U \operatorname{diag}_{m\times n}(\sigma_1, \dots, \sigma_s) V^* = \sigma_1 \mathbf{u}_1 \mathbf{v}_1^* + \dots + \sigma_s \mathbf{u}_s \mathbf{v}_s^* \ .$$

K uložení matice A typu $m \times n$ v počítači potřebujeme mn skalárů. K uložení aproximace $\hat{A}$ stačí $s(m+n+1)$ skalárů, protože máme s sčítanců a každý sčítanec obsahuje skalár σ_i, m-složkový vektor $\mathbf{u}_i$ a n-složkový vektor $\mathbf{v}_i$. Toho lze využít pro komprimaci dat.

Příklad 10.41. Nejlepší aproximace matice

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

z příkladu 10.33 maticí hodnosti 1 je

$$\hat{A} = \sigma_1 \mathbf{u}_1 \mathbf{v}_1^* = 2 \ \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \ \frac{1}{\sqrt{3}} (1 \ 1 \ 1) = \frac{2}{3} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \ .$$

Aproximace je nejlepší v tom smyslu, že $\left\|A - \hat{A}\right\| = \sigma_2 = 1$ a pro žádnou matici B hodnosti 1 neplatí $\|A - B\| < 1$.

Aproximovat A maticí hodnosti 2 se nevyplatí, protože norma rozdílu $A - \hat{A}$ by byla také rovna $\sigma_3 = 1$, takže bychom v tomto smyslu nedosáhli žádného zlepšení. ▲

10.4.4. Pseudoinverze. Uvažujme soustavu rovnic $A\mathbf{x} = \mathbf{b}$, kde A je komplexní nebo reálná matice typu $m \times n$. Soustava nemusí mít žádné řešení. V tom případě z tvrzení 8.91 víme, že aproximace řešení metodou nejmenších čtverců jsou právě všechna řešení příslušné soustavy normálních rovnic

$$A^* A\hat{\mathbf{x}} = A^*\mathbf{b} \ .$$

Takových řešení může být více, z tvrzení 8.95 víme, že mezi nimi existuje právě jedno řešení z $\hat{\mathbf{x}}_{ln}$ s nejmenší normou. Je tvaru $\hat{\mathbf{x}}_{ln} = A^* A\mathbf{z}$, kde $\mathbf{z}$ je libovolné řešení soustavy

$$A^* AA^* A\mathbf{z} = A^*\mathbf{b} \ .$$

Pomocí spektrálního rozkladu najdeme vektor $\hat{\mathbf{x}}_{ln}$ jiným způsobem.

Uvažme nejprve speciální případ, kdy $A = D = \mathrm{diag}_{m\times n}(\sigma_1, \dots, \sigma_r)$, kde $\sigma_1, \dots, \sigma_r$ jsou nenulová reálná čísla. Chceme najít řešení soustavy

$$D^* D\mathbf{x} = D^*\mathbf{b} \ ,$$

s nejmenší normou. Označme $\mathbf{x} = (x_1, \dots, x_n)$ a $\mathbf{b} = (b_1, \dots, b_m)$. Pak

$$D^* D\mathbf{x} = \mathrm{diag}_{n\times n}(\overline{\sigma_1}\sigma_1, \dots, \overline{\sigma_r}\sigma_r)(x_1, \dots, x_n)^T = (\overline{\sigma_1}\sigma_1 x_1, \dots, \overline{\sigma_r}\sigma_r x_r, 0, \dots, 0)^T$$

a

$$D^*\mathbf{b} = \mathrm{diag}_{n\times m}(\overline{\sigma_1}, \dots, \overline{\sigma_r})(b_1, \dots, b_m)^T = (\overline{\sigma_1} b_1, \dots, \overline{\sigma_r} b_r, 0, \dots, 0)^T \ .$$

Řešení $\mathbf{x}$ s nejmenší normou bude tedy

$$(x_1, \dots, x_n)^T = (b_1\sigma_1^{-1}, \dots, b_r\sigma_r^{-1}, 0, \dots, 0)^T \ .$$

Označíme-li

$$D^\dagger = \mathrm{diag}_{n\times m}(\sigma_1^{-1}, \dots, \sigma_r^{-1}) \ ,$$

můžeme vztah maticově zapsat

$$\hat{\mathbf{x}}_{ln} = D^\dagger\mathbf{b} \ .$$

Pomocí singulárního rozkladu $A = UDV^*$ teď tento výsledek zobecníme na obecnou matici. Hledáme $\mathbf{x}$ s nejmenší normou, aby

$$\begin{aligned} A^* A\mathbf{x} &= A^*\mathbf{b} \\ VD^*U^*\ UDV^*\mathbf{x} &= VD^*U^*\mathbf{b} \\ VD^*DV^*\mathbf{x} &= VD^*U^*\mathbf{b} \\ D^*DV^*\mathbf{x} &= D^*U^*\mathbf{b} \ . \end{aligned}$$

Protože $\|V^*\mathbf{x}\| = \|\mathbf{x}\|$ (matice V^* je unitární nebo ortogonální), pro hledané $\mathbf{x}$ podle předchozího výsledku platí

$$V^*\hat{\mathbf{x}}_{ln} = D^\dagger U^*\mathbf{b}$$

a vynásobením maticí V zleva získáme

$$\hat{\mathbf{x}}_{ln} = VD^\dagger U^*\mathbf{b}$$

Matice $A^\dagger = VD^\dagger U^*$ je tzv. *Mooreova-Penroseova pseudoinverze* matice A. Při použití zápisu

$$A = \sigma_1\mathbf{u}_1\mathbf{v}_1^* + \dots + \sigma_r\mathbf{u}_r\mathbf{v}_r^*$$

můžeme psát

$$A^\dagger = \sigma_1^{-1}\mathbf{v}_1\mathbf{u}_1^* + \dots + \sigma_r^{-1}\mathbf{v}_r\mathbf{u}_r^* \ .$$

Ukázali jsme, že pro soustavu $A\mathbf{x} = \mathbf{b}$ je vektor $\hat{\mathbf{x}}_{ln} = A^\dagger\mathbf{b}$ nejkratším vektorem, který je zároveň aproximací řešení metodou nejmenších čtverců. Speciálně, pokud $A\mathbf{x} = \mathbf{b}$ má právě jedno řešení, pak je tímto řešením vektor $\mathbf{x} = A^\dagger\mathbf{b}$ (tj. pro regulární matice A je $A^\dagger = A^{-1}$). Má-li soustava $A\mathbf{x} = \mathbf{b}$ více řešení, pak je $\mathbf{x} = A^\dagger\mathbf{b}$ řešením s nejmenší normou.

Příklad 10.42. Uvažujme soustavu

$$A\mathbf{x} = \mathbf{b}, \quad A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \\ 1 & 2 \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix} .$$

Aproximace soustavy metodou nejmenších čtverců jsou řešení soustavy $A^T A\mathbf{x} = A^T\mathbf{b}$:

$$\begin{pmatrix} 6 & 12 \\ 12 & 24 \end{pmatrix} \mathbf{x} = \begin{pmatrix} 6 \\ 12 \end{pmatrix}$$

$$\mathbf{x} \in \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \mathrm{LO}\left\{ \begin{pmatrix} -2 \\ 1 \end{pmatrix} \right\}$$

OBRAZEK

Z obrázku je vidět, že aproximace s nejmenší normou má směr $\mathrm{LO}\left\{(1,2)^T\right\}$ a snadno vypočteme $\mathbf{x} = (1/5, 2/5)^T$.

Toto řešení můžeme vypočítat pomocí pseudoinverze. V příkladu 10.34 jsme nalezli singulární rozklad

$$A = \sigma_1 \mathbf{u}_1 \mathbf{v}_1^* = \sqrt{30} \begin{pmatrix} \frac{1}{\sqrt{6}} \\ \frac{2}{\sqrt{6}} \\ \frac{1}{\sqrt{6}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{5}} & \frac{2}{\sqrt{5}} \end{pmatrix} .$$

Pseudoinverze je

$$A^\dagger = \sigma_1^{-1} \mathbf{v}_1 \mathbf{u}_1^* = \frac{1}{\sqrt{30}} \begin{pmatrix} \frac{1}{\sqrt{5}} \\ \frac{2}{\sqrt{5}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{6}} & \frac{2}{\sqrt{6}} & \frac{1}{\sqrt{6}} \end{pmatrix} = \frac{1}{30} \begin{pmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \end{pmatrix} ,$$

takže hledaná aproximace je

$$\mathbf{x} = A^\dagger \mathbf{b} = \frac{1}{30} \begin{pmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \end{pmatrix} \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix} = \frac{1}{5} \begin{pmatrix} 1 \\ 2 \end{pmatrix} .$$

▲

Shrnutí desáté kapitoly

(1) Komplexní (resp. reálná) čtvercová matice řádu n je *unitárně diagonalizovatelná* (resp. *ortogonálně diagonalizovatelná*), pokud existuje ortonormální báze B prostoru $\mathbb{C}^n$ (resp. $\mathbb{R}^n$) taková, že $[f_A]_B^B$ je diagonální matice.

(2) Dvě čtvercové matice X, Y téhož řádu nad tělesem $\mathbb{C}$ (resp. $\mathbb{R}$) se nazývají *unitárně (resp. ortogonálně) podobné*, pokud existuje unitární (resp. ortogonální) matice U taková, že $Y = U^{-1}XU$ (což je rovno U^*XU, protože U je unitární nebo ortogonální matice).

(3) Nechť A je komplexní (resp. reálná) čtvercová matice řádu n. Pak následující tvrzení jsou ekvivalentní.
   (i) Matice A je unitárně (resp. ortogonálně) diagonalizovatelná.
   (ii) Aritmetický prostor $\mathbb{C}^n$ (resp. $\mathbb{R}^n$) má ortonormální bázi tvořenou vlastními vektory matice A.
   (iii) Matice A je unitárně (resp. ortogonálně) podobná diagonální matici (přičemž na diagonále jsou vlastní čísla matice A, každé tolikrát kolik je jeho algebraická=geometrická násobnost).

(4) Je-li A komplexní (resp. reálná) čtvercová matice řádu n, pak jsou následující tvrzení ekvivalentní.
   (a) Matice A je unitárně (resp. ortogonálně) diagonalizovatelná.
   (b) Matice A
      - má n vlastních čísel včetně algebraických násobností,
      - geometrická násobnost každého vlastního čísla matice A se rovná jeho algebraické násobnosti a
      - pro libovolná dvě různá vlastní čísla λ_i, λ_j matice A platí $M_{\lambda_i} \perp M_{\lambda_j}$.

(5) Je-li A komplexní matice typu $m \times n$ a $\mathbf{x} \in \mathbb{C}^m$, $\mathbf{y} \in \mathbb{C}^n$, pak

$$A^*\mathbf{x} \cdot \mathbf{y} = \mathbf{x} \cdot A\mathbf{y} \ ,$$

(6) Nechť A je komplexní čtvercová matice řádu. Pak $\lambda \in \mathbb{C}$ je vlastní číslo matice A právě tehdy, když je $\overline{\lambda}$ vlastní číslo matice A^*. Speciálně, reálná čtvercová matice A a transponovaná matice A^T mají stejná reálná vlastní čísla.

(7) Komplexní nebo reálná čtvercová matice A se nazývá *normální*, pokud $A^*A = AA^*$ (v reálném případě můžeme psát $A^TA = AA^T$). Příklady komplexních normálních matic jsou unitární matice a hermitovské matice, dále například diagonální matice a antihermitovské matice, tj. matice splňucí $-A^* = A$. Příklady reálných normálních matic zahrnují všechny ortogonální, symetrické, diagonální a antisymetrické matice.

(8) Je-li A normální komplexní matice řádu n, pak
   (i) pro libovolné $t \in \mathbb{C}$ je matice $A - tI_n$ normální,
   (ii) libovolná matice X unitárně podobná A je normální.

(9) Nechť A je normální matice řádu n a $\mathbf{v} \in \mathbb{C}^n$. Pak platí

$$\|A\mathbf{v}\| = \|A^*\mathbf{v}\| \ .$$

(10) Nechť A je normální komplexní matice řádu n, $\lambda \in \mathbb{C}$ a $\mathbf{v} \in \mathbb{C}^n$. Pak $\mathbf{v}$ je vlastní vektor matice A příslušný vlastnímu číslu λ právě tehdy, když je $\mathbf{v}$ vlastní vektor matice A^* příslušný vlastnímu číslu $\overline{\lambda}$.

(11) **Spektrální věta pro normální matice.** Nechť A je čtvercová komplexní matice. Pak následující tvrzení jsou ekvivalentní.
   (a) Matice A je unitárně diagonalizovatelná.
   (b) Matice A je normální.

(12) **Spektrální věta pro hermitovské matice.** Nechť A je komplexní čtvercová matice. Pak následující tvrzení jsou ekvivalentní.
  (a) Matice A je unitárně diagonalizovatelná a všechna její vlastní čísla jsou reálná.
  (b) Matice A je hermitovská.

(13) **Spektrální věta pro symetrické matice.** Nechť A je reálná čtvercová matice. Pak následující tvrzení jsou ekvivalentní.
  (a) Matice A je ortogonálně diagonalizovatelná.
  (b) Matice A je symetrická.

(14) Čtvercová matice A řádu n nad $\mathbb{C}$ (resp. $\mathbb{R}$) se nazývá
  - *pozitivně definitní*, pokud je hermitovská (resp. symetrická) a pro všechna $\mathbf{o} \neq \mathbf{x} \in \mathbb{C}^n$ (resp. $\mathbf{o} \neq \mathbf{x} \in \mathbb{R}^n$) platí $\mathbf{x}^* A\mathbf{x} > 0$;
  - *pozitivně semidefinitní*, pokud je hermitovská (resp. symetrická) a $\mathbf{x}^* A\mathbf{x} \geq 0$.

(15) Nechť A je hermitovská (nebo symetrická) matice řádu n. Pak A je pozitivně definitní (resp. semidefinitní) právě tehdy, když jsou všechna vlastní čísla matice A kladná (resp. nezáporná).

(16) **Spektrální věta pro pozitivně (semi)definitní matice.** Nechť A je komplexní čtvercová matice. Pak následující tvrzení jsou ekvivalentní.
  (a) Matice A je unitárně diagonalizovatelná a všechna její vlastní čísla jsou kladná reálná (resp. nezáporná reálná).
  (b) Matice A je pozitivně definitní (resp. semidefinitní).

(17) Pro libovolnou komplexní matici A typu $m \times n$ je matice A^*A pozitivně semidefinitní. Je-li navíc A čtvercová regulární matice, pak A^*A je pozitivně definitní.

Naopak, každou pozitivně semidefinitní komplexní matici B lze psát ve tvaru $B = A^*A$, kde A je čtvercová matice. V případě, že B je pozitivně definitní, je nutně A regulární.

(18) **Spektrální věta pro unitární matice.** Nechť A je komplexní čtvercová matice. Pak následující tvrzení jsou ekvivalentní.
  (a) Matice A je unitárně diagonalizovatelná a pro všechna vlastní čísla $\lambda \in \mathbb{C}$ platí $|\lambda| = 1$.
  (b) Matice A je unitární.

(19) Každý ortogonální operátor f na $\mathbb{R}^2$ je buď rotace nebo reflexe. Rotace je to právě když $\det[f]_B^B = 1$ a reflexe je to právě když $\det[f]_B^B = -1$, kde B je libovolná báze $\mathbb{R}^2$.

Složení dvou rotací v $\mathbb{R}^2$ je opět rotace, složení dvou reflexí je rotace a složení rotace s reflexí (v libovolném pořadí) je opět nějaká reflexe.

(20) Každé ortogonální zobrazení v euklidovském prostoru $\mathbb{R}^3$ je buď rotace kolem nějaké osy, reflexe vzhledem k nějaké rovině a nebo složení rotace s reflexí. Rotace je to právě tehdy, když determinant matice tohoto zobrazení vzhledem k jakékoliv bázi je rovný 1.

Složení dvou rotací v $\mathbb{R}^3$ je zase rotace v $\mathbb{R}^3$, složení dvou reflexí je rotace (osa rotace je rovná průniku rovin reflexí).

(21) **Věta o singulárním rozkladu.** Nechť A je komplexní (resp. reálná) matice typu $m \times n$ hodnosti r. Pak existují ortonormální báze $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$, $C = (\mathbf{u}_1, \ldots, \mathbf{u}_m)$ prostorů $\mathbb{C}^n$, $\mathbb{C}^m$ (resp. $\mathbb{R}^n$, $\mathbb{R}^m$) takové, že
  (i) (singulární rozklad, geometrická verze) $[f_A]_C^B$ je obdélníková diagonální matice

$$[f_A]_C^B = D = \operatorname{diag}_{m\times n}(\sigma_1, \ldots, \sigma_r) \ , \qquad \text{kde } \sigma_1, \ldots, \sigma_r > 0 \ ,$$

(ii) (singulární rozklad, algebraická verze) platí

$$A = UDV^{-1} = UDV^* \ ,$$

kde U, V jsou unitární (resp. ortogonální) matice

$$U = [\mathrm{id}]^C_{K_m} = (\mathbf{u}_1|\dots|\mathbf{u}_m), \quad V = [\mathrm{id}]^B_{K_n} = (\mathbf{v}_1|\dots|\mathbf{v}_n) \quad \text{a}$$

(iii) (dyadický rozvoj) platí

$$A = \sigma_1 \mathbf{u}_1 \mathbf{v}_1^* + \dots + \sigma_r \mathbf{u}_r \mathbf{v}_r^* \ .$$

Navíc v této situaci

(iv) $\sigma_1, \dots, \sigma_r$ jsou druhé odmocniny vlastních čísel matice A^*A,

(v) pro každé $i \in \{1, \dots, r\}$ je $\mathbf{v}_i$ vlastní vektor matice A^*A příslušný vlastnímu číslu σ_i^2,

(vi) $\operatorname{Ker} A = \mathrm{LO}\{\mathbf{v}_{r+1}, \dots, \mathbf{v}_n\} = \mathrm{LO}\{\mathbf{v}_1, \dots, \mathbf{v}_r\}^\perp$,

(vii) $\operatorname{Im} A = \mathrm{LO}\{\mathbf{u}_1, \dots, \mathbf{u}_r\} = \mathrm{LO}\{\mathbf{u}_{r+1}, \dots, \mathbf{u}_m\}^\perp$.

(22) Nechť A je komplexní nebo reálná matice. Kladné číslo σ nazýváme *singulární hodnota* matice A, pokud σ^2 je vlastní číslo matice A^*A.

(23) Singulární hodnoty normálního operátoru jsou rovny absolutním hodnotám jeho nenulových vlastních čísel.

(24) Nechť A je komplexní (resp. reálná) matice typu $m \times n$. Pak pro libovolný vektor $\mathbf{o} \neq \mathbf{x} \in \mathbb{C}^n$ (resp. $\mathbf{o} \neq \mathbf{x} \in \mathbb{R}^n$) platí

$$\frac{\|A\mathbf{x}\|}{\|\mathbf{x}\|} \leq \sigma_1 \ ,$$

kde σ_1 je největší singulární hodnota matice A. Rovnost nastává právě tehdy, když $\mathbf{x}$ je nenulový vlastní vektor matice A^*A příslušný vlastnímu číslu σ_1^2.

(25) Maximu výrazu $\|A\mathbf{x}\| / \|\mathbf{x}\|$ se říká *spektrální norma* matice A. Je rovná největší singulární hodnotě. Značí se $\|A\|$. Platí

$$\|A\mathbf{x}\| \leq \|A\| \, \|\mathbf{x}\| \ .$$

(26) Máme-li soustavu $A\mathbf{x} = \mathbf{b}$, kde A je reálná regulární matice, jejíž vektor $\mathbf{b}$ je zatíženo chybou $\delta\mathbf{b}$, pak pro velikost chyby $\delta\mathbf{x}$ platí

$$\|\delta\mathbf{x}\| \leq \left\|A^{-1}\right\| \|\delta\mathbf{b}\| \ .$$

a pro velikost relativní chyby platí

$$\frac{\|\delta\mathbf{x}\|}{\|\mathbf{x}\|} = \|A\| \left\|A^{-1}\right\| \frac{\|\delta\mathbf{b}\|}{\|\mathbf{b}\|} \ .$$

Číslu $\|A\| \left\|A^{-1}\right\|$ se říká *číslo podmíněnosti matice* A, je rovno podílu největší a nejmenší singulární hodnoty.

(27) Je-li dyadický rozvoj reálné nebo komplexní matice A hodnosti r

$$A = \sigma_1 \mathbf{u}_1 \mathbf{v}_1^* + \dots + \sigma_r \mathbf{u}_r \mathbf{v}_r^* \ ,$$

kde $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_r$, pak pro $s < r$ je

$$\hat{A} = \sigma_1 \mathbf{u}_1 \mathbf{v}_1^* + \dots + \sigma_s \mathbf{u}_s \mathbf{v}_s^*$$

nejlepší aproximace matice A maticí hodnosti nejvýše s.

(28) Je-li $A = UDV^*$ singulární rozklad komplexní nebo reálné matice A, pak Matice $A^\dagger = VD^\dagger U^*$ je *Mooreova-Penroseova pseudoinverze* matice A.

(29) Pro soustavu $A\mathbf{x} = \mathbf{b}$ je vektor $A^\dagger\mathbf{b}$ nejkratším vektorem, který je zároveň aproximací řešení soustavy $A\mathbf{x} = \mathbf{b}$ metodou nejmenších čtverců.

KAPITOLA 11

Bilineární formy a kvadratické formy

Cíl. *Bilineární formu lze chápat jako zobecnění skalárního součinu. Ponecháme pouze vlastnosti linearity v každé složce a vzdáme se symetrie a pozitivní definitnosti. Taková zobecnění skalárního součinu se používají například ve fyzice, konkrétně ve speciální teorii relativity. Naší hlavní motivací pro studium bilineárních forem je porozumění kvadratickým formám, které určují „kvadratické útvary“. Ukážeme, že kvadratické formy vzájemně jednoznačně odpovídají symetrickým bilineárním formám. Hlavní náplní bude nalezení báze, vzhledem ke které má symetrická bilineární forma, a tím i příslušná kvadratická forma, jednoduchý tvar. To nám umožní analyzovat tvar kvadratických útvarů.*

Bilineární forma je zobrazení přiřazující každé dvojici vektorů prvek tělesa, které je lineární v obou složkách.

Definice 11.1. Nechť $\mathbf{V}$ je vektorový prostor nad tělesem $\mathbf{T}$. *Bilineární forma* na prostoru $\mathbf{V}$ je zobrazení $f : V \times V \to T$, které je lineární v obou složkách, tj. pro libovolné $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w} \in V$, $t \in T$ platí

(1) $f(\mathbf{u}+\mathbf{v},\mathbf{w}) = f(\mathbf{u},\mathbf{w}) + f(\mathbf{v},\mathbf{w})$, $f(\mathbf{w},\mathbf{u}+\mathbf{v}) = f(\mathbf{w},\mathbf{u}) + f(\mathbf{w},\mathbf{v})$ a
(2) $f(t\mathbf{v},\mathbf{w}) = t\,f(\mathbf{v},\mathbf{w})$, $f(\mathbf{v},t\mathbf{w}) = tf(\mathbf{v},\mathbf{w})$.

Příklad 11.2. Bilineární formou na $\mathbb{R}^3$ je například zobrazení

$$\begin{aligned} f((x_1,x_2,x_3)^T,(y_1,y_2,y_3)^T) &= 2x_1y_1 - 3x_1y_2 + 5x_1y_3 + 6x_2y_1 + x_2y_3 + 10x_3y_2 \\ &= (x_1\ x_2\ x_3)\begin{pmatrix} 2 & -3 & 5 \\ 6 & 0 & 1 \\ 0 & 10 & 0 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}. \end{aligned}$$

▲

Příklad 11.3. Obecněji, pro libovolnou čtvercovou matici A řádu n nad $\mathbf{T}$ je zobrazení $T^n \times T^n \to T$ definované vztahem

$$f(\mathbf{x},\mathbf{y}) = \mathbf{x}^T A\mathbf{y}$$

bilineární forma na $\mathbf{T}^n$. Uvidíme, že každá bilineární forma na $\mathbf{T}^n$ je tohoto tvaru.

▲

Příklad 11.4. Libovolný skalární součin na reálném vektorovém prostoru $\mathbf{V}$ je bilineární forma na $\mathbf{V}$ (která je navíc symetrická a pozitivně definitní). Bilineární formy tedy můžeme chápat jako zobecnění skalárního součinu. Axiomy (1) a (2) jsme využili k odvození formulky pro standardní skalární součin.

Obecněji, pro libovolný operátor g na reálném prostoru $\mathbf{V}$ se skalárním součinem $\langle\,,\rangle$ je $f(\mathbf{x},\mathbf{y}) = \langle\,\mathbf{x}, g(\mathbf{y})\rangle$ bilineární forma. Můžeme se na ní dívat jako na skalární součin zdeformovaný v druhé složce operátorem. Pro standardní skalární

součin na $\mathbf{V} = \mathbb{R}^n$ a $g = f_A$ máme $\langle \mathbf{x}, g(\mathbf{y}) \rangle = \mathbf{x} \cdot A\mathbf{y} = \mathbf{x}^T A\mathbf{y}$, což je stejná bilineární forma jako v předchozím příkladu. Vyjádření ve tvaru $\mathbf{x} \cdot A\mathbf{y}$ bylo důležité v předchozí kapitole o unitární diagonalizaci.

Pozor! Skalární součin na komplexním vektorovém prostoru bilineární forma není — vlastnost $f(t\mathbf{u}, \mathbf{v}) = tf(\mathbf{u}, \mathbf{v})$ bychom museli nahradit vlastností $f(t\mathbf{u}, \mathbf{v}) = \bar{t}f(\mathbf{u}, \mathbf{v})$. Takovým formám se říká *seskvilineární* a nebudeme se jimi podrobněji zabývat. ▲

PŘÍKLAD 11.5. Zobrazení $\mathbf{T}^2 \times \mathbf{T}^2 \to \mathbf{T}$ definované vztahem $f(\mathbf{x}, \mathbf{y}) = \det(\mathbf{x}|\mathbf{y})$ je bilineární forma na $\mathbf{T}^2$. Axiomy (1) a (2) byly také základní vlastnosti použité při odvození vzorce pro determinant matic 2×2.

Pro matice vyšších řádů je determinant příkladem tzv. *multilineární* formy, tedy zobrazení $V \times V \times \cdots \times V \to T$ lineární v každé složce. ▲

My využijeme bilineární formy hlavně při studiu kvadratických forem.

DEFINICE 11.6. Je-li f bilineární forma na vektorovém prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$, pak zobrazení $f_2 : V \to T$ definované předpisem

$$f_2(\mathbf{v}) = f(\mathbf{v}, \mathbf{v}) \quad \text{pro každé } \mathbf{v} \in V$$

nazýváme *kvadratickou formou* vytvořenou bilineární formou f.

Rovněž říkáme, že f_2 je kvadratická forma příslušná bilineární formě f.

PŘÍKLAD 11.7. Pro bilineární formu na $\mathbb{R}^3$ z příkladu 11.2 platí

$$\begin{aligned} f_2((x_1, x_2, x_3)^T) &= 2x_1^2 - 3x_1x_2 + 5x_1x_3 + 6x_2x_1 + x_2x_3 + 10x_3x_2 \\ &= 2x_1^2 + 3x_1x_2 + 5x_1x_3 + 11x_2x_3 \ . \end{aligned}$$

Maticově,

$$f_2(\mathbf{x}) = \mathbf{x}^T A\mathbf{x} \ ,$$

kde A je matice řádu 3 ze stejného příkladu. ▲

PŘÍKLAD 11.8. Je-li f skalární součin na reálném vektorovém prostoru $\mathbf{V}$ (tj. $f(\mathbf{x}, \mathbf{y}) = \langle \mathbf{x}, \mathbf{y} \rangle$), pak $f_2(\mathbf{x}) = \|\mathbf{x}\|^2$. ▲

Kvadratické formy se vyskytují při analýze funkcí více proměnných. Například nás zajímá, jak vypadá daná hladká funkce $h : \mathbb{R}^2 \to \mathbb{R}$ v okolí nějakého bodu $\mathbf{d} \in \mathbb{R}^2$, řekněme $\mathbf{d} = (0, 0)^T$. Velmi hrubá aproximace je nahradit funkci její funkční hodnotou $c = h(\mathbf{d})$

$$h(x_1, x_2) \approx c \ .$$

Přesnější je lineární aproximace, kdy nahradíme funkci její tečnou rovinou

$$h(x_1, x_2) \approx c + b_1x_1 + b_2x_2 \ .$$

Nekonstantní část $g(x_1, x_2) = b_1x_1 + b_2x_2$ je lineární forma na $\mathbb{R}^2$, koeficienty b_1, b_2 se vypočtou pomocí parciálních derivací. Ještě přesnější je aproximace polynomem stupně 2:

$$h(x_1, x_2) \approx c + b_1x_1 + b_2x_2 + a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2$$

Kvadratická část $f(x_1, x_2) = a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2$ je kvadratická forma na $\mathbb{R}^2$ (koeficienty se vypočtou z druhých parciálních derivací). Tato aproximace je důležitá například při hledání extrémů.

Proto nás zajímá, jak vypadá graf kvadratické funkce více proměnných. Obecněji nás zajímá, jak vypadá implicitně zadaný kvadratický útvar, například množina bodů v $\mathbb{R}^3$ splňujících rovnici

$$10x_1^2 + 13x_2^2 + 13x_3^2 + 4x_1x_2 + 4x_1x_3 + 8x_2x_3 = 9 \ .$$

Základní myšlenka na řešení takových problémů je stejná jako u lineárních operátorů: najít bázi, vzhledem ke které je bilineární forma přehledná.

11.1. Matice

Podobně jako v úvodu do determinantů spočítáme, že každá bilineární forma je určena obrazy dvojic prvků libovolné báze. To nám dává maticovou reprezentaci bilineárních forem a tzv. analytické vyjádření. Nechť f je bilineární forma na $\mathbf{V}$ a $B = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ je báze prostoru $\mathbf{V}$. Vezmeme dva vektory $\mathbf{x}, \mathbf{y} \in V$ a vyjádříme $f(\mathbf{x}, \mathbf{y})$ pomocí souřadnic vektorů $\mathbf{x}, \mathbf{y}$ v bázi B a pomocí hodnot $a_{ij} = f(\mathbf{v}_i, \mathbf{v}_j)$:

$$[\mathbf{x}]_B = (x_1, x_2, \dots, x_n)^T, \quad [\mathbf{y}]_B = (y_1, y_2, \dots, y_n)^T \ .$$

$$\begin{aligned} f(\mathbf{x}, \mathbf{y}) &= f(x_1\mathbf{v}_1 + \dots + x_n\mathbf{v}_n, y_1\mathbf{v}_1 + \dots + y_n\mathbf{v}_n) = f\left(\sum_{i=1}^n x_i\mathbf{v}_i, \sum_{i=1}^n y_i\mathbf{v}_i\right) \\ &= \sum_{i=1}^n x_i f\left(\mathbf{v}_i, \sum_{j=1}^n y_j\mathbf{v}_j\right) = \sum_{i=1}^n \sum_{j=1}^n x_i y_j f(\mathbf{v}_i, \mathbf{v}_j) \\ &= \sum_{i=1}^n \sum_{j=1}^n x_i y_j a_{ij} \\ &= (x_1\ x_2\ \dots\ x_n) \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & \dots & \dots & \dots \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \end{aligned}$$

To vede k pojmu matice bilineární formy vzhledem k bázi.

Definice 11.9. Nechť $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ je báze vektorového prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ a f je bilineární forma na $\mathbf{V}$. *Maticí bilineární formy f vzhledem k B* rozumíme čtvercovou matici řádu n nad $\mathbf{T}$, která má na pozici (i, j) prvek $f(\mathbf{v}_i, \mathbf{v}_j)$. Tuto matici značíme $[f]_B$.

Tvrzení 11.10. *Je-li B báze konečně generovaného prostoru $\mathbf{V}$, f bilineární forma na $\mathbf{V}$ a $\mathbf{x}, \mathbf{y} \in V$, pak*

$$f(\mathbf{x}, \mathbf{y}) = [\mathbf{x}]_B^T [f]_B [\mathbf{y}]_B \ .$$

Jsou-li souřadnice vektorů $[\mathbf{x}]_B = (x_1, \dots, x_n)^T$, $[\mathbf{y}]_B = (y_1, \dots, y_n)^T$ a $[f]_B = (a_{ij})_{n\times n}$, pak

$$f(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n \sum_{j=1}^n a_{ij} x_i y_j \ .$$

Tomuto vyjádření také říkáme *analytické vyjádření bilineární formy f*.

Naopak, každou bilineární formu na konečně generovaném prostoru můžeme vztahem $f(\mathbf{x}, \mathbf{y}) = [\mathbf{x}]_B^T A [\mathbf{y}]_B$ definovat a matice A je tímto určená jednoznačně:

Tvrzení 11.11. *Nechť $\mathbf{V}$ je konečně generovaný prostor nad tělesem $\mathbf{T}$, $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ je jeho báze a A je čtvercová matice nad $\mathbf{T}$ řádu n. Pak zobrazení $f : V \times V \to T$ definované vztahem*

$$f(\mathbf{x}, \mathbf{y}) = [\mathbf{x}]_B^T A [\mathbf{y}]_B \qquad \textit{pro každé } \mathbf{x}, \mathbf{y} \in V$$

je bilineární forma na $\mathbf{V}$ a platí $[f]_B = A$.

Důkaz. Pro libovolné $\mathbf{u}, \mathbf{v}, \mathbf{w}$ platí

$$\begin{aligned} f(\mathbf{u} + \mathbf{v}, \mathbf{w}) &= [\mathbf{u} + \mathbf{v}]_B^T A [\mathbf{w}]_B = ([\mathbf{u}]_B^T + [\mathbf{v}]_B^T) A [\mathbf{w}]_B = [\mathbf{u}]_B^T A [\mathbf{w}]_B + [\mathbf{v}]_B^T A [\mathbf{w}]_B \\ &= f(\mathbf{u}, \mathbf{w}) + f(\mathbf{v}, \mathbf{w}) \ . \end{aligned}$$

Ostatní axiomy se ověří podobně.

Dosazením $\mathbf{x} = \mathbf{v}_i$ a $\mathbf{y} = \mathbf{v}_j$ získáme

$$f(\mathbf{v}_i, \mathbf{v}_j) = [\mathbf{v}_i]_B^T A [\mathbf{v}_j]_B = \mathbf{e}_i^T A \mathbf{e}_j \ ,$$

což je prvek na místě (i, j) v matici A, takže skutečně $[f]_B = A$. ▲

Při pevně zvolené bázi B tedy takto bilineární formy na $\mathbf{V}$ vzájemně jednoznačně odpovídají čtvercovým maticím nad $\mathbf{T}$ řádu n.

Příklad 11.12. Zobrazení $f : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ definované předpisem

$$f((x_1, x_2)^T, (y_1, y_2)^T) = 2x_1y_1 + 4x_2y_1 = (x_1 \ x_2) \begin{pmatrix} 2 & 0 \\ 4 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

je bilineární forma na $\mathbb{R}^2$. Jeho matice vzhledem ke kanonické bázi je

$$[f]_{K_2} = \begin{pmatrix} 2 & 0 \\ 4 & 0 \end{pmatrix}.$$

Vezmeme jinou bázi $\mathbb{R}^2$, například

$$B = \left(\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix} \right) \ .$$

Matice f vzhledem k B je podle definice

$$[f]_B = \begin{pmatrix} f((1,-1)^T, (1,-1)^T) & f((1,-1)^T, (2,0)^T) \\ f((2,0)^T, (1,-1)^T) & f((2,0)^T, (2,0)^T) \end{pmatrix} = \begin{pmatrix} -2 & -4 \\ 4 & 8 \end{pmatrix} \ ,$$

kde například prvek na místě $(1, 2)$ spočteme

$$f((1,-1)^T, (2,0)^T) = (1,-1) \begin{pmatrix} 2 & 0 \\ 4 & 0 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \end{pmatrix} = (1,-1) \begin{pmatrix} 4 \\ 8 \end{pmatrix} = -4 \ .$$

Matice bilineární formy f vzhledem k B nám umožňuje rychle spočítat $f((x_1, x_2)^T, (y_1, y_2)^T)$ známe-li vyjádření vektorů vzhledem k bázi B:

$$[(x_1, x_2)^T]_B = (x_1', x_2')^T, \quad [(y_1, y_2)^T]_B = (y_1', y_2')^T,$$

$$\begin{aligned} f((x_1, x_2)^T, (y_1, y_2)^T) &= (x_1' \ x_2') \begin{pmatrix} -2 & -4 \\ 4 & 8 \end{pmatrix} \begin{pmatrix} y_1' \\ y_2' \end{pmatrix} \\ &= -2x_1'y_1' - 4x_1'y_2' + 4x_2'y_1' + 8x_2'y_2' \ . \end{aligned}$$

Matici $[f]_B$ spočítáme ještě jedním způsobem, který nám zároveň ukáže, jak se obecně mění matice bilineární formy při přechodu od báze k bázi. Označme X matici přechodu od B ke kanonické bázi K_2.

$$X = [\mathrm{id}]_{K_2}^B = \begin{pmatrix} 1 & 2 \\ -1 & 0 \end{pmatrix}$$

Pro libovolný vektor $\mathbf{z} \in V$ platí $[\mathbf{z}]_{K_2} = X[\mathbf{z}]_B$ a transponováním získáme $[\mathbf{z}]_{K_2}^T = [\mathbf{z}]_B^T X^T$. Pak

$$\begin{aligned} f(\mathbf{x}, \mathbf{y}) &= (x_1 \ x_2) \begin{pmatrix} 2 & 0 \\ 4 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = (x_1', x_2') \begin{pmatrix} 1 & -1 \\ 2 & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 4 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} y_1' \\ y_2' \end{pmatrix} \\ &= (x_1', x_2') \begin{pmatrix} -2 & -4 \\ 4 & 8 \end{pmatrix} \begin{pmatrix} y_1' \\ y_2' \end{pmatrix} \end{aligned}$$

Z jednoznačnosti maticového vyjádření f nyní plyne, že matice f vzhledem k B je stejná jako u předchozího výpočtu. ▲

Zobecněním výpočtu v předchozím příkladu dostáváme vztah o změně matice při přechodu od báze k bázi.

Tvrzení 11.13. *Nechť f je bilineární forma na vektorovém prostoru $\mathbf{V}$, B a C jsou báze $\mathbf{V}$ a $X = [\mathrm{id}]_B^C$ je matice přechodu od C k B. Pak $[f]_C = X^T [f]_B X$.*

Důkaz. Pro libovolné vektory $\mathbf{x}, \mathbf{y} \in V$ platí

$$f(\mathbf{x}, \mathbf{y}) = [\mathbf{x}]_B^T [f]_B [\mathbf{y}]_B = ([\mathrm{id}]_B^C [\mathbf{x}]_C)^T [f]_B ([\mathrm{id}]_B^C [\mathbf{y}]_C) = [\mathbf{x}]_C^T X^T [f]_B X [\mathbf{y}]_C \ .$$

Z jednoznačnosti matice bilineární formy vzhledem k bázi nyní plyne $[f]_C = X^T [f]_B X$. ▲

Čtvercová matice A řádu n má teď pro nás dva geometrické významy: lineární operátor f_A na $\mathbf{T}^n$ a bilineární forma $\mathbf{x}^T A \mathbf{y}$ na $\mathbf{T}^n$. Všimněte si rozdílu při změně báze. Je-li R matice přechodu od B ke kanonické bázi, pak matice příslušného lineárního operátoru vzhledem k B je $R^{-1}AR$, zatímco matice příslušné bilineární formy vzhledem k B je $R^T AR$.

11.2. Symetrické a antisymetrické formy

Kvadratická forma může být vytvořena různými bilineárními formami, například bilineární formy

$$f((x_1, x_2)^T, (y_1, y_2)^T) = 2x_1y_1 + 3x_1y_2 + x_2y_1, \quad g((x_1, x_2)^T, (y_1, y_2)^T) = 2x_1y_1 + 4x_2y_1$$

vytváří stejnou kvadratickou formu

$$f_2((x_1, x_2)^T) = g_2((x_1, x_2)^T) = 2x_1^2 + 4x_1x_2$$

V této části si, v případě těles charakteristiky různé od dva, jednoznačně rozložíme každou bilineární formu na součet symetrické a antisymetrické, a ukážeme, že vytvořená kvadratická forma je určena symetrickou částí.

Definice 11.14. Bilineární forma f na vektorovém prostoru $\mathbf{V}$ se nazývá

- *symetrická*, pokud pro libovolné $\mathbf{x}, \mathbf{y} \in V$ platí $f(\mathbf{x}, \mathbf{y}) = f(\mathbf{y}, \mathbf{x})$;
- *antisymetrická*, pokud pro libovolné $\mathbf{x}, \mathbf{y} \in V$ platí $f(\mathbf{x}, \mathbf{y}) = -f(\mathbf{y}, \mathbf{x})$.

Příkladem symetrické formy je skalární součin na reálném vektorovém prostoru.

Zda je forma symetrická (antisymetrická) poznáme snadno z matice vzhledem k libovolné bázi.

Tvrzení 11.15. *Nechť $\mathbf{V}$ je konečně generovaný vektorový prostor, B je báze $\mathbf{V}$ a f je bilineární forma na $\mathbf{V}$. Pak*

- *f je symetrická právě tehdy, když je $[f]_B$ symetrická matice;*
- *f je antisymetrická právě tehdy, když je $[f]_B$ antisymetrická matice.*

Důkaz. Dokážeme první ekvivalenci, druhá se dokáže podobně. Označme $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$.

Prvek na místě (i, j) v matici $[f]_B$ je podle definice rovný $f(\mathbf{v}_i, \mathbf{v}_j)$. Je-li tedy f symetrická, pak prvek na místě (i, j) je stejný jako prvek na místě (j, i), takže $[f]_B$ je symetrická matice.

Je-li naopak $[f]_B$ symetrická matice, pak pro libovolné vektory $\mathbf{x}, \mathbf{y} \in V$ platí

$$f(\mathbf{x}, \mathbf{y}) = [\mathbf{x}]_B^T [f]_B [\mathbf{y}]_B = [\mathbf{x}]_B^T [f]_B^T [\mathbf{y}]_B = ([\mathbf{x}]_B^T [f]_B^T [\mathbf{y}]_B)^T = [\mathbf{y}]_B^T [f]_B [\mathbf{x}]_B = f(\mathbf{y}, \mathbf{x}) \ ,$$

kde ve třetí rovnosti jsme využili, že $(t)^T = t$ pro libovolný skalár $t \in T$. ▲

Bilineární formy můžeme přirozeným způsobem sčítat a násobit skalárem. Jsou-li f, g dvě bilineární formy na $\mathbf{V}$ a $t \in T$ pak definujeme

$$(f + g)(\mathbf{x}, \mathbf{y}) = f(\mathbf{x}, \mathbf{y}) + g(\mathbf{x}, \mathbf{y}), \quad (tf)(\mathbf{x}, \mathbf{y}) = tf(\mathbf{x}, \mathbf{y}).$$

S těmito operacemi tvoří množina všech bilineárních forem na $\mathbf{V}$ vektorový prostor. Je-li B konečná báze $\mathbf{V}$, snadno se ověří vztahy

$$[f + g]_B = [f]_B + [g]_B, \quad [tf]_B = t[f]_B \ .$$

Zamyslíme se nyní, jak rozložit danou bilineární formu f na prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ na součet symetrické formy f_s a antisymetrické formy f_a. Pro konečně

generované prostory je tento úkol ekvivalentní rozkladu čtvercové matice na součet symetrické a antisymetrické. Pro libovolné dva vektory $\mathbf{x}, \mathbf{y} \in V$ chceme, aby platilo

$$f(\mathbf{x}, \mathbf{y}) = f_s(\mathbf{x}, \mathbf{y}) + f_a(\mathbf{x}, \mathbf{y})$$
$$f(\mathbf{y}, \mathbf{x}) = f_s(\mathbf{y}, \mathbf{x}) + f_a(\mathbf{y}, \mathbf{x}) = f_s(\mathbf{x}, \mathbf{y}) - f_a(\mathbf{x}, \mathbf{y})$$

Dostali jsme pro $f_s(\mathbf{x}, \mathbf{y})$ a $f_a(\mathbf{x}, \mathbf{y})$ soustavu dvou rovnic s řešením

$$f_s(\mathbf{x}, \mathbf{y})) = \frac{1}{2}(f(\mathbf{x}, \mathbf{y}) + f(\mathbf{y}, \mathbf{x})), \quad f_a(\mathbf{x}, \mathbf{y})) = \frac{1}{2}(f(\mathbf{x}, \mathbf{y}) - f(\mathbf{y}, \mathbf{x})) \ .$$

Je snadné nahlédnout, že bilineární forma f_s definovaná tímto předpisem je symetrická a f_a je antisymetrická. Problém je pouze v případě, kdy soustava má singulární matici, tj. v případě, že $1 = -1$, ekvivalentně, charakteristika tělesa $\mathbf{T}$ je 2. V opačném případě z postupu vyplývá, že f_s, f_a jsou určeny jednoznačně. Dokázali jsme tak následující tvrzení.

Tvrzení 11.16. *Nechť $\mathbf{V}$ je vektorový prostor nad tělesem $\mathbf{T}$ charakteristiky různé od 2. Pak každou bilineární formu f na $\mathbf{V}$ lze psát jako součet $f = f_s + f_a$, kde f_s je symetrická a f_a je antisymetrická. Tento rozklad je jednoznačný a platí*

$$f_s(\mathbf{x}, \mathbf{y}) = \frac{1}{2}(f(\mathbf{x}, \mathbf{y}) + f(\mathbf{y}, \mathbf{x})), \quad f_a(\mathbf{x}, \mathbf{y}) = \frac{1}{2}(f(\mathbf{x}, \mathbf{y}) - f(\mathbf{y}, \mathbf{x})) \ .$$

Množina symetrických bilineárních forem na $\mathbf{V}$ i množina antisymetrických bilineárních forem na $\mathbf{V}$ tvoří podprostory prostoru všech bilineárních forem na $\mathbf{V}$ (cvičení). Tvrzení lze formulovat také tak, že vektorový prostor všech bilineárních forem na $\mathbf{V}$ je direktním součtem těchto dvou podprostorů.

Příklad 11.17. Bilineární forma f na $\mathbb{R}^2$

$$f((x_1, x_2)^T, (y_1, y_2)^T) = 2x_1y_1 + 4x_2y_1 + 2x_1y_2 = (x_1 \ x_2) \begin{pmatrix} 2 & 2 \\ 4 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

je součtem

$$f_s((x_1, x_2)^T, (y_1, y_2)^T) = 2x_1y_1 + 3x_2y_1 + 3x_1y_2 = (x_1 \ x_2) \begin{pmatrix} 2 & 3 \\ 3 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

$$f_a((x_1, x_2)^T, (y_1, y_2)^T) = -x_1y_2 + x_2y_1 = (x_1 \ x_2) \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

To odpovídá maticovému vztahu

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

▲

Pro tělesa charakteristiky dva, například $\mathbf{T} = \mathbb{Z}_2$, je teorie bilineárních forem odlišná, ale tímto případem se nebudeme zvlášť zabývat. Poznamenejme jen, že pojmy symetrická a antisymetrická v tomto případě splývají (cvičení).

Bilineární formy využíváme mimo jiné ke studiu příslušných kvadratických forem. Tato kvadratická forma závisí pouze na symetrické části bilineární formy:

Tvrzení 11.18. *Nechť f, g jsou bilineární formy na vektorovém prostoru $\mathbf{V}$ nad tělesem charakteristiky různé od 2. Pak $f_2 = g_2$ právě tehdy, když $f_s = g_s$. Navíc*

$$f_s(\mathbf{x}, \mathbf{y}) = \frac{1}{2}(f_2(\mathbf{x} + \mathbf{y}) - f_2(\mathbf{x}) - f_2(\mathbf{y})) \ .$$

Důkaz. Je-li g antisymetrická forma, pak pro libovolný vektor $\mathbf{x} \in V$ platí $g(\mathbf{x}, \mathbf{x}) = -g(\mathbf{x}, \mathbf{x})$. Pokud je charakteristika tělesa různá od dvou, vyplývá z tohoto vztahu $g_2(\mathbf{x}) = g(\mathbf{x}, \mathbf{x}) = 0$. Pro libovolnou bilineární formu f pak máme

$$f_2(\mathbf{x}) = f(\mathbf{x}, \mathbf{x}) = f_s(\mathbf{x}, \mathbf{x}) + f_a(\mathbf{x}, \mathbf{x}) = f_s(\mathbf{x}, \mathbf{x}) \ .$$

Vytvořená kvadratická forma tedy závisí jen na symetrické části. Odtud plyne implikace zprava doleva.

Vzorec z tvrzení ověříme přímočarým výpočtem.

$$\begin{aligned}\frac{1}{2}(f_2(\mathbf{x}+\mathbf{y})-f_2(\mathbf{x})-f_2(\mathbf{y})) &= \frac{1}{2}(f_s(\mathbf{x}+\mathbf{y},\mathbf{x}+\mathbf{y})-f_s(\mathbf{x},\mathbf{x})-f_s(\mathbf{y},\mathbf{y}))\\ &= \frac{1}{2}(f_s(\mathbf{x},\mathbf{x})+f_s(\mathbf{x},\mathbf{y})+f_s(\mathbf{y},\mathbf{x})+f_s(\mathbf{y},\mathbf{y})-f_s(\mathbf{x},\mathbf{x})-f_s(\mathbf{y},\mathbf{y}))\\ &= \frac{1}{2}(2f_s(\mathbf{x},\mathbf{y})) = f_s(\mathbf{x},\mathbf{y})\end{aligned}$$

Implikace zleva doprava je nyní zřejmá. ▲

Vztah v předchozí větě je varianta polarizační identity z tvrzení 8.31. Dává explicitní vzorec na výpočet hodnoty symetrické bilineární formy pomocí příslušné formy kvadratické. Tuto jednoznačně určenou symetrickou bilineární formu také nazýváme *symetrická forma příslušná dané kvadratické formě.*

Příklad 11.19. Uvažujme kvadratickou formu

$$f_2((x_1,x_2)^T) = 2x_1^2+7x_1x_2+5x_2^2$$

Pro nalezení symetrické formy f_s není třeba používat vzorec z předchozího tvrzení, stačí si uvědomit z jakých členů bilineární formy pochází členy f_2. Je-li

$$f((x_1,x_2)^T,(y_1,y_2)^T) = a_{11}x_1y_1+a_{12}x_1y_2+a_{21}x_2y_1+a_{22}x_2y_2$$

a $f_2((x_1,x_2)^T) = f((x_1,x_2)^T,(x_1,x_2)^T)$, pak koeficient u x_1^2 v kvadratické formě f_2 musí pocházet ze členu $a_{11}x_1y_1$, tedy $a_{11}=2$. Podobně $a_{22}=5$. Koeficient u x_1x_2 vznikne součtem $a_{12}+a_{21}$ a kvůli symetrii je $a_{12}=a_{21}=7/2$. Takže je

$$f_s((x_1,x_2)^T,(y_1,y_2)^T) = 2x_1^2+3{,}5x_1y_2+3{,}5x_2y_1+5x_2y_2 = (x_1\ x_2)\begin{pmatrix}2 & 3{,}5\\ 3{,}5 & 5\end{pmatrix}\begin{pmatrix}y_1\\ y_2\end{pmatrix}.$$

▲

11.3. Ortogonální báze

V celém zbytku kapitoly se budeme věnovat pouze symetrickým formám nad tělesy charakteristiky různé od 2. Budeme se snažit najít bázi vzhledem k níž má daná bilineární forma co nejjednodušší matici, ideálně diagonální. Narozdíl od lineárních operátorů to vždy lze provést.

Symetrické bilineární formy vzájemně jednoznačně odpovídají kvadratickým. Všechny pojmy a výsledky pro symetrické bilineární pojmy budeme proto používat i pro příslušné kvadratické formy.

Co pro bilineární formu f znamená, že matice vzhledem k bázi $B=(\mathbf{v}_1,\mathbf{v}_2,\dots,\mathbf{v}_n)$ je diagonální? Podle definice musí pro dva různé vektory $\mathbf{v}_i$, $\mathbf{v}_j$, $i\neq j$ platit $f(\mathbf{v}_i,\mathbf{v}_j)=0$. To motivuje pojem ortogonality vektorů.

Definice 11.20. Nechť f je symetrická bilineární forma na $\mathbf{V}$ a $\mathbf{x},\mathbf{y}\in V$. Říkáme, že $\mathbf{x}$ a $\mathbf{y}$ jsou *f-ortogonální*, pokud $f(\mathbf{x},\mathbf{y})=0$. Zapisujeme $\mathbf{x}\perp_f\mathbf{y}$.

Báze $B=(\mathbf{v}_1,\dots\mathbf{v}_n)$ prostoru $\mathbf{V}$ se nazývá *f-ortogonální*, pokud je $[f]_B$ diagonální, tj. pro libovolné $i,j\in\{1,2,\dots,n\}$, $i\neq j$, jsou vektory $\mathbf{v}_i,\mathbf{v}_j$ f-ortogonální.

(Pokud je f zřejmé z kontextu, říkáme někdy pouze ortogonální.)

V případě, že f je skalární součin na reálném vektorovém prostoru, se pojmy shodují s již zavedenými. Na hledání ortogonální báze v takovém případě můžeme použít například Gram-Schmidtův ortogonalizační proces. Pro obecnou symetrickou bilineární formu lze zavést obdoby dalších pojmů z kapitoly o skalárním součinu

(jako například ortogonální doplněk), teorie je ale o něco složitější a nebudeme se jí věnovat.

Má-li f vzhledem k B diagonální matici $\mathrm{diag}(a_1, \dots, a_n)$, pak pro příslušnou kvadratickou formu platí

$$f_2(\mathbf{x}) = a_1 x_1^2 + \cdots + a_n x_n^2, \quad [\mathbf{x}]_B = (x_1, \dots, x_n)$$

Z takového vyjádření lépe vidíme, jak daná kvadratická forma vypadá. Na obrázku jsou znázorněny grafy několika kvadratických forem na $\mathbb{R}^2$.

OBRAZEK

11.3.1. Hodnost. Je-li f bilineární forma na konečně generovaném prostoru $\mathbf{V}$ a B, C jsou báze prostoru $\mathbf{V}$, pak podle tvrzení 11.13 platí $[f]_C = X^T [f]_B X$, kde X je matice přechodu od C k B. Protože X je regulární, podle důsledku 5.93 o hodnosti součinu s regulární maticí platí $r([f]_C) = r([f]_B)$. To nám umožňuje zavést hodnost bilineární formy.

Definice 11.21. *Hodností* bilineární formy f na konečně generovaném prostoru $\mathbf{V}$ rozumíme hodnost její matice vzhledem k libovolné bázi, značíme $r(f)$.

Je-li matice symetrické bilineární formy f vzhledem k B diagonální matice $D = [f]_B$, pak hodnost $r(D)$ je rovná počtu nenulových prvků na diagonále. Počet nul tedy nezávisí na volbě f-ortogonální báze.

11.3.2. Metoda symetrických úprav. Předpokládejme, že f je symetrická bilineární forma na vektorovém prostoru $\mathbf{V}$ dimenze n nad tělesem $\mathbf{T}$, C je báze $\mathbf{V}$ a $A = [f]_C$. Vytvoříme matici typu $n \times 2n$ tak, že vedle symetrické matice A napíšeme jednotkovou matici, tj. $(A|I_n)$. S touto maticí provádíme tzv. *symetrické úpravy.* Jedna symetrická úprava sestává z elementární řádkové úpravy a následné „stejné“ úpravy na sloupce. Máme tedy tři typy symetrických úprav:

- prohození i-tého a j-tého řádku, následné prohození i-tého a j-tého sloupce,
- vynásobení i-tého řádku nenulovým prvkem $t \in T$, následné vynásobení i-tého sloupce prvkem t,
- přičtení t-násobku i-tého řádku k j-tému, kde $t \in T$ a $i \neq j$, následné přičtení t-násobku i-tého sloupce k j-tému.

Řádkové úpravy provádíme s celými řádky (vektory z $\mathbf{T}^{2n}$), sloupcové úpravy se vždy týkají jen levého bloku matice.

Odvodíme maticový popis symetrické úpravy matice $(X|Y)$ typu $n \times 2n$. Označíme E matici příslušné řádkové úpravy. Po provedení řádkové úpravy vznikne matice $E(X|Y) = (EX|EY)$. Příslušná sloupcová úprava odpovídá násobení maticí E^T zprava, takže po provedení obou úprav máme matici $(EXE^T|EY)$. Začneme-li tedy s maticí $(A|I_n)$ a provedeme několik symetrických úprav, dostaneme posloupnost matic

$$(A|I_n), (E_1 A E_1^T | E_1), (E_2 E_1 A E_1^T E_2^T | E_2 E_1), \dots, (E_k \dots E_1 A E_1^T \dots E_k^T | E_k \dots E_1) \ .$$

Z maticového popisu je vidět, že sloupcové úpravy příslušné řádkovým úpravám není nutné provádět okamžitě. Můžeme je provést kdykoliv, musíme ale zachovat pořadí. Rovněž si všimněte, že po každém kroku je levý blok symetrická matice.

Označme $F = (E_k \dots E_1)^T$, tj. poslední matice je $(F^T A F | F^T)$. Matice F je regulární, protože je transponovaným součinem elementárních matic. Označme B bázi $\mathbf{V}$ takovou, že $[\mathrm{id}]_C^B = F$, tj. vyjádření vektorů báze B vzhledem k bázi C je ve sloupcích matice F, neboli v řádcích pravého bloku výsledné matice $(F^T A F | F^T)$. Podle tvrzení 11.13 o změně matice bilineární formy při změně báze je matice $F^T A F$ v levém bloku matice $(F^T A F | F^T)$ rovná matici f vzhledem k B.

Tyto úvahy vedou na metodu diagonalizace bilineární formy f. Symetrickými úpravami převedeme matici $(A|I_n)$ do tvaru $(D|G)$, kde D je diagonální. V řádcích matice G pak máme vyjádření vektorů jisté báze B v původní bázi C a platí $[f]_B = D$, tj. speciálně B je f-ortogonální. Jak převod do diagonálního tvaru provádět ukážeme na příkladě.

PŘÍKLAD 11.22. Najdeme f-ortogonální bázi pro bilineární formu f na $\mathbb{Z}_5^3$.

$$[f]_{K_3} = A = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{pmatrix}$$

Upravujeme matici $(A|I_n)$ symetrickými úpravami do tvaru $(D|G)$, kde D je diagonální.

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

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

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

Komentář k úpravám: V prvním kroku potřebujeme na pivotní pozici $(1,1)$ nenulový prvek, docílíme toho přičtením druhého řádku k prvnímu (a následnou symetrickou úpravou – přičtení druhého sloupce k prvnímu). Všimněte si, že prohozením řádků v tomto případě ničeho nedocílíme. Kdybychom například prohodili první a druhý řádek, a následně symetricky první a druhý sloupec, na pozici $(1,1)$ by byla stále nula. Po této úpravě jsme přičetli 2-násobek prvního řádku ke druhému a první řádek ke třetímu, a symetricky se sloupci (tím se pouze vynulují pozice $(1,2)$ a $(1,3)$). Nakonec jsme přičetli 4-násobek druhého řádku ke třetímu, a symetricky se sloupci.

Z diskuze nad příkladem vyplývá, že $B = ((1,1,0)^T, (2,3,0)^T, (4,3,1)^T)$ je f-ortogonální báze a $[f]_B = \mathrm{diag}(2,2,1)$. ▲

VĚTA 11.23. *Každá symetrická bilineární forma f na konečně generovaném vektorovém prostoru nad tělesem charakteristiky různé od 2 má f-ortogonální bázi.*

DŮKAZ. Podle diskuze nad příkladem se zbývá přesvědčit, že každou čtvercovou matici A řádu n nad tělesem $\mathbf{T}$ lze symetrickými úpravami převést na diagonální tvar. Budeme postupně elimovat řádky a sloupce – po provedení i kroků bude mít matice blokově diagonální tvar

$$A' = \begin{pmatrix} D & 0 \\ 0 & X \end{pmatrix} ,$$

kde D je diagonální matice řádu i. Předpokládejme, že jsme již provedli $i-1$ kroků a provedeme i-tý.

Jsou-li všechny prvky v i-tém sloupci nulové (a tím i prvky v i-tém řádku), nemusíme nic dělat.

Je-li pivot, tj. prvek na místě (i,i) v matice A' nulový a nějaký prvek na místě (j,j), $j > i$, nenulový, pak prohodíme i-tý a j-tý řádek a následně i-tý a j-tý sloupec. Tím převedeme matici do tvaru, kdy je prvek na místě (i,i) nenulový.

Jsou-li všechny prvky na místech (j,j), $j \geq i$, nulové a prvek na místě (j,i), $j > i$, nenulový, řekněme $b \in T$, přičteme j-tý řádek k i-tému a následně j-tý

sloupec k i-tému. Tím převedeme matici do tvaru, kdy prvek na místě (i,i) je roven $2b$. Tento prvek není nulový díky tomu, že charakteristika tělesa není 2.

Konečně, je-li prvek na místě (i,i) nenulový, přičteme vhodné násobky i-tého řádku k ostatním řádkům, aby prvky na místech (j,i), $j \neq i$, byly nulové. Příslušné sloupcové úpravy pak pouze vynulují prvky na místech (i,j), $j \neq i$. ▲

11.3.3. Bez nulových pivotů. Jak je vidět z důkazu předchozí věty, při převodu symetrické matice A symetrickými úpravami na diagonální tvar si v řadě případů vystačíme jen s jedním typem symetrických úprav, a to

(*) přičtení t-násobku i-tého řádku k j-tému, kde $t \in T$ a $j > i$ (!) (a následná symetrická sloupcová úprava).

Nastane to v případě, že v každém kroku máme nenulový pivot nebo je celý sloupec (a řádek) nulový. V takovém případě vlastně provádíme Gaussovu eliminaci bez prohazování řádků s tím, že po vyeliminování sloupce vynulujeme také nediagonální hodnoty v příslušném řádku.

Po provedení úprav dostaneme diagonální matici

$$D = E_k \dots E_1 A E_1^T \dots E_k^T$$

složenou z pivotů. Matice E_i řádkové úpravy typu (*) je dolní trojúhelníková s jedničkami na diagonále, součinem takových matic je opět dolní trojúhelníková matice s jedničkami na diagonále a rovněž invertování tuto vlastnost zachovává. To nám dává následující rozklad.

Tvrzení 11.24. *Je-li A symetrická matice taková, že při Gaussově eliminaci nemusíme prohazovat řádky, pak existuje dolní trojúhelníková matice L s jedničkami na diagonále a diagonální matice D (složená z pivotů) tak, že*

$$A = LDL^T \ .$$

Důkaz. Stačí položit $L = (E_k \dots E_1)^{-1}$. Podle diskuze výše je L dolní trojúhelníková s jedničkami na diagonále a platí $D = L^{-1}A(L^{-1})^T$, neboli $LDL^T = A$. ▲

Příklad 11.25. Najdeme rozklad $A = LDL^T$ pro reálnou symetrickou matici

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

Symetrickými úpravami typu (*) převedeme matici $(A|I_3)$ na tvar $(D|G)$.

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

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

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

Nyní platí $D = GAG^T$. Položíme-li

$$L = G^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 2 & -1 & 1 \end{pmatrix} \ ,$$

platí $A = LDL^T$. ▲

Kvadratickou formu lze také diagonalizovat tzv. Langrangovou metodou doplňování na čtverce. Tato metoda úzce souvisí s metodou symetrických úprav. Ukážeme si princip na příkladu kvadratické formy na $\mathbb{R}^3$, jejíž příslušná symetrická bilineární forma má matici $A = (a_{ij})$, tj.

$$f_2(\mathbf{x}) = f_2(x_1, x_2, x_3) = a_{11}x_1^2 + a_{22}x_2^2 + a_{33}x_3^2 + 2a_{12}x_1x_2 + 2a_{13}x_1x_2 + 2a_{23}x_2x_3 \ .$$

Pokud $a_{11} \neq 0$, smíšených členů x_{12}, x_{13} se můžeme zbavit doplněním na čtverec

$$\begin{aligned} f_2(\mathbf{x}) &= a_{11}\left(x_1 + \frac{a_{12}}{a_{11}}x_2 + \frac{a_{13}}{a_{11}}x_3\right)^2 \\ &\quad + \left(a_{22} - \frac{a_{12}^2}{a_{11}}\right)x_2^2 + \left(a_{33} - \frac{a_{13}^2}{a_{11}}\right)x_3^2 + \left(2a_{23} - 2\frac{a_{12}a_{13}}{a_{11}}\right)x_2x_3 \ . \end{aligned}$$

Zvolíme-li novou bázi B tak, aby $[\mathbf{x}]_B = (x_1', x_2', x_3')$, kde

$$x_1' = x_1 + \frac{a_{12}}{a_{11}}x_2 + \frac{a_{13}}{a_{11}}x_3, \quad x_2' = x_2, \quad x_3' = x_3 \ ,$$

pak analytické vyjádření f_2 vzhledem k B je

$$f_2(\mathbf{x}) = a_{11}(x_1')^2 + \left(a_{22} - \frac{a_{12}^2}{a_{11}}\right)(x_2')^2 + \left(a_{33} - \frac{a_{13}^2}{a_{11}}\right)(x_3')^2 + \left(2a_{23} - 2\frac{a_{12}a_{13}}{a_{11}}\right)(x_2')(x_3')$$

a matice příslušné symetrické bilineární formy vzhledem k B je

$$\begin{pmatrix} a_{11} & 0 & 0 \\ 0 & a_{22} - \frac{a_{12}^2}{a_{11}} & a_{23} - \frac{a_{12}a_{13}}{a_{11}} \\ 0 & a_{23} - \frac{a_{12}a_{13}}{a_{11}} & a_{33} - \frac{a_{13}^2}{a_{11}} \end{pmatrix} \ .$$

To je tatáž matice jako po provedení jednoho kroku metodou důkazu věty 11.23. Vyelimování sloupce (a řádku) metodou symetrických úprav můžeme tedy chápat jako maticový zápis doplnění na čtverce. Symetrické úpravy jsou flexibilnější v tom, že máme více možností úprav a snadnou kontrolu změn bází.

11.4. Ortogonální báze nad $\mathbb{R}$

11.4.1. Setrvačnost, signatura. Ortogonální báze ani matice vzhledem k této bázi není určená jednoznačně. Uvažme bilineární formu f na prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ a f-ortogonální bázi $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ prostoru $\mathbf{V}$. Matice $[f]_B$ je diagonální, řekněme $[f]_B = \operatorname{diag}(a_1, \dots, a_n)$. Vynásobíme i-tý vektor báze B prvkem $t_i \in T$. Vzniklá báze $C = (t_1\mathbf{v}_1, \dots, t_n\mathbf{v}_n)$ je stále f-ortogonální (protože $f(t_i\mathbf{v}_i, t_j\mathbf{v}_j) = t_it_jf(\mathbf{v}_i, \mathbf{v}_j) = 0$ pro $i \neq j$) a na diagonále matice $[f]_C$ jsou prvky $f(t_i\mathbf{v}_i, t_i\mathbf{v}_i) = t_i^2 f(\mathbf{v}_i, \mathbf{v}_i) = t_i^2 a_i$, tj. $[f]_C = \operatorname{diag}(a_1t_1^2, \dots, a_nt_n^2)$.

V případě, že $\mathbf{T} = \mathbb{C}$ z provedené úvahy vyplývá, že pro každou bilineární formu na $\mathbf{V}$ můžeme najít bázi takovou, že $[f]_C = \operatorname{diag}(1, 1, \dots, 1, 0, 0, \dots, 0)$, protože zřejmě pro každé nenulové $a_i \in \mathbb{C}$ můžeme najít $t_i \in \mathbb{C}$ tak, že $a_it_i^2 = 1$.

Pro $\mathbf{T} = \mathbb{R}$ můžeme volbou $t_i = \left(\sqrt{|a_i|}\right)^{-1}$ docílit toho, že $[f]_C$ má na diagonále pouze čísla $1, -1, 0$, tj. při vhodném uspořádání bázových vektorů je $[f]_C = \operatorname{diag}(1, 1, \dots, 1, -1, -1, \dots, -1, 0, 0, \dots, 0)$. Počet jedniček je roven počtu kladných prvků na diagonále $[f]_B$, apod. Víme, že počet nenulových prvků nezávisí na volbě báze, je roven hodnosti bilineární formy f. Na první pohled ale není jasné, že počet jedniček a minus jedniček také na volbě báze nezávisí. Věta 11.26, tzv. *zákon setrvačnosti kvadratických forem* říká, že tomu tak skutečně je.

VĚTA 11.26 (Zákon setrvačnosti kvadratických forem). *Nechť f je symetrická bilineární forma na reálném vektorovém prostoru $\mathbf{V}$ dimenze n a C, C' báze $\mathbf{V}$ takové, že*

$$[f]_C = \operatorname{diag}(\underbrace{1, 1, \dots, 1}_{k\times}, \underbrace{-1, -1, \dots, -1}_{l\times}, \underbrace{0, 0, \dots, 0}_{m\times})$$

$$[f]_{C'} = \operatorname{diag}(\underbrace{1, 1, \dots, 1}_{k'\times}, \underbrace{-1, -1, \dots, -1}_{l'\times}, \underbrace{0, 0, \dots, 0}_{m'\times})$$

Pak $k = k', l = l', m = m'$.

Důkaz. Již víme, že $m = m' = n - r(f)$.

Předpokládejme pro spor, že $k > k'$. Označme

$$C = (\mathbf{u}_1, \dots, \mathbf{u}_k, \mathbf{v}_1, \dots, \mathbf{v}_l, \mathbf{w}_1, \dots, \mathbf{w}_m)$$
$$C' = (\mathbf{u}'_1, \dots, \mathbf{u}'_{k'}, \mathbf{v}'_1, \dots, \mathbf{v}'_{l'}, \mathbf{w}'_1, \dots, \mathbf{w}'_{m'})$$

a definujme

$$U = \mathrm{LO}\{\mathbf{u}_1, \dots, \mathbf{u}_k\}, \quad W = \mathrm{LO}\{\mathbf{v}'_1, \dots, \mathbf{v}'_{l'}, \mathbf{w}'_1, \dots, \mathbf{w}'_{m'}\}.$$

Platí $\dim U = k$, $\dim W = l' + m' = n - k'$ a $\dim(U + W) \le n$. Podle věty o dimenzi součtu a průniku je

$$\dim(U \cap W) = \dim U + \dim W - \dim(U + W) \ge k + n - k' - n > 0 \ ,$$

takže průnik $U \cap W$ obsahuje nenulový vektor $\mathbf{x} \in U \cap W$. Protože $\mathbf{x} \in U$, ve vyjádření $[\mathbf{x}]_C = (a_1, \dots, a_k, b_1, \dots, b_l, c_1, \dots, c_m)^T$ máme $b_1 = \dots = b_l = c_1 = \dots = c_m = 0$. Platí tedy

$$\begin{aligned} f_2(x) &= [\mathbf{x}]_C^T [f]_C [\mathbf{x}]_C = 1a_1^2 + \dots + 1a_k^2 + (-1)b_1^2 + \dots + (-1)b_l^2 + 0c_1^2 + \dots + 0c_m^2 \\ &= a_1^2 + \dots + a_k^2 > 0. \end{aligned}$$

(Nerovnost je ostrá, protože $\mathbf{x} \neq 0$, takže alespoň jedno a_i je nenulové.)

Podobně, z $\mathbf{x} \in W$ plyne, že ve vyjádření $[\mathbf{x}]_{C'} = (a'_1, \dots, a'_{k'}, b'_1, \dots, b'_{l'}, c'_1, \dots, c'_{m'})^T$ je $a'_1 = \dots = a'_{k'} = 0$ a proto

$$\begin{aligned} f_2(x) &= 1(a'_1)^2 + \dots 1(a'_{k'})^2 + (-1)(b'_1)^2 + \dots + (-1)(b'_{l'})^2 + 0(c'_1)^2 + \dots + 0(c'_{m'})^2 \\ &= -(b'_1)^2 + \dots - (b'_{l'})^2 \le 0 \ , \end{aligned}$$

spor.

Obdobně se ukáže, že nemůže platit $k < k'$. Dokázali jsme, že $m = m'$ a $k = k'$, tedy také $l = l'$. ▲

Definice 11.27. Nechť f je symetrická bilineární forma na reálném konečně generovaném vektorovém prostoru $\mathbf{V}$. Číslo k (resp. l) z předchozí věty nazýváme *pozitivní (resp. negativní) index setrvačnosti formy* f, značíme $n_+(f)$ (resp. $n_-(f)$). Číslo m nazýváme *nulita* formy f a značíme $n_0(f)$. *Signaturou formy* f rozumíme trojici $(n_0(f), n_+(f), n_-(f))$.

Příklad 11.28. Určíme signaturu bilineární formy f na $\mathbb{R}^3$, jejíž matice vzhledem ke kanonické bázi je

$$A = [f]_K = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \ .$$

Symetrickými úpravami převedeme matici do diagonálního tvaru.

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

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

Vzniklá matice je maticí stejné bilineární formy f vzhledem k nějaké bázi (která nás teď nezajímala). Signatura f je proto $(1, 1, 1)$. ▲

Příklad 11.29. Určíme signaturu kvadratické formy

$$f_2(x_1, x_2) = 4x_1x_2 + x_2^2$$

na prostoru $\mathbb{R}^2$.

Příslušná symetrická bilineární forma má vzhledem ke kanonické bázi matici

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

Symetrickými úpravami získáme

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

(V úpravách jsme tentokrát nepostupovali podle důkazu věty 11.23 – v první úpravě jsme pro pohodlí prohodili první a druhý řádek a následně první a druhý sloupec.) Signatura kvadratické formy f_2 je $(0, 1, 1)$. ▲

11.4.2. Pozitivní definitnost. Má-li bilineární forma nenulový pouze index $n_+(f) = n$, mluvíme o pozitivně definitní formě. Obdobně se zavádí *pozitivně semidefinitní* a *negativně (semi)definitní* bilineární formy, o těch však mluvit nebudeme.

Definice 11.30. Symetrická bilineární forma f na reálném vektorovém prostoru $\mathbf{V}$ je *pozitivně definitní*, pokud $f_2(\mathbf{x}) > 0$ pro libovolný vektor $\mathbf{o} \neq \mathbf{x} \in V$.

Tvrzení 11.31. *Symetrická bilineární forma f na reálném vektorovém prostoru $\mathbf{V}$ dimenze n je pozitivně definitní právě tehdy, když $n_+(f) = n$.*

Důkaz. Je-li B ortogonální báze a $[f]_B = \operatorname{diag}(a_1, \dots, a_n)$, pak pro libovolný vektor $\mathbf{x} \in V$ je $f_2(\mathbf{x}) = f(\mathbf{x}, \mathbf{x})$ rovno

$$f_2(\mathbf{x}) = a_1x_1^2 + \cdots + a_nx_n^2, \text{ kde } [\mathbf{x}]_B = (x_1, \dots, x_n) .$$

Z toho se snadno vidí obě implikace. Je-li $f_2(\mathbf{x}) > 0$ pro libovolné $\mathbf{o} \neq \mathbf{x} \in V$, pak volbou $[\mathbf{x}]_B = \mathbf{e}_i$ získáme $a_i > 0$ pro každé $i \in \{1, \dots, n\}$, čili $n_+(f) = n$. Naopak, pokud $n_+(f) = n$, neboli $a_1, \dots, a_n > 0$, pak je zřejmě $f_2(\mathbf{x}) > 0$ pro libovolný nenulový vektor $\mathbf{x}$. ▲

Pro reálný vektorový prostor $\mathbf{V}$ je pozitivně definitní symetrická bilineární forma totéž jako skalární součin. Vlastnosti (SL1), (SL2) a (SL3) z definice 8.14 skalárního součinu říkají, že skalární součin je symetrická bilineární forma, a vlastnost (SP) je pozitivní definitnost. Názvy se používají podle toho, jak se na bilineární formu díváme.

Pozitivní definitnost je definovaná v souladu se stejným pojmem pro matice ve smyslu, že reálná matice A řádu n je pozitivně definitní ve smyslu definice 10.18 právě tehdy, když je pozitivně definitní bilineární forma $f(\mathbf{x}, \mathbf{y}) = \mathbf{x}^T A\mathbf{y}$ na aritmetickém prostoru $\mathbb{R}^n$. Navíc platí:

Pozorování 11.32. *Symetrická bilineární forma f na reálném konečně generovaném prostoru $\mathbf{V}$ je pozitivně definitní právě tehdy, když je pozitivně definitní její matice vzhledem k libovolné bázi B.*

Důkaz. Vztah $f_2(\mathbf{x}) > 0$ platí právě tehdy, když $[\mathbf{x}]_B^T[f]_B[\mathbf{x}]_B > 0$. Z toho vyplývá, že $f_2(\mathbf{x}) > 0$ pro každý nenulový vektor $\mathbf{x} \in V$ platí právě tehdy, když $\mathbf{y}^T[f]_B\mathbf{y} > 0$ platí pro každý nenulový vektor $\mathbf{y} \in \mathbb{R}^{\dim \mathbf{V}}$. ▲

Z části o unitární diagonalizovatelnosti víme, že pozitivně definitní matice jsou právě ty symetrické matice, jejichž vlastní čísla jsou kladná. Charakterizaci nyní můžeme doplnit o další kriteria. *Hlavním minorem* matice A řádu n rozumíme determinant matice tvořené prvními i řádky a i sloupci matice A pro nějaké $i \in \{1, \dots, n\}$.

VĚTA 11.33. *Nechť A je reálná symetrická matice řádu n. Následující tvrzení jsou ekvivalentní.*

(1) *A je pozitivně definitní.*
(2) *(Sylvestrovo kritérium) Všechny hlavní minory matice A jsou kladné.*
(3) *Gaussova eliminace použitá na matici A může proběhnout bez prohazování řádků a všechny pivoty vyjdou kladné.*
(4) *$A = LDL^T$ pro nějakou dolní trojúhelníkovou matici L s jedničkami na diagonále a nějakou diagonální matici D s kladnými čísly na diagonále.*
(5) *(Choleského rozklad) $A = RR^T$ pro nějakou regulární dolní trojúhelníkovou matici R.*

DŮKAZ. (1) $\Rightarrow$ (2). Nejprve dokážeme, že každá matice A_i tvořená prvními i řádky a i sloupci matice A je pozitivně definitní. Vezmeme libovolný nenulový vektor $\mathbf{y} \in \mathbb{R}^i$ a doplníme jej nulami na vektor $\mathbf{x} \in \mathbb{R}^n$. Protože A je pozitivně definitní, platí $\mathbf{x}^T A\mathbf{x} > 0$. Pak ale

$$\mathbf{y}^T A_i \mathbf{y} = \mathbf{x}^T A\mathbf{x} > 0 \ .$$

Matice A_i je podle důsledku 10.16 ortogonálně diagonalizovatelná, má proto i vlastních čísel $\lambda_1, \dots, \lambda_i$ včetně násobností a podle tvrzení 10.19 jsou všechna vlastní čísla kladná. Charakteristický polynom $p_{A_i}(t) = (\lambda_1 - t) \dots (\lambda_i - t)$ má podle tvrzení 9.32 absolutní člen rovný $\det(A_i)$. Roznásobením výrazu pro $p_{A_i}(t)$ ale také vidíme, že absolutní člen je rovný $\lambda_1 \lambda_2 \dots \lambda_i > 0$, takže $\det(A_i) > 0$.

(2) $\Rightarrow$ (3). Indukcí podle i dokážeme, že před eliminací i-tého sloupce jsou všechny pivoty (prvky na místech $(1,1)$, ..., (i,i)) kladné (speciálně, Gaussova eliminace bude používat pouze úpravy typu přičtení násobku řádku k jinému řádku). Pro $i = 1$ není co dokazovat, předpokládejme, že tvrzení platí pro $i - 1$. Před eliminací i-tého sloupce má matice tvar

$$B = \begin{pmatrix} X & Y \\ 0 & Z \end{pmatrix} \ ,$$

kde X je horní trojúhelníková matice řádu $i - 1$ s kladnými prvky na diagonále. Všechny dosud použité úpravy byly typu přičtení násobku řádku k jinému. Takové úpravy nemění žádný minor, pro i-tou podmatici B_i tvořenou prvními i sloupci a i řádky matice B tedy platí

$$\det(B_i) = x_{11} \dots x_{i-1,i-1} z_{11} = \det(A_i) > 0 \ .$$

Z toho vyplývá, že $z_{11} > 0$, takže pivot před eliminací i-tého sloupce bude skutečně kladný.

Implikace (3) $\Rightarrow$ (4) je důsledkem v tvrzení 11.24.

(4) $\Rightarrow$ (5). Je-li $A = LDL^T$, kde $D = \operatorname{diag}(d_1, \dots, d_n)$, $d_1, \dots, d_n > 0$, pak položíme $R = L\sqrt{D}$, kde $\sqrt{D} = \operatorname{diag}(\sqrt{d_1}, \dots, \sqrt{d_n})$. Matice R je regulární a dolní trojúhelníková, protože je součinem dvou regulárních dolních trojúhelníkových matic, a platí

$$RR^T = (L\sqrt{D})(L\sqrt{D})^T = L\sqrt{D}\sqrt{D}^T L^T = L(\sqrt{D}\sqrt{D})L^T = LDL^T = A \ .$$

(5) $\Rightarrow$ (1). Pro libovolný nenulový vektor $\mathbf{x} \in \mathbb{R}^n$ platí $R^T\mathbf{x} \neq \mathbf{o}$, protože R^T je regulární. Potom

$$\mathbf{x}^T A\mathbf{x} = \mathbf{x}^T RR^T\mathbf{x} = (R^T\mathbf{x})^T R^T\mathbf{x} = \left\| R^T\mathbf{x} \right\|^2 > 0 \ .$$

▲

11.4.3. Ortonormální diagonalizace. Pro geometrické aplikace se hodí najít f-ortogonální bázi symetrické bilineární formy, která je navíc ortonormální vzhledem k nějakému skalárnímu součinu. Takovou bázi můžeme vždy najít (ale nemůžeme vyžadovat, aby koeficienty u kvadratických členů byly z množiny $\{-1, 0, 1\}$).

TVRZENÍ 11.34. *Nechť* $\mathbf{V}$ *je reálný vektorový prostor dimenze* n *se skalárním součinem* $\langle\,,\rangle$ *a* f *je symetrická bilineární forma na* $\mathbf{V}$. *Pak existuje báze* B *prostoru* $\mathbf{V}$, *která je* f*-ortogonální a zároveň ortonormální vzhledem k* $\langle\,,\rangle$.

DŮKAZ. Pro skalární součin $\langle\,,\rangle$ existuje podle věty 8.70 ortonormální báze C prostoru $\mathbf{V}$. Označme $A = [f]_C$. Matice A je symetrická, takže podle spektrální věty pro symetrické matice je ortogonálně diagonalizovatelná. To znamená, že existuje ortonormální báze $(\mathbf{u}_1, \dots, \mathbf{u}_n)$ prostoru $\mathbb{R}^n$ (ortonormalita je zde vzhledem ke standardnímu skalárnímu součinu!) složená z vlastních vektorů matice A. Maticově napsáno, označíme-li $U = (\mathbf{u}_1|\dots|\mathbf{u}_n)$, je U ortogonální matice a $U^{-1}AU = U^TAU = D$ je diagonální. Vezmeme $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$, aby $[\mathbf{v}_i]_C = \mathbf{u}_i$, tj. báze B je zvolená tak, že U je matice přechodu od B k C. Podle tvrzení 11.13 o změně báze je matice f vzhledem k B rovná $U^TAU = D$, takže B je f-ortogonální báze. Protože vyjádření vektorů $\mathbf{v}_1, \dots, \mathbf{v}_n$ v bázi C tvoří ortonormální bázi vzhledem ke standardnímu skalárnímu součinu a C je ortonormální báze vzhledem k $\langle\,,\rangle$, dostáváme, že $\mathbf{v}_1, \dots, \mathbf{v}_n$ tvoří ortonormální bázi vzhledem ke skalárnímu součinu $\langle\,,\rangle$ (viz tvrzení 8.50). ▲

Z tvrzení vyplývá, že jsou-li f, g dvě symetrické bilineární formy na reálném konečně generovaném prostoru $\mathbf{V}$, **z nichž alespoň jedna je pozitivně definitní**, pak existuje báze B, která je zároveň f-ortogonální a g-ortogonální. To obecně neplatí, vynecháme-li zvýrazněný požadavek, že alespoň jedna z forem je pozitivně definitní, viz cvičení.

11.5. Příklady

Podíváme se na aplikace nabytých poznatků na určení tvaru „kvadratického útvaru“.

PŘÍKLAD 11.35. Podíváme se na množinu bodů $(x_1, x_2, x_3)^T \in \mathbb{R}^3$ splňujících $x_3 = -x_1^2 + x_1x_2 - 3x_2^2$. Je to graf kvadratické formy $f_2((x_1, x_2)^T) = -x_1^2 + x_1x_2 - 3x_2^2$. Příslušná symetrická bilineární forma f na $\mathbb{R}^2$ je

$$f((x_1, x_2)^T, (y_1, y_2)^T) = -x_1y_1 + 1/2x_1y_2 + 1/2x_2y_1 - 3x_2y_2$$

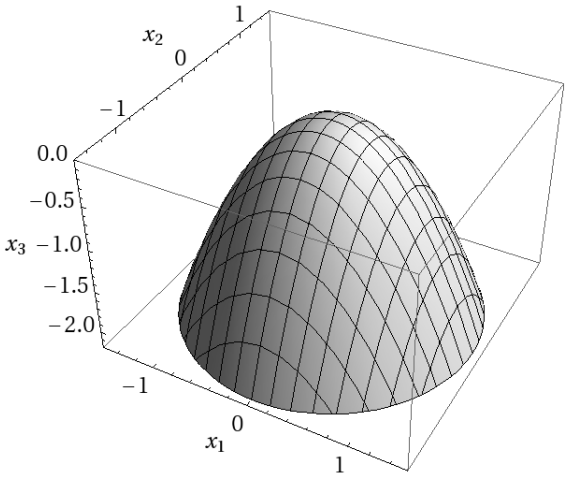
a její matice vzhledem ke kanonické bázi je

$$[f]_{K_2} = A = \begin{pmatrix} -1 & 1/2 \\ 1/2 & -3 \end{pmatrix} \sim \begin{pmatrix} -1 & 0 \\ 0 & -3 + (1/4) \end{pmatrix} .$$

Signatura je tedy $(0, 0, 2)$. Analytické vyjádření f_2 vzhledem k jisté bázi B je proto

$$f_2((x_1, x_2)^T) = -(x_1')^2 - (x_2')^2, \text{ kde } [(x_1, x_2)^T]_B = (x_1', x_2')^T.$$

Grafem $x_3 = -x_1^2 - x_2^2$ je rotační paraboloid otevřený směrem dolů (viz obrázek). Tak vypadá graf vzhledem k bázi B. To nám dává představu, jak vypadá původní útvar – jde o „lineárně zdeformovaný“ rotační paraboloid. Ve skutečnosti je to eliptický paraboloid (ale není to zřejmé).



Abychom přesněji určili tvar útvaru, museli bychom najít f-ortogonální bázi, která je zároveň ortonormální vzhledem ke standardnímu skalárnímu součinu. ▲

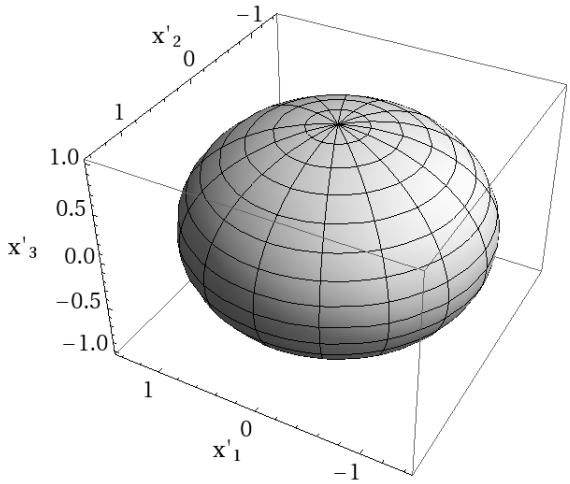
PŘÍKLAD 11.36. Uvažujme množinu bodů $(x_1, x_2, x_3)^T \in \mathbb{R}^3$ splňujících

$$10x_1^2 + 13x_2^2 + 13x_3^2 + 4x_1x_2 + 4x_1x_3 + 8x_2x_3 = 9 \ .$$

Levá strana je kvadratická forma f_2 na $\mathbb{R}^3$. Příslušná symetrická bilineární forma f má matici

$$[f]_{K_3} = A = \begin{pmatrix} 10 & 2 & 2 \\ 2 & 13 & 4 \\ 2 & 4 & 13 \end{pmatrix}$$

Signatura f je $(0, 3, 0)$. Vzhledem k jisté bázi B má tedy útvar rovnici $(x_1')^2 + (x_2')^2 + (x_3')^2 = 9$, takže jde o „lineárně zdeformovanou“ sféru.



OBRAZEK

Ve skutečnosti jde o elipsoid, ale opět to není zřejmé. Abychom určili útvar přesněji, najdeme ortonormální bázi (vzhledem ke standardnímu skalárnímu součinu), která je zároveň f-ortogonální. Jako ortonormální bázi C v tvrzení 11.34 zvolíme kanonickou, tj.

$$[f]_{K_3} = A = \begin{pmatrix} 10 & 2 & 2 \\ 2 & 13 & 4 \\ 2 & 4 & 13 \end{pmatrix}$$

Najdeme ortonormální bázi složenou z vlastních vektorů. Vlastní čísla vyjdou $\lambda_1 = \lambda_2 = 9$ (dvojnásobné) a $\lambda_3 = 18$. V příslušných podprostorech vybereme ortonormální bázi, v M_9 je to např. $(\mathbf{v}_1, \mathbf{v}_2)$ a v M_{18} $(\mathbf{v}_3)$.

$$(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) = \left(\frac{1}{3}\begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix}, \frac{1}{3}\begin{pmatrix} 2 \\ 1 \\ -2 \end{pmatrix}, \frac{1}{3}\begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix} \right)$$

Matice f vzhledem k (ortonormální) bázi $B = (\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ je $[f]_B = \operatorname{diag}(9, 9, 18)$, takže vzhledem k B je rovnice našeho útvaru

$$9(x_1')^2 + 9(x_2')^2 + 18(x_3')^2 = 9$$

a po drobné úpravě

$$\frac{(x_1')^2}{1} + \frac{(x_2')^2}{1} + \frac{(x_3')^2}{\left(\frac{1}{\sqrt{2}}\right)^2} = 1 \ .$$

Vidíme, že jde o elipsoid s poloosami $\mathbf{v}_1, \mathbf{v}_2, \frac{1}{\sqrt{2}}\mathbf{v}_3$, viz obrázek.

OBRAZEK - skutecny (tj. otoceny) elipsoid ▲

Příklad 11.37. Budeme analyzovat následující útvar v $\mathbb{R}^2$:

$$U = \{(x_1, x_2)^T \in \mathbb{R}^2 : 3x_1^2 + 2x_1x_2 + 3x_2^2 - 10x_1 - 14x_2 + 7 = 0\}$$

Výraz z definice je součtem kvadratické formy $f_2((x_1, x_2)^T) = 3x_1^2 + 2x_1x_2 + 3x_2^2$, lineární formy $h((x_1, x_2)^T) = -10x_1 - 14x_2$ a konstanty 7.

Najdeme nejprve ortonormální f-ortogonální bázi $\mathbb{R}^2$, kde f je symetrická bilineární příslušná f_2:

$$[f]_{K_2} = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}$$

Vlastní čísla matice $[f]_{K_2}$ jsou 2 a 4 a příslušné znormované vlastní vektory jsou $\frac{\sqrt{2}}{2}(1, -1)$ a $\frac{\sqrt{2}}{2}(1, 1)$. Hledaná báze B a je tedy

$$B = (\mathbf{v}_1, \mathbf{v}_2) = \left(\frac{\sqrt{2}}{2}\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \frac{\sqrt{2}}{2}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \right) \ .$$

Vyjádříme útvar U v bázi B. Matice f vzhledem k bázi B je $\operatorname{diag}(2, 4)$, matice lineární formy h vzhledem k B je

$$[h]_{K_1}^B = [h]_{K_1}^{K_2}[\mathrm{id}]_{K_2}^B = (-10, -14)\frac{\sqrt{2}}{2}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \sqrt{2}(2, -12) \ ,$$

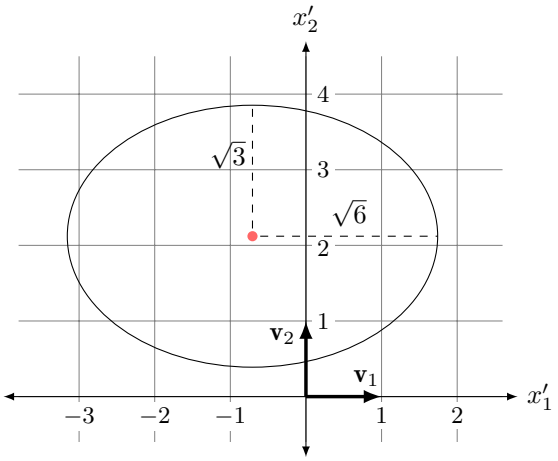
takže U má vzhledem k B vyjádření

$$[U]_B = \{(x_1', x_2')^T \in \mathbb{R}^2 : 2(x_1')^2 + 4(x_2')^2 + 2\sqrt{2}x_1' - 12\sqrt{2}x_2' + 7 = 0\} \ .$$

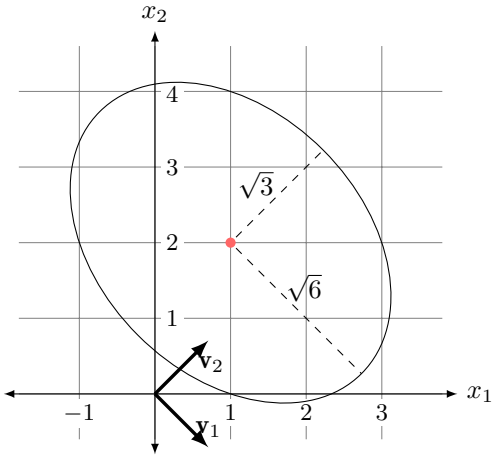
Doplněním na čtverce a drobnými úpravami získáme

$$\begin{aligned}[U]_B &= \left\{ (x_1', x_2')^T \in \mathbb{R}^2 : 2\left(x_1' + \frac{\sqrt{2}}{2}\right)^2 + 4\left(x_2' - \frac{3\sqrt{2}}{2}\right)^2 = 12 \right\} \\ &= \left\{ (x_1', x_2')^T \in \mathbb{R}^2 : \left(\frac{x_1' + \frac{\sqrt{2}}{2}}{\sqrt{6}}\right)^2 + \left(\frac{x_2' - \frac{3\sqrt{2}}{2}}{\sqrt{3}}\right)^2 = 1 \right\}\end{aligned}$$

Z toho vidíme, že vzhledem k B je útvar elipsa se středem $(-\frac{\sqrt{2}}{2}, \frac{3\sqrt{2}}{2})^T$ a velikostmi poloos $\sqrt{6}$ a $\sqrt{3}$.



Přepočteme střed do původních souřadnic: $-\frac{\sqrt{2}}{2}\mathbf{v}_1 + \frac{3\sqrt{2}}{2}\mathbf{v}_2 = (1,2)^T$. Vidíme, že U je elipsa se středem v bodě $(1,2)^T$, hlavní poloosou ve směru LO $\{\mathbf{v}_1\}$ a velikostí $\sqrt{6}$ a vedlejší poloosou ve směru LO $\{\mathbf{v}_2\}$ a velikostí $\sqrt{3}$.



▲

Shrnutí jedenácté kapitoly

(1) Je-li $\mathbf{V}$ lineární prostor nad tělesem $\mathbf{T}$, pak *bilineární forma* na prostoru $\mathbf{V}$ je zobrazení $f : V \times V \to T$, které je lineární v obou složkách, tj. pro libovolné $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w} \in V$ a každý skalár $t \in T$ platí
   (1) $f(\mathbf{u}+\mathbf{v},\mathbf{w}) = f(\mathbf{u},\mathbf{w}) + f(\mathbf{v},\mathbf{w})$, $f(\mathbf{w},\mathbf{u}+\mathbf{v}) = f(\mathbf{w},\mathbf{u}) + f(\mathbf{w},\mathbf{v})$ a
   (2) $f(t\mathbf{v},\mathbf{w}) = t\,f(\mathbf{v},\mathbf{w})$, $f(\mathbf{v},t\mathbf{w}) = tf(\mathbf{v},\mathbf{w})$.

(2) Skalární součin na reálném lineárním prostoru je bilineární forma, skalární součin na komplexním lineárním prostoru není bilineární forma.

(3) Je-li f bilineární forma na lineárním prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$, pak zobrazení $f_2 : V \to T$ definované předpisem

$$f_2(\mathbf{v}) = f(\mathbf{v},\mathbf{v}) \quad \text{pro každé } \mathbf{v} \in V$$

nazýváme *kvadratickou formou* vytvořenou bilineární formou f.

Rovněž říkáme, že f_2 je kvadratická forma příslušná bilineární formě f.

(4) Je-li $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ báze lineárního prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ a f bilineární forma na $\mathbf{V}$, pak *maticí bilineární formy f vzhledem k B* rozumíme čtvercovou matici řádu n nad $\mathbf{T}$, která má na pozici (i,j) prvek $f(\mathbf{v}_i,\mathbf{v}_j)$. Tuto matici značíme $[f]_B$.

(5) Je-li B báze konečně generovaného lineárního prostoru $\mathbf{V}$ a $\mathbf{x},\mathbf{y} \in V$, pak

$$f(\mathbf{x},\mathbf{y}) = [\mathbf{x}]_B^T [f]_B [\mathbf{y}]_B \ .$$

(6) Jsou-li souřadnice vektorů $[\mathbf{x}]_B = (x_1,\dots,x_n)^T$, $[\mathbf{y}]_B = (y_1,\dots,y_n)^T$ a $[f]_B = (a_{ij})_{n\times n}$, pak

$$f(\mathbf{x},\mathbf{y}) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_iy_j \ .$$

Tomuto vyjádření také říkáme *analytické vyjádření bilineární formy f*.

(7) Je-li $\mathbf{V}$ konečně generovaný lineární prostor nad tělesem $\mathbf{T}$, $B = (\mathbf{v}_1,\dots,\mathbf{v}_n)$ jeho báze a A čtvercová matice řádu n nad $\mathbf{T}$, pak zobrazení $f : V\times V \to T$ definované vztahem

$$f(\mathbf{x},\mathbf{y}) = [\mathbf{x}]_B^T A [\mathbf{y}]_B \quad \text{pro každé } \mathbf{x},\mathbf{y} \in V$$

je bilineární forma na $\mathbf{V}$ a platí $[f]_B = A$.

(8) Je-li f bilineární forma na lineárním prostoru $\mathbf{V}$, jsou-li B a C báze $\mathbf{V}$ a $X = [\mathrm{id}]_B^C$ matice přechodu od C k B, pak $[f]_C = X^T[f]_BX$.

(9) Bilineární forma f na lineárním prostoru $\mathbf{V}$ se nazývá
   - *symetrická*, pokud pro libovolné $\mathbf{x},\mathbf{y} \in V$ platí $f(\mathbf{x},\mathbf{y}) = f(\mathbf{y},\mathbf{x})$;
   - *antisymetrická*, pokud pro libovolné $\mathbf{x},\mathbf{y} \in V$ platí $f(\mathbf{x},\mathbf{y}) = -f(\mathbf{y},\mathbf{x})$.

(10) Je-li $\mathbf{V}$ konečně generovaný lineární prostor, B báze $\mathbf{V}$ a f bilineární forma na $\mathbf{V}$, pak
   - f je symetrická právě tehdy, když je $[f]_B$ symetrická matice;
   - f je antisymetrická právě tehdy, když je $[f]_B$ antisymetrická matice.

(11) Je-li $\mathbf{V}$ lineární prostor nad tělesem $\mathbf{T}$ charakteristiky různé od 2, pak každou bilineární formu f na $\mathbf{V}$ lze psát jako součet $f = f_s + f_a$, kde f_s je symetrická a f_a je antisymetrická. Tento rozklad je jednoznačný a platí

$$f_s(\mathbf{x},\mathbf{y}) = \frac{1}{2}(f(\mathbf{x},\mathbf{y}) + f(\mathbf{y},\mathbf{x})), \quad f_a(\mathbf{x},\mathbf{y}) = \frac{1}{2}(f(\mathbf{x},\mathbf{y}) - f(\mathbf{y},\mathbf{x})) \ .$$

(12) Jsou-li f, g bilineární formy na lineárním prostoru $\mathbf{V}$ nad tělesem charakteristiky různé od 2, pak $f_2 = g_2$ právě tehdy, když $f_s = g_s$. Navíc

$$f_s(\mathbf{x}, \mathbf{y}) = \frac{1}{2}(f_2(\mathbf{x} + \mathbf{y}) - f_2(\mathbf{x}) - f_2(\mathbf{y})) \ .$$

(13) Je-li f symetrická bilineární forma na $\mathbf{V}$ a $\mathbf{x}, \mathbf{y} \in V$, pak říkáme, že $\mathbf{x}$ a $\mathbf{y}$ jsou *f-ortogonální*, pokud $f(\mathbf{x}, \mathbf{y}) = 0$. Zapisujeme $\mathbf{x} \perp_f \mathbf{y}$.

Báze $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ prostoru $\mathbf{V}$ se nazývá *f-ortogonální*, pokud je $[f]_B$ diagonální, tj. pro libovolné $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$, jsou vektory $\mathbf{v}_i, \mathbf{v}_j$ f-ortogonální.

(14) *Hodností* bilineární formy f na konečně generovaném lineárním prostoru $\mathbf{V}$ rozumíme hodnost její matice vzhledem k libovolné bázi, značíme $r(f)$.

(15) Každá symetrická bilineární forma f na konečně generovaném vektorovém prostoru nad tělesem charakteristiky různé od 2 má f-ortogonální bázi.

(16) Je-li A symetrická matice taková, že při Gaussově eliminaci nemusíme prohazovat řádky, pak existuje dolní trojúhelníková matice L s jedničkami na diagonále a diagonální matice D (složená z pivotů) tak, že

$$A = LDL^T \ .$$

(17) Je-li f symetrická bilineární forma na reálném lineárním prostoru $\mathbf{V}$ dimenze n a C, C' báze $\mathbf{V}$ takové, že

$$[f]_C = \operatorname{diag}(\underbrace{1, 1, \ldots, 1}_{k\times}, \underbrace{-1, -1, \ldots, -1}_{l\times}, \underbrace{0, 0, \ldots, 0}_{m\times})$$
$$[f]_{C'} = \operatorname{diag}(\underbrace{1, 1, \ldots, 1}_{k'\times}, \underbrace{-1, -1, \ldots, -1}_{l'\times}, \underbrace{0, 0, \ldots, 0}_{m'\times}),$$

pak $k = k', l = l', m = m'$.

(18) Je-li f symetrická bilineární forma na reálném konečně generovaném lineárním prostoru $\mathbf{V}$, pak číslo k (resp. l) z předchozí věty nazýváme *pozitivní (resp. negativní) index setrvačnosti formy* f, značíme $n_+(f)$ (resp. $n_-(f)$). Číslo m je takzvaná *nulita formy* f. *Signaturou formy* f rozumíme trojici $(n_0(f), n_+(f), n_-(f))$.

(19) Symetrická bilineární forma f na reálném lineárním prostoru $\mathbf{V}$ se nazývá *pozitivně definitní*, pokud $f_2(\mathbf{x}) > 0$ pro libovolný nenulový prvek $\mathbf{x} \in V$.

(20) Symetrická bilineární forma f na reálném lineárním prostoru $\mathbf{V}$ dimenze n je pozitivně definitní právě tehdy, když $n_+(f) = n$.

(21) Symetrická bilineární forma f na reálném konečně generovaném prostoru $\mathbf{V}$ je pozitivně definitní právě tehdy, když je pozitivně definitní její matice vzhledem k libovolné bázi B.

(22) Pro reálnou symetrickou matici A řádu n jsou následující podmínky ekvivalentní
   (a) A je pozitivně definitní,
   (b) (Sylvestrovo kritérium) všechny hlavní minory matice A mají kladný determinant,
   (c) Gaussova eliminace použitá na matici A může proběhnout bez prohazování řádků a všechny pivoty vyjdou kladné,
   (d) $A = LDL^T$ pro nějakou dolní trojúhelníkovou matici L s jedničkami na diagonále a nějakou diagonální matici D s kladnými čísly na diagonále,
   (e) (Choleského rozklad) $A = RR^T$ pro nějakou regulární dolní trojúhelníkovou matici R.

(23) Je-li $\mathbf{V}$ reálný vektorový prostor dimenze n se skalárním součinem $\langle\,,\rangle$ a f symetrická bilineární forma na $\mathbf{V}$, pak existuje báze B prostoru $\mathbf{V}$, která je f-ortogonální a zároveň ortonormální vzhledem k $\langle\,,\rangle$.

KAPITOLA 12

Grupy

Cíl. *Seznámíme se s abstraktním pojmem grupy a uvedeme základní příklady grup, které vychází z objektů studovaných v lineární algebře: především tedy grupy permutací a grupy matic. Ukážeme si, jak se grupy používají ke studiu symetrií geometrických objektů.*

12.1. Obecný pojem grupy

12.1.1. Definice a základní příklady. Co má společného množina permutací na množině $\{1, \dots, k\}$, množina regulárních reálných matic rozměru n a množina celých čísel? Na všech je přirozeně definovaná binární operace (skládání, násobení, sčítání), která je asociativní, vůči níž existuje neutrální prvek (identické zobrazení, matice I_n, nula) a také operace invertování (inverzní permutace, inverzní matice, $-a$). Abstrakcí těchto vlastností je motivován pojem grupy.

Definice 12.1. *Grupou* rozumíme množinu G, na které jsou definovány binární operace $*$, unární operace $'$ a konstanta $e \in G$ splňující pro každé $a, b, c \in G$ následující podmínky:

$$a * (b * c) = (a * b) * c, \qquad a * e = e * a = a, \qquad a * a' = a' * a = e.$$

Grupu nazýváme *abelovskou*, pokud navíc pro všechna $a, b \in G$ platí

$$a * b = b * a.$$

Prvku e se říká *jednotka*, prvku a' *inverzní prvek* k prvku a. Grupu formálně zapisujeme jako čtveřici $\mathbf{G} = (G, *, ', e)$.

V konkrétních příkladech bývá typickou trojicí operací buď $+, -, 0$, pak hovoříme o *aditivním zápise* (a místo $x + (-y)$ píšeme $x - y$), anebo trojice $\cdot, ^{-1}, 1$, čemuž říkáme *multiplikativní zápis* (skládání zobrazení se v kontextu grup zpravidla zapisuje multiplikativně).

Hlavní motivací teorie grup je studium nejrůznějších typů symetrií a transformací matematických objektů. Pojem pochází z Galoisovy teorie a původně označoval množinu G (tj. skupinu, grupu) permutací na množině X uzavřenou na skládání, tj. splňující $\pi \circ \sigma \in G$ pro všechna $\pi, \sigma \in G$, typicky šlo o grupy symetrií nějakého objektu. Abstrakcí Galoisova pojmu vznikla rozsáhlá větev algebry, zvaná teorie grup. Aplikace nachází všude, kde se vyskytuje pojem symetrie či transformace.

Projděte si celý kurz lineární algebry a hledejte grupy!

Hned v první kapitole se v principu pracuje s dvěma dobře známými grupami. Reálná čísla s operací sčítání tvoří grupu, $(\mathbb{R}, +, -, 0)$. Nenulová reálná čísla s operací násobení tvoří grupu, $(\mathbb{R} \setminus \{0\}, \cdot, ^{-1}, 1)$. Toto pozorování lze vztáhout na všechna tělesa.

Příklad 12.2 (aditivní a multiplikativní grupa tělesa). Buď $\mathbf{T}$ těleso. Pak

- $(T, +, -, 0)$ je abelovská grupa, tzv. *aditivní grupa* tělesa $\mathbf{T}$,

- $\mathbf{T}^* = (T \setminus \{0\}, \cdot, ^{-1}, 1)$ je abelovská grupa, tzv. *multiplikativní grupa* tělesa $\mathbf{T}$.

Grupové axiomy jsou obsaženy v definici tělesa. ▲

Tělesa jsou vlastně definována pomocí dvou grupových operací navzájem svázaných distributivním zákonem. Definici tělesa bychom mohli přeformulovat takto: množina T s operacemi $+, -, \cdot, ^{-1}$ a prvky $0 \neq 1$ se nazývá těleso, pokud $(T, +, -, 0)$ je abelovská grupa, $(T \setminus \{0\}, \cdot, ^{-1}, 1)$ je abelovská grupa a platí $a(b + c) = ab + ac$ pro všechna $a, b, c \in T$.

Ne všechny abelovské grupy pocházejí z těles. Například $\mathbb{Z}$ ani $\mathbb{Z}_n$ pro n složené netvoří se standardními operacemi těleso, přesto operace sčítání (modulo n) definuje grupu.

Příklad 12.3. Celá čísla tvoří grupu $\mathbb{Z} = (\mathbb{Z}, +, -, 0)$. Čísla v intervalu $0, ..., n-1$ tvoří grupu $\mathbb{Z}_n = (\{0, ..., n-1\}, +, -, 0)$, kde sčítání i odčítání bereme modulo n. ▲

Podobně, definici vektorového prostoru lze formulovat tak, že $(V, +, -, 0)$ je abelovská grupa a dále je definováno násobení skalárem splňující jistá pravidla (související s grupou automorfismů aditivní grupy, ale tenhle pohled si necháme do kurzu obecné algebry).

Ve čtvrté kapitole se definuje sčítání a násobení matic. Matice $n \times n$ nad tělesem $\mathbf{T}$ tvoří grupu vzhledem ke sčítání, ale nikoliv vzhledem k násobení, protože ne každá matice má matici inverzní. Nicméně, pokud se omezíme na regulární matice, grupu vzhledem k násobení dostaneme: Tvrzení 4.88 říká, že součin regulárních matic je regulární a Tvrzení 4.30 říká, že násobení matic je asociativní. Jde o jeden z nejdůležitějších příkladů grup.

Příklad 12.4 (obecná lineární grupa). Buď T těleso. Pak

$$\mathbf{GL}_n(T) = (\{A : \ A \text{ je regulární matice } n \times n \text{ nad tělesem } T\}, \cdot, ^{-1}, I_n)$$

je grupa, tzv. *obecná lineární grupa* nad tělesem T stupně n. ▲

Pozor, vzhledem ke sčítání regulární matice grupu netvoří, protože součet regulárních matic být regulární nemusí.

Skládání zobrazení je asociativní, ale ne každé zobrazení má inverz. Bijektivní zobrazení na dané množině X (neboli permutace na X) ovšem grupu tvoří, jednotkou bude identické zobrazení id. Jde o druhý z nejdůležitějších příkladů grup.

Příklad 12.5 (symetrická grupa). Buď X množina. Pak

$$\mathbf{S}_X = (\{\pi : \ \pi \text{ je permutace na množině } X\}, \circ, ^{-1}, id).$$

je grupa, tzv. *symetrická grupa* na množině X. Je-li $X = \{1, \ldots, n\}$, pak místo $\mathbf{S}_X$ píšeme $\mathbf{S}_n$. ▲

Podobně, lineární operátory na vektorovém prostoru V grupu netvoří (inverzy!), ale ty z nich, které jsou bijektivní, ano. Hovoříme o obecné lineární grupě na prostoru V,

$$\mathbf{GL}(V) = \{f : \ f : V \to V \text{ bijektivní lineární zobrazení } \}, \circ, ^{-1}, id).$$

V definici jsou skryta Tvrzení 6.13 a 6.14, která říkají, že složení lineárních zobrazení jsou lineární, a inverz bijektivní lineárního zobrazení je také lineární. Pro aritmetické prostory jsou prvky $\mathbf{GL}(T^n)$ a $\mathbf{GL}_n(T)$ ve vzájemně jednoznačné korespondenci, a to dokonce tak, že skládání zobrazení odpovídá násobení příslušných matic (viz kapitola 6). Takovým korespondencím se říká *grupové izomorfismy* a detailně se s nimi seznámíme v kurzu obecné algebry.

12.1.2. Podgrupy. Poslední příklad nás navádí na pojem *podgrupy*, analogie pojmu podprostor v kontextu teorie grup. Bijektivní lineární operátory na V jsou vlastně permutace na množině V, jde tedy o jakousi část grupy S_V, dokonce používáme stejné operace skládání a invertování zobrazení (formálně vzato, jde o restrikci operace skládání na podmnožinu lineárních operátorů).

Definice 12.6. Buď $\mathbf{G} = (G, *, ', e)$ grupa a $H \subseteq G$ podmnožina splňující

- $e \in H$,
- pro každé $a \in H$ je $a' \in H$,
- pro každé $a, b \in H$ je $a * b \in H$.

Říkáme, že H je *uzavřena na grupové operace* a že *tvoří podgrupu* grupy $\mathbf{G}$. Čtveřici $\mathbf{H} = (H, *|_H, '|_H, e)$ pak nazýváme *podgrupou*, přičemž $|_H$ značí restrikci operací na množinu H. Značíme $\leq \mathbf{G}$.

Všimněte si, že podgrupa grupy $\mathbf{G}$ je opět grupa: axiomy platné pro všechny prvky G budou jistě splněny i na podmnožině H.

Příklad 12.7. Sudá čísla tvoří podgrupu grupy $\mathbb{Z}$:

- 0 je sudá,
- pro každé a sudé platí, že $-a$ je sudé,
- součet sudých čísel je sudý.

Naopak podgrupu netvoří například lichá čísla (0 není lichá), nezáporná čísla (je-li $a > 0$, pak $-a < 0$) ani množina $H = \{a : 2 \mid a \text{ nebo } 3 \mid a\}$, protože $2 + 3 = 5 \notin H$. ▲

Příklad 12.8. Buď V vektorový prostor. Pak $\mathbf{GL}(V)$ je podgrupou $\mathbf{S}_V$, neboť

- *id* je lineární zobrazení,
- inverz bijektivního lineárního zobrazení je lineární,
- složení lineárních zobrazení je lineární.

▲

Příklad 12.9. Sudé permutace tvoří podgrupu grupy $\mathbf{S}_n$, neboť podle Tvrzení 7.11

- *id* je sudá,
- inverz sudé permutace je sudý,
- složení sudých permutací je sudá permutace.

Tato grupa se nazývá *alternující* a značí se $\mathbf{A}_n$. ▲

Řada maticových pojmů definuje zajimavé podgrupy obecné lineární grupy.

Příklad 12.10. Matice s determinantem 1 tvoří podgrupu grupy $\mathbf{GL}_n(T)$, neboť podle Vět 7.26 a 7.27

- $\det I_n = 1$,
- je-li $\det A = 1$, pak $\det A^{-1} = (\det A)^{-1} = 1$,
- je-li $\det A = \det B = 1$, pak $\det AB = \det A \det B = 1$.

Tato grupa se nazývá *speciální lineární grupa* a značí se $\mathbf{SL}_n(T)$. ▲

Příklad 12.11. Ortogonální matice tvoří podgrupu grupy $\mathbf{GL}_n(\mathbb{R})$, neboť

- I_n je ortogonální,
- inverz ortogonální matice A je ortogonální matice A^T,
- součin ortogonálních matic je ortogonální (Důsledek 8.83).

Tato grupa se nazývá *ortogonální grupa* a značí se $\mathbf{O}_n$. Analogicky se definují *unitární grupy* $\mathbf{U}_n \leq \mathbf{GL}_n(\mathbb{C})$. ▲

Tvrzení 12.12. *Průnik podgrup je podgrupa.*

Důkaz. Buď $\mathbf{G} = (G, *, ', e)$ grupa, uvažujme podgrupy i, $i \in I$, a označme $H = \bigcap_{i \in I} H_i$. Pak

- $e \in H_i$ pro všechna i, a tedy $e \in \bigcap H_i$,
- pokud $a \in \bigcap H_i$, pak $a \in H_i$ pro všechna i, tedy také $a' \in H_i$ pro všechna i, a tedy $a' \in \bigcap H_i$,
- pokud $a, b \in \bigcap H_i$, pak $a, b \in H_i$ pro všechna i, tedy také $a * b \in H_i$ pro všechna i, a tedy $a * b \in \bigcap H_i$.

▲

Příklad 12.13. Ortogonální matice s determinantem 1 tvoří podgrupu grupy $\mathbf{GL}_n(\mathbb{R})$, protože jsou průnikem podgrup $\mathbf{SL}_n(\mathbb{R})$ a $\mathbf{O}_n$. Této grupě se říká speciální ortogonální grupa a značí se $\mathbf{SO}_n$. Podle Tvrzení 10.26 lze grupu $\mathbf{SO}_3$ ztotožnit s rotacemi v $\mathbb{R}^3$. ▲

12.1.3. Kvaternionová grupa. Posledním příkladem, který uvedeme, je kvaternionová grupa, která se poněkud vymyká předchozím příkladům.

Příklad 12.14. *Kvaternionová grupa* $\mathbf{Q}_8$ je definovaná na množině $\{\pm 1, \pm i, \pm j, \pm k\}$. Násobení je dáno vzorci

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

a dále pravidly $xy = -(yx)$ a $(-x)y = x(-y) = -(xy)$ pro všechna $x, y \in \{i, j, k\}$. ▲

Pomocí kvaternionové grupy se definuje nekomutativní těleso kvaternionů jako těleso všech výrazů $a + bi + cj + dk$, $a, b, c, d \in \mathbb{R}$. Podobnou konstrukci lze provést v principu pro jakoukoliv grupu, ale těleso kvaternionů se vymyká tím, že jeho multiplikativní grupa úzce souvisí s grupou rotací $\mathbf{SO}_3$. O tom se dočtete více v sekci 3.5.5, jejímž hlavním sdělením je, že rotaci o úhel α kolem osy dané vektorem $(a, b, c)^T$ lze reprezentovat kvaternionem

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

přičemž rotace se skládají tak, jak se příslušné kvaterniony násobí (ejhle, izomorfismus grup). Více se dozvíte v kurzu geometrie v druhém ročníku.

12.2. Grupy symetrií geometrických objektů

Jedním z hlavních využití teorie grup je popis symetrií nejrůznějších matematických obejktů. Metodu si ilustrujeme na geometrických objektech v rovině či prostoru (čtverec, krychle, ...), přičemž za symetrie budeme uvažovat ortogonální zobrazení, tj. lineární zobrazení zachovávající délky a úhly (tzv. izometrie) a počátek souřadnic. Jinými slovy, budeme uvažovat podgrupy ortogonální grupy $\mathbf{O}_n$, kterou budeme ztotožňovat z grupou ortogonálních zobrazení na $\mathbb{R}^n$.

Pro podmnožinu $X \subseteq \mathbb{R}^n$ uvažujte množinu

$$\{f : \mathbb{R}^n \to \mathbb{R}^n \text{ ortogonální} : f(X) = X\}.$$

Všimněte si, že jde o podgrupu grupy $\mathbf{O}_n$: indetita zachovává jakoukoliv množinu, a pokud $f(X) = g(X) = X$, pak také $(gf)(X) = X$ a $f^{-1}(X) = X$. Mluvíme o *grupě symetrií* množiny X.

Příklad 12.15. Uvažujme kouli v $\mathbb{R}^n$ se středem v počátku. Její grupa symetrií sestává ze všech ortogonálních zobrazení. ▲

Příklad 12.16. Uvažujme přímku v $\mathbb{R}^2$ procházející počátkem. Její grupa symetrií sestává z identity, rotace o 180 stupňů a dvou reflexí podle os daných směrovým a normálovým vektorem. Více symetrií přímka nemá, neboť směrový i normálový vektor se musí zobrazit buď na sebe sama, nebo na vektor opačný, jsou tedy nejvýše čtyři možnosti. ▲

Nakreslete si spoustu obrázků v rovině (bod, trojúhelník, čtverec, hvězdička, sluníčko, domeček, prasátko) a určete grupy symetrií!

PŘÍKLAD 12.17. Uvažujme pravidelný n-úhelník v $\mathbb{R}^2$ se středem v počátku. Jeho grupa symetrií sestává z n rotací (o úhel $k \cdot 2\pi/n$, kde $k = 0, ..., n-1$) a n reflexí (podle os spojujících protilehlé vrcholy, resp. středy hran) a říká se jí *dihedrální grupa*. (Striktně vzato, dihedrální grupa není jednoznačně určena, záleží na „natočení" obrazce. Volbou vhodné ortonormální báze můžeme bez újmy na obecnosti předpokládat, že jedna z reflexí je například podle osy x.) ▲

PŘÍKLAD 12.18. Uvažujme hákovou hvězdu s n-rameny v $\mathbb{R}^2$ se středem v počátku. TODO: OBRAZEK (pro $n = 4$ jde o klasický hákový kříž). Její grupa symetrií sestává z n rotací (o úhel $k \cdot 2\pi/n$, kde $k = 0, ..., n-1$), budeme ji značit $\mathbf{R}_n$. ▲

Pokud jste zkoumali dostatek obrázků, kromě zmíněných grup vám nejspíš vyšla také jednorpvková grupa (asymetrické obrázky) či dvouprvková grupa sestávající z identity a jedné reflexe (například postava člověka). Umíte namalovat obrázek v rovině, který má konečný počet symetrií, ale jeho grupa symetrií je jiná než výše zmíněné triviální grupy, dihedrální grupy a grupy $\mathbf{R}_n$? Leonardo da Vinci to také neuměl a všiml si faktu, který lze v moderním jazyce zformulovat jako následující tvrzení.

TVRZENÍ 12.19. *Buď* $\mathbf{G}$ *konečná podgrupa* $\mathbf{O}_2$ *s alespoň třemi prvky. Pak* $\mathbf{G} = \mathbf{R}_n$ *pro nějaké* n*, nebo je* $\mathbf{G}$ *dihedrální.*

IDEA DŮKAZU. Uvažme podgrupu $\mathbf{R} = \mathbf{G} \cap \mathbf{SO}_2$, tj. podgrupu těch prvků $\mathbf{G}$, které jsou rotací.

Je-li $\mathbf{R} = \{id\}$, pak $|\mathbf{G}| \leq 2$, neboť složením různých reflexí bychom dostali netriviální rotaci. Ve zbytku důkazu budeme předpokádat, že je $\mathbf{R}$ netriviální.

Složením rotací o úhly α a β dostaneme rotaci o úhel $\alpha + \beta$. Protože je $\mathbf{R}$ konečná, nutně musí být úhel libovolné rotace r z $\mathbf{R}$ racionálním násobkem 2π, jinak by $r, r^2, r^3, \ldots$ byly po dvou různé rotace. Není těžké dokázat (ale ani to není očividné), že musí existovat $n \in \mathbb{N}$ takové, že $\mathbf{R}$ sestává z rotací o úhel $k \cdot 2\pi/n$, kde $k = 0, ..., n-1$, tedy $\mathbf{R} = \mathbf{R}_n$.

Pokud je $\mathbf{G} = \mathbf{R}$, jsme hotovi. V opačném případě si všimněte, že počet rotací a reflexí v $\mathbf{G}$ je stejný, neboť $r \mapsto sr$ je bijekcí mezi množinami R a $G \setminus R$ (dokažte!). Složení dvou reflexí je rotace o úhel daný dvojnásobkem úhlu, který svírají jejich osy. Z toho plyne, že osy reflexí z $\mathbf{G}$ mohou svírat pouze úhly $k \cdot \pi/n$, kde $k = 0, ..., n-1$, a protože jich má být n, musí tam být všechny, a to přesně v konfiguraci os symetrie pravidelného n-úhelníka. ▲

Analogické tvrzení platí i v dimenzi 3, ale výjimečných grup je více: kromě dvouprvkových grup určených reflexí jsou to ještě grupy symetrií platónských těles.

Cvičení

1. Rozhodněte, zda existuje unární operace $'$ a prvek e tak, aby následující čtveřice byla grupou:

(a) $(\mathbb{Z}, -, ', e)$
(b) $(\mathbb{Q}, *, ', e)$ kde $a * b = |a \cdot b|$.
(c) $(P(X), \cap, ', e)$, kde $P(X)$ značí množinu všech podmnožin množiny X
(d) $(P(X), *, ', e)$, kde $*$ značí symetrickou diferenci, tj. $A * B = (A \cup B) \setminus (A \cap B)$.

[ne, ne, ne, ano]

2. Určete, v kterých z následujících grup tvoří sudá čísla podgrupu: $\mathbb{Z}$, $\mathbb{Z}_{15}$, $\mathbb{Z}_{16}$, $\mathbb{Z}_7^*$. [ano, ne, ano, ne]

3. Ověřte, že $\{z \in \mathbb{C} : \ |z| = 1\}$ tvoří podgrupu grupy $\mathbb{C}^*$. Ověřte, že množina sestávající ze všech kořenů polynomu $x^n - 1$ tvoří podgrupu této grupy.

4. Tvoří matice s kladným determinantem podgrupu grupy $\mathbf{GL}_n(T)$? A co horní, resp. dolní trojúhelníkové matice? A co symetrické, resp. antisymetrické matice? [ano, ano/ano, ne/ne]

5. Doplňte detaily v důkazu tvrzení 12.19.

Rejstřík

A^T, *viz* matice, transponovaná
δ_{ij}, *viz* Kroneckerovo delta

adjungovaná matice, *viz* matice, adjungovaná
algebraický doplněk, 233
aritmetický vektor, *viz* vektor, aritmetický
aritmetický vektorový prostor, *viz* vektorový prostor, aritmetický
asociativita
  násobení, 71
automorfismus, 204
axiom výběru, 37

bijekce, *viz* zobrazení, vzájemně jednoznačné
binární operace, *viz* operace, binární
báze, 157, 178
  kanonická, 106, 157
bázové sloupce matice, 168

charakteristika tělesa, 80
Cramerovo pravidlo, 232
cyklický zápis permutace, 221
cyklus, 220
cykly
  nezávislé, 220

definiční obor, 28
determinant, 225
  Vandermondův, 238
diagonála
  hlavní, 89
dimenze, 161
direktní součet podprostorů, *viz* součet, podprostorů direktní
distributivita, 72
duál vektorového prostoru, 210

ekvivalentní úprava, *viz* úprava, ekvivalentní
elementární úprava, *viz* úprava, elementární
eliminace neznámé, 46
endomorfismus, *viz* operátor, lineární
epimorfismus, 204
Eulerova formule, 26

Gaussova eliminace, 54
grupa, 424
  abelovská, 424

Hammingova
  vzdálenost, 180
  váha, 180
hlavní diagonála, *viz* diagonála, hlavní
hodnost matice, 55, 169
homogenní soustava lineárních rovnic, *viz* soustava, homogenní lineární
homomorfismus, *viz* lineární zobrazení

identické zobrazení, *viz* zobrazení, identické
identita, *viz* zobrazení, identické, *viz* zobrazení, identické
inverzní zobrazení, *viz* zobrazení, inverzní
inverzní prvek
  existence, 72
  existence v $\mathbb{Z}_n$, 77
izomorfismus, 204
  vektorových prostorů, 208

jednotkový prvek
  existence, 71
jádro
  lineárního zobrazení, 205

kanonická báze, *viz* báze, kanonická
kanonická báze, *viz* báze, kanonická
komplexní rovina, 22
komplexní sdružení, 20
komplexní čísla, 20
komplexně sdružené kořeny, 21
komutativita
  sčítání, 72
Kroneckerovo delta, 89
kvaterniony, 82, 110
kód
  binární blokový, 179
  lineární, 182
  paritní, 181

linearní zobrazení
  skládání, 202
lineární forma, 204
lineární kombinace, 61
  v obecném vektorovém prostoru, 144
lineární obal množiny, 145
lineární rovnice, 45
lineární zobrazení, 194
lineárně nezávislá posloupnost, *viz* posloupnost, lineárně nezávislá

lineárně závislá posloupnost, *viz* posloupnost, lineárně závislá
LU rozklad, *viz* věta o LU rozkladu

matice, 88
  adjungovaná, 236
  blokové násobení, 99
  diagonální, 89
  dolní trojúhelníková, 89
  horní trojúhelníková, 89
  inverzní, 112
  jednotková, 89
  lineárního zobrazení vzhledem k bázím B a C, 199
  nulová, 90
  násobení skalárem, 90
  opačná k matici, 90
  osobé symetrie v rovině, 102
  otočení v rovině, 102
  permutační, 89
  přechodu mezi bázemi, 166
  přechodu od jedné báze ke druhé, 200
  regulární, 119
  singulární, 119
  sloupcový prostor, 148
  soustavy, 49
  součet, 90
  součin s maticí, 93
  součin s vektorem, 92
  symetrická, 89
  transponovaná, 91
  v odstupňovaném tvaru, 52
  v redukovaném odstupňovaném tvaru, 172
  Vandermondova, 237
  zobrazení, *viz* zobrazení určené maticí
  řádkový prostor, 148
matice v odstupňovaném tvaru, *viz* matice v odstupňovaném tvaru
minor matice, 231
množina generátorů vektorového prostoru, 146
monomorfismus, 204

nulové zobrazení, *viz* zobrazení, nulové

obor hodnot zobrazení, *viz* zobrazení, obor hodnot
obraz
  lineárního zobrazení, 205
obraz množiny při zobrazení, *viz* zobrazení, obraz množiny
operace, 139
  binární, 71
operátor
  lineární, 204
ortogonální projekce
  v rovině, 109
otočení v rovnině, 100

permutace, 219
  lichá, 223
  sudá, 223
podgrupa, 426
podprostor, 142
polární souřadnice v rovině, 23
posloupnost
  lineárně závislá, 150, 178
  lineárně nezávislá, 150, 178
proměnná, 50
přímka
  parametrický tvar, 12

redukovaný odstupňovaný tvar, *viz* matice, v redukovaném odst. tvaru
redukovaný cyklický zápis permutace, 221
rovina, 7
rovnice přímky
  v parametrickém tvaru, 17
  v rovině, 10
rovnice roviny
  v parametrickém tvaru, 16
  v prostoru, 15
rozšířená matice soustavy, *viz* matice soustavy

skalár, 139
skládání lineárních zobrazení, *viz* lineární zobrazení, skládání
sloupcový prostor matice, *viz* matice, sloupcový prostor
složené zobrazení, *viz* zobrazení, skládání
soustava
  homogenní lineární, 125
  lineárních rovnic, 45
  špatně podmíněná, 63
součet
  podprostorů, 175
  podprostorů direktní, 177
souřadnice, 163
  v prostoru (trojrozměrném), 14
  v rovině, 8
spojení podprostorů, *viz* součet, podprostorů
stopa matice, 197
symetrie v rovině, 108

transpozice, 220
trojúhelníková nerovnost
  pro komplexní čísla, 27
těleso, 72
  $\mathbb{Z}_p$, 74
  charakteristika, *viz* charakteristika tělesa
  charakteristiky 0, 82
  konečné obecné, 82
  čtyřprvkové, 81

vektor, 139
  aritmetický, 45
  neformálně, 5
  nulový, 9
  pravých stran, 50
vektorový prostor
  aritmetický, 139
vektorový prostor, 139
  $\mathbb{C}$ nad $\mathbb{R}$, 141
  konečně generovaný, 159
  matic, 140

polynomů, 140
reálných funkcí, 141
reálných posloupností, 141
vzor množiny při zobrazení, *viz* zobrazení, vzor množiny
vzor prvku při zobrazení, *viz* zobrazení, vzor prvku
věta
Frobeniova, 173
Moivrova, 25
o dimenzi jádra a obrazu, 209
o determinantu součinu, 232
o dimenzi obrazu A a A^T, 169
o dimenzi součtu a průniku, 175
o falešném rozvoji determinantu, 236
o isomorfismu konečně generovaných prostorů, 209
o LU rozkladu, 129
o regulárních maticích, 120
o rozvoji determinantu podle sloupce, 234
o tvaru řešení SLR, 56
o řešení SLR pomocí jádra matice, 126
Steinitzova o výměně, 160
že $\mathbb{Z}_p$ je těleso, 78

znaménko permutace, 223
zobrazení, 28
bijektivní, *viz* zobrazení, vzájemně jednoznačné
duální, 112
identické, 34, 111, 197
injektivní, 32
inverzní, 35
na, 32, 204
nulové, 197
obor hodnot, 32
obraz množiny, 32
prosté, 32, 204
skládání, 33
surjektivní, 32
určené maticí, 103
vzor množiny, 33
vzor prvku, 33
vzájemně jednoznačné, 32, 204
zpětná substituce, 55

úprava
ekvivalentní, 46
elementární, 47, 52

řádkový prostor matice, *viz* matice, řádkový prostor

Obsah

Jak používat tato skripta 3

Kapitola 1. Opakování 5
1.1. Základní geometrické pojmy 5
1.2. Analytická geometrie v rovině 8
1.3. Analytická geometrie v prostoru 14
1.4. Komplexní čísla 20
1.5. Zobrazení 28

Kapitola 2. Řešení soustav lineárních rovnic 39
2.1. Úlohy vedoucí na soustavy lineárních rovnic 39
2.2. Soustavy lineárních rovnic a aritmetické vektory 45
2.3. Ekvivalentní a elementární úpravy 46
2.4. Gaussova eliminační metoda 52
2.5. Geometrie soustav lineárních rovnic 57
2.6. Praktické problémy při numerickém řešení velkých soustav rovnic 62
2.7. Jak dlouho to bude trvat 63
Cvičení 65
Shrnutí druhé kapitoly 67

Kapitola 3. Tělesa 71
3.1. Motivace 71
3.2. Definice tělesa 73
3.3. Tělesa $\mathbb{Z}_p$ 75
3.4. Charakteristika 81
3.5. Další příklady těles 82
Cvičení 84
Shrnutí třetí kapitoly 86

Kapitola 4. Matice 88
4.1. Matice, jednoduché operace, typy matic 89
4.2. Součin matic 92
4.3. Matice jako zobrazení 106
4.4. Inverzní matice 118
4.5. Soustavy lineárních rovnic podruhé 131
Cvičení 136
Shrnutí čtvrté kapitoly 138

Kapitola 5. Vektorové prostory 144
5.1. Definice, příklady a základní vlastnosti 144
5.2. Podprostory 148
5.3. Lineární závislost a nezávislost 156
5.4. Báze 162
5.5. Hodnost matice 173

5.6. Průnik a součet podprostorů 180
5.7. Prostory nekonečné dimenze 184
5.8. Samoopravné kódy 184
Cvičení 191
Shrnutí páté kapitoly 194

Kapitola 6. Lineární zobrazení 200
6.1. Definice a příklady 200
6.2. Matice lineárního zobrazení 204
6.3. Skládání lineárních zobrazení 208
6.4. Speciální typy lineárních zobrazení 210
6.5. Prostor lineárních zobrazení 215
Shrnutí šesté kapitoly 219

Kapitola 7. Determinant 222
7.1. Motivace 222
7.2. Permutace 225
7.3. Definice determinantu a základní vlastnosti 231
7.4. Rozvoj, adjungovaná matice 239
7.5. Vandermondův determinant 243
7.6. Orientace vektorového prostoru 244
Cvičení 245
Shrnutí sedmé kapitoly 247

Kapitola 8. Skalární součin 251
8.1. Standardní skalární součin v $\mathbb{R}^n$ a $\mathbb{C}^n$ 251
8.2. Obecný skalární součin 258
8.3. Kolmost 266
8.4. Ortogonální projekce a ortogonalizace 272
8.5. Unitární a ortogonální zobrazení a matice 288
8.6. Aplikace: aproximace a optimalizace 291
8.7. Orientovaný objem 296
8.8. Vektorový součin 299
Cvičení 300
Shrnutí osmé kapitoly 302

Kapitola 9. Vlastní čísla a vlastní vektory 309
9.1. Lineární dynamické systémy 309
9.2. Vlastní čísla a vlastní vektory 315
9.3. Diagonalizovatelné operátory 328
9.4. Jordanův kanonický tvar 344
9.5. Google 370
Cvičení 373
Shrnutí deváté kapitoly 375

Kapitola 10. Unitární diagonalizace 381
10.1. Unitární a ortogonální diagonalizovatelnost 382
10.2. Spektrální věty 385
10.3. Singulární rozklad 393
10.4. Použití singulárního rozkladu 401
Shrnutí desáté kapitoly 406

Kapitola 11. Bilineární formy a kvadratické formy 409
11.1. Matice 411

11.2. Symetrické a antisymetrické formy 413
11.3. Ortogonální báze 415
11.4. Ortogonální báze nad $\mathbb{R}$ 419
11.5. Příklady 423
Shrnutí jedenácté kapitoly 427

Kapitola 12. Grupy 430
12.1. Obecný pojem grupy 430
12.2. Grupy symetrií geometrických objektů 433
Cvičení 434

Rejstřík 436