Lineární algebra

Obsah

OrgPage Lineární algebra **1**

Filtrování . . . 1

Soustavy lineárních rovnic **2**

Soustavy lineárních rovnic: Ax=b . . . 2

Maticový zápis . . . 2

Historie . . . 3

Analýza dynamických systémů . . . 3

Úpravy . . . 4

Gaussova eliminace . . . 5

Příklady eliminací . . . 6

Geometrie elementárních úprav . . . 6

Geometrie Gaussovy eliminace . . . 7

Iterační metody . . . 8

Geometrická struktura množiny všech řešení . . . 9

Řádková interpretace . . . 10

Sloupcová interpretace . . . 10

Vektorové prostory **12**

Geometrie vektorů . . . 12

Vlastnosti vektorů $\mathbb{R}^n$ . . . 12

Grupy . . . 13

Algebraická tělesa . . . 14

Konečná tělesa . . . 15

Vektorové prostory . . . 15

Vektorové podprostory . . . 16

Afinní podprostory . . . 17

Lineární kombinace . . . 17

Lineární obal a generátory . . . 18

Lineární (ne)závislost . . . 19

Báze . . . 19

Konstrukce báze . . . 20

Lemma o výměně . . . 21

Steinitzova věta o výměně . . . 21
Dimenze . . . 22
Motivace pro různé báze . . . 22
Faktorprostory . . . 23
Interpolace polynomů . . . 24
Lagrangeova interpolace . . . 24

Matice **26**

Matice . . . 26
Maticové násobení . . . 26
Matice úprav . . . 27
Maticové inverze . . . 28
Regulární matice . . . 29
Determinant . . . 29
Transpozice . . . 29
Hodnost transpozice . . . 29
Hodnost matice . . . 29
Fundamentální podprostory . . . 30
Speciální matice . . . 31
Diagonální matice . . . 31
Vlastní čísla . . . 32
Trojúhelníkové matice . . . 32
Permutační matice . . . 33
Blokové matice . . . 33
Hodnost 1 . . . 34
SVD . . . 34
LU dekompozice . . . 34
Symetrické matice . . . 35
Normální matice . . . 35

Lineární zobrazení **36**

Lineární zobrazení (homomorfismy) . . . 36
Geometrické příklady $\mathbb{R}^2 \to \mathbb{R}^2$ . . . 36
Derivace a integrál . . . 38
Maticová reprezentace $f : x \mapsto Ax$ . . . 38
Matice přechodu . . . 40
Podobnost . . . 40
Skládání zobrazení . . . 41
Inverzní zobrazení . . . 42

Endomorfismy, izomorfismy, automorfismy . . . 42
Hledání vzorů . . . 43
Věta o izomorfismu . . . 43
Věta o homomorfismu . . . 44
Duální zobrazení . . . 45

Skalární součin **46**

Skalární součin, norma a kolmost . . . 46
Skalární součin . . . 46
Cauchy-Schwarzova nerovnost . . . 47
Norma . . . 48
Nestandardní normy v $\mathbb{R}^2$ . . . 48
Nestandardní skalární součin . . . 49
Pozitivně definitní matice . . . 50
Kvadratické formy a definitnost . . . 51
Ortogonalita . . . 51
Ortogonální doplněk . . . 51
Ortonormální báze . . . 52
Fourierova transformace . . . 53
Ortogonální matice . . . 53
Gram-Schmidtova ortogonalizace . . . 53
QR dekompozice . . . 54
Ortogonální projekce . . . 54
Metoda nejmenších čtverců . . . 55
Fundamentální podprostory . . . 55

OrgPage Lineární algebra

Autor: Pavel Klavík

Poslední změna: 26.9.2026

Poděkování: Zdeněk Hedrlín, Peter Zeman, studenti pokročilých cvičení.

V současné chvíli jsou tato hlavní témata:

- Soustavy lineárních rovnic A**x**=**b**.
- Matice.
- Vektorové prostory.
- Lineární zobrazení (homomorfismy).

Následující témata jsou rozpracovaná:

- Skalární součin, norma, ortogonalita.
- Determinanty.
- Vlastní čísla.
- Kvadratické formy a definitnost.

Zdroje

Obsah je utvořen podle výuky na Pokročilých cvičeních z Lineární algebry a knih Povídání o lineární algebře a Lineární algebra II: Pokročilé cvičení (převzaty skoro všechny obrázky).

Filtrování

- Všechny uzly
- Pouze klíčové uzly
- Jednotlivá témata:
  - Soustavy
  - Vektory
  - Matice
  - Zobrazení
  - Skalární součin

Soustavy lineárních rovnic

Soustavy lineárních rovnic: Ax=b

Začneme příkladem soustava tří lineárních rovnic o třech neznámých:

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

Hledáme **množinu všech řešení**, což jsou trojice (x, y, z), které po dosazení splňují všechny tři rovnice současně. V tomto případě je **řešením jediná trojice** $(1, 3, 2)$.

Obecně soustava *m* lineárních rovnic o *n* neznámých:

$$\begin{aligned} a_{1,1}x_1 &+ a_{1,2}x_2 &+ a_{1,3}x_3 &+ \cdots + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 &+ a_{2,2}x_2 &+ a_{2,3}x_3 &+ \cdots + a_{2,n}x_n &= b_2 \\ a_{3,1}x_1 &+ a_{3,2}x_2 &+ a_{3,3}x_3 &+ \cdots + a_{3,n}x_n &= b_3 \\ \vdots & & \vdots & \ddots \quad \vdots & \vdots \\ a_{m,1}x_1 &+ a_{m,2}x_2 &+ a_{m,3}x_3 &+ \cdots + a_{m,n}x_n &= b_m \end{aligned}$$

Čísla $a_{i,j}$ a b_j jsou pevně zadaná a nazývají se **koeficienty**. Čísla x_j se nazývají **neznámé** a jejich hodnoty chceme nalézt.

Hledáme **množinu řešení** tvořenou n-ticemi $(x_1, \dots, x_n)$ takovými, že po dosazení budou **zároveň splněny** všechny rovnice.

Maticový zápis

Můžeme zjednodušit zápis soustavy tak, že vynecháme zbytečné informace:

- V jednotlivých sloupcích jsou stejná jména proměnných, která vynecháme.
- Odstraníme operace + a =.

Pro řešení soustavy jsou důležité pouze **koeficienty**, které zapíšeme do tabulky zvané **matice**.

Původní soustava:

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

Maticový zápis:

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

Soustavu lze v řeči matic a vektorů vyjádřit v elegatní formě $A\boldsymbol{x} = \boldsymbol{b}$. Zde A je matice koeficentů, $\boldsymbol{x}$ je vektor neznámých a $\boldsymbol{b}$ je vektor pravých stran.

$$A = \begin{pmatrix} 2 & -1 & \\ -1 & 2 & -1 \\ & -1 & 2 \end{pmatrix}, \qquad \boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \qquad \boldsymbol{b} = \begin{pmatrix} -1 \\ 3 \\ 1 \end{pmatrix}.$$

Rozepsáním **definice maticového násobení** získáme soustavu lineárních rovnic.

Interpretace **maticového násobení po sloupcích** A vede na sloupcovou interpretaci soustavy.

Historie

Řešení soustav lineárních rovnic je odvěký problém se spoustou aplikací. Konkrétní soustavy lineárních rovnic se v matematice objevují již před více než pěti tisíci lety. V čínské knize **Devět kapitol** napsané zhruba dvě stě let před naším letopočtem se objevuje postup, jak vyřešit **konkrétní soustavu tří lineárních rovnic o třech neznámých**. Jakékoliv formální zdůvodnění chybí, ale při zobecnění dostaneme Gaussovu eliminaci.

V západní matematice Gaussovu eliminaci poprvé popsal **Newton ve své algebraické knize**, i když se jednalo o postup mezi matematiky běžně známý.

Gauss se zabýval **metodou nejmenších čtverců** (v souvislosti s geodézií), pro níž popsal algoritmus podobný Gaussově eliminaci. Jméno Gaussova eliminace se začalo používat až v padesátých letech díky implementaci metody nejmenších čtverců v počítačích. **Historie řady pojmů lineární algebry je značně složitá!**

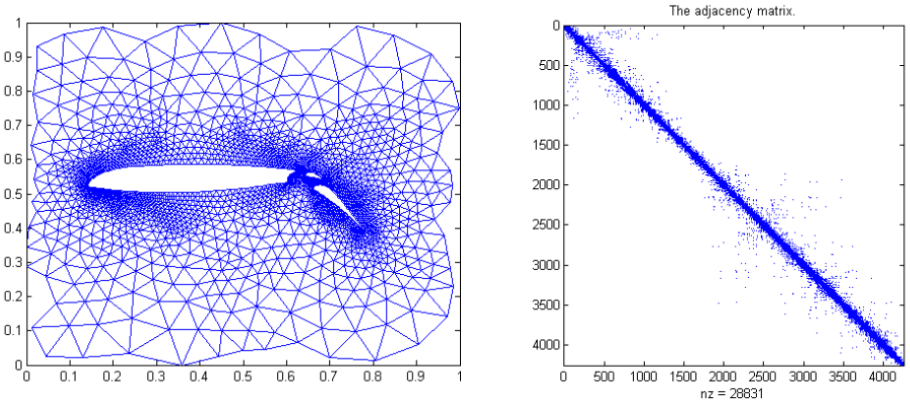
Analýza dynamických systémů

Velká část matematiky se zabývá studiem modelů reálného světa. To jsou často **dynamické systémy**, jejichž stav (například vektor reálných čísel) se mění v závislosti na čase. Změna stavu je popsána matematickými vztahy, například lokálně diferenciálními rovnicemi. Při analýze chceme odpovídat na otázky následujícího typu: predikce vývoje z počátečního stavu, pochopit kvalitativní chování (konvergence k ustálenému stavu, oscilace, chaotické chování).

Problém je, že typický dynamický systém je příliš složitý a nemůže být přesně popsán jeho vývoj. Ve většině situací se spokojíme s tím, že nalezneme přibližné řešení jeho **diskretizací** (simulace, metoda konečné mřížky, metoda konečných prvků), čímž se v řadě situací převede na řešení **velké soustavy lineárních rovnic**

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

Zde matice A popisuje zdiskretizované vztahy v systému, zatímco vektor $\boldsymbol{b}$ odpovídá stavu nebo vývoji stavu. Při řešení se často využívá specifické struktury koeficientů matice A.



Úpravy

Z rovnic lze vyvozovat **nové informace jejich kombinováním**. Budeme uvažovat dvě elementární operace a jejich kombinace:

- **Násobení reálným číslem:** z $A = B$ získáme $\alpha A = \alpha B$.
- **Součet dvou rovnic:** z $A = B$ a $C = D$ získáme $A + C = B + D$.

Protože nechceme, aby počet rovnic **rostl**, vždy odvozenou rovnicí **nahradíme** nějakou předchozí, čímž získáme **upravenou soustavu**. Výše uvedené úpravy nazýváme **elementární úpravy**.

Dále uvažujeme **odvozené elementární úpravy**:

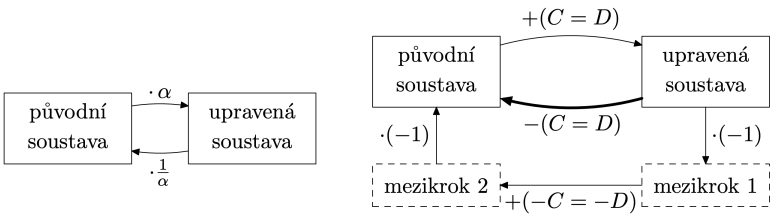
- Přičtení α-násobku jedné rovnice k druhé.
- Prohození dvou rovnic.

Pokud nějaká n-tice $(x_1, \dots, x_n)$ řeší soustavu, bude řešit i upravenou soustavu. Avšak obrácená implikace nemusí platit, množina řešení se může úpravou **zvětšit**.

Úprava se nazývá **regulární** (nebo ekvivalentní), pokud nemění množinu řešení obecně libovolné soustavy.

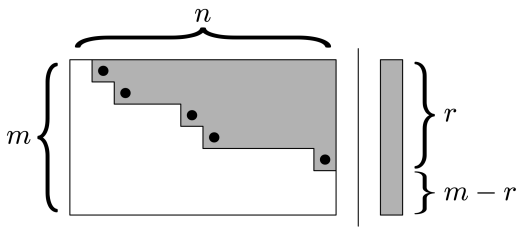
Tvrzení: Úpravy vynásobení nenulovým reálným číslem, přičtení jedné rovnice k druhé a jejich kombinace jsou regulární.

Důkaz: Výše uvedené úpravy lze invertovat, tedy existují úpravy, které převedou upravenou soustavu zpět do původního tvaru. Protože se množina řešení může pouze zvětšovat, nemohla se změnit.



Gaussova eliminace

Algoritmus na řešení soustavy lineárních rovnic. Jedná se o **strategii**, jak aplikovat elementární úpravy tak, aby se matice zjednodušila do odstupňovaného tvaru.

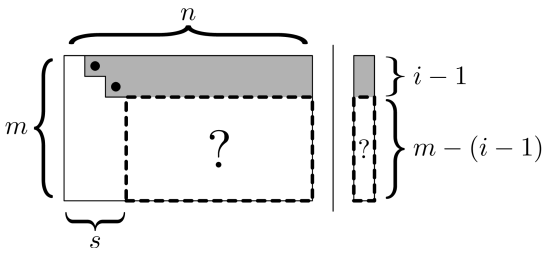


Černě vyznačené koeficienty se nazývají **pivoti** a jsou to první nenulové hodnoty na jednotlivých řádcích. Gaussova eliminace se skládá ze dvou fází:

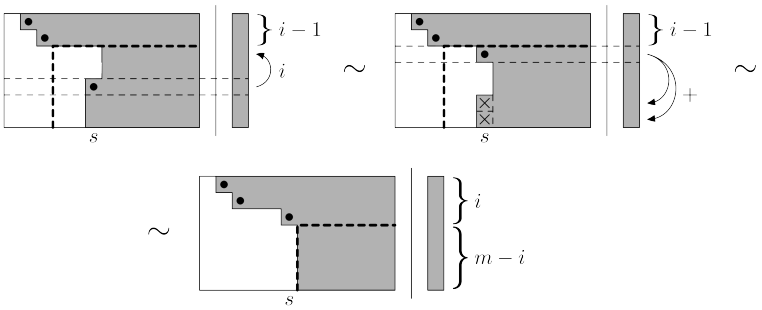
- **dopředná eliminace**, která vypočítá odstupňovaný tvar,
- **zpětná substituce**, která nalezne všechna řešení z odstupňovaného tvaru.

Odstupňovaný tvar je konstruován v n **krocích**, celkově k jeho spočítání potřebujeme $n^3/3$ elementárních operací (násobení, sčítání).

Stav na počátku i-tého kroku:



V i-tém kroku se aplikují následující elementární úpravy:



Příklady eliminací

Dopředná eliminace:

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

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

Zpětná substituce:

- Nejprve určíme $z = 2$.
- Poté dosadíme za z do druhé rovnice a určíme $y = 3$.
- Nakonec dosadíme za y a z do první rovnice a získáme $x = 1$.

Tedy existuje jednoznačné řešení soustavy $(1, 3, 2)$.

Nekonečně mnoho řešení.

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

Má nekonečně mnoho řešení ve tvaru $(3 - 2y, y)$, kde y je libovolné reálné číslo. Lze popsat také jako $(3, 0) + y(-2, 1)$.

Neexistuje řešení.

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

Neexistuje žádné řešení, neboť jsme úpravami odvodili, že musí platit $0x + 0y = 2$, což není splněno pro žádnou dvojici (x, y) reálných čísel.

Geometrie elementárních úprav

Řádkové úpravy z pohledu sloupcové interpretace:

Řádkové úpravy transformují prostor $\mathbb{R}^m$ spolu s vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ a pravou stranou $\boldsymbol{b}$. Klíčová vlastnost je, že pokud úprava prostor nikde nesplácne (tedy je regulární), je vztah mezi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ a pravou stranou $\boldsymbol{b}$ zachován.

Elementární řádkové úpravy odpovídají následujícím geometrickým transformacím prostoru $\mathbb{R}^m$:

- **Násobení i-tého řádku skalárem** α odpovídá α-násobnému natažení prostoru ve směru i-té souřadné osy.
- **Přičtení i-tého řádku k j-tému** odpovídá zkosení i-té souřadné osy do j-té souřadné osy.

V maticovém zápisu, nechť R je regulární matice řádkových úprav reprezentující geometrickou transformaci. Ze soustavy lineárních rovnic $A\boldsymbol{x} = \boldsymbol{b}$ získáme transformovanou soustavu $RA\boldsymbol{x} = R\boldsymbol{b}$.

Sloupcové úpravy z pohledu sloupcové interpretace:

Sloupcová úprava transformuje jednotlivé sloupcové vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$. Jejich vztah k pravé straně $\boldsymbol{b}$ se může změnit, tedy mění se množina všech řešení. Je možné provádět sloupcové úpravy, ale musíme si je zapamatovat a na závěr příslušně upravit nalezené řešení.

Elementární sloupcové úpravy odpovídají následujícím transformacím:

- **Násobení i-tého sloupce skalárem** α odpovídá α-násobnému natažení vektoru $\boldsymbol{u}_i$.
- **Přičtení i-tého sloupce k j-tému** odpovídá zkosení $\boldsymbol{u}_i$ do $\boldsymbol{u}_j$.

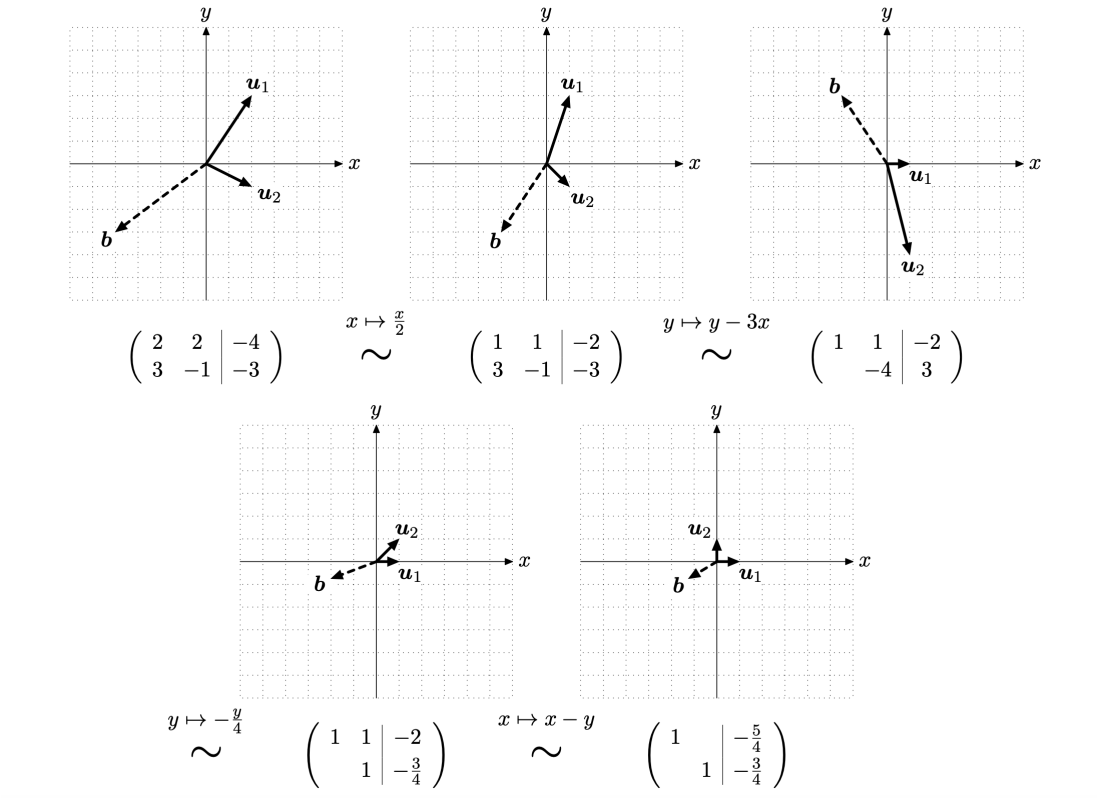
V maticovém zápisu, nechť S je regulární matice sloupcové úpravy reprezentující transformaci sloupcových vektorů. Ze soustavy lineárních rovnic $A\boldsymbol{x} = \boldsymbol{b}$ získáme transformovanou soustavu $ASS^{-1}\boldsymbol{x} = \boldsymbol{b}$, která vede na soustavu $AS\boldsymbol{y} = \boldsymbol{b}$. Když ji vyřešíme a nalezneme hodnotu $\boldsymbol{y}$, musíme dopočítat $\boldsymbol{x} = S\boldsymbol{y}$.

Geometrie Gaussovy eliminace

Gaussova eliminace provádí geometrické transformace sloupcových vektorů a pravé strany elementárními řádkovými úpravami. Převede soustavu do odstupňovaného tvaru se sloupcovými vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ a pravou stranou $\boldsymbol{b}$, ve kterém je snadné ji vyřešit.

Pokud $\boldsymbol{b}$ ukazuje jiným směrem než sloupcové vektory, poznáme to podle toho, že ukazuje ve směru souřadné osy, která není obsažena v žádném ze sloupcových vektorů $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$. Tedy $\boldsymbol{b}$ nelze vyjádřit pomocí sloupcových vektorů $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ a řešení soustavy neexistuje.

Pokud jsou všechny tyto koeficienty $\boldsymbol{b}$ nulové, řešení existuje. Najdeme ho tak, že hodnoty volných proměnných zvolíme libovolně, čímž známe natažení příslušných sloupcových vektorů. Můžeme je odečíst od pravé strany a získat upravenou pravou stranu $\boldsymbol{b}'$. Pro sloupcové vektory s pivoty dopočteme hodnotu řešení, protože vždy pouze jeden z nich ukazuje určitým směrem $\boldsymbol{b}'$, tedy jeho hodnota natažení je jednoznačně určena a lze příslušný sloupcový vektor odečíst.



Iterační metody

Obecně existují v matematice dva druhy výpočetních metod. **Přímé metody** (například Gaussova eliminace) provádějí dlouhou sekvenci kroků, na jejichž koncí získáme řešení. Oproti tomu **iterační metody** postupují v kratších krocích a konstruují lepší a lepší aproximaci řešení.

V případě soustavy $A\boldsymbol{x} = \boldsymbol{b}$ počítají iterační metody posloupnost přibližných řešení $\boldsymbol{x}_0, \dots, \boldsymbol{x}_k$. Skončíme v k-tém kroku, když je chyba $\boldsymbol{e}_k = \boldsymbol{x} - \boldsymbol{x}_k$ dostatečně malá. Protože typicky vektor chyby $\boldsymbol{e}_k$ neznáme, testujeme dostatečně malou velikost residua

$$\boldsymbol{r}_k = A\boldsymbol{e}_k = A(\boldsymbol{x} - \boldsymbol{x}_k) = \boldsymbol{b} - A\boldsymbol{x}_k.$$

Jeden ze zásadních rozdílů je, že pokud iterační metodu zastavíme v půlce, získáme alespoň nějaký odhad řešení, narozdíl od přímé metody. (Co víme o řešení soustavy, pokud Gaussova eliminace spočítá pouze polovinu odstupňovaného tvaru?)

Štěpící metody. Předpokládejme, že $A = S - T$ a že pro matici S umíme snadno vyřešit soustavu (řekněme, že známe S^{-1}). Potom $A\boldsymbol{x} = \boldsymbol{b}$ vede na $S\boldsymbol{x} = T\boldsymbol{x} + \boldsymbol{b}$, neboli $\boldsymbol{x} = S^{-1}T\boldsymbol{x} + S^{-1}\boldsymbol{b}$. Tento vzorec můžeme použít k iterování:

$$\boldsymbol{x}_{k+1} = S^{-1}T\boldsymbol{x}_k + S^{-1}\boldsymbol{b}$$

Metoda konverguje pouze pro určité volby matic S a T, a velice pomalu. Typická volba S je diagonální část A nebo horní trojúhelníková část A. Jiný pohled na metody je, že S je aproximace matice A.

Metoda konjugovaných gradientů CG. Konstruuje postupně aproximace výpočtem Krylovova podprostoru

$$K_k = \langle \boldsymbol{b}, A\boldsymbol{b}, A^2\boldsymbol{b}, \dots, A^{k-1}\boldsymbol{b} \rangle$$

Volíme $\boldsymbol{x}_k \in K_k$ tak, aby minimalizovalo chybu řešení přes všechny vektory K_k, což lze udělat velice efektivně. Pro rozšíření Krylovova podprostoru je potřeba vynásobit vektor maticí, což vyžaduje n^2 operací. Protože typicky stačí udělat $n^{1/2}$ iterací, je metoda typicky rychlejší než Gaussova eliminace: $n^{5/2}$ operací.

Geometrická struktura množiny všech řešení

Věta: Množina všech řešení soustavy $A\boldsymbol{x} = 0$ je vektorový podprostor, který se značí $\mathrm{Ker}(A)$.

Důkaz: Stačí ukázat, že množina všech řešení je **uzavřená na sčítání a násobení skalárem**. Když $\boldsymbol{x}$ je řešením soustavy $A\boldsymbol{x} = 0$, platí pro i-tou rovnici:

$$a_{i,1}x_1 + a_{i,2}x_2 + \cdots + a_{i,n}x_n = 0. \qquad (\star)$$

Množina řešení je uzavřená na sčítání, neboť se zachovává se splnění i-té rovnice:

$$\begin{aligned} a_{i,1}(x_1 + y_1) + a_{i,2}(x_2 + y_2) + \cdots + a_{i,n}(x_n + y_n) &= \underbrace{a_{i,1}x_1 + a_{i,2}x_2 + \cdots + a_{i,n}x_n}_{=0 \text{ podle } (\star)} \\ &\quad + \underbrace{a_{i,1}y_1 + a_{i,2}y_2 + \cdots + a_{i,n}y_n}_{=0 \text{ podle } (\star) \text{ s } \boldsymbol{y} \text{ místo } \boldsymbol{x}} \\ &= 0 + 0 = 0. \end{aligned}$$

Důkaz uzavřenosti na násobení je podobný.

V **maticovém zápisu** je to ještě jednodušší. Pokud $A\boldsymbol{x} = 0$ a $A\boldsymbol{y} = 0$, potom

$$A(c\boldsymbol{x}) = c(A\boldsymbol{x}) = c \cdot 0 = 0,$$

$$A(\boldsymbol{x} + \boldsymbol{y}) = A\boldsymbol{x} + A\boldsymbol{y} = 0 + 0 = 0.$$

Věta: Množina všech řešení soustavy $A\boldsymbol{x} = \boldsymbol{b}$ je afinní podprostor $\mathrm{Ker}(A) + \boldsymbol{p}$, kde $\boldsymbol{p}$ je libovolné řešení soustavy.

Důkaz: Stačí si všimnout, že kdykoliv máme dvě řešení $A\boldsymbol{x} = \boldsymbol{b}$ a $A\boldsymbol{y} = \boldsymbol{b}$, jejich rozdíl $\boldsymbol{x} - \boldsymbol{y}$ patří do $\mathrm{Ker}(A)$:

$$A(\boldsymbol{x} - \boldsymbol{y}) = A\boldsymbol{x} - A\boldsymbol{y} = \boldsymbol{b} - \boldsymbol{b} = 0.$$

Zbytek plyne z vlastností afinních podprostorů.

Klíčový důsledek: Uvažme různé pravé strany $\boldsymbol{b}$. Pro některé nebude existovat žádné řešení, což odpovídá neexistenci vektoru $\boldsymbol{p}$. Pro ty zbývající jsou to afinní podprostory vzniklé různými posunutími W. Tedy množiny řešení soustav $A\boldsymbol{x} = \boldsymbol{b}$ a $A\boldsymbol{x} = \boldsymbol{c}$ mají totožnou strukturu až na posunutí.

Označíme $\mathrm{Im}(A)$ množinu všech pravých stran, pro kterou existuje řešení. To je vektorový podprostor $\mathbb{R}^m$, stačí ověřit uzavřenost na sčítání a násobení skalárem:

$$A(\boldsymbol{x} + \boldsymbol{y}) = A\boldsymbol{x} + A\boldsymbol{y} = \boldsymbol{b} + \boldsymbol{c}.$$

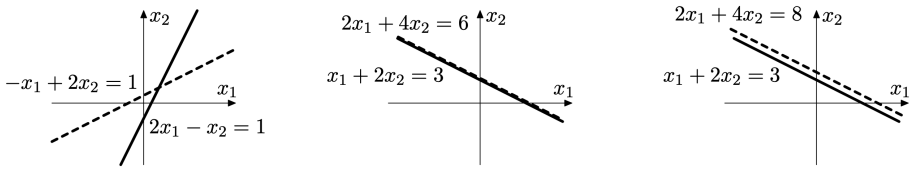
Platí, že **čím větší** je $\mathrm{Ker}(A)$, tím méně jeho posunutí existuje, tedy **tím méně** pravých stran má řešení. **Tento vztah lze přesně popsat pomocí dimenzí:**

$$\dim \mathrm{Ker}(A) + \dim \mathrm{Im}(A) = n.$$

Řádková interpretace

Mějme soustavu m rovnic o n neznámých. Jednotlivá ohodnocení neznámých můžeme identifikovat s vektory $\mathbb{R}^n$. Jak vypadá **množina všech řešení geometricky?** Můžeme postupovat tak, že určíme množinu řešení R_i pro každý z řádků $i = 1, \dots, m$. Celá množina řešení soustavy je průnik $R_1 \cap \cdots \cap R_m$.

Příklady soustav 2 rovnic o 2 neznámých:



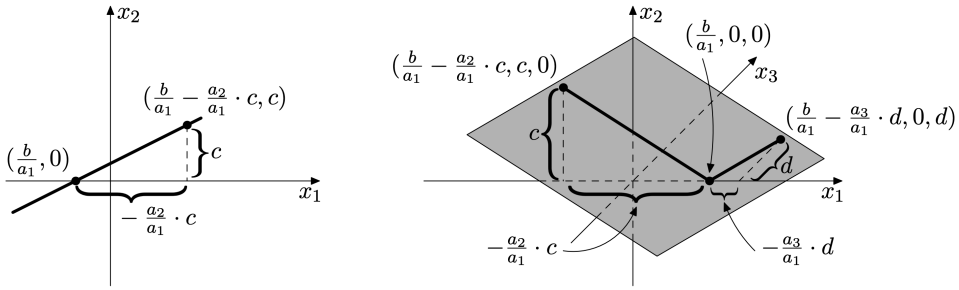
Vlevo je to jeden bod, ležící v průniku dvou přímek. Uprostřed je v průniku celá přímka. Vpravo je prázdný průnik, neboť jsou přímky rovnoběžné.

Jak vypadá množina R_i obecně?

Povšimněme si, že hodnoty **libovolných $n-1$ proměnných můžeme zvolit libovolně**, čímž je hodnota zbývající proměnné jednoznačně určena. Tedy R_i má $n-1$ „stupňů volnosti".

Geometricky R_i tvoří **nadrovinu posunutou z počátku**, což je afinní podprostor dimenze $n-1$, zobecnění rovin v $\mathbb{R}^3$. Koeficienty $a_{i,1}, \dots, a_{i,n}$ určují **směr normálového vektoru**, který je kolmý k nadrovině. Koeficient b_i určuje **posunutí nadroviny z počátku**.

Abychom toto mohli dokázat, museli bychom mít jinou geometrickou definici nadroviny. Zkuste si však rozmyslet, že to tak funguje pro malé hodnoty n. Konkrétně pro $n = 2$ (vlevo) dostaneme přímku posunutou z počátku, pro $n = 3$ (vpravo) získáme rovinu posunutou z počátku.



Sloupcová interpretace

I když se tato interpretace často ignoruje, považuji ji za **mnohem užitečnější** než tu řádkovou. Myšlenka je, že budeme uvažovat **sloupcové vektory** matice a pravé strany, které patří do $\mathbb{R}^m$:

$$\boldsymbol{u}_i = \begin{pmatrix} a_{1,i} \\ a_{2,i} \\ \vdots \\ a_{m,i} \end{pmatrix}, \qquad i = 1, 2, \dots, n \qquad \text{a} \qquad \boldsymbol{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}.$$

Nyní učiníme klíčové pozorování, že se neznámá x_i objevuje přesně u koeficientů jednoho sloupcového vektoru $\boldsymbol{u}_i$. Tedy soustava lineárních rovnic je **ekvivalentní s vektorovou rovnicí**

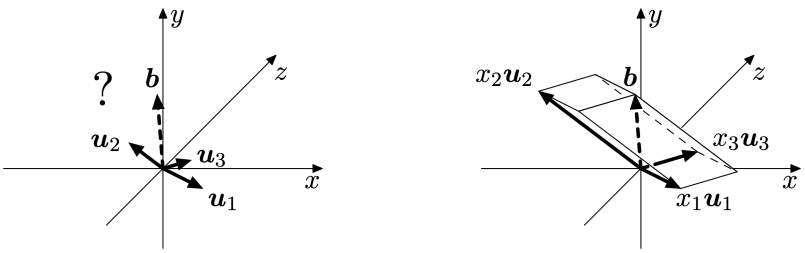
$$x_1\boldsymbol{u}_1 + x_2\boldsymbol{u}_2 + \cdots + x_n\boldsymbol{u}_n = \boldsymbol{b},$$

kde rovnost má platit v každé složce.

Tedy máme rovnici

$$x_1\boldsymbol{u}_1 + x_2\boldsymbol{u}_2 + \cdots + x_n\boldsymbol{u}_n = \boldsymbol{b},$$

kterou chceme interpretovat geometricky. Hledáme koeficienty $x_1, \ldots, x_n$ natažení vektorů $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$, tak aby se zkombinovali pravou stranu $\boldsymbol{b}$.



Voleb koeficientů může být spousta, což vede k nekonečně mnoha řešením. Pokud vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ ukazují „jiným“ směrem než $\boldsymbol{b}$, soustava nemá žádné řešení.

Vektorové prostory

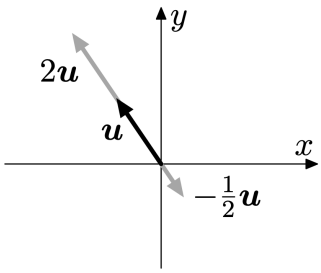
Geometrie vektorů

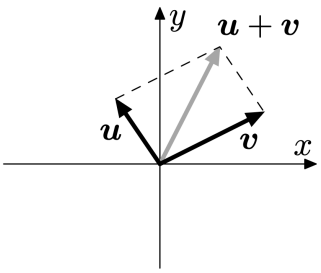
Vektorový prostor $\mathbb{R}^n$ je tvořen vektory, které **geometricky odpovídají bodům**. Vznikne zobecněním $\mathbb{R}^2$ a $\mathbb{R}^3$. Pro ně Descartes vymyslel, že sice prostor přímo nevidíme, ale můžeme v něm popisovat pozici **pomocí trojice souřadnic** (x, y, z).

Poznamenejme, že za vektory jsou někdy označovány **orientované úsečky**. Toto dělení bodů a vektorů je historické a dnes již zbytečné. Někdy s vektorem budeme pracovat jako s bodem, jindy se nám bude hodit interpretace, že je to šipka vycházející z počátku do tohoto bodu.

Násobení skalárem odpovídá **natažení vektoru v daném směru**. Pokud je koeficient záporný, bude výsledný vektor ukazovat opačným směrem.

Motivace pro sčítání dvou vektorů vychází z fyziky, konkrétně z Newtonovské mechaniky. Pokud vektory reprezentují působení síly (ta má velikost a směr), tak **sčítání reprezentuje skládání těchto sil**, tedy určení jedné zkombinované síly.





Vlastnosti vektorů $\mathbb{R}^n$

Pokud pracujeme s abstraktní definicí vektorového prostoru, máme **zaručeno několik vlastností vektorů**: sčítání vektorů je komutativní, asociativní, platí distributivity s násobením, existuje nulový vektor, atd.

Pokud použijeme konstruktivní definici $\mathbb{R}^n$, můžeme snadno dokázat, že vektory **také splňují všechny tyto vlastnosti**. Například nulový vektor je počátek $0 = (0, \dots, 0)$.

Ukažme si myšlenku alespoň na jednom příkladu.

Tvrzení: Sčítání vektorů v $\mathbb{R}^n$ je komutativní, tedy platí $\boldsymbol{u} + \boldsymbol{v} = \boldsymbol{v} + \boldsymbol{u}$.

Důkaz: Nejprve si uvědomme, že vektory $\boldsymbol{u} + \boldsymbol{v}$ a $\boldsymbol{v} + \boldsymbol{u}$ jsou si rovny, právě když se shodují v každém koeficientu. A protože tyto koeficienty jsou reálná čísla, přenese se jejich komutativita i na vektory:

$$(\boldsymbol{u} + \boldsymbol{v})_i = \boldsymbol{u}_i + \boldsymbol{v}_i \overset{\text{kom. } \mathbb{R}}{=} \boldsymbol{v}_i + \boldsymbol{u}_i = (\boldsymbol{v} + \boldsymbol{u})_i\,, \qquad \forall i = 1, \dots, n.$$

Tento důkaz ilustruje **obecný princip algebry**. Matematické struktury jsou definovány tak, že jsou složeny **z jednodušších struktur spolu s přidanými operacemi a vztahy**. Pochopitelně tento řetěz někdy musí skončit, tedy nějakou základní strukturu musíme přímo popsat. Situace je podobná jako s ruskými panenkami Matrjoška.



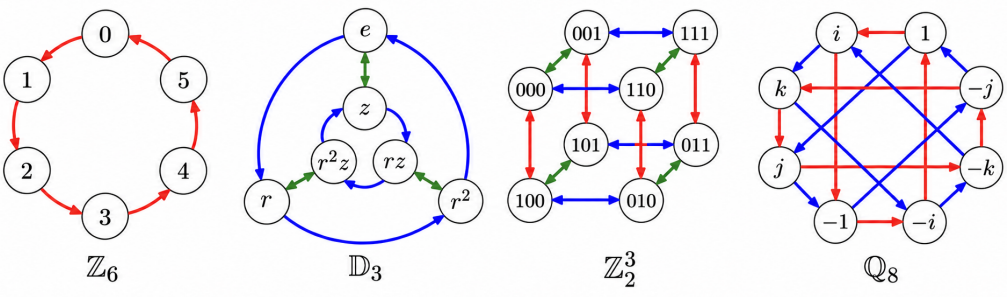
Důležité je, že vlastnosti jednodušších struktur **se přenášejí o hladinu výše** na strukturu, která je obsahuje. Například vektory jsou tvořeny reálnými čísly, které vzniknou z podmnožin racionálních čísel, které vzniknou z dvojic celých čísel, které vzniknou jako dvě kopie přirozených čísel. Tedy to, že sčítání vektorů je komutativní je důsledek toho, že sčítání přirozená čísla je komutativní.

Grupy

Matematická struktura $\mathbb{G}$ spolu s **binární operací** $\circ : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$ se nazývá **grupa**, pokud splňuje následující vlastnosti:

- Platí asociativita: $a \circ (b \circ c) = (a \circ b) \circ c$.
- Existuje neutrální prvek e, že $a \circ e = e \circ a = a$.
- Existují inverzní prvky a^{-1}, že $a \circ a^{-1} = a^{-1} \circ a = e$.

Čísla typicky tvoří grupu, například $\mathbb{Z}$ je grupa pro sčítání. Struktura $\mathbb{Z}_n$ tvořená prvky $\{0, 1, \dots, n-1\}$, s operací sčítání **modulo** n je grupa. Tyto grupy jsou však značně speciální, typická grupa je nekomutativní.



Cayley vymyslel v 1878 způsob, jak vizualizovat grupy pomocí diagramů. Vrcholy jsou **jednotlivé prvky** grupy $\mathbb{G}$. Hrany popisují **množinu generátorů** $g_1, \dots, g_k$, pro kterou

$$\langle g_1, \dots, g_k \rangle = \mathbb{G}.$$

Jednotlivým generátorům přiřadíme barvy a i-tou barvou **nakreslíme šipky z x do $g_i \circ x$**. Tím je zachycena struktura celé grupy a je to mnohem přehlednější než popisovat binární operaci $\circ$ tabulkou.

Grupy vlevo jsou **komutativní**: grupa sčítání modulo 6 a grupa binárních vektorů. Grupy vpravo však **komutativní nejsou**, například pro $\mathbb{D}_3$ je modrá šipka následovaná zelenou něco jiného než naopak. Grupa $\mathbb{D}_3$ je grupa **symetrických transformací rovnostranného trojúhelníka**, kde operace $\circ$ je skládání. Grupa $\mathbb{Q}_8$ je grupa imaginárních jednotek kvaternionů (zobecnění komplexních čísel) a operace popisuje jejich násobení.

Algebraická tělesa

I když jsme skoro celou lineární algebru popisovali nad reálnými čísly $\mathbb{R}$. Avšak celou řadu speciálních vlastností $\mathbb{R}$ jsme nikdy nepoužili. Například pro řešení soustavy lineárních rovnic Gaussovou eliminací nepotřebujeme vědět, že existují odmocniny nebo limity Cauchyovských posloupností. Můžeme proto místo $\mathbb{R}$ použít libovolnou matematickou strukturu čísel zvanou **algebraické těleso**, která splňuje několik pravidel.

Definice algebraického tělesa. Matematická struktura $\mathbb{T}$ spolu s dvěma **binárními operacemi** sčítání $+ : \mathbb{T} \times \mathbb{T} \to \mathbb{T}$ a násobení $* : \mathbb{T} \times \mathbb{T} \to \mathbb{T}$ se nazývá **těleso**, pokud splňuje následující vlastnosti:

- $\mathbb{T}$ je vzhledem k operaci sčítání **komutativní grupa** a označme 0 její neutrální prvek.
- $\mathbb{T} \setminus \{0\}$ je **komutativní grupa** vzhledem k operaci násobení, jejíž neutrální prvek označme 1.
- Platí distributivita: $a * (b + c) = a * b + a * c$.

Tedy těleso jsou dvě grupy svázané distributivitou.

Příklady těles. Vyjma $\mathbb{R}$ jsou standardní příklady nekonečných těles komplexní čísla $\mathbb{C}$ a racionální čísla $\mathbb{Q}$. Existují i konečná tělesa, která jsou dokonce přesně charakterizovaná.

Zobecnění vektorových prostorů. Ve většině diagramu se uvažují vektorové prostory nad tělesem reálných čísel $\mathbb{R}$, tedy prostory $\mathbb{R}^n$. Je však možné uvažovat prostory nad libovolným tělesem $\mathbb{T}$. V konkrétní definici dostáváme prostory $\mathbb{T}^n$, v abstraktní defici jsou skaláry z $\mathbb{T}$ místo $\mathbb{R}$. Také matice se uvažují nad tělesem $\mathbb{T}$ jako $\mathbb{T}^{m \times n}$. Například v informatice je užitečný prostor binárních vektorů $\mathbb{Z}_2^n$.

Velká část výsledků lineární algebry popisovaných v tomto diagramu **funguje bez jakékoliv změny** pro vektorové prostory nad obecnými tělesy $\mathbb{T}$. V následujících částech jsou odlišnosti:

- Nemusí platit nezávislost fundamentálních podprostorů, jediný možný důkaz musí využívat ortogonalitu. Například matice $A = (1, 1)$ nad $\mathbb{Z}_2$ má $R(A) = \mathrm{Ker}(A)$.
- Standardní skalární součin lze uvažovat, ale nemusí splňovat pozitivní definitnost.
- Norma proto nedává smysl a ortogonalita se chová velice odlišně: nenulový vektor může být kolmý sám k sobě, například $(1, 1)$ nad $\mathbb{Z}_2$.
- Vlastní čísla nemusí existovat, protože polynom nad jiným tělesem než $\mathbb{C}$ nemusí mít kořeny.
- Definitnost matic nedává smysl, protože nad tělesem nemusí existovat uspořádání.

Konečná tělesa

Konečné těleso je tvořeno **konečně mnoha prvky** a nazývá se Galoisovo těleso, značeno GF(n) pro n prvků. S konečnými tělesy se dobře pracuje v počítačích a mají třeba řadu aplikací v kryptografii a teorii kódování.

Nejjednodušší příklady těles jsou prvočíselné velikosti:

Tvrzení: Struktura $\mathbb{Z}_n$ je tvořena prvky $\{0, 1, \dots, n-1\}$, s operacemi sčítání a násobení definovanými **modulo** n. Struktura $\mathbb{Z}_n$ je **těleso**, právě když n **je prvočíslo** p.

Důkaz: Pokud n není prvočíslo, je snadné ukázat, že neexistují inverzní prvky pro násobení. Existují $1 < a, b < n$ takové, že $a * b = n$. Tedy $a * b = 0$ v $\mathbb{Z}_n$, což není v tělese možné.

Obtížnější je dokázat, že existují inverzní prvky pro násobení v $\mathbb{Z}_p$. Stačí ukázat, že násobení k je bijekce na $\mathbb{Z}_p$.

Složitější konečná tělesa však existují i pro jiné velikosti, například GF(4).

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

$\mathbb{GF}(4)$

Věta: Každé konečné těleso je řádu p^k, kde p je nějaké prvočíslo a k je přirozené číslo. Navíc pro každé p^k těleso vždy existuje a je určené jednoznačně až na izomorfismus, tedy značení GF(p^k) dává smysl.

Náznak důkazu: Mějme konečné těleso $\mathbb{T}$, chceme dokázat, že jeho velikost je p^k. **Charakteristika** $\mathbb{T}$ je nejmenší počet jedniček, který se sečte na nulu, a vždy je to prvočíslo p. Tyto součty jedniček tvoří podtěleso izomorfní $\mathbb{Z}_p$. Hlavní trik je, že $\mathbb{T}$ tvoří **vektorový prostor** nad tělesem $\mathbb{Z}_p$. Ten má nějakou dimenzi k, a proto obsahuje p^k prvků.

Jednoznačnost tělesa velikosti p^k vyplývá z **věty o izomorfismu**. Konstrukce takového tělesa je složitější a postupuje se přes okruhy polynomů a jejich rozkladová tělesa, detaily vynecháme.

Vektorové prostory

Jeden z pohledů na lineární algebru je ten, že je to studium vektorových prostorů a jejich transformací (lineární zobrazení). Vektorové prostory jsou proto jedny z nejzákladnějších struktur v matematice. Jsou tvořené body, které se nazývají **vektory**, a tyto vektory umíme aplikovat dvě operace: sčítání a násobení skalárem.

Jsou **dva možné přístupy**, jak lze vektorový prostor definovat. (A ty obecně odpovídají dvěma rozdílným přístupům, jak lze v matematice popisovat objekty.) První je konstrukcí, kdy **přesně specifikujeme**, co jsou vektory a jak se na ně aplikují operace. Druhý abstraktní postup je přes **popis vlastností**. Řekneme, že vektorový prostor je tvořen nějakou množinou vektorů spolu s operacemi, které splňují daný seznam vlastností.

Jsou dva možné způsoby, jak lze definovat vektorový prostor.

Konkrétní konstrukce: Vektorový prostor $\mathbb{R}^n$ je tvořen n-ticemi $\boldsymbol{x} = (x_1, \dots, x_n)$, zvanými **vektory**, spolu s operacemi sčítání a násobení skalárem definovaných po složkách:

- $\boldsymbol{x} + \boldsymbol{y} = (x_1 + y_1, \dots, x_n + y_n)$.
- $c \cdot \boldsymbol{x} = (c \cdot x_1, \dots, c \cdot x_n)$.

Abstraktní definice: Vektorový prostor je tvořen nějakou množinou prvků, kterým se říká **vektory**, spolu s operacemi sčítání $+$ a násobení skalárem $\cdot$, které splňují následující vlastnosti:

- Komutativita $+$: $\boldsymbol{u} + \boldsymbol{v} = \boldsymbol{v} + \boldsymbol{u}$.
- Asociativita $+$: $\boldsymbol{u} + (\boldsymbol{v} + \boldsymbol{w}) = (\boldsymbol{u} + \boldsymbol{v}) + \boldsymbol{w}$.
- Neutrální prvek $+$: Existuje vektor 0 takový, že $\boldsymbol{u} + 0 = \boldsymbol{u}$ pro každý vektor $\boldsymbol{u}$.
- Inverzní prvky $+$: Pro každý vektor $\boldsymbol{u}$ existuje vektor $-\boldsymbol{u}$ takový, že $\boldsymbol{u} + (-\boldsymbol{u}) = 0$.
- Asociativita $\cdot$: $(a \cdot b) \cdot \boldsymbol{u} = a \cdot (b \cdot \boldsymbol{u})$.
- Neutrální prvek $\cdot$: $1 \cdot \boldsymbol{u} = \boldsymbol{u}$.
- První distributivita: $(a + b) \cdot \boldsymbol{u} = a \cdot \boldsymbol{u} + b \cdot \boldsymbol{u}$.
- Druhá distributivita: $a \cdot (\boldsymbol{u} + \boldsymbol{v}) = a \cdot \boldsymbol{u} + a \cdot \boldsymbol{v}$.

Vektorové podprostory

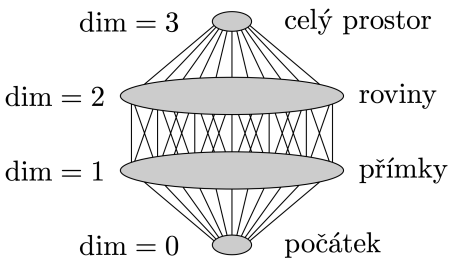
Vektorový podprostor W je **neprázdná množina vektorů uzavřená na operace**. To přesně znamená, že kdykoliv $\mathbf{u}$ a $\mathbf{v}$ patří do W, patří tam také $\boldsymbol{u} + \boldsymbol{v}$ a $c \cdot \boldsymbol{u}$ pro libovolné c. Speciálně počátek 0 vždy patří do W.

Studovat vektorové podprostory je užitečné ze dvou důvodů:

- Mají **speciální strukturální vlastnosti**, například sami o sobě tvoří vektorový prostor.
- Setkáváme se s nimi v lineární algebře na **každém rohu**.

Geometricky jsou vektorové podprostory $\mathbb{R}^n$přímky, roviny a jejich vícerozměrná zobecnění procházející počátkem.

Uvažme **všechny vektorové podprostory uspořádané inkluzí**. Například pro $\mathbb{R}^3$ získáme níže uvedený Hasseho diagram:



Vidíme, že podprostory jsou rozděleny **do vrstev podle dimenze**.

Tvrzení: Vektorové podprostory P tvoří **úplný svaz**, což znamená, že pro libovolnou podmnožinu vektorových prostorů S existuje **infimum** a **supremum**. Infimum je průnik všech podprostorů v S, kde průnik

přes prázdnou podmnožinu je celý prostor. Supremum se definuje jako infimum všech podprostorů, které obsahují všechny podprostory v S, tedy jako jejich průnik.

$$\inf(S) = \bigcap_{X \in S} X \qquad \text{a} \qquad \sup(S) = \bigcap_{W \in P, S \subseteq W} W.$$

Pokud vám definice suprema pomocí infima připadá podivná, rozmyslete si, že obecně **stačí ukázat existenci pouze infim, nebo pouze suprem**, existence toho druhého automaticky vyplývá.

Afinní podprostory

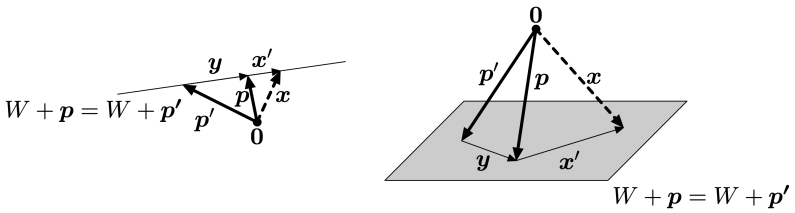
Afinní podprostory jsou **zobecněním vektorových podprostorů**. Afinní podprostor $W + \boldsymbol{p}$ vznikne z vektorového podprostoru W posunutím z počátku o vektor $\boldsymbol{p}$:

$$W + \boldsymbol{p} = \{\boldsymbol{x} + \boldsymbol{p} \mid \boldsymbol{x} \in W\}.$$

Navíc uvažujeme i **prázdnou množinu** jako afinní podprostor. Například afinní podprostory $\mathbb{R}^3$ jsou prázdná množina, všechny body, všechny přímky, všechny roviny a celý prostor.

Tvrzení: Platí, že $W + \boldsymbol{p} = W + \boldsymbol{q}$, právě když $\boldsymbol{p} - \boldsymbol{q} \in W$.

Důkaz:



Navíc $W + 0 = W$, tedy $W + \boldsymbol{p} = W$, právě když $\boldsymbol{p} \in W$.

Afinní podprostory jsou **velice zajímavé strukturálně**, více informací u faktorprostorů.

Lineární kombinace

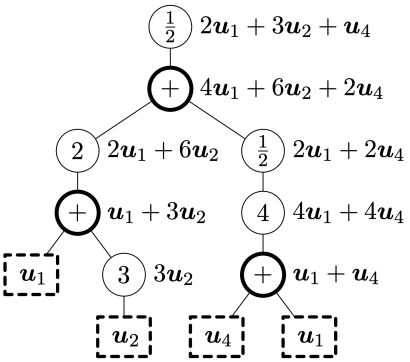
Výraz $c_1\boldsymbol{x}_1 + \cdots + c_n\boldsymbol{x}_n$ se nazývá **lineární kombinace** vektorů $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$.

Zároveň se výsledný vektor nazývá lineární kombinace.

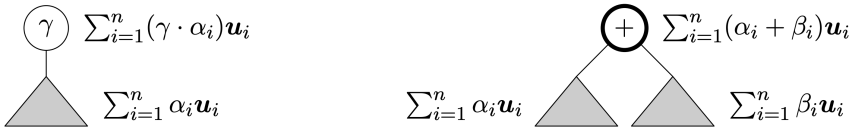
Motivace pro studium lineárních kombinací je, že to jsou univerzální operace s vektory:

Tvrzení: Libovolná konečná posloupnost operací je ekvivalentní nějaké lineární kombinaci.

$$o'(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4, \boldsymbol{u}_5) = \frac{1}{2}\left(2\left(\boldsymbol{u}_1 + 3\boldsymbol{u}_2\right) + \frac{1}{2}\left(4\left(\boldsymbol{u}_4 + \boldsymbol{u}_1\right)\right)\right)$$

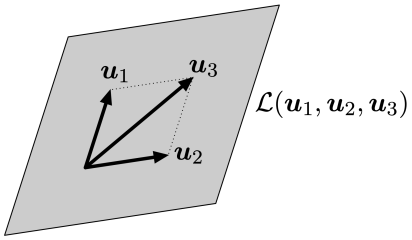


Důkaz: Indukcí podle stromu posloupnosti operací:



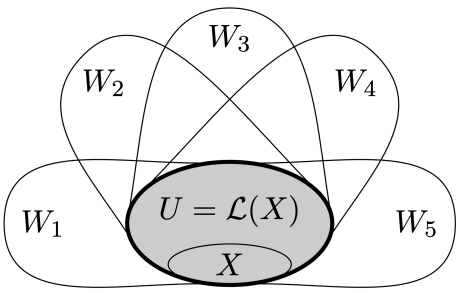
Lineární obal a generátory

Lineární obal $\langle X \rangle$ množiny vektorů X je **množina všech lineárních kombinací** vektorů z X. Podle lemmatu jsou to všechny vektory, které lze získat z X aplikováním konečných posloupností operací. Lineární obal se někdy také značí $L(X)$ nebo $\operatorname{span}(X)$. Říkáme, že X **generuje** $\langle X \rangle$.



Pozorování: Lineární obal $\langle X \rangle$ je **vektorový podprostor**.

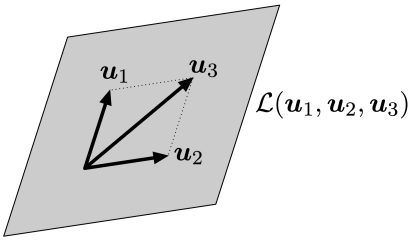
Tvrzení: Lineární obal $\langle X \rangle$ je **nejmenší vektorový podprostor**, který obsahuje všechny vektory z X, což je infimum ve svazu podprostorů. Tedy $\langle X \rangle$ je průnik přes všechny vektorové podprostory, které obsahují X.



Lineární (ne)závislost

Vektor $\boldsymbol{u}$ je v množině X **nadbytečný**, pokud $\langle X \setminus \{\boldsymbol{u}\}\rangle = \langle X\rangle$. Nadbytečné vektory můžeme z množiny postupně odebírat a nezmění se její lineární obal. Motivace je, že chceme lineární obal $\langle X\rangle$ popsat pomocí **co nejmenší množiny vektorů**.

Uvažme rovinu vzniklou jako lineární obal tří vektorů. Libovolný z nich je nadbytečný, jeho odebráním se obal nezmění. Po odebrání nejsou již zbývající dva vektory nadbytečné.



Povšimněme si, že počátek 0 je vždy nadbytečný.

Množina vektorů X je **lineárně závislá**, pokud obsahuje nadbytečný vektor, a **lineárně nezávislá** jinak.

Tvrzení: Následující definice lineární závislosti $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ jsou ekvivalentní:

1. Obsahuje **nadbytečný vektor**.
2. Existuje vektor $\boldsymbol{x}_i$, který je **lineární kombinací zbývajících**.
3. Existuje **netriviální lineární kombinace nuly**: $0 = c_1\boldsymbol{x}_1 + \dots + c_n\boldsymbol{x}_n$, že alespoň jeden z koeficientů c_i je nenulový.
4. Existuje vektor v lineárním obalu, který lze vyjádřit jako **dvě různé lineární kombinace**.

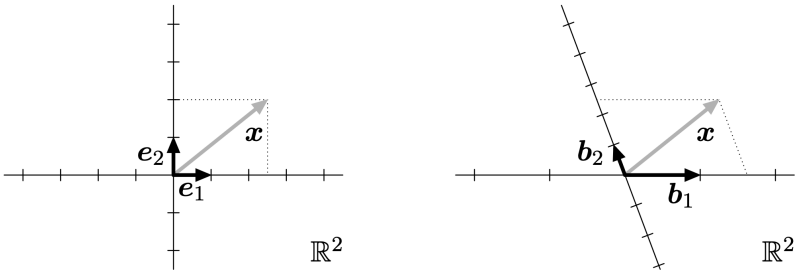
Báze

Množina vektorů se nazývá **báze**, pokud je **lineárně nezávislá** a **generuje celý prostor**. Chceme tedy co nejméně vektorů, které umožnují popsat vektorový prostor. Podobně můžeme báze uvažovat i pro libovolný vektorový podprostor.

Každá báze $\boldsymbol{b}_1, \dots, \boldsymbol{b}_n$ definuje **systém souřadnic nad vektorovým prostorem**:

Pokud $\boldsymbol{x} = c_1\boldsymbol{b}_1 + \dots + c_n\boldsymbol{b}_n$, jsou jeho **souřadnice** $(c_1, \dots, c_n)$.

Různé báze definují různé systémy souřadnic. Například pro kanonickou bázi vlevo jsou souřadnice vektoru $\boldsymbol{x}$ rovny $(5/2, 2)$, zatímco pro bázi vpravo jsou $(8/5, 5/2)$.



Následující vlastnost vyplývá z lineární nezávislosti báze:

Tvrzení: Pro každý vektor $\boldsymbol{x}$ jsou jeho **souřadnice určené jednoznačně**.

Konstrukce báze

Celá teorie bází by byla nezajímavá, pokud by žádná báze neexistovala. Dokážeme si s následujícím předpokladem, že **báze vždycky existuje** (a dokonce je spousta způsobů, jak je zvolit).

Předpoklad: Vektorový prostor má **konečnou dimenzi**, tedy libovolná báze má **konečnou velikost**. (Dokonce podle Steinitzovy věty by stačilo, že existuje báze konečné velikosti.)

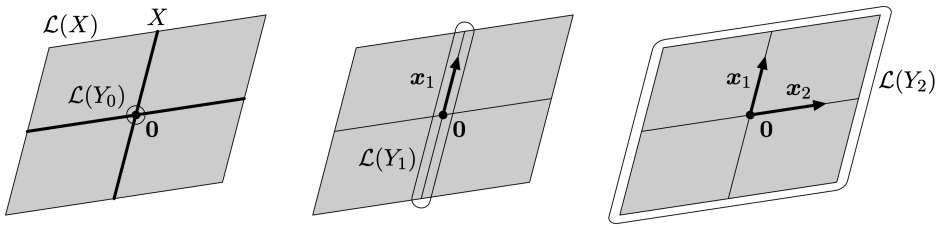
Bez předpokladu bychom museli uvažovat i **nekonečně dimenzionální vektorové prostory** (třeba prostory funkcí nebo posloupností), pro než jsou potřeba **nekonečné báze**. Myšlenkově to funguje totožně, ale je s tím řada technických problémů, například musíme uvažovat nekonečné lineární kombinace.

Nefungující nápad: odebírání z generátoru. Začneme s libovolným generátorem vektorového prostoru (například celým vektorovým prostorem U) a budeme z něj postupně odebírat nadbytečné vektory. Skončíme s lineárně nezávislým generátorem, neboli bází.

Problém je, že typicky bude generátor nekonečný i v konečně dimenzionálním vektorovém prostoru. Odebíráme nekonečně mnoho vektorů, navíc můžeme skončit s prázdnou množinou (problém nekonečna). Například v $\mathbb{R}$ postupně odebereme všechny vektory přímky, protože každý bude nadbytečný vůči zbývajícím.

Fungující nápad: přidávání vektorů. Půjdeme na to proto obráceně, začneme s prázdnou množinou a budeme do ní postupně přidávat vektory při zachování lineární nezávislosti.

Nechť $Y_0 = \emptyset$ a Y_k je zkonstruovaná nezávislá množina s k vektory. Skončíme, pokud $\langle Y_k \rangle$ je celý prostor U. Jinak zvolíme libovolný vektor $\boldsymbol{y}_{k+1} \in U \setminus \langle Y_k \rangle$ a pokračujeme dál. Postup skončí po konečně mnoha krocích kvůli předpokladu a zkonstruuje bázi U.



Lemma o výměně

Jednodušší verze Steinitzovy věty. Říká, že je možné nahradit jeden vektor množiny za libovolný nenulový vektor z jejího lineárního obalu.

Lemma: Nechť X je **libovolná množina** vektorů a $\boldsymbol{y} \neq 0$ patří do $\langle X \rangle$. Potom existuje $\boldsymbol{z} \in X$ takové, že

$$\big\langle X \setminus \{\boldsymbol{z}\} \cup \{\boldsymbol{y}\} \big\rangle = \langle X \rangle.$$

Důkaz: Protože $\boldsymbol{y}$ patří do $\langle X \rangle$, platí následující:

$$\boldsymbol{y} = \alpha_1 \boldsymbol{x}_1 + \alpha_2 \boldsymbol{x}_2 + \cdots + \alpha_n \boldsymbol{x}_n.$$

Proto $\langle X \rangle = \big\langle X \cup \{\boldsymbol{y}\} \big\rangle \supseteq \big\langle X \setminus \{\boldsymbol{z}\} \cup \{\boldsymbol{y}\} \big\rangle$.

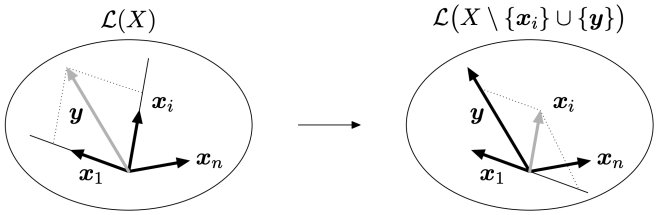
Pro druhou inkluzi zvolíme jako $\boldsymbol{z}$ libovolný vektor $\boldsymbol{x}_i$, jehož $\alpha_i \neq 0$. Snadnou úpravou ukážeme, že $\boldsymbol{x}_i$ lze vyjádřit pomocí ostatních $\boldsymbol{x}_j$ a $\boldsymbol{y}$:

$$\begin{aligned} \boldsymbol{x}_i &= \frac{\boldsymbol{y} - \alpha_1 \boldsymbol{x}_1 - \cdots - \alpha_{i-1} \boldsymbol{x}_{i-1} - \alpha_{i+1} \boldsymbol{x}_{i+1} - \cdots - \alpha_n \boldsymbol{x}_n}{\alpha_i} = \\ &= \frac{1}{\alpha_i} \boldsymbol{y} - \frac{\alpha_1}{\alpha_i} \boldsymbol{x}_1 - \cdots - \frac{\alpha_{i-1}}{\alpha_i} \boldsymbol{x}_{i-1} - \frac{\alpha_{i+1}}{\alpha_i} \boldsymbol{x}_{i+1} - \cdots - \frac{\alpha_n}{\alpha_i} \boldsymbol{x}_n. \end{aligned}$$

Tedy

$$\langle X \rangle \subseteq \big\langle X \setminus \{\boldsymbol{x}_i\} \cup \{\boldsymbol{y}\} \big\rangle$$

.



Steinitzova věta o výměně

Věta: Nechť X je **libovolná množina** vektorů a Y je **lineárně nezávislá množina** vektorů z $\langle X \rangle$. Potom **existuje** $Z \subseteq X$, že $|Z| = |Y|$ taková, že

$$\langle X \setminus Z \cup Y \rangle = \langle X \rangle.$$

Tato věta má řadu zajímavých důsledků:

- Vektorový prostor **obsahuje spoustu bází** a na jejich vektorech není nic speciálního.
- Libovolnou lineárně nezávislou množinu **lze rozšířit** na bázi.
- Vždy platí, že $|X| \geq |Y|$. Proto každá lineárně nezávislá množina má velikost menší či rovnou libovolnému generátoru, a **všechny báze jsou stejně velké**.

Důkaz: Nechť $Y = \{\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n\}$. Postupně vkládáme vektory Y jeden za druhým do X za pomocí lemmatu o výměně. Problém by však mohl být, že při vložení $\boldsymbol{y}_i$ by lemma mohlo vyjmout předtím vložené $\boldsymbol{y}_j$.

Uvědomme si však, že **v lemmatu o výměně můžeme zvolit** jako z libovolné x_k takové, že koeficient $\alpha_k \neq 0$. Proto vždy při vkládání y_i vyjmeme některý z vektorů X. Pokud by to nebylo možné, dostáváme, že y_i je lineární kombinace ostatních vektorů z Y, což je spor s **lineární nezávislostí** Y.

Dimenze

Dimenze vektorového prostoru či jeho podprostoru je velikost libovolné jeho báze. Pro vektorový prostor V se dimenze značí $\dim(V)$.

To, že je dimenze **dobře definována**, vyplývá ze Steinitzovy věty o výměně. Mějme dvě libovolné báze X a Y. Můžeme vektory báze X vyměnit za vektory báze Y a naopak, proto musí mít stejně prvků.

Pozorování: Pokud U je podprostor V, potom $\dim(U) \leq \dim(V)$.

Motivace pro různé báze

Je přirozené se ptát, proč chceme uvažovat různé báze a nevystačíme si s přirozenou kanonickou bází:

- Pro $\mathbb{R}^n$ je přirozené uvažovat **kanonickou bázi**, protože má speciální roli z pohledu složek vektorů (proto se nazývá kanonická). Avšak pro abstaktní vektorový prostor V žádná přirozená kanonická báze neexistuje. Bází je spousta a není žádná speciální, kterou bychom chtěli vždy zvolit. Tedy je lepší pracovat s **teorii obecných bází**.
- Řada problémů se **mnohem zjednodušší při vhodné volbě báze**. Lineární zobrazení je reprezentováno různými maticemi pro různé volby bází. Jedna z klíčových otázek lineární algebry je, jakou bázi zvolit, aby byla reprezentující matice co nejjednodušší, což vede na vlastní čísla a třeba dekompozici podle singulárních hodnot SVD. Další příklad je Lagrangeova interpolace.
- Často hledáme **vhodnou bázi**, která je co nejlepší k popisu dané situace. Například ve statistice můžeme mít data jako vektory v hodně rozměrném prostoru. Hledáme bázi, ve které by bylo možné popsat data co nejjednodušším způsobem, například by se mohlo stát, že skoro všechna leží v nějaké rovině či podprostoru malé dimenze. (I když typicky kvůli chybám měření to nevyjde přesně tak, ale s tím se umí lineární algebra vypořádat přes SVD.) Skvělá metafora jsou **procesy se skrytou bází** i mimo lineární algebru. To jsou procesy, které jsou na první pohled strašně složité, dokud se neobjeví vhodná **skrytá báze**, ve které je jejich popis strašně jednoduchý. Třeba pohyb planet je jednoduchý z pohledu univerzální gravitace.

Fibonacciho čísla je posloupnost definovaná následující rekurencí:

$$f_0 = 0, \quad f_1 = 1, \quad f_{n+2} = f_{n+1} + f_n.$$

Posloupnost je to zajímavá a splňuje řadu pěkných matematických vlastností. S pomocí volby vhodné báze nalezneme následující vzorec pro n-té Fibonacciho číslo:

$$f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Uvažme prostor všech fibonacciovských posloupností, což jsou posloupnosti splňující rekurenci s libovolnými hodnotami prvních dvou členů (a_0, a_1). Ty tvoří vektorový prostor dimenze dva.

Pro ten chceme najít bázi tvořenou posloupnostmi, pro které bude jednoduchý vzorec pro n-tý člen: $a_n = x^n$ pro nějaké reálné číslo x. Protože taková posloupnost musí splňovat rekurenci, platí $x^{n+2} = x^{n+1} + x^n$, neboli $x^2 = x + 1$. Řešením jsou dvě fibonacciovské posloupnosti tvořící bázi prostoru:

$$a_n = \left(\frac{1+\sqrt{5}}{2}\right)^n, \qquad b_n = \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

K získání vzorce zbývá dopočítat souřadnice vektoru $f_n = (0, 1) = \alpha a_n + \beta b_n$:

$$\begin{aligned} \alpha &+ \beta &&= 0, \\ \frac{1+\sqrt{5}}{2}\alpha &+ \frac{1-\sqrt{5}}{2}\beta &&= 1. \end{aligned}$$

Výsledek je $\alpha = 1/\sqrt{5}$ a $\beta = -1/\sqrt{5}$.

Faktorprostory

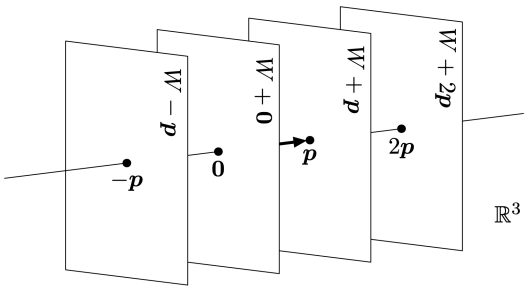
Afinní podprostory jsou zajímavé strukturálně.

Tvrzení: Množina všech afinní podprostorů vzniklých posunutím W tvoří vektorový prostor.

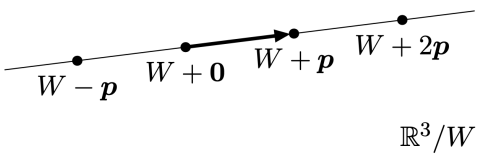
Důkaz: Stačí definovat vektorové operace:

- sčítání: $(W + \boldsymbol{p}) + (W + \boldsymbol{q}) = W + (\boldsymbol{p} + \boldsymbol{q})$.
- násobení: $c \cdot (W + \boldsymbol{p}) = W + c\boldsymbol{p}$.

Rozmyslete si, že splňují definice vektorového prostoru.



Tyto vektorové prostory jsou důležité a říká se jim **faktorprostory**. Nechť V je vektorový prostor a W je jeho podprostor. Vektorový prostor všech afinních podprostorů vzniklých posunutím W se značí V/W a nazývá se **faktorprostor** nebo také **kvocient**.



Faktorprostor V/W si můžeme představit tak, že **ve V „splácneme“ každý afinní podprostor vzniklý posunutím W do jednoho vektoru**.

Tvrzení: Platí, že $\dim(W) + \dim(V/W) = \dim(V)$.

Interpolace polynomů

Soustavami lineárních rovnic lze rešit problém, který s nimi na první pohled vůbec nesouvisí. Uvažme polynomy

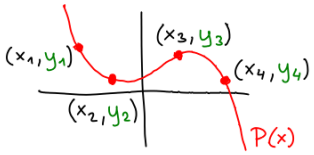
$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

stupně n. Platí následující algebraická věta, úzce související s fundamentální větou algebry.

Věta: Existuje **právě jeden polynom** $P(x)$ **stupně** n, který prochází libovolnými $n+1$ body

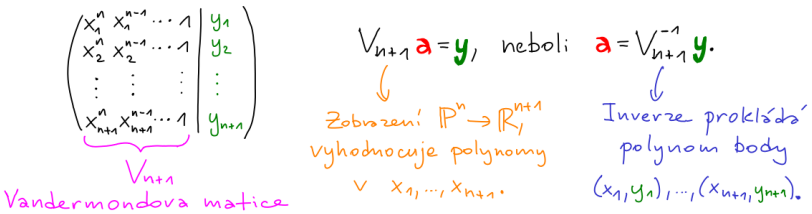
$$(x_1, y_1), \ldots, (x_{n+1}, y_{n+1}),$$

kde $x_i \neq x_j$ pro $i \neq j$, tedy $P(x_i) = y_i$.



Hledání koeficientů tohoto polynomu se nazývá **interpolace polynomů** a je možné to udělat vyřešením **soustavy lineárních rovnic**.

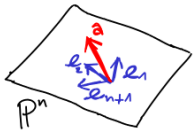
K nalezení koeficientů **stačí vyřešit následující soustavu**, kde $\boldsymbol{y} = (y_1, \ldots, y_{n+1})$ a vektor $\boldsymbol{a}$ je vektor hledaných koeficientů polynomu $P(x)$.



Větu o jednoznačnosti interpolace je možné dokázat pomocí lineární algebry. Stačí dokázat, že **Vandermondova matice** V_{n+1} **je regulární**, právě když $x_i \neq x_j$ pro $i \neq j$. Jiný důkaz vyplývá z **Lagrangeovy interpolace**.

Lagrangeova interpolace

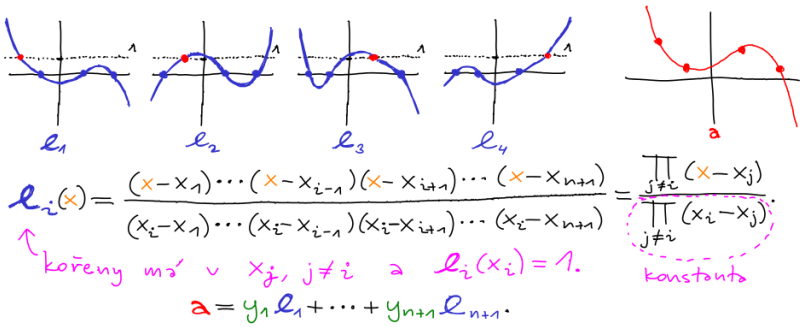
K vyřešení interpolace chceme najít **vektor koeficientů** $\boldsymbol{a}$ na prostoru polynomů $\mathbb{P}_n$ stupně nejvýše n. Najít jeho **souřadnice vůči kanonické bázi je obtížné** a vede to řešení soustavy



$$V_{n+1}\boldsymbol{a} = \boldsymbol{y}$$

Lagrangeova interpolace je založena na myšlence, že **problém se stane velice jednoduchý při volbě vhodné báze** $\ell_1, \ldots, \ell_{n+1}$.

Bázi $\ell_1, \ldots, \ell_{n+1}$ zvolíme, aby každý z vektorů ℓ_i **interpoloval jeden z bodů** (x_i, y_i). Jejich jednoduchou lineární kombinací získáme hledaný vektor $\boldsymbol{a}$.



Podle **Steinitzovy věty** víme, že $\ell_1, \dots, \ell_{n+1}$ je báze. Její existence **dokazuje větu o jednoznačnosti polynomu** $P(x)$ stupně n procházejícího body $(x_1, y_1), \dots, (x_{n+1}, y_{n+1})$.

Samozřejmě je možné volit i jiné báze. Jedním příkladem je **Newtonova interpolace**, vůči bázi $\boldsymbol{n}_1, \dots, \boldsymbol{n}_{n+1}$. Ta funguje skvěle na přidávání dalších bodů, neboť vektor $\boldsymbol{n}_i$ závisí pouze na bodech $(x_1, y_1), \dots, (x_i, y_i)$.

Matice

Matice

Matice je **tabulka** $m \times n$ **reálných čísel:**

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2,n} \\ a_{3,1} & a_{3,2} & a_{3,3} & \cdots & a_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & a_{m,3} & \cdots & a_{m,n} \end{pmatrix}, \qquad \text{například} \qquad A = \begin{pmatrix} 2 & 1 \\ 0 & -1 \end{pmatrix}.$$

Matice velikosti $m \times n$ popisuje **geometrickou transformaci** vektorového prostoru $\mathbb{R}^n$ do vektorového prostoru $\mathbb{R}^m$.

Pro matici A označme $(A)_{i,j} = a_{i,j}$ koeficient v i-tém řádku a j-tém sloupci. Řádky matice tvoří **řádkové vektory** $\mathbb{R}^n$, sloupce tvoří **sloupcové vektory** $\mathbb{R}^m$.

Základní maticové operace jsou násobení skalárem a sčítání:

$$\alpha A = \begin{pmatrix} \alpha \cdot a_{1,1} & \alpha \cdot a_{1,2} & \alpha \cdot a_{1,3} & \cdots & \alpha \cdot a_{1,n} \\ \alpha \cdot a_{2,1} & \alpha \cdot a_{2,2} & \alpha \cdot a_{2,3} & \cdots & \alpha \cdot a_{2,n} \\ \alpha \cdot a_{3,1} & \alpha \cdot a_{3,2} & \alpha \cdot a_{3,3} & \cdots & \alpha \cdot a_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha \cdot a_{m,1} & \alpha \cdot a_{m,2} & \alpha \cdot a_{m,3} & \cdots & \alpha \cdot a_{m,n} \end{pmatrix}.$$

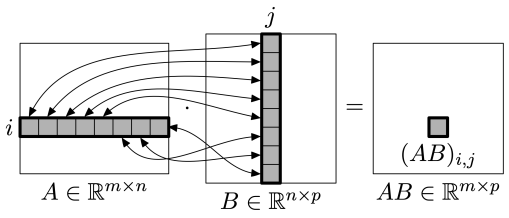
$$A + B = \begin{pmatrix} a_{1,1} + b_{1,1} & a_{1,2} + b_{1,2} & a_{1,3} + b_{1,3} & \cdots & a_{1,n} + b_{1,n} \\ a_{2,1} + b_{2,1} & a_{2,2} + b_{2,2} & a_{2,3} + b_{2,3} & \cdots & a_{2,n} + b_{2,n} \\ a_{3,1} + b_{3,1} & a_{3,2} + b_{3,2} & a_{3,3} + b_{3,3} & \cdots & a_{3,n} + b_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m,1} + b_{m,1} & a_{m,2} + b_{m,2} & a_{m,3} + b_{m,3} & \cdots & a_{m,n} + b_{m,n} \end{pmatrix}.$$

Všechny matice velikosti $m \times n$ proto tvoří **vektorový prostor** $\mathbb{R}^{m \times n}$.

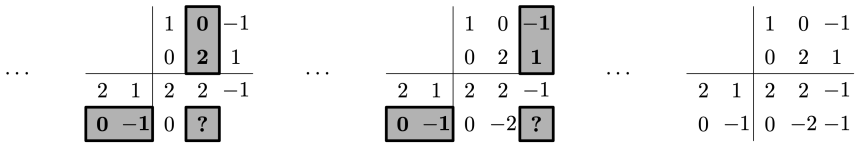
Maticové násobení

Nechť $A \in \mathbb{R}^{m \times n}$ a $B \in \mathbb{R}^{n \times p}$. Potom je **součin** AB matice velikosti $m \times p$ s následujícími koeficienty:

$$(AB)_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,j}, \qquad \forall i = 1, \dots, m,\ j = 1, \dots, p.$$



Příklad maticového součinu: (vlevo A, nahoře B)



Toto je **pohled řádek-sloupec** na maticové násobení. Existují však ještě tři další užitečné pohledy:

- **Pohled sloupec-sloupec:** Nejprve se zaměřme na součin $A\boldsymbol{x}$. (Zde s vektorem pracujeme jako s maticí, co má jeden sloupec.) Podle definice jsou jednotlivé sloupcové vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ matice A násobeny jednotlivými koeficienty vektoru $\boldsymbol{x}$ a sečteny. Tedy dostáváme lineární kombinaci $A\boldsymbol{x} = x_1\boldsymbol{u}_1 + \cdots + x_n\boldsymbol{u}_n$. Matice AB obsahuje jako sloupcové vektory **lineární kombinace sloupcových vektorů A s koeficienty podle sloupcových vektorů B.**
- **Pohled řádek-řádek:** Identický s předchozím, pouze transponovaně, získáváme lineární kombinace řádků B podle koeficientů matice A.
- **Pohled sloupec-řádek:** V definici součinu vždy koeficienty i-tého sloupce matice A násobí pouze koeficienty i-tého řádku matice B. S využitím distributivity lze tedy spárovat sloupce $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ matice A s řádky $\boldsymbol{y}_1^\mathsf{T}, \dots, \boldsymbol{y}_n^\mathsf{T}$ matice B. Dostáváme **následující součet n matic $m \times p$:** $AB = \boldsymbol{x}_1\boldsymbol{y}_1^\mathsf{T} + \cdots + \boldsymbol{x}_n\boldsymbol{y}_n^\mathsf{T}$.

Matice úprav

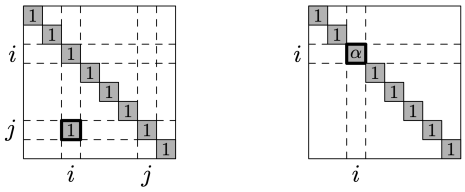
Regulární úpravy odpovídají **regulárním maticím**. Soustava $A\boldsymbol{x} = \boldsymbol{b}$ se upraví na soustavu $RA\boldsymbol{x} = R\boldsymbol{b}$, kde R je nějaká regulární matice.

Tvrzení: Pokud R je regulární matice, je množina řešení $A\boldsymbol{x} = \boldsymbol{b}$ a $RA\boldsymbol{x} = R\boldsymbol{b}$ je **stejná**.

Důkaz: Pokud **x** řeší původní soustavu, určitě také řeší upravenou soustavu. Tedy množina řešení se může každou úpravou pouze zvětšit. Protože je R regulární, existuje inverzní úprava R^{-1}, která **převede upravenou soustavu zpět do původního stavu:**

$R^{-1}RA\boldsymbol{x} = R^{-1}R\boldsymbol{b} \implies A\boldsymbol{x} = \boldsymbol{b}$. Proto musí být **množina řešení stejná**, jinak by se úpravou R^{-1} zmenšila, což není možné.

Regulární matice R elementárních řádkových úprav jsou velice jednoduché. Vlevo je přičtení i-tého řádku k j-tému. Vpravo je vynásobení i-tého řádku koeficientem $\alpha \neq 0$.



Čtenář si může rozmyslet, jak vypadají matice odvozených elementárních úprav: přičtení α-násobku i-tého řádku k j-tému a prohození dvou řádků.

Maticové inverze

Mějme matici A velikosti $m \times n$. Pokud existuje matice A^{-1} velikosti $n \times m$ splňující $AA^{-1} = I_m$, nazývá se A^{-1} **pravá inverze** A. Nemusí být určena jednoznačně. Podobně se definuje **levá inverze** A^{-1}, která splňuje $A^{-1}A = I_n$.

Označme $\boldsymbol{u}_1, \dots, \boldsymbol{u}_m$ sloupce pravé inverze A^{-1}. **Musí splňovat soustavy**

$$A\boldsymbol{u}_i = \boldsymbol{e}_i, \qquad \forall i = 1, \dots, m.$$

Lze nalézt **jednou Gaussovou eliminací** s více pravými stranami.

Například pro

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

vyřešíme soustavu:

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

$$\sim \left(\begin{array}{cc|cc} 1 & 0 & 2/3 & 1/3 \\ 0 & 1 & 1/3 & 2/3 \end{array}\right), \qquad A^{-1} = \begin{pmatrix} 2/3 & 1/3 \\ 1/3 & 2/3 \end{pmatrix}.$$

Uveďme několik tvrzení o existence inverzí, čtenář si může rozmyslet jejich důkazy:

Tvrzení: Pro matici A existuje pravá inverze, právě když má soustava $A\boldsymbol{x} = \boldsymbol{b}$ řešení pro každou pravou stranu $\boldsymbol{b}$. Neboli $\mathrm{Im}(A)$ je celý prostor $\mathbb{R}^m$.

Tvrzení: Nechť A je matice velikosti $m \times n$. Pokud existuje pravá inverze, je $m \leq n$. Pokud existuje levá inverze, je $m \geq n$. Tedy oboustranná inverze může existovat pouze pro čtvercové matice.

Tvrzení: Pro matici A existuje pravá inverze, právě když existuje levá inverze pro matici A^T.

Tvrzení: Matice A velikosti $m \times n$ má pravou inverzi, právě když $\mathrm{rank}(A) = m$, a levou, právě když $\mathrm{rank}(A) = n$. (To vychází z netriviálního faktu, že $\mathrm{rank}(A) = \mathrm{rank}(A^\mathsf{T})$.)

Úprava inverzní maticí: Pokud má matice A levou inverzi, můžeme provést úpravu $A\boldsymbol{x} = \boldsymbol{b}$ na $A^{-1}A\boldsymbol{x} = A^{-1}\boldsymbol{b}$, neboli $\boldsymbol{x} = A^{-1}\boldsymbol{b}$. Nepoužívá se při výpočtech, protože spočítat inverzní matici je složitější než vyřešit soustavu; avšak hodí se v teorii.

Regulární matice

Čtvercová matice se nazývá **regulární**, pokud je invertovatelná. Ostatní čtvercové matice se nazývají **singulární**. O inverzích regulárních matic platí následující věta:

Věta: Pro čtvercovou matici existuje levá inverze, právě když existuje pravá inverze. Navíc jsou stejné a určené jednoznačně.

Těžká je první část, která je speciální případ rovnosti $\operatorname{rank}(A) = \operatorname{rank}(A^\mathsf{T})$. Druhá část snadno vyplývá z asociativity. Pokud X je levá inverze a Y je pravá inverze, platí:

$$X = XI_m = X(AY) = (XA)Y = I_nY = Y.$$

Determinant

Transpozice

Nechť A je matice $m \times n$. Její **transpozice** A^T je matice $n \times m$ s následujícími koeficienty:

$$(A^\mathsf{T})_{i,j} = (A)_{j,i}.$$

Tedy koeficienty matice A^T **vzniknou zrcadlením** koeficientů A podle hlavní diagonály.

Pro matice s **komplexními čísly se transpozice definuje jinak**. Značí se A^H a čísla jsou navíc komplexně sdružená (což odpovídá jinému skalárnímu součinu). Transpozice se často také značí A^* (jak reálná, tak komplexní).

Pro transponované matice platí **následující vztahy**, rozmyslete si jejich důkazy z definice maticových operací:

- $(A^\mathsf{T})^\mathsf{T} = A$.
- $(cA)^\mathsf{T} = cA^\mathsf{T}$.
- $(A + B)^\mathsf{T} = A^\mathsf{T} + B^\mathsf{T}$.
- $(AB)^\mathsf{T} = B^\mathsf{T}A^\mathsf{T}$. Povšimněme si, že pořadí transponovaných matic **musí být obrácené**, aby měl součin **kompatibilní rozměry**. Jak vypadá transpozice obecně pro součin více matic?
- Pokud je A regulární matice, pak $(A^{-1})^\mathsf{T} = (A^\mathsf{T})^{-1} = A^{-\mathsf{T}}$.

Hodnost transpozice

Následující věta je jedním z divů lineární algebry. Říká, že pro libovolnou matici A je $\dim \operatorname{Im}(A) = \dim R(A)$, přestože se jedná o zcela jiné prostory.

Věta: Pro libovolnou matici A platí, že $\operatorname{rank}(A) = \operatorname{rank}(A^\mathsf{T})$.

Hodnost matice

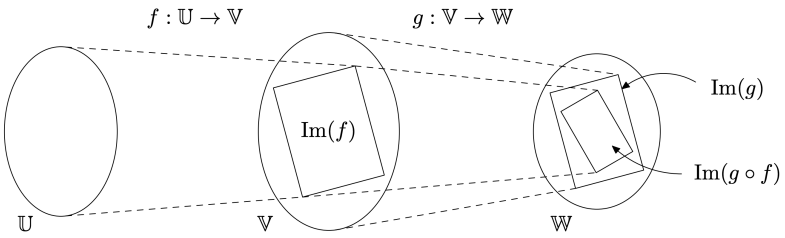
Hodnost matice A se značí $\operatorname{rank}(A)$ a udává, jak moc je matice A blízká regulární matici. Několik ekvivalentních definic $\operatorname{rank}(A)$:

- $\dim \mathrm{Im}(A)$, což je počet lineárně nezávislých sloupců matice a také dimenze obrazu příslušného lineárního zobrazení.
- $\dim R(A)$, neboli počet lineárně nezávislých řádků matice.
- počet nenulových řádků a počet pivotů v odstupňovaném tvaru A.
- nejmenší počet matic hodnosti jedna, jejichž součet je A.

Pro hodnost platí následující horní odhady:

- $\mathrm{rank}(A) \leq \min\{m, n\}$ pro matici A velikosti $m \times n$.
- $\mathrm{rank}(A + B) \leq \mathrm{rank}(A) + \mathrm{rank}(B)$.
- $\mathrm{rank}(AB) \leq \min\{\mathrm{rank}(A), \mathrm{rank}(B)\}$.

Poslední nerovnost má následující důkaz v řeči lineárních zobrazení:



Tvrzení: Násobení regulární maticí zleva/zprava **nemění hodnost**.

Důkaz: Dokažme pro násobení zleva. Podle nerovnosti je

$$\mathrm{rank}(RA) \leq \mathrm{rank}(A).$$

Na druhou stranu, protože R je regulární, $A = R^{-1}RA$. Tedy

$$\mathrm{rank}(A) = \mathrm{rank}(R^{-1}RA) \leq \mathrm{rank}(RA).$$

Fundamentální podprostory

Nechť A je matice $m \times n$ s řádkovými vektory $\boldsymbol{r}_1, \ldots, \boldsymbol{r}_m$ a sloupcovými vektory $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n$. Matice A definuje čtyři **fundamentální podprostory**:

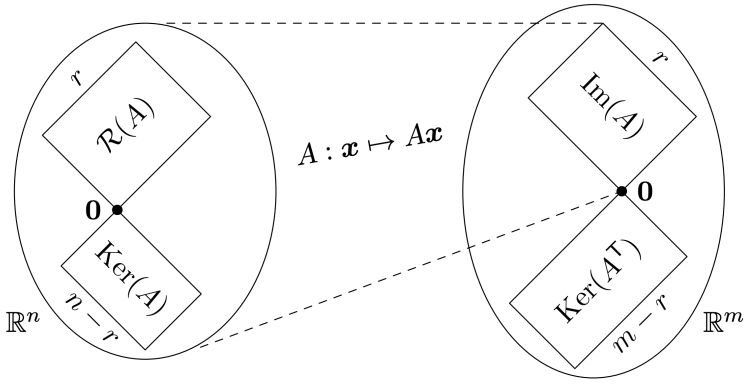
- **Jádro** $\mathrm{Ker}(A) = \{\boldsymbol{x} : A\boldsymbol{x} = 0\}$ (neboli **kernel**).
- **Řádkový prostor** $R(A) = \mathrm{Im}(A^\mathsf{T}) = \langle \boldsymbol{r}_1, \ldots, \boldsymbol{r}_m \rangle = \{A^\mathsf{T}\boldsymbol{x} : \boldsymbol{x} \in \mathbb{R}^m\}$ (neboli **levý obraz**).
- **Levé jádro** $\mathrm{Ker}(A^\mathsf{T}) = \{\boldsymbol{y} : \boldsymbol{y}^\mathsf{T}A = 0\}$ (neboli **levý kernel**).
- **Sloupcový prostor** $S(A) = \mathrm{Im}(A) = \langle \boldsymbol{s}_1, \ldots, \boldsymbol{s}_n \rangle = \{A\boldsymbol{x} : \boldsymbol{x} \in \mathbb{R}^m\}$ (neboli **obraz**).

Povšimněme si, že jádro a řádkový prostor jsou **podprostory** $\mathbb{R}^n$, zatímco levé jádro a sloupcový prostor jsou **podprostory** $\mathbb{R}^m$.

Fundamentální věta lineární algebry:

1. Nechť $r = \mathrm{rank}(A)$. Platí, že $\dim R(A) = \dim \mathrm{Im}(A) = r$, $\dim \mathrm{Ker}(A) = n - r$ a $\dim \mathrm{Ker}(A^\mathsf{T}) = m - r$.

2. $R(A)$ a $\mathrm{Ker}(A)$ jsou **lineárně nezávislé a generují** $\mathbb{R}^n$. Podobně $\mathrm{Im}(A)$ a $\mathrm{Ker}(A^\mathsf{T})$ jsou **lineárně nezávislé a generují** $\mathbb{R}^m$.
3. Navíc jsou $R(A)$ a $\mathrm{Ker}(A)$ **ortogonální doplňky**, tedy každý vektor z $R(A)$ je **kolmý** na každý vektor z $\mathrm{Ker}(A)$. Podobně pro $\mathrm{Im}(A)$ a $\mathrm{Ker}(A^\mathsf{T})$.



Poznamenejme, že vlastnost 1 platí nad obecným algebraickým tělesem. **Vlastnosti 2 a 3 vyžadují** $\mathbb{R}$ (a při drobné změně definic fungují i nad $\mathbb{C}$).

Speciální matice

Některé druhy matic se objevují v lineární algebře často, že se pro ně vyplatí mít **speciální jména**.

Jsou zajímavé ze dvou důvodu:

1. **Vyskytují se často** v lineární algebře a v různých aplikacích.
2. Mají **speciální vlastnosti**, kterých lze využít například při výpočtech či strukturální analýze.

Diagonální matice

Diagonální matice D má všechny koeficienty mimo hlavní diagonálu nulové, tedy $(D)_{i,j} = 0$ pro $i \neq j$. Definice funguje i pro obdelníkové matice.

$$D = \begin{pmatrix} 1 & & \\ & 2 & \\ & & 3 \end{pmatrix}, \qquad D' = \begin{pmatrix} 0 & & \\ & 0 & \\ & & 0 \end{pmatrix}, \qquad D'' = \begin{pmatrix} 3 & & \\ & 0 & \\ & & -4 \end{pmatrix}.$$

Jednotková matice I_n je diagonální matice $n \times n$ s jedničkami na diagonále.

$$I_3 = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}, \qquad I_4 = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}.$$

Pokud reprezentují endomorfismus vůči jedné bázi, odpovídají **natažení souřadních os**. V případě jednotkové matice se jedná o **identitu**.

Tvrzení: Libovolné lineární zobrazení f je reprezentováno vůči vhodným bázím X a Y diagonální maticí, která má na diagonále pouze 1 a 0.

Důkaz: Nechť X_r je libovolná **báze levého obrazu** $\mathrm{Im}(f^*)$ a X_k je libovolná **báze jádra** $\mathrm{Ker}(f)$. Zvolíme $X = X_r \cup X_k$.

Protože f definuje izomorfismus mezi $\mathrm{Im}(f^*)$ a $\mathrm{Im}(f)$, zobrazuje libovolnou bázi $\mathrm{Im}(f^*)$ na bázi $\mathrm{Im}(f)$. Tedy $f(X_r)$ je báze $\mathrm{Im}(f)$, kterou doplníme bází $\mathrm{Ker}(f^*)$ a získáme druhou hledanou bázi Y. Protože $f(X_k) = \{0\}$, je zobrazení f reprezentováno vůči X a Y popsanou diagonální matici.

Tvrzení: Čtvercová matice A komutuje s každou čtvercovou maticí, právě když $A = cI_n$.

Vlastní čísla

Trojúhelníkové matice

Rozlišujeme dva druhy trojúhelníkových matic. Typicky se uvažují čtvercové matice, ale definice funguje i pro obdélníkové.

Dolní trojúhelníková matice L má všechny koeficienty nad hlavní diagonálou nulové. Tedy $(L)_{i,j} = 0$ pro $i < j$.

Horní trojúhelníková matice U má všechny koeficienty pod hlavní diagonálou nulové. Tedy $(U)_{i,j} = 0$ pro $i > j$.

$$L = \begin{pmatrix} 1 & & \\ 2 & 1 & \\ 3 & 2 & 1 \end{pmatrix}, \quad L' = \begin{pmatrix} 4 & & & \\ 0 & 0 & & \\ 0 & 1 & 0 & \\ 1 & 0 & 0 & \frac{1}{2} \end{pmatrix},$$

$$U = \begin{pmatrix} 1 & 2 & 3 \\ & 2 & 3 \\ & & 3 \end{pmatrix}, \quad U' = \begin{pmatrix} -1 & 1 & -1 & 1 \\ & -1 & 1 & -1 \\ & & -1 & 1 \\ & & & -1 \end{pmatrix}.$$

Diagonální matice jsou současně dolní a horní trojúhelníkové.

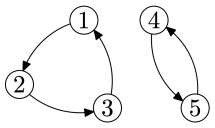
Nechť horní trojúhelníková matice U reprezentuje zobrazení vůči jedné bázi $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$. Protože $U\boldsymbol{b}_i$ leží v $\langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_i \rangle$ (a podobně pro dolní trojúhelníkové matice L), je celá řada problémů s trojúhelníkovými maticemi výrazně jednodušších. Například soustavy $L\boldsymbol{x} = \boldsymbol{b}$ a $U\boldsymbol{x} = \boldsymbol{b}$ lze řešit přímo substitucí. Je také jednoduché najít inverzní matice a určit vlastní čísla (prvky na diagonále).

Čtenář si může rozmyslet následující vlastnosti:

- **Trojúhelníkové matice jsou uzavřené na součin**. Tedy součin dolních trojúhelníkových matic je dolní trojúhelníková matice a podobně pro horní trojúhelníkové matice.
- Trojúhelníková matice je regulární právě tehdy, když jsou **koeficienty na diagonále nenulové**.
- **Trojúhelníkové matice jsou uzavřené na inverze**. Tedy inverzí dolní trojúhelníkové matice je dolní trojúhelníková matice, inverzí horní trojúhelníkové je horní trojúhelníková.
- Přímo z definice si můžeme rozmyslet, že **čtvercová trojúhelníková matice má inverzi z jedné strany, právě když ji má z druhé strany**. To je důležité pro důkaz obecné věty o oboustranné inverzi pomocí LU dekompozice.

Permutační matice

Nechť π je permutace množiny $\{1, \dots, n\}$. Je reprezentována **permutační maticí** P. To je čtvercová matice $n \times n$, jejíž koeficienty jsou nuly a jedničky, a $(P)_{i,j} = 1$, právě když $\pi(j) = i$.



$$P = \begin{pmatrix} & & 1 & & \\ 1 & & & & \\ & 1 & & & \\ & & & & 1 \\ & & & 1 & \end{pmatrix}.$$

Nechť A je libovolná matice, kterou násobíme permutační maticí P.

- Násobení **zleva PA permutuje řádky** A podle π: i-tý řádek se přesune na řádek $\pi(i)$.
- Násobení **zprava AP permutuje sloupce** A podle π^{-1}: i-tý sloupec se přesune na sloupec $\pi^{-1}(i)$.

Nechť P_π značí permutační matici reprezentující π. Čtenář si může rozmyslet a dokázat následující vlastnosti.

Součin permutačních je permutační matice, která reprezentuje složení příslušných permutací. Tedy

$$P_\pi P_\sigma = P_{\pi \circ \sigma}.$$

Každá permutační matice P je **regulární**, dokonce **ortogonální**, tedy existuje **inverzní matice**, která je také permutační. Pro ni platí, že

$$P_\pi^{-1} = P_{\pi^{-1}} = P_\pi^{\mathsf{T}}.$$

Snadné je přímo z definice ověřit, že tato inverze je oboustranná.

Permutační matice tvoří **grupu**. Podle Cayleyho věty je možné libovolnou grupu o n prvcích reprezentovat jako **grupu permutací** $\{1, \dots, n\}$. Proto je možné libovolnou grupu o n prvcích reprezentovat **permutačními maticemi** $n \times n$. To přirozeně vede ke zkoumání pojmu maticových grup.

Blokové matice

Blokové matice jsou tvořené menšími maticemi, které se nazývají **bloky**. Můžeme definovat operace na blokových maticích kompatibilního typu. To umožňuje využívat blokový jazyk k efektivnímu popisu některých věcí.

Nechť A a B jsou dvě blokové matice velikosti $2n \times 2n$, tvořené čtyřmi bloky velikosti $n \times n$.

$$A = \begin{pmatrix} A_{1,1} & A_{1,2} \\ A_{2,1} & A_{2,2} \end{pmatrix}, \qquad B = \begin{pmatrix} B_{1,1} & B_{1,2} \\ B_{2,1} & B_{2,2} \end{pmatrix},$$

Tyto matice lze **sčítat po blocích a násobit po blocích**:

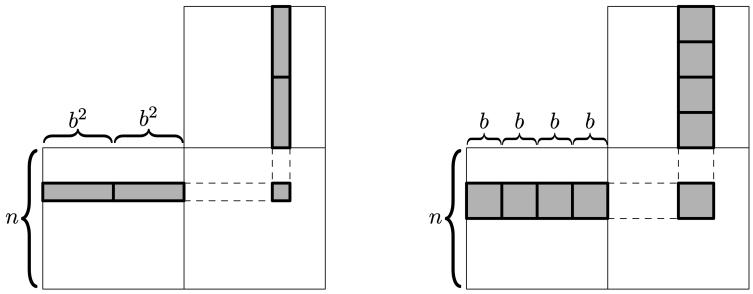
$$AB = \begin{pmatrix} A_{1,1}B_{1,1} + A_{1,2}B_{2,1} & A_{1,1}B_{1,2} + A_{1,2}B_{2,2} \\ A_{2,1}B_{1,1} + A_{2,2}B_{2,1} & A_{2,1}B_{1,2} + A_{2,2}B_{2,2} \end{pmatrix}.$$

Čtenář si může rozmyslet, za jakých podmínek lze definovat operace obecně. Také lze definovat **blokově diagonální matice**, **blokově trojúhelníkové matice**, atd.

Blokové násobení se prakticky využívá při **násobení velkých matic**. Pro ně je potřeba číst koeficienty z paměti (řekněme RAM), která je **mnohem pomalejší než rychlost výpočtů počítače.** Řekněme, že násobíme matice velikosti $n \times n$ a do paměti dokážeme naráz načíst zhruba $2b^2$ koeficientů.

Pokud budeme postupovat podle definice, tak vždy určíme jeden koeficient AB vynásobením koeficientů řádku A a sloupce B. Na to potřebujeme udělat n/b^2 čtení z paměti, tedy **celkem n^3/b^2 součinů**.

Místo toho rozdělíme obě matice na bloky $b \times b$ (pro jednoduchost nechť n je násobek b). Pro výpočet hodnot jednoho bloku AB musíme vynásobit jeden řádek bloků A s jeden sloupcem bloků B. Na to potřebujeme udělat n/b čtení. Bloků AB je n^2/b^2, tedy dohromady děláme **n^3/b^3 čtení, což je b-krát efektivnější**.



Hodnost 1

Matice A má hodnost 1, pokud je nenulová a každý její řádek/sloupec je násobek ostatních. Existuje elegantní zápis

$$A = \boldsymbol{x}\boldsymbol{y}^{\mathsf{T}}$$

kde $\boldsymbol{x}$ a $\boldsymbol{y}$ jsou nenulové vektory.

SVD

LU dekompozice

Věta: Pro libovolnou matici A velikosti $m \times n$ **existuje dekompozice** $PA = LU$, kde

- P je **permutační matice** $m \times m$,
- L je **dolní trojúhelníková matice** $m \times m$ s jednotkovou diagonálou,
- U je **horní trojúhelníková matice** $m \times n$.

Občas se uvažuje symetričtější varianta dekompozice $PA = LDU$, kde obě trojúhelníkové matice L a U mají **jednotkové diagonály** a D je **diagonální matice pivotů**.

Příklad: Nechť A je následující matice:

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

Získáváme následující LU a LDU dekompozice pro $P = I_3$:

$$LU = \begin{pmatrix} 1 & & \\ -\frac{1}{2} & 1 & \\ & -\frac{2}{3} & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 & \\ & \frac{3}{2} & -1 \\ & & \frac{4}{3} \end{pmatrix},$$

$$LDU = \begin{pmatrix} 1 & & \\ -\frac{1}{2} & 1 & \\ & -\frac{2}{3} & 1 \end{pmatrix} \begin{pmatrix} 2 & & \\ & \frac{3}{2} & \\ & & \frac{4}{3} \end{pmatrix} \begin{pmatrix} 1 & -\frac{1}{2} & \\ & 1 & -\frac{2}{3} \\ & & 1 \end{pmatrix}.$$

LU dekompozice je **maticový zápis Gaussovy eliminace** aplikované na A. Význam jednotlivých matic v dekompozici je následující:

- Permutační matice P popisuje **proházení řádků** A tak, aby bylo možné provést **Gaussovu eliminace** PA **bez pivotace**.
- Matice L popisuje **elementární úpravy dopředné eliminace**. Protože jsme proházeli řádky pomocí P, stačí využívat pouze **elementární úpravy přičtení** α**-násobku** i-tého řádku k j-tému, kde $i < j$.
- Matice U je výsledný **odstupňovaný tvar** A, spolu s hodnotami pivotů.

Nechť jsou $R_1, \dots, R_k$ matice techto elementárních úprav, které převedou PA v U. Platí maticová rovnost

$$R_k R_{k-1} \cdots R_2 R_1 PA = U.$$

Matice úprav R_i jsou **dolní trojúhelníkové matice s jednotkovou diagonálou**. Proto je $L = (R_k R_{k-1} \cdots R_2 R_1)^{-1}$ také dolní trojúhelníková matice s jednotkovou diagonálou. Získáváme dekompozici $PA = LU$.

Poznámka: Pokud je matice A **symetrická a lze ji eliminovat bez prohazování řádků**, má její *LDU* dekompozice speciální **symetrickou formu** $A = LDL^\mathsf{T}$.

Symetrické matice

Čtvercová matice A se nazývá **symetrická**, pokud platí $A = A^\mathsf{T}$. Symetrické matice reprezentují endomorfismy, které jsou samy sobě duální.

Symetrické matice mají řadu speciálních vlastností, například jsou uzavřené na součty a inverze.

Normální matice

Matice A se nazývá **normální**, pokud komutuje se svoji transpozicí: $AA^* = A^*A$. Normální matice jsou zobecněním symetrických matic.

Lineární zobrazení

Lineární zobrazení (homomorfismy)

Nechť U a V jsou dva vektorové prostory. **Zobrazení $f\colon U \to V$ je lineární**, pokud splňuje:

$$\begin{aligned} f(\boldsymbol{x}+\boldsymbol{y}) &= f(\boldsymbol{x}) + f(\boldsymbol{y}) \quad && \forall \boldsymbol{x}, \boldsymbol{y} \in U, \\ f(\alpha \boldsymbol{x}) &= \alpha f(\boldsymbol{x}) && \forall \boldsymbol{x} \in U, \alpha \in \mathbb{R}. \end{aligned}$$

Lineární zobrazení f **vnořuje strukturu U do struktury V**. Například pokud platí libovolná rovnost $\boldsymbol{x} + \boldsymbol{y} = \boldsymbol{z}$, platí i pro jejich obrazy: $f(\boldsymbol{x}) + f(\boldsymbol{y}) = f(\boldsymbol{z})$. Poznamenejme, že obrazy rovností mohou být velice triviální.

Lineární zobrazení se nazývají **homomorfismy**. Homomorfismy se uvažují nad obecnými matematickými strukturami a jejich zkoumání je velice důležité. Název se skládá z **homo** (zachovávání struktury) a **morfismus** (transformace jedné struktury v druhou).

Učiňme nejprve pozorování, že pro libovolné lineární zobrazení f platí, že $f(0) = 0$. Obrazem počátku musí být počátek z linearity:

$$f(0) = f(0 \cdot 0) = 0 f(0) = 0.$$

Podobně platí následující:

Tvrzení: Obrazem libovolné lineární kombinace je lineární kombinace obrazů. Proto je **lineární zobrazení jednoznačně určené obrazy libovolné báze**.

Důkaz: Využijeme linearitu:

$$f\left(\sum_{i=1}^{n} \alpha_i \boldsymbol{x}_i\right) = \sum_{i=1}^{n} f(\alpha_i \boldsymbol{x}_i) = \sum_{i=1}^{n} \alpha_i f(\boldsymbol{x}_i).$$

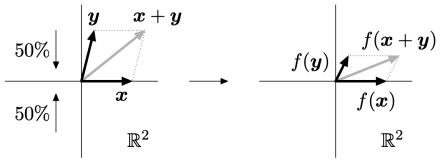
Geometrické příklady $\mathbb{R}^2 \to \mathbb{R}^2$

Řada geometrických zobrazení $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ splňuje linearitu:

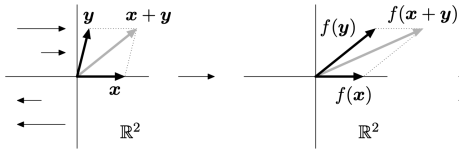
- natažení,
- rotace,
- zkosení,
- projekce a
- jejich kombinace.

Příklad **nelineárního** geometrického zobrazení $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ je posunutí $\mathbb{R}^2$ o libovolný nenulový vektor $\boldsymbol{x}$.

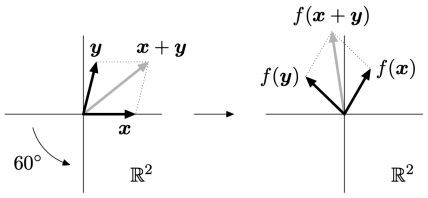
Natažení:



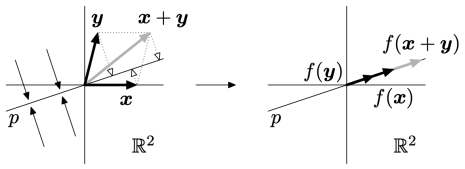
Zkosení:



Rotace:



Kolmá projekce:



Zkonstruujme maticové reprezentace jednoduchých geometrických zobrazení v $\mathbb{R}^2$. Stačí určit souřadnice obrazů $f(\boldsymbol{e}_1)$ a $f(\boldsymbol{e}_2)$ a zapsat je do sloupců:

$$\begin{pmatrix} | & | \\ f(\boldsymbol{e}_1) & f(\boldsymbol{e}_2) \\ | & | \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}.$$

Dvojnásobné roztažení osy y

Platí, že $f(\boldsymbol{e}_1) = \boldsymbol{e}_1 = (1, 0)$, ale $f(\boldsymbol{e}_2) = 2\boldsymbol{e}_2 = (0, 2)$. Výsledná matice je diagonální:

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

Kolmá projekce na osu x

Platí, že $f(\boldsymbol{e}_1) = \boldsymbol{e}_1 = (1, 0)$ a $f(\boldsymbol{e}_2) = (0, 0)$. Výsledná matice je diagonální s hodností 1.

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

Rotace o úhel φ

Stačí spočítat rotace $\boldsymbol{e}_1$ a $\boldsymbol{e}_2$ o úhel φ:

$$\begin{aligned} f(\boldsymbol{e}_1) &= (\cos\varphi, \sin\varphi), \\ f(\boldsymbol{e}_2) &= \big(\cos(\varphi + \pi/2), \sin(\varphi + \pi/2)\big) = (-\sin\varphi, \cos\varphi). \end{aligned}$$

Výsledná matice je:

$$C = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}.$$

Derivace a integrál

Uvažme prostor funkcí spojitě diferencovatelných funkcí C^1 na $\mathbb{R}$ a prostor všech spojitých funkcí C na $\mathbb{R}$. Derivace $\frac{d}{dx} : C^1 \to C$ je lineární zobrazení:

$$\begin{aligned} \frac{d}{dx}(\boldsymbol{f}+\boldsymbol{g}) &= \frac{d}{dx}\boldsymbol{f} + \frac{d}{dx}\boldsymbol{g} \quad \forall \boldsymbol{f},\boldsymbol{g} \in C^1, \\ \frac{d}{dx}(\alpha \boldsymbol{f}) &= \alpha \frac{d}{dx}\boldsymbol{f} \qquad\qquad \forall \boldsymbol{f} \in C^1, \alpha \in \mathbb{R}. \end{aligned}$$

Podobně integrál $\int : C \to C^1$ je lineární zobrazení. Navíc je integrál pravá inverze derivace, tedy

$$\frac{d}{dx} \circ \int = \mathrm{id}\,.$$

Celou řadu vlastností lineární algebry popsaných v tomto textu lze aplikovat na analýzu.

Například uvažme hledání primitivní funkce pro zadanou funkci $\boldsymbol{f}$, tedy řešíme $\int \boldsymbol{f} = \boldsymbol{g}$. To odpovídá řešení "soustavy lineárních rovnic" $\frac{d}{dx}\boldsymbol{g} = \boldsymbol{f}$, což je obdoba $A\boldsymbol{x} = \boldsymbol{b}$.

Věta: Primitivní funkce $\boldsymbol{g}$ je určena jednoznačně až na konstantu.

Důkaz: Víme pro $A\boldsymbol{x} = \boldsymbol{b}$, že pokud existuje řešení $\boldsymbol{p}$, množina všech řešení tvoří afinní podprostor $\mathrm{Ker}(A) + \boldsymbol{p}$. Tedy stačí určit $\mathrm{Ker}\left(\frac{d}{dx}\right)$, což jsou přesně funkce $\boldsymbol{h}$, které se zderivují na nulovou funkci 0. A to jsou konstantní funkce.

Takovým způsobem se tento fakt v analýze typicky nedokazuje. Když si však typický důkaz projdete, jedná se o přesně identický argument jako důkaz obecné věty o struktuře řešení $A\boldsymbol{x} = \boldsymbol{b}$.

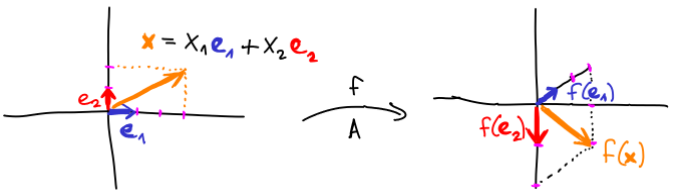
Nechť P_n je prostor polynomů stupně nejvýše n. Zkuste rozmyslet, jak vypadají matice reprezentující derivaci $\frac{d}{dx} : P_{n+1} \to P_n$ a integrál $\int : P_n \to P_{n+1}$.

Maticová reprezentace f : x ↦ Ax

Věta: Libovolné lineární zobrazení $f\colon \mathbb{R}^n \to \mathbb{R}^m$ je reprezentováno maticí A tak, že $f\colon \boldsymbol{x} \mapsto A\boldsymbol{x}$, tedy $f(\boldsymbol{x}) = A\boldsymbol{x}$.

Důkaz: Zobrazení $\boldsymbol{x} \mapsto A\boldsymbol{x}$ je vždy lineární zobrazení z distributivity maticového násobení: $A(\boldsymbol{x}+\boldsymbol{y}) = A\boldsymbol{x} + A\boldsymbol{y}$ a $A(c\boldsymbol{x}) = c(A\boldsymbol{x})$.

Na druhou stranu, zobrazení $f\colon \mathbb{R}^n \to \mathbb{R}^m$ je z linearity jednoznačně popsané obrazy $f(\boldsymbol{e}_1), \dots, f(\boldsymbol{e}_n)$. Pro $\boldsymbol{x} = (x_1, \dots, x_n) = x_1\boldsymbol{e}_1 + \cdots + x_n\boldsymbol{e}_n$ je $f(\boldsymbol{x}) = x_1 f(\boldsymbol{e}_1) + \cdots + x_n f(\boldsymbol{e}_n)$.



Každý z obrazů $f(\boldsymbol{e}_i)$ má m souřadnic, dohromady je tedy f jednoznačně určené pomocí $m \times n$ souřadnic, které zapíšeme po sloupcích do tabulky A zvané matice.

$$A = \begin{pmatrix} | & | & & | \\ f(\boldsymbol{e}_1) & f(\boldsymbol{e}_2) & \cdots & f(\boldsymbol{e}_n) \\ | & | & & | \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}.$$

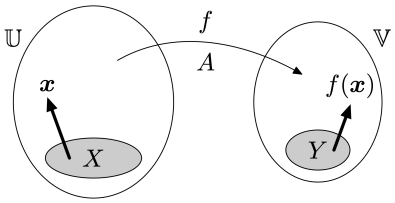
Z definice maticového násobení je $A\boldsymbol{x} = x_1 f(\boldsymbol{e}_1) + \cdots + x_n f(\boldsymbol{e}_n)$, tedy $f(\boldsymbol{x}) = A\boldsymbol{x}$. Proto tato matice reprezentuje f.

Celý postup chceme zobecnit pro libovolné prostory U a V a jejich libovolné báze, protože na kanonických bazích není nic speciálního. Mějme **libovolně dvě báze**:

- $X = \{\boldsymbol{x}_1, \dots, \boldsymbol{x}_n\}$ jako bázi prostoru U,
- $Y = \{\boldsymbol{y}_1, \dots, \boldsymbol{y}_m\}$ jako bázi prostoru V.

Věta: Libovolné lineární zobrazení $f\colon U \to V$ vůči bázím X a Y je reprezentováno maticí A tak, že $f\colon \boldsymbol{x} \mapsto A\boldsymbol{x}$, tedy $f(\boldsymbol{x}) = A\boldsymbol{x}$.

Důkaz: Víme, že lineární zobrazení $f\colon U \to V$ je **jednoznačně určeno obrazy libovolné báze**. K popisu zobrazení stačí znát $f(\boldsymbol{x}_1), \dots, f(\boldsymbol{x}_n)$, kde každý z těchto obrazů lze **popsat pomocí m souřadnic** vůči bázi Y.



Rozhodneme se zapsat těchto $m \times n$ souřadnic do tabulky A, které budeme říkat **matice**. Souřadnice jednotlivých vektorů $f(\boldsymbol{x}_i)$ zapíšeme do sloupců:

$$A = \begin{pmatrix} | & | & & | \\ f(\boldsymbol{x}_1) & f(\boldsymbol{x}_2) & \cdots & f(\boldsymbol{x}_n) \\ | & | & & | \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2,n} \\ a_{3,1} & a_{3,2} & a_{3,3} & \cdots & a_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & a_{m,3} & \cdots & a_{m,n} \end{pmatrix}.$$

Tedy $a_{i,j}$ je souřadnice $f(\boldsymbol{x}_j)$ vůči $\boldsymbol{y}_i$.

Klíčové: Pro **různé volby bází X a Y můžeme získat různé maticové reprezentace** lineárního zobrazení f. Naopak **jedna matice může reprezentovat různá lineární zobrazení** pro různou volbu bází.

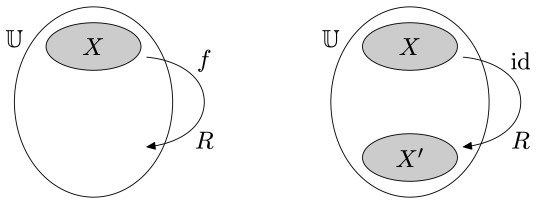
Například uvažme rotaci o úhel φ v rovině. Ta je reprezentovaná maticí A, pokud $X = Y$ je kanonická báze tvořená vektory $(1, 0)$ a $(0, 1)$. Pokud však X je kanonická báze a Y je X otočená o úhel φ, je rotace reprezentovaná maticí B. Na druhou stranu, pokud $X = Y$ a zobrazení je endomorfismus, reprezentuje matice B identické zobrazení.

$$A = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Matice přechodu

Čtvercová regulární matice reprezentující identitu se nazývá **matice přechodu**. Přepočítává souřadnice od jedné báze X k jiné bázi X'.

Čtvercová regulární matice může reprezentovat různá lineární zobrazení. Pokud zvolíme jednu bázi X, dostáváme nějaký endomorfismus. Lze ji však uvažovat jako reprezentace identity vůči volbě bází X a X'.



Pokud $\boldsymbol{x}$ jsou souřadnice vektoru vůči bázi X, jsou $A\boldsymbol{x}$ souřadnice stejného vektoru vůči bázi X'.

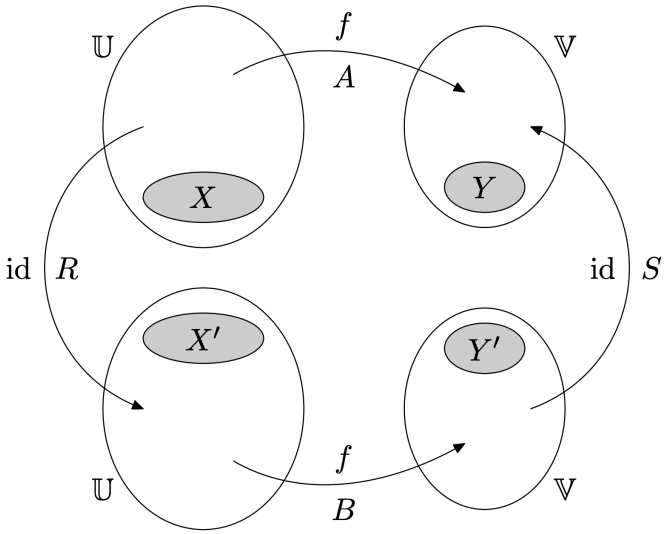
Podobnost

Než definujeme podobnost, nejprve definujme slabší maticovou ekvivalenci.

Matice A a B jsou **ekvivalentní**, pokud reprezentují stejné lineární zobrazení pro různou volbu bází. Jsou ekvivalentní, právě když existují dvě regulární matice R a S (přechodu), pro které platí:

$$A = SBR, \quad \text{neboli} \quad B = S^{-1}AR^{-1}.$$

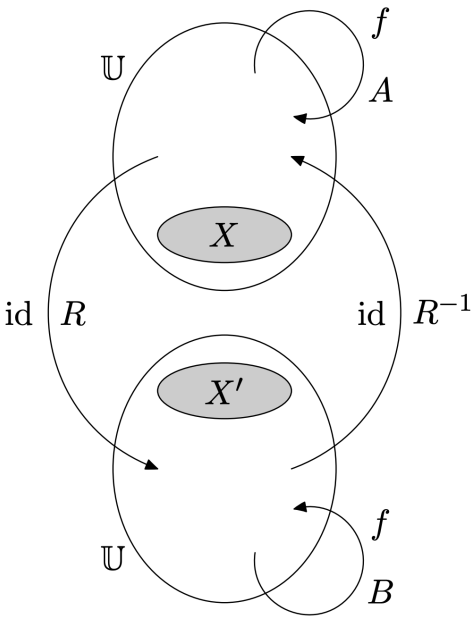
Tvrzení: Matice A a B stejné velikosti jsou ekvivalentní, právě když $\operatorname{rank}(A) = \operatorname{rank}(B)$.



Podobnost je maticová ekvivalence pro čtvercové matice reprezentující endomorfismy vůči jedné bázi. Tedy dvě matice A a B jsou **podobné**, právě když reprezentují **stejný endomorfismus pro jinou volbu báze**. To je právě tehdy, když existuje regulární matice R (matice přechodu), že platí:

$$A = R^{-1}BR, \quad \text{neboli} \quad B = RAR^{-1}.$$

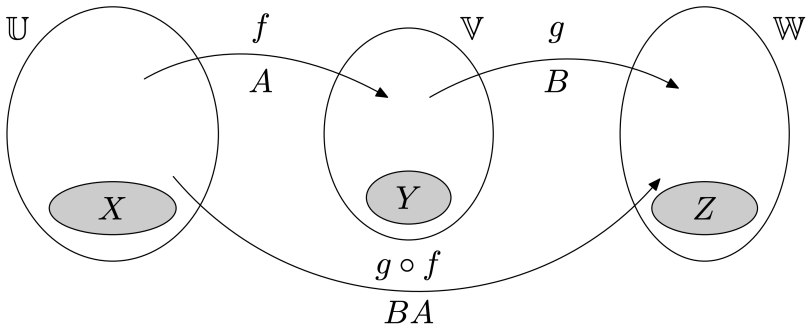
Jeden z klíčových problémů lineární algebry je najít pro daný endomorfismus nejjednodušší možnou maticovou reprezantaci.



Skládání zobrazení

Mějme lineární zobrazení $f\colon U \to V$ a $g\colon V \to W$. Existuje **složené zobrazení** $g \circ f\colon U \to W$, které je také **lineární**. Jak vypadá jeho maticová reprezentace?

Věta: Nechť A **reprezentuje** $f\colon U \to V$ vůči bázím X a Y, B **reprezentuje** $g\colon V \to W$ vůči bázím Y a Z. Potom BA **reprezentuje** $g \circ f\colon U \to W$ vůči bázím X a Z.



Tato věta vysvětluje definici maticového násobení. **Matice musíme násobit tak zvláštně právě proto, aby jejich násobení odpovídalo skládání lineárních zobrazení**. Pokud bychom lineární algebru budovali od lineárních zobrazení, můžeme z definice maticové reprezentace odvodit definici maticového násobení.

Proto také definice maticového násobení **vyžaduje kompatibilní rozměry**. Nechť A je velikosti $n \times p$, reprezentující zobrazení $\mathbb{R}^p \to \mathbb{R}^n$, a B je velikosti $m \times n$, reprezentující zobrazení $\mathbb{R}^n \to \mathbb{R}^m$. Potom je prostor uprostřed totožný, tedy má i stejnou dimenzi, a složené zobrazení $\mathbb{R}^p \to \mathbb{R}^m$ je reprezentováno maticí BA velikosti $m \times p$.

Důkaz z definice: Matice reprezentující $g \circ f$ vůči bázím X a Z musí mít v i-tém sloupci souřadnice $g(f(\boldsymbol{x}_i))$ vůči bázi Z. Povšimneme si, že v i-tém sloupci matice A máme souřadnice $f(\boldsymbol{x}_i)$ vůči bázi Y, a

obrazy jednotlivých vektorů báze Y jsou ve sloupcích B. Tedy souřadnice $g(f(\boldsymbol{x}_i))$ vůči bázi Z získáme jako zkombinování sloupců B podle souřadnic v i-tém sloupci A, což přesně odpovídá maticovému násobení.

Důkaz z asociativity: Z asociativity maticového násobení víme, že $(BA)\boldsymbol{x} = B(A\boldsymbol{x})$ pro libovolný vektor $\boldsymbol{x}$. Pravá strana odpovída složenému zobrazení $g \circ f\colon\ \boldsymbol{x} \mapsto B(A\boldsymbol{x})$. Protože rovnost platí pro libovolný vektor $\boldsymbol{x}$, musí být $g \circ f$ reprezentováno BA.

Poznamenejme, že naopak z této věty vyplývá asociativita maticového násobení. To totiž odpovídá skládání lineárních zobrazení, a skládání libovolných zobrazení je asociativní.

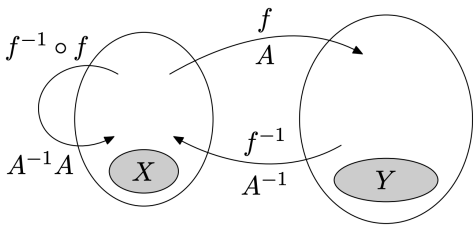
Inverzní zobrazení

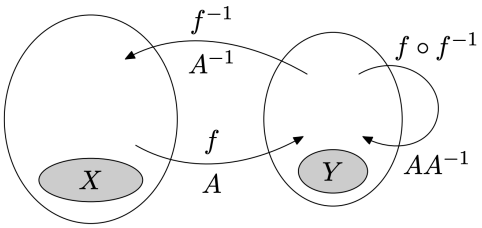
Pro lineární zobrazení $f\colon\ U \to V$ může existovat inverzní zobrazení $f^{-1}\colon\ V \to U$, nebo nemusí. Rozlišujeme tyto druhy inverzí:

- **Levá inverze** $f^{-1} \circ f = \mathrm{id}$ existuje, právě když je zobrazení f **prosté**.
- **Pravá inverze** $f \circ f^{-1} = \mathrm{id}$ existuje, právě když je zobrazení f **na**.
- **Oboustranná inverze** $f^{-1} \circ f = f \circ f^{-1} = \mathrm{id}$ existuje, právě když je zobrazení f **bijektivní**.

Protože identita je reprezentováná jednotkovou maticí I_n, je inverzní zobrazení reprezentováno inverzní maticí. Přesněji řečeno, nechť f je reprezentováno maticí A vůči bázím X a Y.

- **Levá inverze** $\boldsymbol{f^{-1}}$ je reprezentována **levou inverzí** $\boldsymbol{A^{-1}}$ vůči bázím Y a X (obrázek vlevo).
- **Pravá inverze** $\boldsymbol{f^{-1}}$ je reprezentována **pravou inverzí** $\boldsymbol{A^{-1}}$ vůči bázím Y a X (obrázek vpravo).
- **Oboustranná inverze** $\boldsymbol{f^{-1}}$ je reprezentována **oboustrannou inverzí** $\boldsymbol{A^{-1}}$ vůči bázím Y a X.



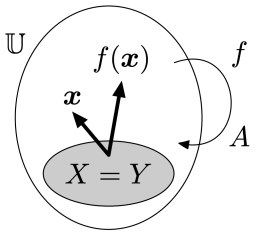


Endomorfismy, izomorfismy, automorfismy

Používají se tři prefixy pro speciální druhy homorofismů: **endomorfismy**, **izomorfismy** a **automorfismy**. Ty rozlišují jestli je f zobrazení obecné nebo bijektivní, a jestli f zobrazuje mezi dvěma prostory U a V, nebo z prostoru U do téhož prostoru U.

	$f\colon\ U \to V$	$f\colon\ U \to U$
obecně	*homo*morfismus	*endo*morfismus
f je bijekce	*izo*morfismus	*auto*morfismus

Každý endomorfismus je homomorfismus a každý automorfismus je izomorfismus, ale jména specificky zdůrazňují, že je uvažujeme jako zobrazení z jednoho prostoru do téhož prostoru. Složení endomorfismů jsou endomorfismy, navíc je lze mocnit: $f^k = f \circ f \circ \cdots \circ f$.



Endomorfismy jsou reprezentované **čtvercovými maticemi** a typicky se volí pouze jedna báze, tedy $X = Y$. Výhody takových reprezentací jsou, že iterování homomorfismu odpovídá mocninám reprezentující matice:

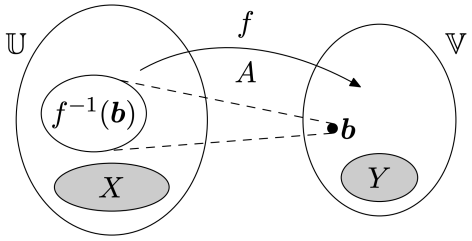
Pokud je f reprezentováno A, je f^k reprezentováno A^k.

Izomorfismy jsou reprezentované **regulárními maticemi**. Pokud existuje izomorfismus $f\colon U \to V$, mají prostory U a V stejnou algebraickou strukturu vektorových operací + a ·. Protože f je bijekce, můžeme **vektory** U **spárovat s vektory** V, a operace se na nich aplikují identicky. Neznamená to, že by tyto prostory byly totožné matematické objekty, akorát jejich **algebraická struktura je totožná** a v řadě případů můžeme **pracovat v** U **stejně jako ve** V.

Hledání vzorů

Nechť $f\colon U \to V$ je lineární zobrazení a $\boldsymbol{b}$ je libovolný vektor V. Chceme nalézt množinu vzorů

$$f^{-1}(\boldsymbol{b}) = \{\boldsymbol{x} \,:\, f(\boldsymbol{x}) = \boldsymbol{b}\}.$$



Nechť lineární zobrazení f je **reprezentováno maticí** $\boldsymbol{A}$**.** Víme, že $f\colon \boldsymbol{x} \mapsto A\boldsymbol{x}$. Tedy hledáme všechny vektory $\boldsymbol{x}$, které splňují $A\boldsymbol{x} = \boldsymbol{b}$, což vede na **soustavu lineárních rovnic**. Tedy i kdybychom lineární algebru budovali abstraktně, od vektorových prostorů a jejich homomorfismů, je řešení soustav lineárních rovnic **klíčové**.

Víme, že množina vzorů $f^{-1}(\boldsymbol{b})$ je neprázdná, právě když $\boldsymbol{b} \in \mathrm{Im}(f)$. V takovém případě je to afinní podprostor $\mathrm{Ker}(f) + \boldsymbol{p}$, kde $\boldsymbol{p}$ je libovolný vzor $\boldsymbol{b}$.

Věta o izomorfismu

Věta: Libovolný vektorový prostor V dimenze n je **izomorfní vektorovému prostoru** $\mathbb{R}^n$.

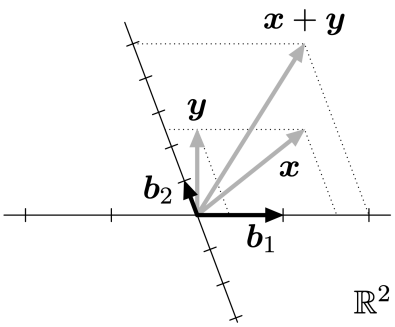
Slovo izomorfní znamená, že existuje **izomorfismus** $f\colon V \to \mathbb{R}^n$. Ten zaručuje, že algebraická struktura prostorů V a $\mathbb{R}^n$ je **totožná**, tedy struktura jejich operací. Platí $f(\boldsymbol{x} + \boldsymbol{y}) = f(\boldsymbol{x}) + f(\boldsymbol{y})$, podobně pro násobení, tedy jednotlivé vektory $\boldsymbol{x}$ prostoru V lze identifikovat s vektory $f(\boldsymbol{x})$ prostoru $\mathbb{R}^n$.

Neznamená to, že by tyto prostory byly totožné, například V může být prostor polynomů stupně nejvýše $n-1$, a tedy jeho prvky jsou úplně jiné matematické objekty než n-tice reálných čísel. Avšak izomorfismus říká, že **v řadě situací můžeme pracovat s V přesně jako s $\mathbb{R}^n$**, například lze řešit soustavy nad $\mathbb{R}^n$ místo nad abstraktním prostorem V.

Důkaz: Zvolíme libovolnou bázi prostoru V. Ta definuje souřadnice $(c_1, \dots, c_n)$ nad V. Tato definice souřadnic je hledaný izomorfismus:

$$f\colon\ c_1\boldsymbol{b}_1 + \dots + c_n\boldsymbol{b}_n \mapsto (c_1, \dots, c_n).$$

Protože souřadnice jsou definované pro každý vektor V jednoznačně, je definované zobrazení bijekce. Zbývá ověřit, že to skutečně je lineární zobrazení. Stačí si všimnout, že sčítání vektorů ve V odpovídá sčítání jejich souřadnic, podobně pro skalární násobení.



Věta o homomorfismu

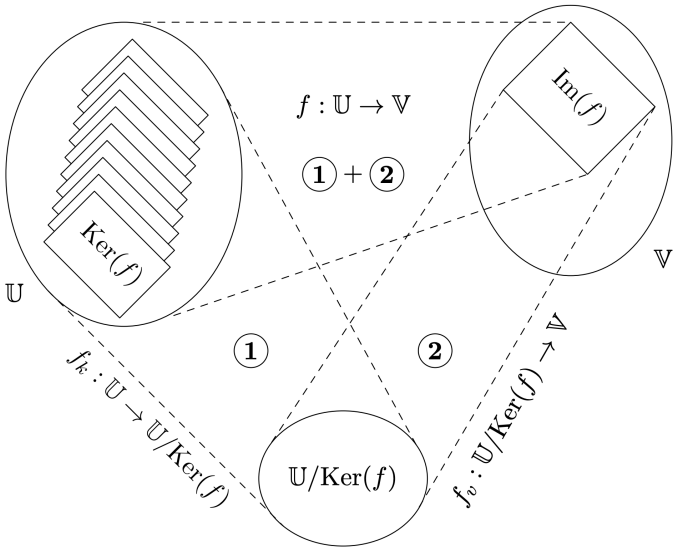
Věta: Pro libovolné lineární zobrazení $f\colon\ U \to V$ platí, že

$$U/\operatorname{Ker}(f) \cong \operatorname{Im}(f).$$

Víme, že vzorem jednotlivých vektorů z $\operatorname{Im}(f)$ jsou afinní podprostory U vzniklé posunutím $\operatorname{Ker}(f)$. Tedy vzory jednotlivých vektorů z $\operatorname{Im}(f)$ mají stejnou strukturu až na posunutí.

Platí, že **čím větší** je $\operatorname{Ker}(f)$, tím méně jeho posunutí existuje, tedy **tím méně** vzorů má řešení. **Přesněji, v řeči dimenzí:**

$$\dim \operatorname{Ker}(f) + \dim \operatorname{Im}(f) = \dim(U).$$



Podle věty lze homomorfismus $f\colon U \to V$ rozdělit na složení dvou jednodušších homomorfismů:

- **Kvocientový homomorfismus** $f_k : U \to U/\operatorname{Ker}(f)$, který je na a obecně není prostý.
- **Vnořovací homomorfismu** $f_v : U/\operatorname{Ker}(f) \to V$, který je prostý, ale obecně není na.

Duální zobrazení

K lineárnímu zobrazení $f\colon U \to V$ je přiřazeno **duální zobrazení** $f^* : V \to U$, které má speciální vlastnosti. Povšimněme si, že inverzní zobrazeni $f^{-1} : V \to U$ zobrazuje mezi stejnými prostory (pokud existuje), avšak **duální zobrazení je něco zcela jiného** (například vždy existuje).

Definice přes skalární součin: Duální zobrazení $f^* : V \to U$ je jediné zobrazení, které pro libovolné vektory $\boldsymbol{x} \in U$ a $\boldsymbol{y} \in V$ splňuje:

$$\langle f(\boldsymbol{x}) \mid \boldsymbol{y} \rangle = \langle \boldsymbol{x} \mid f^*(\boldsymbol{y}) \rangle.$$

Povšimněme si, že levá strana rovnosti je skalární součin ve V, zatímco pravá v U.

Nechť A reprezentuje f vůči bázím X a Y. Pro standardní skalární součin je f^* **reprezentováno** A^T. Tedy **transpozice odpovídá dualitě**.

Pro jaké báze reprezentuje A^T zobrazení f^*? Souřadnice bází X a Y můžeme popsat vůči kanonickým bázím maticemi přechodu X a Y (tedy jejich sloupcové vektory jsou souřadnice bazických vektorů).

Tvrzení: Pro standardní skalární součin je zobrazení f^* jednoznačně určené a reprezentuje ho matice A^T vůči **duálním bázím** Y^* **a** X^*, což jsou sloupcové vektory $Y^{-\mathsf{T}}$ a $X^{-\mathsf{T}}$.

Důkaz: Dokažme to nejprve vůči kanonickým bázím. Nechť B je matice splňující $\langle A\boldsymbol{x} \mid \boldsymbol{y} \rangle = \langle \boldsymbol{x} \mid B\boldsymbol{y} \rangle$. Zjevně pro $B = A^\mathsf{T}$ to platí. Je to jediná taková matice, protože

$$a_{ji} = (A\boldsymbol{e}_i)_j = \sum_{k=1}^{n} (A\boldsymbol{e}_i)_k \cdot (\boldsymbol{e}_j)_k = \sum_{k=1}^{n} (\boldsymbol{e}_i)_k \cdot (B\boldsymbol{e}_j)_k = b_{ij}.$$

nenulové pouze pro $k=j$ — Tedy $B = A^\mathsf{T}$. — nenulové pouze pro $k=i$

Pro obecné báze to platí z následujícího důvodu. Matice $Y^{-1}AX$ reprezentuje f vůči kanonické bázi. Proto duální zobrazení f^* je reprezentováno $(Y^{-1}AX)^\mathsf{T} = X^\mathsf{T}A^\mathsf{T}Y^{-\mathsf{T}}$ vůči kanonické bázi.

Skalární součin

Skalární součin, norma a kolmost

Cíl je nad vektorovým prostorem $\mathbb{R}^n$ zavést další geometrické pojmy.

- **Skalární součin** $\langle \boldsymbol{x} \mid \boldsymbol{y} \rangle$ dvou vektorů $\boldsymbol{x}$ a $\boldsymbol{y}$ popisuje, jak moc ukazují společným směrem a souvisí s úhlem, které vektory svírají.
- **Kolmé vektory** (neboli ortogonální vektory) nemají žádný společný směr, což je právě tehdy, když $\langle \boldsymbol{x} \mid \boldsymbol{y} \rangle = 0$.
- **Norma** $\|\boldsymbol{x}\|$ je geometrická délka vektoru.

V matematice se často objevují prostory prvků (nemusí být vektorové prostory) obohacené nějakými geometrickými vlastnostmi. Dostáváme následující hierarchii možných geometrii:

skalární součin ⇒ norma ⇒ metrika ⇒ topologie.

Například prostor může být povrch koule, na kterém můžeme uvažovat geometrické vzdálenosti. Z těchto definic lze uvažovat topologii a metriku, ale nemůžeme definovat skalární součin a normu.

- **Prostor se skalárním součinem.** Nad prostorem lze uvažovat úhly a kolmost. Existence skalárního součinu indukuje normu: $\|\boldsymbol{x}\| = \sqrt{\langle \boldsymbol{x} \mid \boldsymbol{x} \rangle}$.
- **Prostor s normou.** Nad prostorem lze uvažovat vzdálenosti, které se chovají lineárně vůči natahování vektorů: $\|c\boldsymbol{x}\| = |c| \cdot \|\boldsymbol{x}\|$. Norma indukuje metriku $\rho(\boldsymbol{x}, \boldsymbol{y}) = \|\boldsymbol{x} - \boldsymbol{y}\|$.
- **Prostor s metrikou.** Metrika je funkce vzdálenosti $\rho(x, y)$, která je nezáporná (a kladná pro $x \neq y$), symetrická a splňuje trojúhelníkovou nerovnost. Oproti normě nemusí mít prostor strukturu vektorového prostoru, tedy nemusí platit linearita. Norma indukuje topologii pomocí otevřených a uzavřených ε-okolí, což jsou množiny $B_\varepsilon(x) = \{y \mid \rho(x, y) \leq \varepsilon\}$ (případně s ostrou nerovností).
- **Prostor s topologií.** Nemáme přímo definovanou vzdálenost, ale topologie popisuje blízkost. To se dělá pomocí systému uzavřených a otevřených okolí. Výhoda je, že v řadě situací vzdálenost vůbec nepotřebujeme. Nad topologickými prostory lze dělat velkou část analýzy. Například můžeme definovat limitu posloupnosti: $\lim x_n = x$, pokud pro každé otevřené okolí bodu x existuje $N > 0$ takové, že pro $n > N$ leží každé x_n v tomto okolí x.

Skalární součin

Skalární součin lze definovat konkrétně formulí nebo abstraktně pomocí vlastností.

Standardní skalární součin je definován výrazem

$$\langle \boldsymbol{x} \mid \boldsymbol{y} \rangle = \boldsymbol{x}^\mathsf{T} \boldsymbol{y} = \sum_{i=1}^{n} x_i y_i = x_1 y_1 + \cdots + x_n y_n.$$

Abstaktní definice popisuje skalární součin jako libovolné zobrazení $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ splňující vlastnosti:

1. **Linearita:** $\forall x, y, z \in \mathbb{R}^n : \langle x + y \mid z\rangle = \langle x \mid z\rangle + \langle y \mid z\rangle$ a $\forall x, y \in \mathbb{R}^n, \alpha \in \mathbb{R} : \langle \alpha x \mid y\rangle = \alpha\langle x \mid y\rangle$.
2. **Symetrie:** $\forall x, y \in \mathbb{R}^n : \langle x \mid y\rangle = \langle y \mid x\rangle$.
3. **Pozitivní definitnost:** $\forall x \in \mathbb{R}^n, x \neq 0 : \langle x \mid x\rangle > 0$. (Poznámka: Pro $x = 0$ je $\langle x \mid x\rangle = 0$ z linearity.)

Libovolné zobrazení splňující první vlastnost (v obou složkách) se nazýva **bilineární forma**, dvojicím vektorů přiřazuje reálná čísla a je lineární v obou složkách. Tedy skalární součin je **symetrická pozitivně definitní bilineární forma**. Rozmyslete si, že standardní skalární součin vlastnosti 1 až 3 splňuje.

Nad tělesem komplexních čísel $\mathbb{C}$ se komplexně sdružuje: Standardní skalární součin má komplexně sdružené koeficienty x. Abstraktní skalární součin má ve vlastnosti 2 komplexní sdružení.

Skalární součin (třeba standardní) je možné definovat stejně i nad obecnými algebraickými tělesy, ale **pozitivní definitnost nemůže být splněna** (nad obecným tělesem dokonce nerovnost nedává smysl). Tedy skalární součin je výrazně slabší pojem nad obecnými tělesy.

Cauchy-Schwarzova nerovnost

Věta: (Cauchy-Schwarz) Pro libovolné vektory x a y platí nerovnost

$$|\langle x \mid y\rangle| \leq \|x\|\|y\|.$$

Poznámka: Věta má následující aplikaci ve **funkcionální analýze**. Na prostoru funkcí můžeme definovat skalární součin a příslušnou indukovanou normu, například

$$\langle f \mid g\rangle = \int_0^{2\pi} f(x)\, g(x)\, dx.$$

∫ je jako Σ i
rozmyslete si, že splňuje
vlastnosti (i) až (iii).

Protože se chceme vyhnout nekonečným hodnotám, můžeme uvažovat **Hilbertův podprostor všech funkcí, které mají konečnou normu**. Podle Cauchy-Schwarzovy věty jsou i jejich skalární součiny konečné.

Cosinová věta: Pro libovolné vektory x a y svírající úhel φ platí, že

$$\langle x \mid y\rangle = \|x\|\|y\| \cos(\varphi)$$

Skalární součin je **kladný** pro **ostrý úhel** φ, **nulový** pro **kolmý úhel** φ a **záporný** pro **tupý úhel** φ.

Důkaz: Uvažme kolmou projekci p vektoru x na vektor y. Platí, že norma $\|e\|$ rozdílu projekce a vektoru $e = p - x$ je nezáporná. Úpravou získáváme Cauchy-Schwarzovu nerovnost:

$$0 \leq \|e\|^2 = \langle e \mid e\rangle = \langle p - x \mid p - x\rangle = \left\langle \frac{\langle x|y\rangle}{\langle y|y\rangle} y - x \,\middle|\, \frac{\langle x|y\rangle}{\langle y|y\rangle} y - x \right\rangle =$$

stačí elementární úpravy

symetrie, linearita

$$= \left\langle \frac{\langle x|y\rangle}{\langle y|y\rangle} y \,\middle|\, \frac{\langle x|y\rangle}{\langle y|y\rangle} y \right\rangle - 2\left\langle \frac{\langle x|y\rangle}{\langle y|y\rangle} y \,\middle|\, x \right\rangle + \langle x|x\rangle =$$

opět linearita

$$= \frac{\langle x|y\rangle^2}{\langle y|y\rangle^2}\langle y|y\rangle - 2\frac{\langle x|y\rangle^2}{\langle y|y\rangle} + \langle x|x\rangle,$$

neboli $\langle x|y\rangle^2 \leq \langle x|x\rangle\langle y|y\rangle$.

Cauchy–Schwarzova nerovnost plyne odmocněním.

Norma

Norma $\|x\|$ je geometrická délka vektoru x. Opět má různé definice.

Norma indukovaná skalárním součinem. Libovolný skalární součin $\langle x \mid y \rangle$ definuje normu $\|x\| = \sqrt{\langle x \mid x \rangle}$. Například standardní skalární součin definuje **standardní normu**

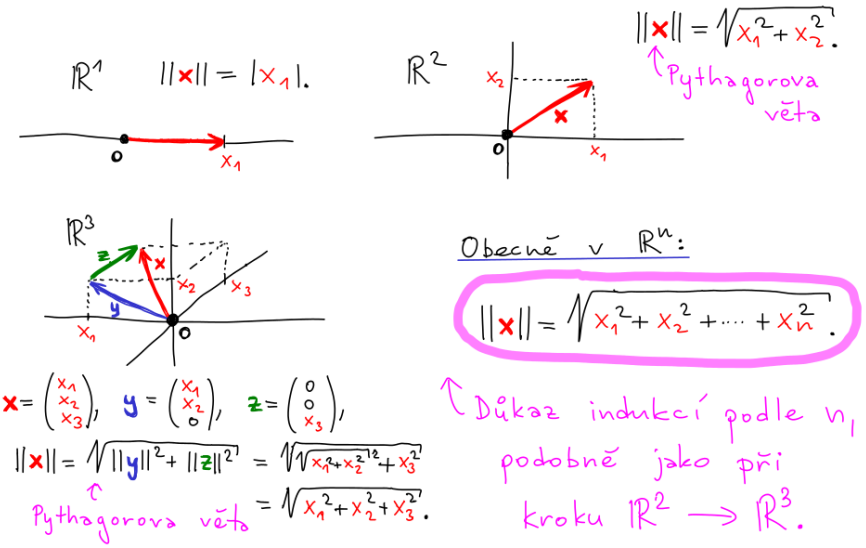
$$\|x\| = \sqrt{x^T x} = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2}.$$

Vlastnosti 1 a 3 vyplývají z příslušných vlastností skalárního součinu. Pro trojúhelníkovou nerovnost:

$$\begin{aligned} \|x+y\| &\le \|x\| + \|y\| \qquad \downarrow \text{ vše kladné, umocníme druhou mocninou} \\ \langle x+y \mid x+y \rangle &\le \langle x \mid x \rangle + 2\|x\|\cdot\|y\| + \langle y \mid y \rangle \\ \langle x \mid x \rangle + 2\langle x \mid y \rangle + \langle y \mid y \rangle &\le \langle x \mid x \rangle + 2\|x\|\cdot\|y\| + \langle y \mid y \rangle \\ \langle x \mid y \rangle &\le \|x\|\cdot\|y\| \qquad \rightarrow \text{Cauchy-Schwarzova nerovnost} \end{aligned}$$

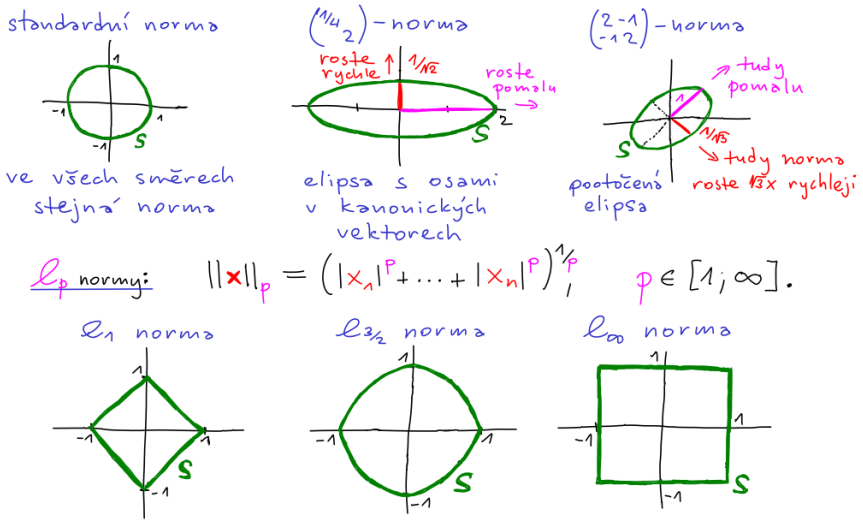
Abstaktní definice popisuje normu jako libovolné zobrazení $\mathbb{R}^n \to \mathbb{R}$ splňující vlastnosti:

1. **Linearita:** $\forall\, x \in \mathbb{R}^n, \alpha \in \mathbb{R} :\ \|\alpha x\| = |\alpha| \|x\|$.
2. **Trojúhelníková nerovnost:** $\forall\, x, y \in \mathbb{R}^n :\ \|x + y\| \le \|x\| + \|y\|$.
3. **Nezápornost:** $\forall\, x \in \mathbb{R}^n, x \neq 0 :\ \|x\| > 0$. (Poznámka: Pro $x = 0$ je $\|x\| = 0$ z linearity.)



Nestandardní normy v $\mathbb{R}^2$

Podle charakterizace jsou normy indukované skalárním součinem tzv. A-**normy** $\|x\|_A = \sqrt{x^T A x}$, kde A je symetrická pozitivně definitní matice. Norem však existuje **mnohem víc než skalárních součinů**.



Uvažme pro danou normu jednotkovou sféru S a kouli B:

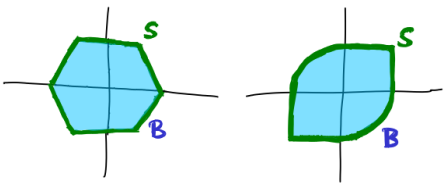
$$S = \{\boldsymbol{x} \mid \|\boldsymbol{x}\| = 1\}, \quad B = \{\boldsymbol{x} \mid \|\boldsymbol{x}\| \leq 1\}$$

.

Geometrické vlastnosti sféry a koule. Z axiomů normy můžeme vyvodit geometrické vlastnosti S a B.

- Množina S protíná každou přímku procházející počátkem **přesně ve dvou bodech** (podle linearity a nezápornosti).
- Množina S je **symetrická podle počátku**: $S = -S$ (podle linearity se záporným koeficientem), a neobsahuje počátek: $0 \notin S$ (podle nezápornosti).
- Množina B je **konvexní** (nejobtížnější, podle trojúhelníkové nerovnosti).

Klíčové je, že norma je **jednoznačně popsaná jednotkovou sférou** S. Na libovolném paprsku z počátku má přesně jeden vektor $\boldsymbol{y}$ jednotkovou normu. Norma zbývajících vektorů $\boldsymbol{x}$ paprsku je určena z linearity.

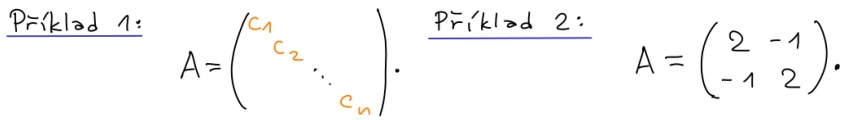


Tvrzení: Nechť B je uzavřená omezená podmnožina $\mathbb{R}^n$, symetrická podle počátku. Nechť S je hranice B a $0 \notin S$. Potom je zobrazení $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}$, kde $\|\boldsymbol{x}\| = |\alpha|$ pro $\boldsymbol{x} = \alpha\boldsymbol{y}$ a $\boldsymbol{y} \in S$, norma.

Tvrzení: Pro normy indukované skalárním součinem je **jednotková sféra** S **pootočený elipsoid**, jehož osy jsou vlastní vektory matice A.

Nestandardní skalární součin

Výraz $\boldsymbol{x}^\mathsf{T}\boldsymbol{y}$ lze přirozeným způsobem zobecnit na $\boldsymbol{x}^\mathsf{T}A\boldsymbol{y}$, kde A je nějaká matice.



V příkladu 1 je potřeba kvůli třetí vlastnosti, aby každé c_i bylo kladné. V příkladu 2 lze vlastnost 3 dokázat převodem na součet čtverců:

$$\langle \boldsymbol{x} \mid \boldsymbol{x} \rangle = 2x_1^2 - 2x_1x_2 + 2x_2^2 = x_1^2 + x_2^2 + (x_1 - x_2)^2 > 0$$

Výraz $\boldsymbol{x}^\mathsf{T} A \boldsymbol{y}$ je obecně bilineární forma.

- Pokud je matice A **symetrická**, je to **symetrická bilineární forma**.
- Pokud je A navíc **pozitivně definitní** ($\forall\, \boldsymbol{x} \neq 0 :\ \boldsymbol{x}^\mathsf{T} A \boldsymbol{x} > 0$), je to **symetrická pozitivně definitní bilineární forma**, neboli skalární součin.

Věta: Libovolný skalární součin $\langle \boldsymbol{x} \mid \boldsymbol{y} \rangle$ je roven $\boldsymbol{x}^\mathsf{T} A \boldsymbol{y}$, kde A je nějaká **symetrická pozitivně definitní matice**.

Důkaz: Nechť $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ je kanonická báze. Z linearity je skalární součin jednoznačně určený hodnotami pro libovolnou bázi:

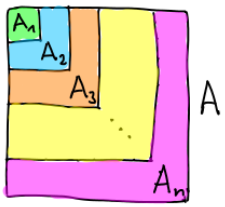
$$\langle \boldsymbol{x} \mid \boldsymbol{y} \rangle = \sum\sum x_i\, y_j \langle \boldsymbol{e}_i \mid \boldsymbol{e}_j \rangle, \quad \text{kde} \quad \boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad \boldsymbol{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

$$A = \begin{pmatrix} \langle \boldsymbol{e}_1 \mid \boldsymbol{e}_1 \rangle & \cdots & \langle \boldsymbol{e}_1 \mid \boldsymbol{e}_n \rangle \\ \vdots & & \vdots \\ \langle \boldsymbol{e}_n \mid \boldsymbol{e}_1 \rangle & \cdots & \langle \boldsymbol{e}_n \mid \boldsymbol{e}_n \rangle \end{pmatrix}$$

Jako A zvolíme **Gramovu matici** tvořenou skalárními součiny $\langle \boldsymbol{e}_i \mid \boldsymbol{e}_j \rangle$. Potom je $\langle \boldsymbol{x} \mid \boldsymbol{y} \rangle = \boldsymbol{x}^\mathsf{T} A \boldsymbol{y}$. Z vlastností 2 a 3 skalárního součinu vyplývá, že A je symetrická pozitivně definitní matice.

Pozitivně definitní matice

Čtvercová symetrická matice A se nazývá **pozitivně definitní**, právě když platí jedna z následujících šesti ekvivalentních vlastností:



1. Pro každé $\boldsymbol{x} \neq 0$ je $\boldsymbol{x}^\mathsf{T} A \boldsymbol{x} > 0$.
2. **Všechna vlastní čísla** $\lambda_i > 0$. (Vlastní čísla jsou reálná ze symetrie A.)
3. **Determinanty principiálních minorů** $\det(A_1), \dots, \det(A_n) > 0$. Principiální minor A_k je čtvercová podmatice A velikosti $k \times k$ v levém rohu.
4. Lze provést **Gaussovu eliminaci bez prohazování a násobení řádků** a všechny pivoty $p_i > 0$.
5. Existuje regulární matice R taková, že $A = R^\mathsf{T} R$, což je Choleského rozklad.
6. Výraz $\boldsymbol{x}^\mathsf{T} A \boldsymbol{y}$ je skalární součin a $\sqrt{\boldsymbol{x}^\mathsf{T} A \boldsymbol{x}}$ je norma.

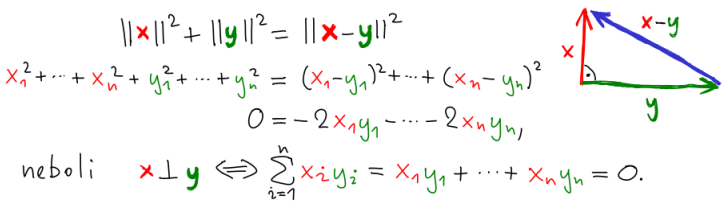
Tvrzení: Pro symetrické matice A jsou vlastnosti 1 až 6 ekvivalentní.

Kvadratické formy a definitnost

Ortogonalita

Vektory $\boldsymbol{x}$ a $\boldsymbol{y}$ jsou **ortogonální** neboli **kolmé**, právě když $\langle \boldsymbol{x} \mid \boldsymbol{y} \rangle = 0$. Kolmost značíme $\boldsymbol{x} \perp \boldsymbol{y}$.

Odvození přes Pythagorovu větu. Vektory $\boldsymbol{x}$ a $\boldsymbol{y}$ jsou kolmé, právě když splňují Pythagorovu větu.



Podle definice je počátek 0 kolmý na všechny vektory.

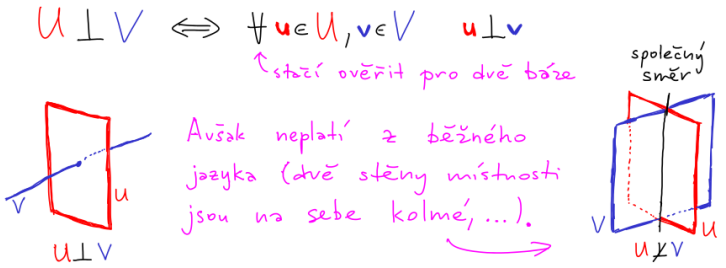
Lemma: Nechť $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ jsou nenulové **po dvou ortogonální vektory**, tedy $\boldsymbol{x}_i \perp \boldsymbol{x}_j$ pro $i \neq j$. Potom jsou vektory $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ **lineárně nezávislé**.

Důkaz: Nechť $\alpha_1\boldsymbol{x}_1 + \cdots + \alpha_n\boldsymbol{x}_n = 0$. Chceme dokázat, že všechna $\alpha_i = 0$. Vynásobíme-li celý výraz zleva $\boldsymbol{x}_i^\mathsf{T}$, **dostáváme z ortogonality**

$$0 = \alpha_1\boldsymbol{x}_i^\mathsf{T}\boldsymbol{x}_1 + \cdots + \alpha_i\boldsymbol{x}_i^\mathsf{T}\boldsymbol{x}_i + \cdots + \alpha_n\boldsymbol{x}_i^\mathsf{T}\boldsymbol{x}_n = \alpha_i\boldsymbol{x}_i^\mathsf{T}\boldsymbol{x}_i = \alpha_i\|\boldsymbol{x}_i\|^2.$$

Protože $\boldsymbol{x}_i \neq 0$, víme, že $\alpha_i = 0$. Protože to platí při násobení libovolným $\boldsymbol{x}_i^\mathsf{T}$, je lineární kombinace $\alpha_1\boldsymbol{x}_1 + \cdots + \alpha_n\boldsymbol{x}_n$ **triviální**.

Kolmost vektorových podprostorů.



Ortogonální doplněk

Nechť U je libovolný vektorový podprostor. **Ortogonální doplněk** U je množina

$$U^\perp = \{\boldsymbol{x} : \boldsymbol{x} \perp \boldsymbol{y}\, \forall \boldsymbol{y} \in U\}.$$

Tvrzení: Ortogonální doplněk $U^\perp$ má následující vlastnosti:

1. $U^\perp$ je vektorový podprostor.
2. $U \cap U^\perp = \{0\}$ a $\langle U \cup U^\perp \rangle = \mathbb{R}^n$.
3. $\dim U + \dim U^\perp = n$.
4. $(U^\perp)^\perp = U$.

Důkaz: Vlastnosti 1 a první část 2 jsou jednoduché. Pro zbytek potřebujeme existenci ortogonálních bází. Zvolme ortogonální bázi $\boldsymbol{b}_1, \dots, \boldsymbol{b}_k$ prostoru U a doplňme ji vektory $\boldsymbol{b}_{k+1}, \dots, \boldsymbol{b}_n$ na ortogonální bázi $\mathbb{R}^n$. Vektory $\boldsymbol{b}_{k+1}, \dots, \boldsymbol{b}_n$ tvoří ortogonální bázi $U^\perp$. Pokud totiž nějaký vektor má nenulovou souřadnici vůči $\boldsymbol{b}_1, \dots, \boldsymbol{b}_k$, nemůže ležet v $U^\perp$.

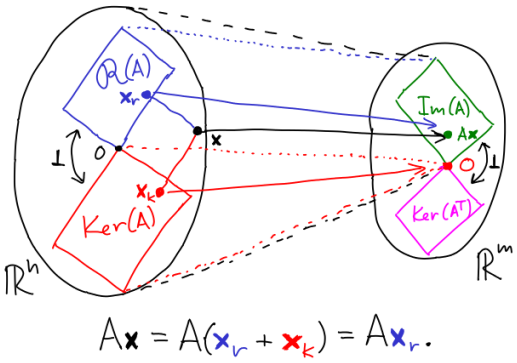
Věta: Fundamentální podprostory matice A jsou svoje **ortogonální doplňky**:

$$\mathrm{Ker}(A) = \mathrm{R}(A)^\perp, \qquad \mathrm{Ker}(A^\mathsf{T}) = \mathrm{Im}(A)^\perp.$$

Důkaz: Nechť $\boldsymbol{x} \in \mathrm{Ker}(A)$ a $\boldsymbol{u}_1, \dots, \boldsymbol{u}_m$ jsou řádky matice A. Z definice je

$$\boldsymbol{u}_1^\mathsf{T}\boldsymbol{x} = 0, \quad \boldsymbol{u}_2^\mathsf{T}\boldsymbol{x} = 0, \quad \dots, \quad \boldsymbol{u}_m^\mathsf{T}\boldsymbol{x} = 0.$$

Tedy $\boldsymbol{x}$ je ortogonální na $\mathrm{R}(A)$, a naopak libovolný ortogonální vektor na $\mathrm{R}(A)$ patří do $\mathrm{Ker}(A)$. Proto je $\mathrm{Ker}(A) = \mathrm{R}(A)^\perp$. Druhá rovnost se získá pro A^T.



Ortonormální báze

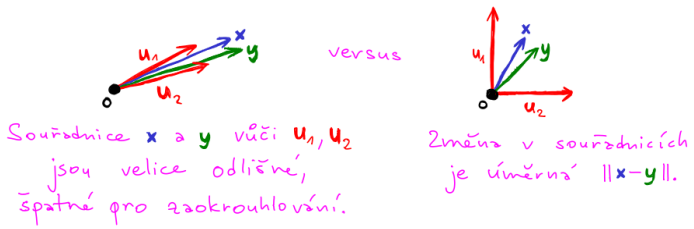
Z lineární nezávislosti ortogonálních vektorů má pojem **ortogonální báze smysl**. Typicky navíc máme **ortonormální** s jednotkovou normou: není to klíčové, ale zjednodušuje to vzorce.

Tvrzení: Libovolnou ortogonální/ortonormální množinu nenulových vektorů **lze rozšířit** na ortogonální/ortonormální bázi.

Důkaz: Doplníme ortonormální množinu na libovolnou bázi a aplikujeme Gram-Schmidtovu ortogonalizaci. Alternativní důkaz je možný přes fundamentální větu lineární algebry.

Tedy ortogonálních bází je **spousta** a jsou to **hezké báze**, mající řadu skvělých vlastností.

1. Ortonormální báze mají výhodné numerické vlastnosti.



2. Snadný výpočet souřadnic pomocí ortogonálních projekcí. Pro obecnou bázi je to řešení soustavy lineárních rovnic $A\boldsymbol{\alpha} = \boldsymbol{x}$. Pro ortogonální bázi $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ je

$$\alpha_i = \frac{\langle \boldsymbol{x} \mid \boldsymbol{v}_i \rangle}{\langle \boldsymbol{v}_i \mid \boldsymbol{v}_i \rangle} \cdot$$ ← kolmá projekce na jednotlivé přímky

Důkaz vyplývá z ortogonality: $\langle \boldsymbol{x} \mid \boldsymbol{v}_i \rangle = \langle \alpha_1 \boldsymbol{v}_1 + \cdots + \alpha_n \boldsymbol{v}_n \mid \boldsymbol{v}_i \rangle = \alpha_i \langle \boldsymbol{v}_i \mid \boldsymbol{v}_i \rangle$.

Jiný pohled je přes ortogonální matice: $\boldsymbol{\alpha} = Q^{\mathsf{T}} Q \boldsymbol{\alpha} = Q^{\mathsf{T}} \boldsymbol{x}$, pokud sloupce Q jsou ortonormální vektory $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$.

Fourierova transformace

Ortogonální matice

Matice Q se nazývá **ortogonální**, pokud má **ortonormální sloupce** (ortogonalita + normy rovné jedné). V maticovém zápisu dostáváme $Q^{\mathsf{T}} Q = I_n$.

Tedy pro ortogonální matice platí, že $Q^{-1} = Q^{\mathsf{T}}$. Protože inverze libovolné čtvercové matice je oboustranná, dostáváme navíc, že $Q Q^{\mathsf{T}} = I_n$. Tedy pokud má čtvercová matice ortonormální sloupce, má také ortonormální řádky, a také matice Q^{T} je ortogonální.

Gram-Schmidtova ortogonalizace

Algoritmus na ortogonalizaci vstupních vektorů.

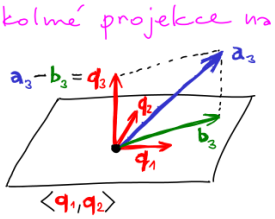
Pro vstupní vektory $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ vytvoří ortogonální vektory $\boldsymbol{q}_1, \ldots, \boldsymbol{q}_k$ tak, že

$$\langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_k \rangle = \langle \boldsymbol{q}_1, \ldots, \boldsymbol{q}_k \rangle.$$

$\boldsymbol{q}_1 = \boldsymbol{a}_1$,

$\boldsymbol{q}_i = \boldsymbol{a}_i - \sum_{j=1}^{i-1} \frac{\langle \boldsymbol{a}_i \mid \boldsymbol{q}_j \rangle}{\langle \boldsymbol{q}_j \mid \boldsymbol{q}_j \rangle} \boldsymbol{q}_j$ ← odečítáme kolmé projekce na $\boldsymbol{q}_1, \ldots, \boldsymbol{q}_{i-1}$

$= \boldsymbol{b}_i$



Tvrzení: Vektory $\boldsymbol{q}_1, \ldots, \boldsymbol{q}_k$ jsou ortogonální.

$$\langle \boldsymbol{q}_i \mid \boldsymbol{q}_t \rangle = \left\langle \boldsymbol{a}_i - \sum_{j=1}^{i-1} \frac{\langle \boldsymbol{a}_i \mid \boldsymbol{q}_j \rangle}{\langle \boldsymbol{q}_j \mid \boldsymbol{q}_j \rangle} \boldsymbol{q}_j \,\middle|\, \boldsymbol{q}_t \right\rangle \overset{\text{linearita}}{=} \langle \boldsymbol{a}_i \mid \boldsymbol{q}_t \rangle -$$

$\forall t < i$ ← nenulové pouze pro $j = t$

$$\sum_{j=1}^{i-1} \frac{\langle \boldsymbol{a}_i \mid \boldsymbol{q}_j \rangle}{\langle \boldsymbol{q}_j \mid \boldsymbol{q}_j \rangle} \langle \boldsymbol{q}_j \mid \boldsymbol{q}_t \rangle = \langle \boldsymbol{a}_i \mid \boldsymbol{q}_t \rangle - \langle \boldsymbol{a}_i \mid \boldsymbol{q}_t \rangle = 0.$$

Tvrzení: Pro každé $i \leq k$ platí, že

$$\langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_i \rangle = \langle \boldsymbol{q}_1, \ldots, \boldsymbol{q}_i \rangle.$$

QR dekompozice

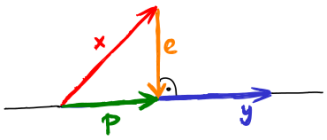
Tvrzení: Pro libovolnou čtvercovou matici A existuje dekompozice

$$A = QR,$$

kde Q je **ortogonální matice** a R je **horní trojúhelníková matice**.

Důkaz: Jedná se o **maticový zápis Gram-Schmidtovy ortogonalizace**, podobně jako LU dekompozice je zápis Gaussovy eliminace.

Ortogonální projekce



Mějme dva vektory $\boldsymbol{x}$ a $\boldsymbol{y}$. Chceme nalézt kolmou projekci $\boldsymbol{x}$ na přímku $\langle \boldsymbol{y} \rangle$. Ekvivalentně je kolmá projekce vektor přímky, který je nejbližší k $\boldsymbol{x}$.

Víme, že $\boldsymbol{p} = c\boldsymbol{y}$. Hledáme hodnotu c, aby vektor $\boldsymbol{e} = \boldsymbol{p} - \boldsymbol{x}$ byl kolmý na $\boldsymbol{y}$:

$$0 = \langle \boldsymbol{p} - \boldsymbol{x} \mid \boldsymbol{y} \rangle = \langle c\boldsymbol{y} - \boldsymbol{x} \mid \boldsymbol{y} \rangle = c\langle \boldsymbol{y} \mid \boldsymbol{y} \rangle - \langle \boldsymbol{x} \mid \boldsymbol{y} \rangle, \text{ neboli } c = \frac{\langle \boldsymbol{x} \mid \boldsymbol{y} \rangle}{\langle \boldsymbol{y} \mid \boldsymbol{y} \rangle}.$$

pouze normovací faktor

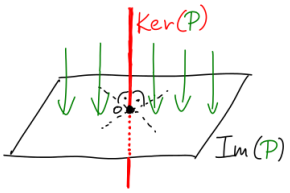
Tvrzení: Kolmá projekce na přímku $\langle \boldsymbol{y} \rangle$ je lineární zobrazení

$$\boldsymbol{x} \mapsto \frac{\langle \boldsymbol{x} \mid \boldsymbol{y} \rangle}{\langle \boldsymbol{y} \mid \boldsymbol{y} \rangle} \boldsymbol{y} = \frac{\boldsymbol{x}^\mathsf{T}\boldsymbol{y}}{\boldsymbol{y}^\mathsf{T}\boldsymbol{y}} \boldsymbol{y} = \frac{\boldsymbol{y}\boldsymbol{y}^\mathsf{T}}{\boldsymbol{y}^\mathsf{T}\boldsymbol{y}} \boldsymbol{x}$$

← matice P kolmé projekce

Nechť P je matice kolmé projekce na podprostor $\mathrm{Im}(P)$. Splňuje dvě následující podmínky:

1. Charakteristika libovolné projekce: $P^2 = P$. Projekce je identita na $\mathrm{Im}(P)$, tedy $P\boldsymbol{y} = \boldsymbol{y}$ pro libovolné $\boldsymbol{y} \in \mathrm{Im}(P)$. Protože $\boldsymbol{y} = P\boldsymbol{x}$ pro každé $\boldsymbol{x}$, získáváme rovnost.



2. Charakteristika kolmosti projekce: $P^\mathsf{T} = P$. $\mathrm{Ker}(P)$ je tvořen vektory, které se projektují na 0, což jsou přesně vektory kolmé na $\mathrm{Im}(P)$. Tedy $\mathrm{Ker}(P) = \mathrm{Im}(P)^\perp$ a z fundamentální věty lineární algebry je $\mathrm{Ker}(P) = \mathrm{Ker}(P^\mathsf{T})$ a $\mathrm{R}(P) = \mathrm{Im}(P)$.

Zbytek plyne z duality, pokud $\langle P\boldsymbol{x} \mid \boldsymbol{y} \rangle = \langle \boldsymbol{x} \mid P\boldsymbol{y} \rangle$. Zvolme

$$\boldsymbol{x} = \boldsymbol{x}_K + \boldsymbol{x}_I, \quad \boldsymbol{y} = \boldsymbol{y}_K + \boldsymbol{y}_I, \quad \text{kde} \quad \boldsymbol{x}_K, \boldsymbol{y}_K \in \mathrm{Ker}(P), \quad \boldsymbol{x}_I, \boldsymbol{y}_I \in \mathrm{Im}(P).$$

Protože $P\boldsymbol{x} = \boldsymbol{x}_I$ a $P\boldsymbol{y} = \boldsymbol{y}_I$,

$$\langle Px \mid y \rangle = \langle x_\perp \mid y_k + y_\perp \rangle = \langle x_\perp \mid y_k \rangle + \langle x_\perp \mid y_\perp \rangle = \langle x_\perp \mid y_\perp \rangle.$$
$$\langle x \mid Py \rangle = \langle x_k + x_\perp \mid y_\perp \rangle = \langle x_k \mid y_\perp \rangle + \langle x_\perp \mid y_\perp \rangle$$
$= 0$ z ortogonality

Tvrzení: Pokud sloupce matice A tvoří bázi podprostoru W, je kolmá projekce na W popsána maticí

$$P = A(A^\mathsf{T}A)^{-1}A^\mathsf{T}.$$

Metoda nejmenších čtverců

Fundamentální podprostory

Lineární zobrazení $f\colon U \to V$ definuje dva **fundamentální podprostory**:

- **Jádro** $\mathrm{Ker}(f) = \{x \in U \mid f(x) = 0\}$ (neboli **kernel**).
- **Obraz** $\mathrm{Im}(f) = \{f(x) \mid x \in U\}$.

Jádro je podprostor U, zatímco obraz je podprostor V. Pokud matice A reprezentuje f, tyto podprostory odpovídají $\mathrm{Ker}(A)$ a $\mathrm{Im}(A)$.

Čemu však odpovídají zbývající dva fundamentální podprostory A^T?

Jsou to jádro a obraz duálního zobrazení $f^* : V \to U$.

- **Levé jádro** $\mathrm{Ker}(f^*) = \{x \in V \mid f^*(x) = 0\}$ (neboli **levý kernel**).
- **Levý obraz** $\mathrm{Im}(f^*) = \{f^*(x) \mid x \in V\}$.

Na obrázku je naznačeno duální zobrazení spolu se svými fundamentálními podprostory.

