Lineární algebra : Soustavy lineárních rovnic

(2. přednáška)

Daniel Dombek, Luděk Kleprlík,
Karel Klouda

daniel.dombek@fit.cvut.cz, ludek.kleprlik@fit.cvut.cz,
karel.klouda@fit.cvut.cz

Katedra aplikované matematiky
Fakulta informačních technologií

České vysoké učení technické v Praze

LS 2021/2022

vytvořeno: 15. února 2022, 13:47

Hlavní body

Úvod

„Classification of mathematical problems as linear and nonlinear is like classification of the universe as bananas and non-bananas.“ *(autor neznámý)*

- polynomiální rovnice, kořeny
- lineární rovnice
- diskrétní matematika, fyzika,. . .

$$ax = b$$

Věta

Nechť $a, b \in \mathbb{R}$ *a* $a \neq 0$. *Potom* $x = a^{-1}b$ *je jediné reálné číslo splňující rovnici* $ax = b$.

Geometrická interpretace

- přímka v rovině $\mathbb{R}^2$, dvě neznámé $x, y \in \mathbb{R}$:

$$ax + by = c, \quad a, b, c \in \mathbb{R}$$

- rovina v prostoru $\mathbb{R}^3$, tři neznámé $x, y, z \in \mathbb{R}$:

$$ax + by + cz = d, \quad a, b, c, d \in \mathbb{R}$$

- výjimky, příklad

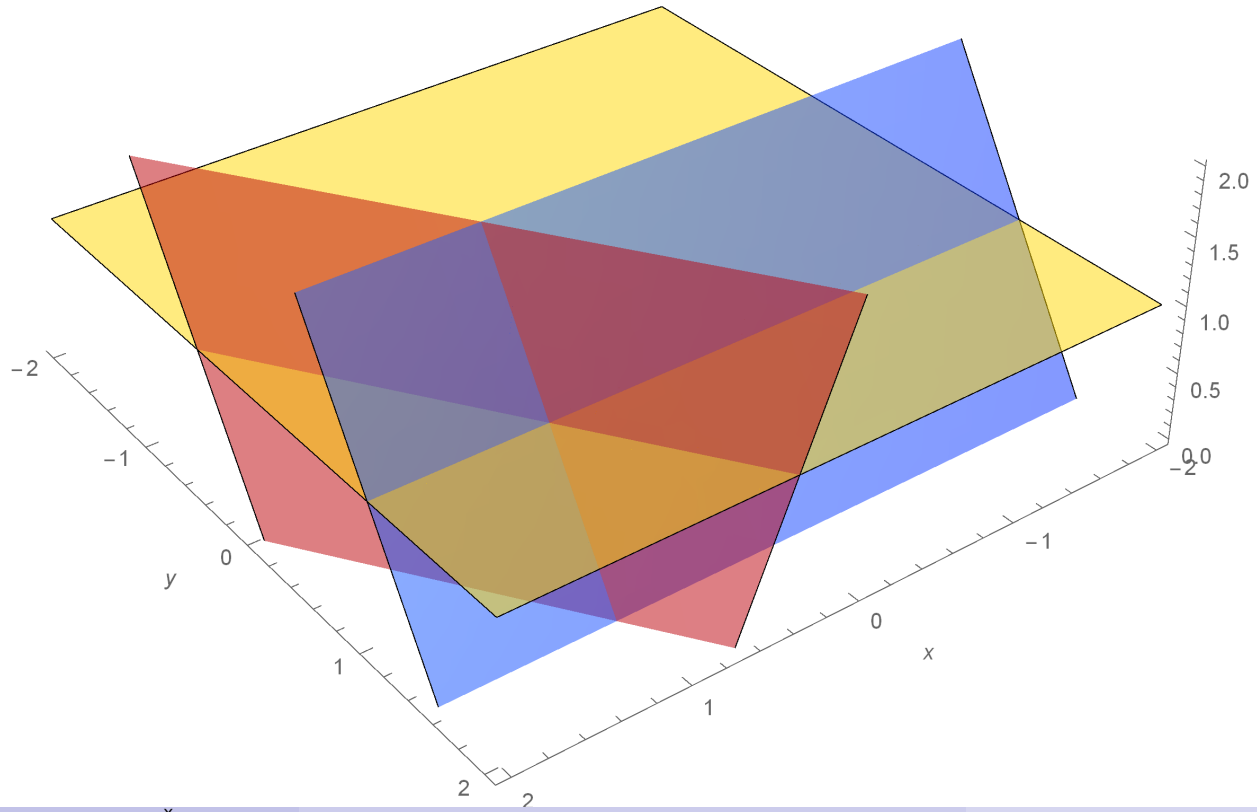
Soustavy lineárních rovnic 1

- soustava rovnic $\leftrightarrow$ průnik přímek/rovin
- teorie...
- počet řešení?
- Frobeniova věta
- příklady:

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

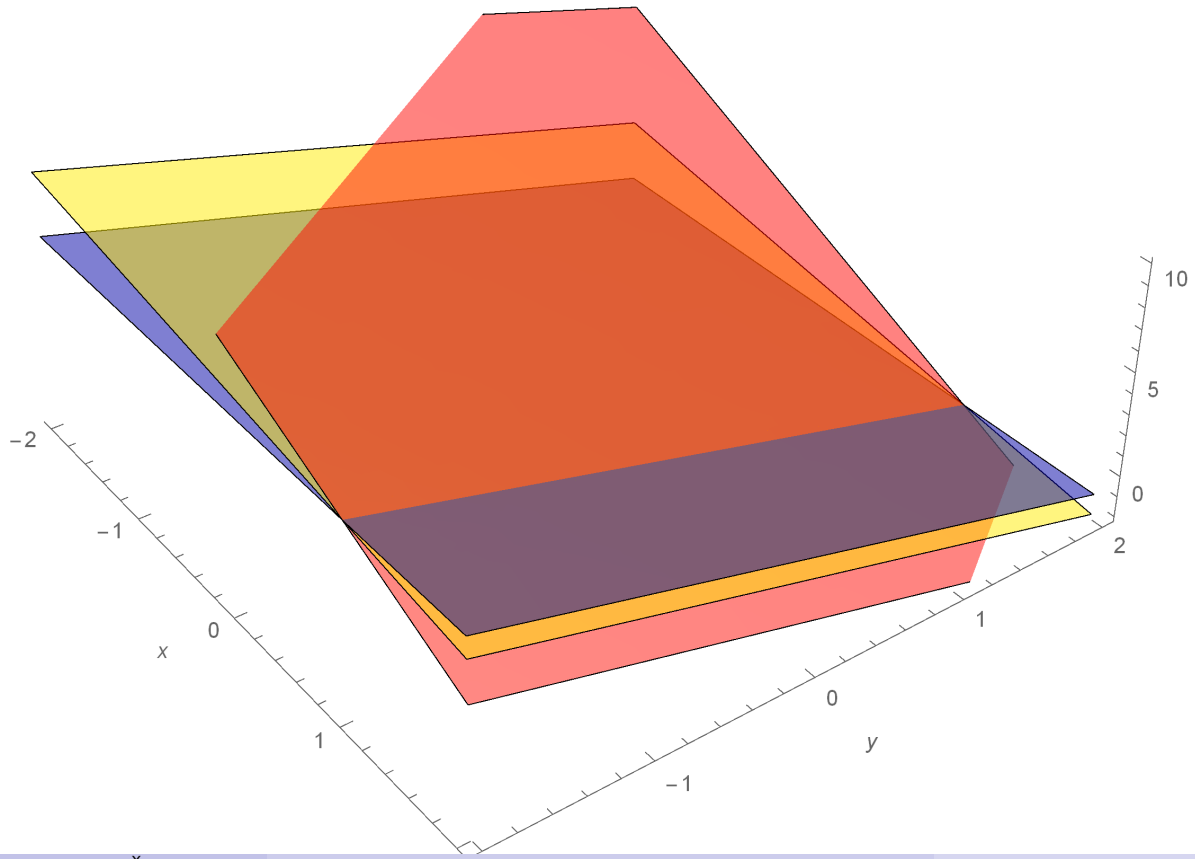
Soustavy lineárních rovnic 2

$$\begin{aligned} 3x + 2y + z &= 6, \\ 2y + z &= 3, \\ z &= 1, \end{aligned} \tag{2}$$



Soustavy lineárních rovnic 3

$$\begin{aligned} 3x + 2y + \ \ z &= 6, \\ 2y + \ \ z &= 3, \\ 3x + 6y + 3z &= 12, \end{aligned} \tag{3}$$



Soustavy lineárních rovnic 4

$$\begin{aligned} 3x + 2y + \ \ z &= 6, \\ 6x + 4y + 2z &= 12, \\ 9x + 6y + 3z &= 18. \end{aligned}$$

Počet řešení?

Definice SLR

Definice

Nechť n a m jsou přirozená čísla a pro všechna $i \in \{1, \ldots, m\}$ a $j \in \{1, \ldots, n\}$ platí, že $a_{ij} \in \mathbb{R}$ a $b_i \in \mathbb{R}$. Systém rovnic

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ \vdots & & \vdots & & \ddots & & \vdots & = & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n & = & b_m \end{array} \tag{4}$$

*nazýváme **soustavou** m **lineárních rovnic o** n **neznámých** $x_1, \ldots, x_n \in \mathbb{R}$. Číslu a_{ij} říkáme j**tý koeficient** i**té rovnice**.*
*Množinu všech uspořádaných ntic $(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$, pro které po dosazení do (4) je splněno všech m rovnic, nazýváme **množinou řešení soustavy** a značíme ji S.*
*Platí-li $b_1 = b_2 = \cdots = b_m = 0$, říkáme, že soustava (4) je **homogenní**. Není-li soustava homogenní, je **nehomogenní**.*

Množina řešení

Pozorování

Následující pozorování se týkají soustavy rovnic (4), z definice 2 je přebráno i značení.

1. *Číslo a_{ij} je číslo, kterým se násobí proměnná x_j v $i$té rovnici.*
2. *Množina řešení soustavy je rovna průniku množin řešení jednotlivých rovnic.*
3. *Homogenní soustava má vždy alespoň jedno řešení $(0, 0, \ldots, 0) \in \mathbb{R}^n$.*
4. *$(0, 0, \ldots, 0) \in \mathbb{R}^n$ není nikdy řešení nehomogenní soustavy rovnic.*
5. *Je-li $(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$ řešení homogenní soustavy, pak pro libovolné $\alpha \in \mathbb{R}$ je $(\alpha x_1, \alpha x_2, \ldots, \alpha x_n) \in \mathbb{R}^n$ také řešení (přepsat!).*
6. *Má-li homogenní soustava i jiné řešení než $(0, 0, \ldots, 0) \in \mathbb{R}^n$, pak má nekonečně mnoho řešení.*

Úpravy SLR

(U1) Prohození dvou rovnic.

(U2) Vynásobení jedné rovnice nenulovým číslem.

(U3) Přičtení libovolného násobku jedné rovnice k jiné rovnici.

Příklad

$$\begin{aligned} 3x + 2y + \ \ z &= 6 \\ 3x + 6y + 4z &= 13 \\ 4y + 2z &= 6 \end{aligned} \xrightarrow[r2-r1]{U3} \begin{aligned} 3x + 2y + \ \ z &= 6 \\ 4y + 3z &= 7 \\ 4y + 2z &= 6 \end{aligned} \xrightarrow[r2-r3]{U3}$$

$$\begin{aligned} 3x + 2y + \ \ z &= 6 \\ z &= 1 \\ 4y + 2z &= 6 \end{aligned} \xrightarrow[r2 \leftrightarrow r3]{U1} \begin{aligned} 3x + 2y + \ \ z &= 6 \\ 4y + 2z &= 6 \\ z &= 1 \end{aligned} \xrightarrow[\frac{1}{2} \cdot r2]{U2}$$

$$\begin{aligned} 3x + 2y + z &= 6 \\ 2y + z &= 3 \\ z &= 1. \end{aligned}$$

Hlavní body

Zjednodušení zápisu

$$\begin{aligned} 3x + 2y + z &= 6 \\ 3x + 6y + 4z &= 13 \\ \ 4y + 2z &= 6 \end{aligned} \quad \text{budeme zapisovat jako} \quad \left(\begin{array}{ccc|c} 3 & 2 & 1 & 6 \\ 3 & 6 & 4 & 13 \\ 0 & 4 & 2 & 6 \end{array}\right). \tag{5}$$

Pokud není řečeno jinak, sloupce odpovídají pořadí proměnných podle abecedy či indexu.

Matice

Definice

Nechť $m, n \in \mathbb{N}$. Uspořádaný soubor mn čísel zapsaný do tabulky o m řádcích a n sloupcích nazýváme ***matice*** *typu $m \times n$. Matice obvykle značíme takto:*

$$\mathbb{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix},$$

kde a_{ij} jsou ***prvky*** *matice (někdy je značíme taky jako $\mathbb{A}_{ij}$ a nazýváme je ij**té prvky**). Číslu i říkáme* ***řádkový*** *a číslu j* ***sloupcový*** *index.*

Množinu všech matic typu *$m \times n$ (s reálnými prvky) značíme $\mathbb{R}^{m,n}$.*

*Jako $\mathbb{A}_{:j} \in \mathbb{R}^{m,1}$ značíme j**tý sloupec**, podobně $\mathbb{A}_{i:} \in \mathbb{R}^{1,n}$ značí i**tý řádek** matice $\mathbb{A}$.*

Operace s maticemi

- součet, rozdíl, násobení číslem – po složkách
- transpozice $\mathbb{A}^T$
- zachování rozměrů

Pozorování:

- komutativita, asociativita
- distributivita
- n-tý násobek
- „$a + x = b$“

Násobení matic

Definice

Buďte $m, n, p \in \mathbb{N}$, $\mathbb{A} \in \mathbb{R}^{m,n}$ *matice s prvky* a_{ij} *a* $\mathbb{B} \in \mathbb{R}^{n,p}$ *matice s prvky* b_{ij}. *Součinem matic* $\mathbb{A}$ *a* $\mathbb{B}$ *je matice* $\mathbb{D} \in \mathbb{R}^{m,p}$ *s prvky* d_{ij}, *pro kterou platí*

$$d_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}, \tag{6}$$

značíme $\mathbb{D} = \mathbb{AB}$.

Vlastnosti násobení

- na velikosti záleží
- na pořadí taky
- příklady...

Věta

Nechť $m, n, s, t \in \mathbb{N}$. *Pro libovolné matice* $\mathbb{A} \in \mathbb{R}^{m,n}$, $\mathbb{B} \in \mathbb{R}^{n,s}$ *a* $\mathbb{D} \in \mathbb{R}^{s,t}$ *platí*

$$\mathbb{A}(\mathbb{B}\mathbb{D}) = (\mathbb{A}\mathbb{B})\mathbb{D}.$$

(Důkaz...)

- distributivita
- asociativita násobení s číslem
- transpozice součinu

Maticový zápis SLR 1

Definice

Nechť $m, n \in \mathbb{N}$. Prvky $\mathbb{R}^{m,1}$ budeme nazývat mprvkové ***vektory*** *a namísto $\mathbb{R}^{m,1}$ budeme často psát pouze $\mathbb{R}^m$. Vektor z $\mathbb{R}^m$, jehož všechny prvky jsou nuly, budeme nazývat* ***nulový vektor*** *a značit θ. Matici z $\mathbb{R}^{m,n}$, jejíž všechny prvky jsou nuly, budeme nazývat* ***nulovou maticí*** *a značit Θ.*

Poznámka: řádky vs. sloupce. . .

Maticový zápis SLR 2

Definice (Maticový zápis soustavy lineárních rovnic)

Nechť $m, n \in \mathbb{N}$, $\mathbb{A} \in \mathbb{R}^{m,n}$, $\mathbb{b} \in \mathbb{R}^m$. *Rovnici*

$$\mathbb{A}\mathbb{x} = \mathbb{b} \tag{7}$$

nazýváme ***soustavou*** m ***lineárních rovnic pro*** n ***neznámých*** $x_1, x_2, \ldots, x_n$.
Vektor $\mathbb{x} \in \mathbb{R}^{n,1}$, *kde* $\mathbb{x}^T = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix}$ *nazýváme* ***vektorem neznámých*** *a vektor* $\mathbb{b} \in \mathbb{R}^{m,1}$, *kde* $\mathbb{b}^T = \begin{pmatrix} b_1 & b_2 & \cdots & b_m \end{pmatrix}$ *vektorem* ***pravých stran***.
Matici $\mathbb{A}$ *nazýváme* ***maticí soustavy*** *a matici*

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

rozšířenou maticí soustavy. *Je-li* $\mathbb{b} = \theta \in \mathbb{R}^m$, *mluvíme o* ***homogenní soustavě***.
Soustava $\mathbb{A}\mathbb{x} = \theta$ *je* ***přidruženou homogenní soustavou lineárních rovnic*** *k soustavě* $\mathbb{A}\mathbb{x} = \mathbb{b}$.
Množinu všech řešení značíme S *(pro nehomogenní) nebo* S_0 *(pro homogenní).*

Struktura řešení SLR 1

Věta

Uvažujme soustavu rovnic $\mathbb{A}\mathbb{x} = \mathbb{b}$. *Platí následující:*

1. *Je-li* $\mathbb{x} \in S_0$ *a* $\alpha \in \mathbb{R}$, *je také* $\alpha\mathbb{x} \in S_0$.
2. *Je-li* $\mathbb{x}, \mathbb{y} \in S_0$, *je také* $\mathbb{x} + \mathbb{y} \in S_0$.
3. *Je-li* $\mathbb{x}, \mathbb{y} \in S$, *je* $\mathbb{x} - \mathbb{y} \in S_0$.
4. *Buď* $\mathbb{x} \in S$, *potom pro každý vektor* $\mathbb{y} \in S$ *existuje nějaký vektor* $\mathbb{z} \in S_0$ *tak, že* $\mathbb{y} = \mathbb{x} + \mathbb{z}$.
5. *Buď* $\mathbb{x} \in S$, *potom pro každý vektor* $\mathbb{z} \in S_0$ *platí, že* $\mathbb{x} + \mathbb{z} \in S$.

(Důkaz. . .)

Kompaktní značení množinových operací

Definice

Buďte A a B libovolné podmnožiny nějaké množiny M, pro jejíž prvky je definováno sčítání $+ : M \times M \to M$ a násobení $\cdot : \mathbb{R} \times M \to M$ číslem z $\mathbb{R}$.
Součet množin *A a B definujeme následovně:*

$$A + B := \{a + b \mid a \in A, b \in B\}.$$

Je-li $A = \{a\}$ jednoprvková, píšeme $a + B$ namísto $\{a\} + B$.
Podobně ***součin reálného čísla*** $\alpha \in \mathbb{R}$ ***a množiny*** *A definujeme jako*

$$\alpha A := \{\alpha a \mid a \in A\}.$$

- příklady...

Struktura řešení SLR 2

Věta

Nechť $\tilde{\mathbb{x}}$ je nějaké řešení soustavy $\mathbb{A}\mathbb{x} = \mathbb{b}$, potom pro tuto soustavu platí, že

$$S = \tilde{\mathbb{x}} + S_0.$$

(Důkaz. . .)

Hlavní body

Cíle GEM

Naše prozatimní cíle:

- Poznat, zda má soustava alespoň jedno řešení nebo nemá řešení žádné.
- Poznat, jestli má daná soustava právě jedno řešení nebo jich má nekonečně mnoho.
- V případě, že má soustava právě jedno řešení, toto řešení nalézt.
- V případě, že má soustava více než jedno řešení, nalézt jich nekonečně mnoho.

Jak poznat soustavy s jedním řešením

- $$\left(\begin{array}{ccc|c} 3 & 2 & 1 & 6 \\ 0 & 2 & 1 & 3 \\ 0 & 0 & 1 & 1 \end{array}\right) \tag{8}$$
- $$\left(\begin{array}{ccc|c} 0 & 1 & 0 & 2 \\ 0 & 2 & -1 & 2 \\ 3 & 0 & 1 & 8 \end{array}\right) \tag{9}$$
- proč snadno řešitelné?
- převedení (řádky/sloupce)

Horní trojúhelníkové matice

Pozorování

Nechť pro matici soustavy $\mathbb{A}\mathbb{x} = \mathbb{b}$ *platí následující:*

1. $\mathbb{A} \in \mathbb{R}^{n,n}$,
2. $\mathbb{A}_{ii} \neq 0$ *pro všechny* $i \in \{1, 2, \ldots, n\}$,
3. *je-li* $i > j$ *je* $\mathbb{A}_{ij} = 0$,

potom má soustava právě jedno řešení.

Maticím splňující body (i) a (iii) se říká **horní trojúhelníkové**.

Jak poznat soustavy bez řešení

- $$\left(\begin{array}{ccc|c} 3 & 1 & 0 & 8 \\ 0 & -1 & 2 & 2 \\ 3 & 1 & 1 & 10 \\ 6 & 1 & 3 & 21 \end{array}\right)$$
- $$\left(\begin{array}{ccc|c} 3 & 1 & 0 & 8 \\ 0 & -1 & 2 & 2 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{array}\right) \tag{10}$$

- proč bez řešení?
- v jakém tvaru lze snadno rozpoznat?

Soustavy s nekonečně mnoha řešeními

$$\left(\begin{array}{ccccc|c} 3 & 1 & 0 & 2 & 0 & 7 \\ 0 & -1 & 2 & 2 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 2 \end{array}\right). \tag{11}$$

- speciální volby proměnných $\rightarrow$ více různých řešení
- nalezneme nekonečně mnoho řešení
- alternativně: **parametrizace**
- chybí teorie, nevíme, jestli máme všechna řešení!!!

Poznámka – co s nulovými sloupci?

Horní stupňovitý tvar matice SLR

Pro přehlednější zápis si zavedeme následující značení:

$$\text{Je-li } n \in \mathbb{N} \text{ potom definujeme } \hat{n} = \{1, 2, \ldots, n\}.$$

Definice

*O matici $\mathbb{D} \in \mathbb{R}^{m,n}$ řekneme, že je v **horním stupňovitém tvaru**, jestliže všechny řádky jsou nulové, nebo existuje $k \in \hat{m}$ tak, že řádky 1 až k matice $\mathbb{D}$ jsou nenulové a řádky $k+1$ až m jsou nulové a jestliže platí následující:*
Označme pro každé $i \in \hat{k}$ index nejlevějšího nenulového prvku v $i$tém řádku jako j_i, tj.

$$j_i = \min\{\ell \in \hat{n} \mid \mathbb{D}_{i\ell} \neq 0\}.$$

Potom platí $1 \leq j_1 < j_2 < \cdots < j_k$.
*Je-li matice v horním stupňovitém tvaru, potom sloupcům s indexy $j_1, j_2, \ldots, j_k$ říkáme **hlavní sloupce**, ostatním říkáme **vedlejší sloupce**.*
O soustavě $\mathbb{A}\mathbb{x} = \mathbb{b}$ řekneme, že je v horním stupňovitém tvaru, pokud matice této soustavy $(\mathbb{A} \mid \mathbb{b})$ je v horním stupňovitém tvaru.

Horní stupňovitý tvar matice SLR - schema

Schéma obecné matice $\mathbb{D}$ v horním stupňovitém tvaru:

$$\begin{pmatrix}
0 & \cdots & 0 & \underbrace{\mathbb{D}_{1j_1}}_{\neq 0} & \cdots & * & * & \cdots & * & * & \cdots & * & * & \cdots & * \\
0 & \cdots & 0 & 0 & \cdots & 0 & \underbrace{\mathbb{D}_{2j_2}}_{\neq 0} & \cdots & * & * & \cdots & * & * & \cdots & * \\
0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & \underbrace{\mathbb{D}_{3j_3}}_{\neq 0} & \cdots & * & * & \cdots & * \\
\vdots & & & \vdots & & & \vdots & & & \vdots & \ddots & & \vdots & & \vdots \\
0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & \underbrace{\mathbb{D}_{kj_k}}_{\neq 0} & \cdots & * \\
0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\
\vdots & & & \vdots & & & \vdots & & & \vdots & & & \vdots & & \vdots \\
0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0
\end{pmatrix}$$

Počet řešení SLRvHST

Věta

Mějme soustavu lineárních rovnic $\mathbb{A}\mathbb{x} = \mathbb{b}$, kde $\mathbb{A} \in \mathbb{R}^{m,n}$. Je-li tato soustava v horním stupňovitém tvaru, platí následující:

1. *Je-li poslední sloupec matice $(\mathbb{A} \mid \mathbb{b})$ hlavní, soustava nemá řešení.*
2. *Je-li poslední sloupec matice $(\mathbb{A} \mid \mathbb{b})$ jediný vedlejší sloupec, má soustava právě jedno řešení.*
3. *Je-li poslední sloupec matice $(\mathbb{A} \mid \mathbb{b})$ vedlejší a existuje-li ještě jiný vedlejší sloupec, má soustava více než jedno řešení.*

Jiný případ než tyto tři nastat nemůže.

(Důkaz. . .)

Elementární kroky GEM

Úpravy SLR (U1), (U2) a (U3) $\rightarrow$ přeznačíme pro maticový zápis SLR:

(G1) Prohození dvou řádků.

(G2) Vynásobení jednoho řádku matice nenulovým číslem.

(G3) Přičtení libovolného násobku jednoho řádku k jinému.

(formálně rozepsat!)

Zřejmý důsledek:

Věta

Převedeme-li rozšířenou matici jedné soustavy na rozšířenou matici jiné pomocí jedné z úprav (G1), (G2) nebo (G3), mají obě soustavy stejnou množinu řešení.

Cíl GEM: převést libovolnou matici SLR do horního stupňovitého tvaru!

GEM $\rightarrow$ „hezký“ první sloupec

Upravujeme matici $\mathbb{A} \in \mathbb{R}^{m,n}$ s prvky a_{ij} a **nenulovým** prvním sloupcem:

1. Pokud není $a_{11} \neq 0$, prohodíme 1. řádek s $i$tým řádkem, pro který je $a_{i1} \neq 0$. (úprava (G1) a využití předpokladu o nenulovosti sloupce)
2. Pro $j = 2, 3, \ldots, m$ přičteme k $j$tému řádku α násobek prvního řádku (úprava (G3)), kde α splňuje rovnici

$$a_{j1} + \alpha a_{11} = 0. \tag{12}$$

Pozor na značení, zjednodušeno!

($\mathbb{A}$ vs. $(\mathbb{A} \mid \mathbb{b})$)

Co „znamená“ nulový sloupec?

Proč to funguje?

Věta

Nechť $a, b \in \mathbb{R}$. Potom $x = -a + b$ je jediné reálné číslo splňující rovnici $a + x = b$.

(Důkaz. . .)

Gaussova eliminační metoda (GEM)

Algoritmus (GEM)

Cíl algoritmu: Pro matici $\mathbb{B} \in \mathbb{R}^{m,n}$, *hledáme takovou posloupnost úprav (G1) a (G3), která ji převede do horního stupňovitého tvaru. Postup: Položme* $\mathbb{B} = (\mathbb{A} \mid \mathbb{b})$, $k = \ell = 1$. *Dokud je* $k \leq n$ *a* $\ell \leq m$, *provádíme následující:*

1. *Platí-li* $\mathbb{B}_{jk} = 0$ *pro všechna* $j = \ell, \ell + 1, \ldots, m$, *položte* $k = k + 1$ *a opakujeme krok 1.*
2. *Je-li* $\mathbb{B}_{\ell k} = 0$ *a* $\mathbb{B}_{jk} \neq 0$ *pro nějaké* $j \in \{\ell + 1, m\}$ *prohodíme pomocí pravidla (G1)* j*tý a* ℓ*tý řádek a pokračujeme do kroku 3.*
3. *Máme* $\mathbb{B}_{\ell k} \neq 0$. *Pomocí (G3) odečteme od všech spodnějších řádků vhodný násobek* ℓ*tého řádku tak, abychom vynuluvali všechny prvky* k*tého sloupce pod prvkem na* ℓ*tém řádku. Položte* $k = k + 1$, $\ell = \ell + 1$ *a pokračujme krokem 1.*

($\ell \to$ řádky, $k \to$ sloupce)

Poznámky a příklad

- „bloková“ či „škrtací“ představa
- neexistuje jediný nejlepší postup
- možné zjednodušující mezikroky
- volné pořadí úprav, zvolených řádků,...
- je třeba zkušenost a myslet dopředu!
- „máme rádi jedničky a nuly“

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

Hlavní body

Co jsme potřebovali? (1 ze 2)

Abychom dokázali vše, co jsme doposud dokázali, nepotřebovali jsme toho o reálných číslech a jejich násobení vědět mnoho.

1. množina reálných čísel je vůči násobení uzavřená, neboli $\forall a, b \in \mathbb{R} : ab \in \mathbb{R}$,
2. násobení je asociativní, neboli $\forall a, b, c \in \mathbb{R} : a(bc) = (ab)c$,
3. existuje reálné číslo 1 tak, že $\forall a \in \mathbb{R}$: $1a = a1 = a$,
4. každé nenulové číslo má inverzi, neboli $\forall a \in \mathbb{R} \setminus \{0\}$, $\exists a^{-1} \in \mathbb{R}$: $aa^{-1} = a^{-1}a = 1$.

Co jsme potřebovali? (2 ze 2)

Pro sčítání jsme potřebovali totéž:

1. množina reálných čísel je vůči sčítání uzavřená, neboli $\forall a, b \in \mathbb{R} : a + b \in \mathbb{R}$,
2. sčítání je asociativní, neboli $\forall a, b, c \in \mathbb{R} : a + (b + c) = (a + b) + c$,
3. existuje reálné číslo 0 tak, že $\forall a \in \mathbb{R}$: $0 + a = a + 0 = a$,
4. každé číslo má opačný prvek, neboli $\forall a \in \mathbb{R}$, $\exists(-a) \in \mathbb{R}$: $a + (-a) = (-a) + a = 0$.

K tomu všemu jsme ještě potřebovali distributivní zákon (vytýkání ze závorky resp. roznásobení závorky):

$$\forall a, b, c \in \mathbb{R} : a(b + c) = ab + ac \wedge (b + c)a = ba + ca.$$

Nutně jsme nepotřebovali komutativitu násobení ani sčítání, ale dost nám při počítání usnadňovaly život.

Kde jinde to ještě máme?

- Všechny tyto vlastnosti máme ale i v množině $\mathbb{Q}$ a $\mathbb{C}$ (s klasickým sčítáním a násobením)!
- Jak jsme na tom v $\mathbb{Z}$ a $\mathbb{N}$?
- Určete počet řešení násl. soustavy v množinách $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$:

$$\left(\begin{array}{ccc|c} 2 & 4 & 6 & 0 \\ 3 & 6 & 11 & 1 \end{array}\right).$$

Modulární aritmetika

- Značení pro **zbytek po dělení** přirozeným číslem $n \geq 2$:

$$m \pmod{n}.$$

- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$
- **sčítání modulo** n

$$m +_n q := (m + q) \pmod{n}$$

- **násobení modulo** n:

$$m \cdot_n q := (m \cdot q) \pmod{n}$$

Splňuje $(\mathbb{Z}, +_n, \cdot_n)$ nebo alespoň $(\mathbb{Z}_n, +_n, \cdot_n)$ vše potřebné pro řešení soustav lineárních rovnic?

Množina $\mathbb{Z}_p$

Lemma

Sčítání a násobení celých čísel modulo n jsou asociativní a komutativní binární operace a platí pro ně distributivní zákon.

- Role „neutrálních“ prvků pro sčítání a násobení stále hrají 0 resp. 1.
- Opačné prvky $-m$ existují pro každé $m \in \mathbb{Z}_n$.
- Inverzní prvky m^{-1} existují pro nenulová m, jenom když je m nesoudělné s n.
- Chceme-li, aby nám vše fungovalo v $(\mathbb{Z}_n, +_n, \cdot_n)$ jako v $(\mathbb{R}, +, \cdot)$, musí být n prvočíslo (obvykle znač. p).

Grupa

Nebudeme již konstruovat další množiny, půjdeme na to z druhé strany: zajímá nás, jaké vlastnosti musí mít množina a dvě binární operace, aby se v nich daly řešit soustavy lin. rovnic tak, jak jsme si ukázali pro $(\mathbb{R}, +, \cdot)$.

Pro ilustraci začněme jednodušší otázkou: Pro jaké množiny a jaké binární operace má řešení lin. rovnice jedné neznámé?

Definice

Nechť M je neprázdná množina a $\circ : M \times M \to M$ binární operace. Platí-li

1. $\forall a, b, c \in M : a \circ (b \circ c) = (a \circ b) \circ c$ *(asociativní zákon),*
2. *existuje $e \in M$ tak, že $\forall a \in M : a \circ e = e \circ a = a$ (existence* ***neutrálního prvku****),*
3. $\forall a \in M, \exists a^{-1} \in M : \; a \circ a^{-1} = a^{-1} \circ a = e$ *(existence* ***inverzních prvků****),*

říkáme že uspořádaná dvojice $G = (M, \circ)$ je ***grupa****.*
Je-li navíc $\circ$ komutativní, tj. $\forall a, b \in M : a \circ b = b \circ a$, mluvíme o ***Abelovské grupě****.*

Grupa a lineární rovnice

Grupu můžeme chápat, jako nejjednodušší strukturu, kde umíme zformulovat lin. rovnici jedné neznámé a navíc ji umíme i jednoznačně vyřešit.

Věta

Nechť $(M, \circ)$ je grupa a $a, b \in M$. Potom $x = a^{-1} \circ b$ je jediný prvek M splňující rovnici $a \circ x = b$.

- Následující uspořádané dvojice (množina, binární operace) tvoří grupu:

  $$(\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{C}, +), (\mathbb{R}\backslash\{0\}, \cdot), (\mathbb{Q}\backslash\{0\}, \cdot), (\mathbb{C}\backslash\{0\}, \cdot), (\mathbb{Z}_n, +_n), (\mathbb{Z}_p\backslash\{0\}, \cdot_p),$$

  kde $n \geq 2$ je přirozené číslo a p je prvočíslo.

- Ve všech těchto množinách má tedy rovnice $a \circ x = b$, kde $\circ$ je příslušná binární operace, jednoznačné řešení!

Těleso

Definice

Nechť M je neprázdná množina a $+ : M \times M \to M$, $\cdot : M \times M \to M$ dvě binární operace. Platí-li, že

1. $(M, +)$ *je Abelovská grupa (neutrální prvek značíme* 0 *a nazýváme* ***nulovým prvkem****),*
2. $(M \setminus \{0\}, \cdot)$ *je grupa (neutrální prvek značíme* 1 *a nazýváme* ***jednotkový prvek****),*
3. *platí levý a pravý distributivní zákon, tj.*

$$\forall a, b, c \in M : a(b + c) = ab + ac \wedge (b + c)a = ba + ca,$$

nazýváme uspořádanou trojici $T = (M, +, \cdot)$ ***tělesem****.*
Je-li navíc $(M \setminus \{0\}, \cdot)$ Abelovská grupa, je T ***komutativní těleso****.*

Těleso a soustavy lineárních rovnic

Těleso můžeme podobně jako grupu chápat jako nejjednodušší strukturu, kde umíme zformulovat a pomocí GEM „vyřešit“ soustavy lineárních rovnic.

Budeme také používat značení $T^{m,n}$ pro matice s prvky z tělesa T. Jejich násobení prvkem z tělesa T, jejich sčítání a (maticové) násobení zavádíme úplně stejně jako v $\mathbb{R}$.

V celém kurzu BI-LIN budeme pracovat **pouze s komutativními tělesy**.