

- 1 Definujte rozšířenou matici soustavy.
- 2 Definujte elementární řádkové operace.
- 3 Definujte odstupňovaný tvar matice.
- 4 Napište pseudokód pro Gaussovu eliminaci.
- 5 Definujte pivot a to slovně i formálně.
- 6 Definujte volné a bazické proměnné.
- 7 Definujte hodnotu matice.
- 8 Definujte jednotkovou matici.
- 9 Definujte transponovanou matici.
- 10 Definujte symetrickou matici.
- 11 Definujte maticový součin.
- 12 Definujte inverzní matici.
- 13 Definujte regulární matici.
- 14 Definujte singulární matici.
- 15 Definujte binární operaci.
- 16 Definujte komutativní a asociativní binární operace.
- 17 Definujte neutrální prvek v množině s binární operací.
- 18 Definujte inverzní prvek v množině s binární operací.
- 19 Definujte grupu.
- 20 Definujte Abelovskou grupu.
- 21 Definujte permutaci.
- 22 Definujte symetrickou grupu a určete její neutrální a inverzní prvky.
- 23 Definujte transpozici.
- 24 Definujte inverzi v permutaci.
- 25 Definujte znaménko permutace.
- 26 Definujte permutační matici.
- 27 Definujte těleso.
- 28 Definujte charakteristiku tělesa.
- 29 Definujte vektorový prostor.
- 30 Definujte podprostor vektorového prostoru.
- 31 Definujte lineární kombinaci.
- 32 Definujte podprostor generovaný množinou (lineární obal).
- 33 Definujte řádkový prostor matice a to slovně i formálně pomocí maticového součinu.
- 34 Definujte sloupcový prostor matice a to slovně i formálně pomocí maticového součinu.
- 35 Definujte jádro matice.
- 36 Definujte množinu lineárně nezávislých vektorů.
- 37 Definujte bázi vektorového prostoru.
- 38 Definujte dimenzi vektorového prostoru.
- 39 Definujte vektor souřadnic.
- 40 Definujte lineární zobrazení.
- 41 Definujte afinní prostor a jeho dimenzi.
- 42 Definujte jádro lineárního zobrazení.
- 43 Definujte matici lineárního zobrazení.
- 44 Definujte matici přechodu.

44 Definujte isomorfismus vektorových prostorů.

45 Uveďte a dokažte vztah mezi elementárními řádkovými operacemi a soustavami rovnic.

46 Vyslovte a dokažte větu o jednoznačnosti volných a bazických proměnných.

47 Vyslovte a dokažte Frobeniovu větu o existenci řešení soustavy.

48 Vyslovte a dokažte větu o vztahu mezi řešeními $Ax = b$ a $Ax = 0$.

49 Uveďte a dokažte větu popisující všechna řešení $Ax = b$.

50 Vyslovte a dokažte větu o ekvivalentních definicích regulárních matic.

51 Vyslovte a dokažte větu o znaménku složené permutace.

52 Uveďte a dokažte větu charakterizující, kdy $\mathbb{Z}_n$ je těleso.

53 Vyslovte a dokažte malou Fermatovu větu.

54 Vyslovte a dokažte větu o průniku vektorových prostorů.

55 Vyslovte a dokažte větu o ekvivalentních definicích lineárního obalu.

56 Vyslovte a dokažte tvrzení o mohutnostech lineárně nezávislé množiny a generující množiny.

57 Uveďte a dokažte Steinitzovu větu o výměně (včetně lemmatu a jeho důkazu, pokud jej potřebujete).

58 Vyslovte a dokažte větu o dimenzi průniku vektorových prostorů.

59 Vyslovte a dokažte větu o vektorových prostorech souvisejících s maticí A (včetně lemmatu, které se týká součinu matic a jeho důkazu, pokud jej potřebujete).

60 Vyslovte a dokažte větu o dimenzi jádra matice.

61 Vyslovte a dokažte větu o jedinečnosti lineárního zobrazení.

62 Vyslovte a dokažte tvrzení, že převod na vektor souřadnic je lineární zobrazení.

63 Vyslovte a dokažte pozorování o matici složeného lineárního zobrazení.

64 Vyslovte a dokažte větu o charakterizaci isomorfismu mezi vektorovými prostory pomocí matic.

65 Vyslovte a dokažte větu o řešení rovnice s lineárním zobrazením.

66 Zformulujte problém o počtu sudých podgrafů a vyřešte jej.

67 Zformulujte problém o množinových systémech s omezeními na mohutnosti a vyřešte jej.

68 Zformulujte problém o dělení obdélníku na čtverce a vyřešte jej.

70 Přehledově sepište, co víte o elementárních řádkových operacích a Gaussově eliminaci.

71 Přehledově sepište, co víte o řešení homogenních a nehomogenních soustav lineárních rovnic.

72 Přehledově sepište, co víte o maticových operacích.

73 Přehledově sepište, co víte o regulárních a singulárních maticích.

74 Přehledově sepište, co víte o binárních operacích a jejich vlastnostech.

75 Přehledově sepište, co víte o (obecných) grupách.

76 Přehledově sepište, co víte o permutačních grupách.

77 Přehledově sepište, co víte o tělesech.

78 Přehledově sepište, co víte o vektorových prostorech a jejich podprostorech.

79 Přehledově sepište, co víte o vektorových prostorech určených maticí A .

80 Přehledově sepište, co víte o lineární závislosti.

81 Přehledově sepište, co víte o bázích vektorových prostorů.

82 Přehledově sepište, co víte o lineárních zobrazeních.

83 Přehledově sepište, co víte o maticích lineárních zobrazení.

84 Přehledově sepište, co víte o afinních prostorech.

1) Definujte rozšířenou matici soustavy

Necht $\tilde{A} \in \mathbb{R}^{m \times n}$ - matice soustavy

• $b \in \mathbb{R}^m$ - vektor pravých stran

• $x = (x_1, x_2, \dots, x_n)^T$ - vektor neznámých

Pak matice $(A|b) \in \mathbb{R}^{m \times (n+1)}$ je rozšířená matice soustavy,

kde vektor $x \in \mathbb{R}^n$ je řešením soustavy $Ax=b$, který musí splňovat

$$\forall i \in \{1, \dots, m\} : a_{i1}x_1 + a_{i2}x_2 + \dots + a_{in}x_n = b_i$$

2) Definujte elementární řádkové operace

↳ elementární ekvivalentní řádkové úpravy jsou takové, které nemění množinu řešení

$A \sim A'$, kde $A \in \mathbb{R}^{m \times n}$ matice o m řádcích a n sloupcích

1) vynásobení i -tého řádku nenulovým $t \in \mathbb{R} \setminus \{0\}$

↳ pro prvky řádku k , pokud je $i \rightarrow$ vynásobím jen jeden řádek

$$a'_{kl} = \begin{cases} a_{kl} & \text{pro } k \neq i \\ ta_{il} & \text{pro } k = i \end{cases}$$

2) přičtení j-tého řádku k i-tému

$$a'_{kl} = \begin{cases} a_{kl} & \text{pro } k \neq i \\ a_{il} + a_{kl} & \text{pro } k = i \end{cases}$$

3) přičtení j-tého řádku vynásobeného $t \in \mathbb{R} \setminus \{0\}$ k i-tému

↳ lze odvodit z předchozích, ale formálně

$$a'_{kl} = \begin{cases} a_{kl} & \text{pro } k \neq i \\ a_{il} + t a_{kl} & \text{pro } k = i \end{cases}$$

4) sámení dvou řádků

↳ matice $A \in \mathbb{R}^{m \times n}$, kde k a i jsou indexy řádků a μ, δ jsou

$$\begin{array}{l} A_{ij} = \mu \\ A_{kj} = \delta \end{array} \xrightarrow{+\delta} \begin{array}{l} A_{ij} = \mu + \delta \\ A_{kj} = \delta \end{array} \xrightarrow{-\mu - \delta} \begin{array}{l} A_{ij} = \mu + \delta \\ A_{kj} = -\mu \end{array} \xrightarrow{1 \cdot (-1)} \begin{array}{l} A_{ij} = \mu + \delta \\ A_{kj} = \mu \end{array} \xrightarrow{-\mu} \begin{array}{l} A_{ij} = \delta \\ A_{kj} = \mu \end{array}$$

hodnoty prvků matice

provedení několika (postupnosti) řádkových operací se značí $A \sim A'$

3) Definujte odstupňovaný tvar matice

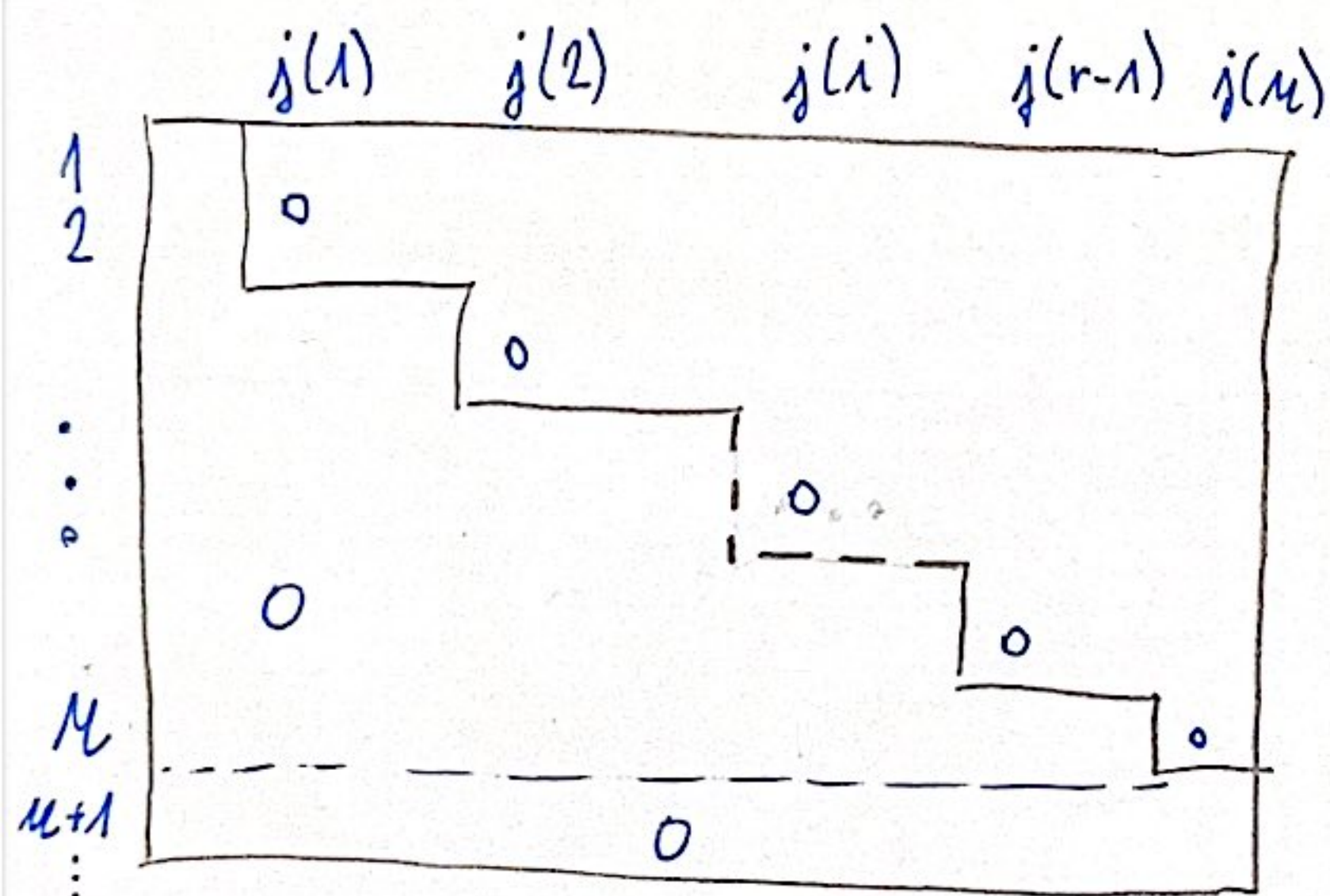
↳ Matice $A \in \mathbb{R}^{m \times n}$ je v REF (row echelon form) = řádkově odstupňovaném tvaru matice pokud

Matice pokud

$$\exists r \in \{1, \dots, m\} : \begin{cases} \textcircled{1} j(1) < j(2) < \dots < j(r) & \leftarrow \text{sloupce, kde je pivot mají indexy za sebou, tedy 1. až r-tý řádek jsou nenulové} \\ \textcircled{2} \forall i > r : \forall j : a_{ij} = 0 & \leftarrow \text{řádky } r+1 \text{ až } m \text{ jsou nulové} \end{cases}$$

↳ $\textcircled{1}$ platí, když určíme, že $j(i) := \min \{j : a_{ij} \neq 0\}$ - definice pivotu

↳ první nenulový prvek v řádku je pivot $\uparrow$



tedy:

existuje $r \in \{1, \dots, m\} \rightarrow \exists r \in \{1, \dots, m\}$

pro které platí:

$\textcircled{1}$ všechny řádky s indexem menším než r mají pivot nebo-li jsou nenulové

$\textcircled{2}$ řádky s indexy $r+1$ až m jsou nulové

4) Napište pseudokód pro Gaussovu eliminaci

↖ algoritmus 1

Vstup: matice $A \in \mathbb{R}^{m \times n}$

seřadit řádky podle $j(i)$, kde $j(i) := \min \{j : a_{ij} \neq 0\}$, musí
podle pivotů, aby byly pivoty s nižším indexem sloupce byly na nižším
indexu řádku

donekonečna:

if $\exists i : j(i) = j(i+1) < \infty$:
↖ nebo-li pivoty jsou ve stejném sloupci, musím
definovat, že $j(i) = \infty$ je prázdný řádek

přičíst k $(i+1)$ -tému řádku $-\frac{a_{i+1, j(i)}}{a_{i, j(i)}}$ násobek i -tého řádku

aktualizujte $j(i+1)$ a seřadte $(i+1)$ -lý řádek na místo → musí
pohravit
else:

return A ↖ bude v REF tvaru, protože $\nexists i : j(i) = j(i+1) < \infty$

↖ algoritmus 2

Vstup: matice $A \in \mathbb{R}^{m \times n}$

1. $i := 1$; $j := 1$

2. if $a_{ke} = 0$ pro všechna $k \geq i$ a $l \geq j$ then konec

3. $j := \min \{l : l \geq j, a_{kl} \neq 0 \text{ pro nějaké } k \geq i\}$ → přeskóť nějaké podsloupce

4. najdi k takové, že $a_{kj} \neq 0$, $k \geq i$ a vyměň řádky A_{i*} a A_{k*}

5. pro všechna $k > i$ polož $A_{k*} := A_{k*} - \frac{a_{kj}}{a_{ij}} A_{i*}$

6. polož $i := i+1$, $j := j+1$ a jdi na krok 2

5) Definujte pivot a to slovně i formálně

↳ pivot je první nenulový prvek v řádku matice

↳ sloupce v REF tvaru, kde je pivot jsou báze, naopak kde pivot není, tak jsou volné

Formálně Necht' $A \in \mathbb{R}^{m \times n}$ v REF tvaru, pak $\forall i \in \{1, \dots, m\}: j(i) = \min \{j: a_{ij} \neq 0\}$

↳ pokud je řádek nenulový, pak pivot je $a_{i,j(i)}$

↳ kde $a_{i,j}$ je prvek na i -tém řádku v j -tém sloupci

6) Definujte volné a báze proměnné

↳ Necht' $A \in \mathbb{R}^{m \times n}$ a pivot je $a_{i,j(i)}$, kde $j(i) = \min \{j: a_{ij} \neq 0\}$

↳ $a_{i,j}$ je prvek matice A na i -tém řádku v j -tém sloupci

↳ množina řešení $x = (x_1, \dots, x_n)^T$ soustavy $A'x = b'$ v REF tvaru,

kde $b = (b_1, \dots, b_m)^T$ je vektor pravých stran

↳ báze proměnné jsou takové $x_{j(1)}, x_{j(2)}, \dots, x_{j(\kappa)}$, kde $\kappa = \text{rank}(A)$

nebo-li hodnost jako počet nenulových řádků a kde $j(1) < j(2) < \dots < j(\kappa)$

↳ indexy sloupců

↳ volné proměnné jsou takové

$$\{1, \dots, n\} = \{j(1), \dots, j(\kappa)\} \cup F$$

↳ x_k , kde $k \in F$

↳ disjunkt ní
sjednocen

↳ počet volných proměnných je $f = n - \kappa$

7) Definujte hodnotu matice

- ↳ hodnota matice A je počet pivotů po převedení do odstupňovaného tvaru
- ↳ značí se $\text{rank}(A)$
- ↳ z toho vychází Frobeniova věta $\rightarrow$ soustava $Ax = b$ má řešení právě tehdy, když se hodnota matice A rovná hodnotě rozšířené matice $(A|b)$
- ↳ matice $A \in \mathbb{R}^{m \times n}$, pivot je $j(i) := \min \{j : a_{ij} \neq 0\}$

8) Definujte jednotkovou matici

Pro $n \in \mathbb{N}$ je jednotková matice $I_n \in \mathbb{R}^{n \times n}$ definována pomocí

$$(I_n)_{ij} = \begin{cases} 1 & \text{pokud } i=j \\ 0 & \text{jinak} \end{cases}$$

Pro nulovou matici: Pro libovolná $m, n \in \mathbb{N}$ existuje $O_{m,n} \in \mathbb{R}^{m \times n}$, pro které platí $\forall i, j: (O_{m,n})_{i,j} = 0$

↳ na hlavní diagonále nebo-li prvky (a_{ii}) jsou neutrální vůči násobení ^(matice) v algebraické struktuře

$$\forall A \in M_n(K) : IA = AI = A$$

↳ I je jednotková matice

9) Definujte transponovanou matici

Transponovaná matice k matici $A \in \mathbb{R}^{m \times n}$ je matice $A^T \in \mathbb{R}^{n \times m}$,

kteřá splňuje $(A^T)_{ij} = (A)_{ji}$

↳ vzniká záměnou řádků a sloupců matice

10) Definujte symetrickou matici

↳ symetrická matice je čtvercová matice, co se rovná své transpozici

Nechť $A \in T^{n \times n}$ nad tělesem T , pak platí $A = A^T$ pro symetrickou matici

↳ $\forall i, j \in \{1, \dots, n\} : a_{ij} = a_{ji}$, kde $a_{ij} = (A)_{ij}$ prvek matice na indexu řádku i a sloupce j

11) Definujte maticový součin

↳ Pro $A \in \mathbb{R}^{m \times n}$ a $B \in \mathbb{R}^{n \times p}$ je $(AB) \in \mathbb{R}^{m \times p}$ definován jako

$$(AB)_{ij} = \sum_{k=1}^n a_{ik} b_{kj} \quad \Leftarrow \text{platí pro } \forall i \in \{1, \dots, m\}, j \in \{1, \dots, p\}$$

$$\begin{array}{c|cc} B = & b_{11} & b_{12} \\ & b_{21} & b_{22} \\ \hline A = \begin{array}{cc} a_{11} & a_{12} \\ a_{21} & a_{22} \end{array} & \Rightarrow (AB) = & \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix} \end{array}$$

↳ není komutativní

↳ aby součin platil musí matice zleva ^{tohoto sloupce} a zprava ^{co} ^{matice} ^{zprava} ^{řádků}

12) Definujte inverzní matici

Buď $A \in \mathbb{R}^{n \times n}$ Pak $B \in \mathbb{R}^{n \times n}$ je inverzní matice pokud splňuje $A \cdot B = B \cdot A = I_n$

↳ kde I_n je jednotková matice $I_n \in \mathbb{R}^{n \times n}$ pro kterou platí

$$(I_n)_{ij} = \begin{cases} 1 & \text{pokud } i=j \\ 0 & \text{jinak} \end{cases}$$

↳ inverzní k I_n je I_n , k O_n neexistuje

↳ inverzní matice je určena jednoznačně

↳ pokud k matici existuje inverzní, pak je regulární, jinak singulární

13) Definujte regulární matici

↳ matice je regulární pokud k ní existuje inverze

$A \in \mathbb{R}^{n \times n}$ a $B \in \mathbb{R}^{n \times n}$ pro které platí $A \cdot B = B \cdot A = I_n$, Pak jedna je inverzní k druhé

↳ ekvivalentní definice

↳ 1. existuje inverze $\rightarrow A$ je regulární, tj. $\exists B \in \mathbb{R}^{n \times n} : A \cdot B = I_n$

↳ 2. soustava $Ax=0$ má pouze triviální řešení $x=0$

↳ 3. $RREF(A) = I_n$ nebo-li $A \sim I_n$. Gauss-Jordanovoe eliminací
ke elementárními řádkovými úpravami dostal jednotkovou
matici

↳ 4. $\text{rank}(A) = n$. Hlost matice je rovna jejímu řádku (matice má
plnou hodnost.)

14) Definujte singulární matici

↳ Čtvercová matice $A \in \mathbb{R}^{n \times n}$ je singulární právě tehdy, když není regulární, tedy platí negace definice regulární matice

1. $A \in \mathbb{R}^{n \times n}$ je singulární, tj. $\nexists B \in \mathbb{R}^{n \times n} : A \cdot B = I_n$

↳ nemá inverzi

2. Soustava $Ax = 0$ má netriviální řešení. Nebo-li řádky (a sloupce) matice jsou lineárně závislé.

3. $\text{rank}(A) < n$. Hodnota je menší než řád matice.

↳ pokud matice $A \in \mathbb{R}^{m \times n}$ $\wedge m = n$, tak je to matice n -tého řádu.

↳ pokud $m \neq n$, tak je obdelníková, tedy singularita nemůže být definována

15) Definujte binární operaci

Binární operace je zobrazení, kde každé uspořádané dvojici prvků přiřadí jednoznačný prvek ze stejné množiny

$\circ : A \times A \rightarrow A$, kde A je množina

↳ platí uzavřenost $\forall a, b \in M : a * b \in M$

↑ binární operace

16) Definujte komutativní a asociativní binární operace

↳ Binární operace $\circ : A \times A \rightarrow A$ platí, že uspořádané dvojici prvků z množiny A příslušný jednoznačně určený prvek také z množiny A

↳ komutativní: $\rightarrow$ pak se jedná o Abelovskou grupu

$$\forall a, b \in M : a \cdot b = b \cdot a \quad \wedge \quad \forall a, b \in M : a \cdot b \in M \quad \text{z uzavřenost}$$

↳ asociativní:

↳ pokud navíc definovanou binární operaci $\circ : A \times A \rightarrow A$, tak asociativita je:

$$\forall a, b, c \in A : a \circ (b \circ c) = (a \circ b) \circ c$$

17) Definujte neutrální prvek v množině s binární operací

↳ Binární operace : $\circ : M \times M \rightarrow M$, kde M je neprázdná množina

↳ neutrální prvek platí: $\exists e \in M : \forall a \in M : e \circ a = a \circ e = a$

↳ neutrální prvek je určen jednoznačně, protože kdyby existovaly dva, tak

by vyšel první důkaz : $\exists e_1, e_2 \in M : e_1 = e_1 \circ e_2 = e_2 \circ e_1 = e_2$

↳ kde $e_1 = e_2$, takže jsou stejné prvky

18) Definujte inverzní prvek v množině s binární operací

↳ binární operace: $\circ: M \times M \rightarrow M$

↳ inverzní prvek: $\forall a \in M: \exists b \in M: a \circ b = b \circ a = e$, kde e je

jednoznačně určený neutrální prvek: $\exists e \in M: \forall a \in M: a \circ e = e \circ a = a$

↳ inverzní prvek je ke konkrétnímu prvku nazorčí od neutrálního, který se vztahuje na celou množinu

19) Definujte grupu

↳ grupa $(G, \circ)$ je množina G spolu s binární operací $\circ: G \times G \rightarrow G$, tedy roztvořením uspořádané dvojice prvků na jednoznačně určený prvek v množině G

↳ platí tam 3 axiomy:

1) asociativita

$$\forall a, b, c \in G: a \circ (b \circ c) = (a \circ b) \circ c$$

2) neutrální prvek $\rightarrow$ (neutrální prvek je pro grupu jednoznačný)

$$\exists e \in G: \forall a \in G: e \circ a = a \circ e = a$$

3) inverzní prvek $\rightarrow$ (ke každému prvku existuje právě jeden inverzní - jednoznačný)

$$\forall a \in G: \exists b \in G: a \circ b = b \circ a = e, \text{ kde } e \text{ je neutrální prvek grupy}$$

↳ grupa je Abelovská pokud tam zároveň platí komutativita: $\forall a, b \in G: a \circ b = b \circ a$

↳ nejmenší grupa je $(\{e\}, \circ)$, kde platí $e \circ e = e$

- $\rightarrow$ asociativita $\checkmark$
- $\rightarrow$ neutrální $\checkmark$
- $\rightarrow$ inverzní $\checkmark$
- $\rightarrow$ (komutativita $\checkmark$)

↳ musí být uzavřená: $\forall a, b \in G: a \circ b \in G$

20) Definujte Abelovskou grupu

↳ Grupa $(G, \circ)$ je abelovská pokud k axiomů pro definici

grupy splňuje i komutativitu $\forall a, b \in G: a \circ b = b \circ a$

↳ potřeba definovat grupu, binární operaci atd.

21) Definujte permutaci

↳ Permutace na množině $\{1, 2, \dots, n\}$ je ^{↖ konečné množině} bijektivní zobrazení

$$\mu: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$$

↳ množina všech permutací se značí S_n

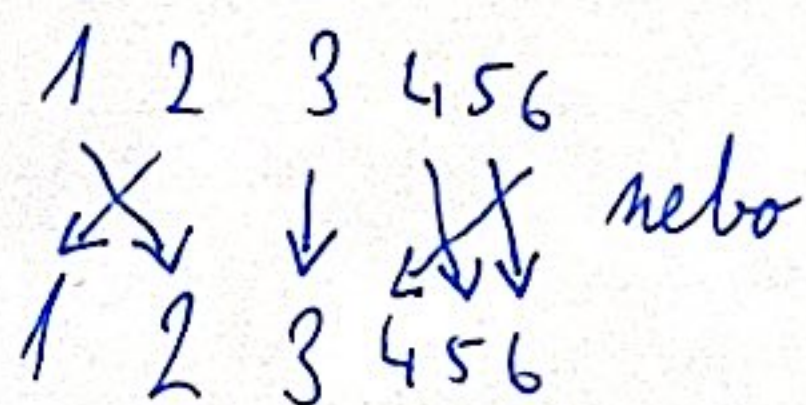
↳ dá se zobrazit tabulkou, grafem, rozložením na cykly

Tabulka

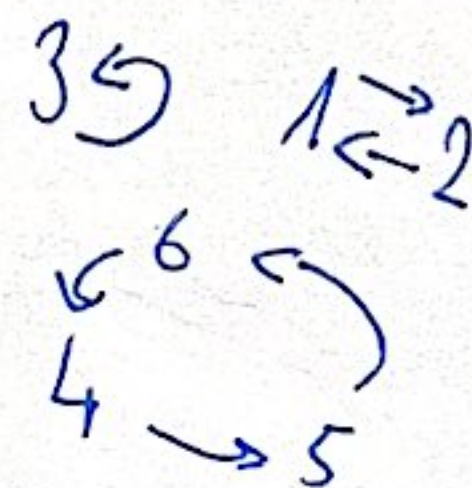
$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$ ↖ nahore vzory
↖ dole zobrazení, píše se většinou zvlášť $\mu =$

grafem

↳ kam se který prvek zobrazí



nebo



rozložením na cykly

$\mu = (213564)$ ↖ tabulkou

$$\Rightarrow \mu = (1, 2)(3)(4, 5, 6)$$

22) Definujte symetrickou grupu

↳ Grupa (uvést 3 axiomy grupy) tvořená množinou všech permutací na n prvcích $\rightarrow S_n$ a operací skládání $\circ \rightarrow (S_n, \circ)$

↳ skládání se zapisuje $(q \circ p)(i) = q(p(i))$

↳ neutrální prvek symetrické grupy je identita $id \rightarrow \forall i \in \{1, \dots, n\} : id(i) = i$

↳ inverzní prvek symetrické grupy je $\forall p \in S_n : \exists p^{-1} \in S_n : p \circ p^{-1} = p^{-1} \circ p = id$

↳ asociativní $\rightarrow \forall p, q, r \in S_n : (p \circ q) \circ r = p \circ (q \circ r)$

↳ uzavřenost $\rightarrow$ složení dvou permutací je permutace $\forall p, q \in S_n : p \circ q \in S_n$

↳ inverzní permutace $p(i) = j \quad p^{-1}(j) = i \Rightarrow p(p^{-1}(j)) = j \Rightarrow id(j) = j$

$\uparrow$
nejdříve se aplikuje p^{-1}

23) Definujte Transpozici

↳ je jednoduchá, ale netriviální (triviální permutace je jen identita), která prohodí 2 prvky a ostatní nemění, tedy permutace $\Delta = (i, j)$ s jedním cyklem délky 2

↳ Transpozice tedy musí splňovat:

- $\Delta(i) = j$

- $\Delta(j) = i$

- $\forall k \in X \setminus \{i, j\} : \Delta(k) = k \rightarrow$ ostatní prvky

↳ $X = \{1, \dots, n\}$ a S_n - symetrická grupa

množina indexů
body

↳ každá netriviální permutace

se rozloží na složení Transpozic

$$\bullet (\mu_1, \dots, \mu_r) = (\mu_1, \mu_2) \circ (\mu_2, \mu_3) \circ \dots \circ (\mu_{r-1}, \mu_r)$$

$$\bullet (\mu_1, \dots, \mu_r) = (\mu_1, \mu_r) \circ (\mu_1, \mu_{r-1}) \circ \dots \circ (\mu_1, \mu_2)$$

24) Definujte inverzi v permutaci

↳ inverze v permutaci není to samé co inverzní permutace

↳ inverze v permutaci je dvojice indexů i, j , pro které platí, že pokud index i je menší než j , tak obraz i je větší než obraz j

$$(i, j) : (i < j) \wedge (\mu(i) > \mu(j))$$

↳ příklad : $i \quad j$
 $\swarrow \searrow$
 $i \quad j$
 $\mu(i) = j$
 $\mu(j) = i$, kdyby byly čísla

$1 \quad 2$
 $\swarrow \searrow$
 $1 \quad 2$
 $\mu(1) = 2$
 $\mu(2) = 1$

25) Definujte znaménko permutace

↳ znaménko je buď sudé $+1$ nebo liché -1

↳ Necht' $\mu \in S_n$, pak znaménko permutace je : $\text{sgn}(\mu) = (-1)^{\# \text{inverzí } \mu}$

$$\text{sgn}(\mu) = (-1)^{\# \text{počet sudých cyklů } \mu}$$

$$\text{sgn}(\mu) = (-1)^{\# \text{transpozic libovolného rozkladu } \mu \text{ na transpozice}}$$

$\mu \in S_n$ a k počet cyklů, pak $\text{sgn}(\mu) = (-1)^{n-k}$

↳ platí $\text{sgn}(\text{id}) = 1$

$$\text{sgn}((i, j)) = -1$$

↳ $\forall \mu, q \in S_n : \text{sgn}(\mu \circ q) = \text{sgn}(\mu) \cdot \text{sgn}(q)$

26) Definujte permutační matici

↳ permutační matice je zápis permutace v číselné matici

$$\hookrightarrow \pi \in S_n; \quad P \in T^{n \times n}$$

pro $\pi = (1, 2)(3) \rightarrow$ zapísáno v cyklech

$$\hookrightarrow (P)_{i,j} = \begin{cases} 1 & \text{pokud } \pi(i) = j \\ 0 & \text{jinak} \end{cases}$$

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

$$A \in T^{m \times n}$$

↳ násobení zleva $P \cdot A \rightarrow$ permutovala řádky A podle π

↳ násobení zprava $A \cdot P \rightarrow$ permutovala sloupce A podle π

27) Definujte těleso

↳ těleso $(T; +; \cdot)$ je množina T spolu se dvěma komutativními operacemi $+$ a $\cdot$, kde $(T; +)$ a $(T \setminus \{0\}; \cdot)$ jsou dvě Abelovské grupy

↳ takže je potřeba uvést 4 axiomy pro $(T; +)$, 4 axiomy pro $(T \setminus \{0\}; \cdot)$ a distributivní zákon $\rightarrow$ celkově 9

1) $(T; +)$ je Abelova grupa

a) asociativita $\forall a, b, c \in T: a + (b + c) = (a + b) + c$

b) neutrální prvek $\exists 0 \in T: \forall a \in T: 0 + a = a + 0 = a$

↳ značí se 0 , protože

c) komutativita $\forall a, b \in T: a + b = b + a$

d) inverzní (opačný) prvek $\forall a \in T: \exists -a \in T: a + (-a) = 0$

↳ značí se $-a$, protože

2) $(T \setminus \{0\}, \cdot)$ je Abelova grupa

a) asociativita $\forall a, b, c \in T: a \cdot (b \cdot c) = (a \cdot b) \cdot c$

b) neutrální prvek $\exists 1 \in T: \forall a \in T: 1 \cdot a = a$

c) inverzní prvek $\forall a \in T: \exists a^{-1} \in T: a \cdot a^{-1} = a^{-1} \cdot a = 1$

d) komutativita $\forall a, b \in T: a \cdot b = b \cdot a$

3) distributivita

$$\forall a, b, c \in T: a \cdot (b + c) = a \cdot b + a \cdot c$$

↳ prvky tělesa jsou skaláry

↳ $0 \neq 1 \Rightarrow$ proto je nutné, aby těleso mělo minimálně 2 prvky, tedy neutrální prvky pro obě grupy

↳ potřeba dokázat, že násobení je komutativní $0a = a0 = 0$, protože

$(T \setminus \{0\}, \cdot)$ to nezahrnuje ve svých axiomech, ale v množině je

↳ $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ jsou tělesa, $\mathbb{N}, \mathbb{Z}$ nejsou tělesa

28) Definujte charakteristiku tělesa

↳ charakteristika tělesa je nejmenší přirozené číslo, které nedaří kolikrát ke sečištění jednotkový prvek, aby potom zůstali 0

$$\exists m \in \mathbb{N}: \underbrace{1 + 1 + \dots + 1}_{n\text{-krát}} = 0 \quad \text{nebo-li} \quad \exists m \in \mathbb{N}: \sum_{k=1}^m 1 = 0$$

↳ pokud takové číslo neexistuje pak je charakteristika tělesa 0

↳ charakteristika tělesa je vždy prvočíslo nebo 0

$$\text{char}(\mathbb{R}) = 0 \quad \text{char}(\mathbb{Z}_p) = p$$

29) Definujte vektorový prostor

↳ Vektorový prostor $(V, +, \cdot)$ nad tělesem $(T, +, \cdot)$, kde $+$ u vektorového prostoru je binární operace $+: V \times V \rightarrow V$ a $\cdot$ je skalární násobek $\cdot: T \times V \rightarrow V$

↳ musí platit axiomy: (10)

1) $(V, +)$ je Abelova grupa

a) uzavřenost, platí bin. operace $\forall u, v \in V: u + v \in V$

b) asociativita $\forall u, v, w \in V: u + (v + w) = (u + v) + w$

c) komutativita $\forall u, v \in V: u + v = v + u$

d) neutrální prvek $\exists 0 \in V: \forall u \in V: u + 0 = 0 + u = u$

e) inverzní prvek $\forall u \in V: \exists -u \in V: u + (-u) = 0$, kde 0 je neutrální prvek

2) asociativita skalárního násobku

$$\underline{\forall \alpha, \beta \in T: \forall u \in V: \alpha \cdot (\beta \cdot u) = (\alpha \cdot \beta) \cdot u}$$

3) násobek s 1

$$\underline{\forall u \in T: 1 \cdot u = u}$$

4) distributivita zleva

$$\underline{\forall \alpha \in T: \forall u, v \in V: \alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v}$$

5) distributivita zprava

$$\underline{\forall \alpha, \beta \in T: \forall u \in V: (\alpha + \beta) \cdot u = \alpha \cdot u + \beta \cdot u}$$

6) uzavřenost, $\cdot: T \times V \rightarrow V$, skalární násobek je bin. operace

$$\underline{\forall \alpha \in T: \forall u \in V: \alpha \cdot u \in V}$$

30) Definujte podprostor vektorového prostoru

↳ Bud' U podmnožinou vektorového prostoru V nad tělesem T , pak
pak podprostor vektorového prostoru V je neprázdná množina a splňuje:

1) obsahuje počátek $0 \in U$ (neprázdnost) $\leftarrow$ může nemusí

2) uzavřenost na vektorový součet $\forall u, v \in U : u + v \in U$

3) uzavřenost na skalární násobek $\forall a \in T : \forall u \in U : a \cdot u \in U$

↳ Každý vektorový prostor má 2 triviální podprostory V a $\{0\}$

↳ Vlastní podprostor je podprostor, který se nerovná celku $U \subsetneq V$

31) Definujte lineární kombinaci

Bud' V vektorový prostor nad tělesem T a $v_1, \dots, v_n \in V$ konečná
postupnost vektorů. Pak lineární kombinací je

$$u = \sum_{i=1}^n a_i v_i, \text{ kde } a_1, \dots, a_n \in T \text{ jsou koeficienty lineární kombinace}$$

↳ $\forall i : a_i = 0 \rightarrow$ jedná se o triviální lineární kombinaci a výsledný
vektor je nulový

32) Definujte podprostor generovaný množinou (lineární obal)

32) Definujte podprostor generovaný množinou (lineární obal) W je množina
vektorů
 $W \subseteq V$

Bud' V vektorový prostor nad tělesem T a $W \subseteq V$.
Potom lineární obal nebo-li podprostor generovaný množinou W je $\text{span}(W)$ a je to průnik všech podprostorů $U \subseteq V$ obsahujících množinu W .

$$\text{span}(W) = \bigcap \{ U \subseteq V \mid U \subseteq V \wedge W \subseteq U \} \quad \text{nebo} \quad \text{span}(W) = \bigcap_{U: W \subseteq U \subseteq V} U$$

↳ lineárním obalem se také rozumí množina všech lineárních kombinací
 $W \subseteq V$ a $W \subseteq V$

$$\text{span}(W) = \left\{ \sum_{i=1}^n a_i v_i \mid n \in \mathbb{N}_0; v_1, \dots, v_n \in W; W \subseteq V; a_1, \dots, a_n \in T \right\}$$

- 33)
- $\text{span}(W) = U \rightarrow$ " W generuje prostor U "
 - $\rightarrow$ "prvky množiny W jsou generátory prostoru U "
 - $\rightarrow$ "prostor U je konečně generovaný právě když je generován konečnou množinou vektorů"

33) Definujte řádkový prostor matice a to slovně i formálně pomocí maticového součinu

↳ řádkový prostor je prostor generovaný ^(transponovanými řádky) matice $A \in T^{m \times n}$ a podprostorem T^n

$$R(A) = \{ A \cdot c : c \in T^n \} = \{ v \in T^n : \exists d \in T^m : v = A^T d \}$$

34) Definujte sloupkový prostor matice a to slovně i formálně pomocí maticového součinu.

↳ sloupkový prostor je prostor generovaný sloupci matice A a podprostorem T^m

$$S(A) = \{ A \cdot c : c \in T^n \} = \{ u \in T^m : \exists c \in T^n : u = A \cdot c \}$$

35) Definujte jádro matice

↳ jádro $\ker(A)$ matice A je množina vektorů, co se po vynásobení matice rovná nulovému vektoru. Je to množina všech řešení homogenní soustavy rovnic $Ax=0$

$$\ker(A) := \{x \in T^n : Ax=0\}$$

36) Definujte množinu lineárně nezávislých vektorů

Nechť V je vektorový prostor nad tělesem T a B je lineárně nezávislá množina vektorů, pak pro každou n -tici n vektorů

B platí, že mají pouze triviální řešení

$$\sum_{i=1}^n a_i v_i = 0 \quad \wedge \quad \underline{a_1 = a_2 = \dots = a_n = 0}$$

↳ v ostatních případech je množina lineárně závislá

37) Definujte bázi vektorového prostoru

↳ báze je lineárně nezávislá množina B , ω generuje prostor V

Platí $\text{span}(B) = V \quad \wedge \quad \sum_{i=1}^n a_i v_i = 0 \quad \wedge \quad a_1 = \dots = a_n = 0 \quad \wedge \quad v_1, v_2, \dots, v_n \in B$

$$\text{span}(B) = \{ U \subseteq V \mid B \subseteq U \wedge U \subseteq V \} \quad \text{span}(B) = \bigcap_{U: B \subseteq U \subseteq V} U$$

↳ je možné určit každý vektor prostoru

38) Definujte dimenzi vektorového prostoru

↳ dimenze konečně generovaného vektorového prostoru V je mohutnost kdekoli z jeho bází. Značí se $\dim(V)$

$$\dim(V) = |B|$$

↳ báze

$$\text{span}(B) = V \quad \wedge \quad \text{LN}$$

$\dim(R(A)) = \text{rank}(A) \rightarrow$ dimenze řádkového prostoru matice je rovná její hodnotě

$$\dim(T^n) = n$$

39) Definujte vektor souřadnic

↳ Necht' $B = \{v_1, \dots, v_n\}$ je báze vektorového prostoru V a
necht' vektor $u \in V$ má vyjádření $u = \sum_{i=1}^n a_i v_i$, pak souřadnicemi
vektoru $u \in V$ vzhledem k bázi B je $[u]_B := (a_1, a_2, \dots, a_n)^T$

↳ díky lineární nezávislosti báze je zaručeno, že vektor souřadnic je jednoznačný

$$[u+w]_B = [u]_B + [w]_B \quad - \text{ sčítání vektoru souřadnic}$$

$$[a \cdot w]_B = a \cdot [w]_B \quad - \text{ izomorfismus souřadnic}$$

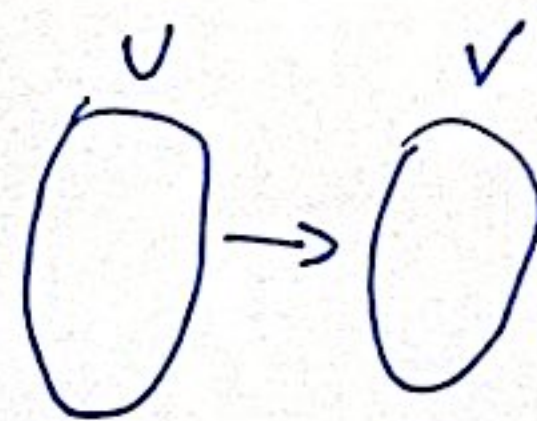
40) Definujte lineární zobrazení

Neht' U a V jsou vektorové prostory nad stejným tělesem T , a

Zobrazení $f: U \rightarrow V$. Zobrazení je lineární pokud splňuje:

aditivita

$$\forall u, v \in U: f(u+v) = f(u) + f(v)$$



homogenita

$$\forall v \in U: \forall a \in T: f(a \cdot v) = a \cdot f(v)$$

↳ lineární zobrazení neničí prostor

↳ platí $f(0) = 0$

↳ protože každý vektorový prostor obsahuje počátek

41) Definujte afinní prostor a jeho dimenzi

Nechť W je podprostor vektorového prostoru U a $u \in U$. Pak

afinní prostor určený $u+W$ je množina $\{u+w : w \in W\}$

Dimenze afinního prostoru $u+W$ je hodnota $\dim(W)$

42) Definujte jádro lineárního zobrazení

↳ Jádro lineárního zobrazení $f: U \rightarrow V$ je $\ker(f) = \{w \in U : f(w) = 0\}$.

Jádro je vektorový podprostor prostoru U

43) Definujte matici lineárního zobrazení

Nechť U a V jsou vektorové prostory nad tělesem T a bázemi

$B = (b_1, \dots, b_n)$ a $C = (c_1, \dots, c_m)$

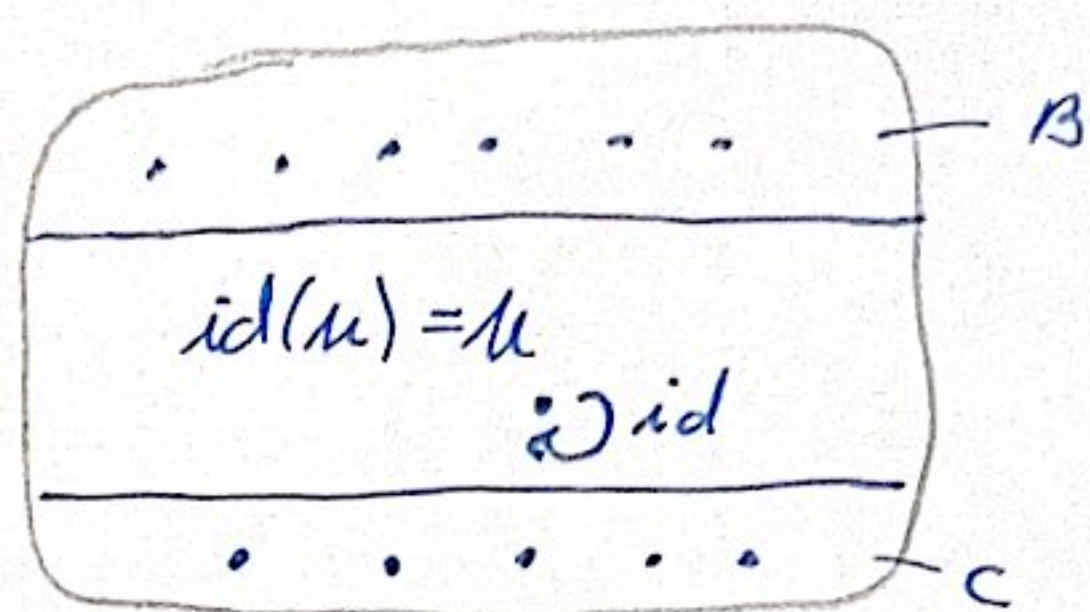
Pak matice lineárního zobrazení vzhledem k bázím B a C je

$$[f]_{B,C} \in T^{m \times n} = \begin{pmatrix} | & | & & | \\ [f(b_1)]_C & [f(b_2)]_C & \dots & [f(b_n)]_C \\ | & | & & | \end{pmatrix}$$

vzhledem k celé bázi

44) Definujte matici přechodu

Necht' B a C jsou dvě konečné uspořádané báze vektorového prostoru V . Matice přechodu od B k C je $[id]_{B,C}$.



44) Definujte isomorfismus vektorových prostorů

↳ Isomorfismus mezi prostory U a V nad tělesem T je isomorfismus právě tehdy, když je vzájemně jednoznačné lineární zobrazení $f: U \rightarrow V$.

↳ Mezi prostory existuje isomorfismus, nebo-li lineární zobrazení

$f: U \rightarrow V$ je isomorfismus prostorů U a V s konečnými bázemi B

a C právě tehdy, když $[f]_{B,C}$ je regulární, nebo-li má inverzi

45) Uveďte a dokažte vztah mezi elementárními řádkovými operacemi a soustavami rovnic

Věta: Necht $Ax=b$ a $A'x=b'$ jsou soustavy a by splňují, že

že se dostal elementárními řádkovými úpravami $(A|b) \rightsquigarrow (A'|b')$. Pak

množina řešení obou soustav je stejná. $\{x \in \mathbb{R}^n : Ax=b\} = \{x \in \mathbb{R}^n : A'x=b'\}$

$$A \in \mathbb{R}^{m \times n}$$

elementární řádkové úpravy:

1. Vynásobení i -tý řádek matice nenulovým $t \in \mathbb{R}$

$$a'_{kl} = \begin{cases} a_{kl} & \text{pokud } k \neq i \\ ta_{il} & \text{pokud } k = i \end{cases}$$

2. přičtení i -tého řádku matice k j -tému

$$a'_{kl} = \begin{cases} a_{kl} & \text{pokud } k \neq i \\ a_{il} + a_{jl} & \text{pokud } k = i \end{cases}$$

Důkaz:

vyjde z dvou inkluzí $\{x \in \mathbb{R}^n : Ax=b\} = \{x \in \mathbb{R}^n : A'x=b'\}$

(a) $Ax=b \Rightarrow A'x=b'$

(b) $A'x=b' \Rightarrow Ax=b$

1a. $Ax=b \Rightarrow A'x=b'$

$$a_{i1}x_1 + a_{i2}x_2 + \dots + a_{in}x_n = ta_{i1}x_1 + \dots + ta_{in}x_n = t(a_{i1}x_1 + \dots + a_{in}x_n) = tb_i = b'_i$$

$$\underline{1.a.} \quad Ax=b \Rightarrow A'x=b'$$

$$a'_{i1}x_1 + \dots + a'_{in}x_n = (a_{i1} + a_{j1})x_1 + \dots + (a_{in} + a_{jn})x_n = a_{i1}x_1 + \dots + a_{in}x_n +$$

$$a_{j1}x_1 + \dots + a_{jn}x_n = b_i + b_j = b'_i$$

$$\underline{1.b.} \quad A'x=b' \Rightarrow Ax=b$$

$$a_{i1}x_1 + \dots + a_{in}x_n = \frac{1}{t}(a'_{i1}x_1 + \dots + a'_{in}x_n) = \frac{1}{t}b'_i = b_i$$

$$\underline{2.b} \quad A'x=b' \Rightarrow Ax=b$$

$$a_{i1}x_1 + \dots + a_{in}x_n = a_{i1}x_1 + \dots + a_{in}x_n + b_j - b_j = a_{i1}x_1 + \dots + a_{in}x_n + a_{j1}x_1 + \dots +$$

$$a_{jn}x_n - a_{j1}x_1 - \dots - a_{jn}x_n = (a_{i1}x_1 + a_{j1}x_1) + \dots + (a_{in}x_n + a_{jn}x_n) - b_j =$$

$$= a'_{i1}x_1 + \dots + a'_{in}x_n - b_j = b'_i - b_j = b_i + b_j - b_j = b_i$$

46) Vyslovte a dokažte větu o jednoznačnosti volných a bázech proměnných

Věta: Pro libovolnou matici A a libovolnou A' v REF tvaru, kdy
mátně platí $A \sim A'$, pak jsou indexy sloupců s pivoty určeny
jednoznačně podle matice A .

Důkaz: (sporem)

↳ matice lze převést na 2 odstupňované tvary $A \sim A' \sim A''$,

kteřé se liší v indexích sloupců s pivoty

↳ najdeme největší index i , kde se v A' a A'' liší proměnné v
diagonále a b.i.n.o. si zvolíme, že A'' má x_i volné a

A' má x_i báze

↳ pak pro $A'x=0$ máme jednoznačné řešení po zvolení libovolných
volných proměnných $\rightarrow$ takže x_i určena jednoznačně

↳ pro A'' si zvolíme volné proměnné stejně jako pro A' , ale pro x_i
si zvolíme jinou hodnotu

↳ řešení $A'x=0$ a $A''x=0$ se neshodují, spor

Γ doplnění:

zvolení volných proměnných v REF tvaru a bez pivotu v b' má jednoznačné řešení
soustavy $A'x=b'$

↳ pomocí indukce

↳ kde $j(i) := \min \{j : a_{ij} \neq 0\} \rightarrow$ pivot

$$0x_1 + \dots + 0x_{j(i)-1} + a'_{i,j(i)} x_{j(i)} + a'_{i,j(i)+1} x_{j(i)+1} + \dots + a'_{in} x_n = b'_i$$

$$x_{j(i)} = \frac{1}{a'_{i,j(i)}} (b'_i - a'_{i,j(i)+1} x_{j(i)+1} - \dots - a'_{in} x_n)$$

47) Vyslovte a dokažte Frobeniovu větu o existenci řešení soustavy

Věta: Soustava $Ax=b$ má řešení právě tehdy, když se hodnost matice A rovná hodnosti rozšířené matice $(A|b)$.

↑
↳ Hodnost nebo-li $\text{rank}(A)$ je počet pivotů v matici A v REF tvaru $A \sim A'$

Důkaz:

$(A|b) \sim (A'|b')$ elementárními řádkovými úpravami
↳ v REF

Soustava má řešení x : $\Leftrightarrow$

$\Leftrightarrow$ 1. pivot není ve vektoru pravých stran b'

$\Leftrightarrow$ 2. pivoty A' se shodují s pivoty $(A'|b')$

$\Leftrightarrow$ 3. $\text{rank}(A) = \text{rank}(A|b)$

↳ protože $A \sim A'$ lze provést podle předpokladu $(A|b) \sim (A'|b')$ stejnými elementárními úpravami

48) Vyslovte a dokažte větu mezi řešeními $Ax=b$ a $Ax=0$

Věta: Necht' $A \in \mathbb{R}^{m \times n}$ a $b \in \mathbb{R}^m$ a soustava $Ax=b$ má alespoň jedno řešení a y je řešení této soustavy. Pak zobrazení $\bar{x} = \bar{x} + y$ je bijekce mezi množinami $\{\bar{x} : A\bar{x} = 0\}$ a $\{y : Ay = b\}$

Důkaz:

Pro předpoklady si uvažme $U = \{\bar{x} : A\bar{x} = 0\}$ a $V = \{x : Ax = b\}$, pak

zobrazení $f: U \rightarrow V$ dané $f(\bar{x}) = \bar{x} + y$

$g: V \rightarrow U$ dané $g(x) = x - y$

pokud $Ay = b$, pak $Af = A(\bar{x} + y) = A\bar{x} + Ay = 0 + b = b$

pokud $Ay = b$, pak $Ag = A(x - y) = Ax - Ay = b - b = 0$

$\hookrightarrow f$ zobrazí řešení soustavy $Ax=b$

$\hookrightarrow g$ zobrazí řešení soustavy $Ax=0$

$$(f \circ g)(x) = \bar{x} - y + \bar{x} + y = \bar{x} + \bar{x}$$

$$f(g(x)) = x - y + y = x \rightarrow f \text{ je surjektivní}$$

$$g(f(\bar{x})) = \bar{x} + y - y = \bar{x} \rightarrow f \text{ je injektivní}$$

49) Uveďte a dokažte větu popisující všechna řešení $Ax=b$ - nej správně

Věta: Necht $A \in \mathbb{R}^{m \times n}$ matice s hodností r a $b \in \mathbb{R}^m$ vektor pravých stran. Pak všechna řešení soustavy $Ax=b$ jsou

$$x = y + \mu_1 \bar{x}_1 + \mu_2 \bar{x}_2 + \dots + \mu_{n-r} \bar{x}_{n-r}$$

$\hookrightarrow \bar{x}_1, \dots, \bar{x}_{n-r}$ jsou řešení soustavy $A\bar{x}=0$

$\hookrightarrow y$ je jedno řešení $Ax=b$

$\hookrightarrow \mu_1, \dots, \mu_{n-r}$ jsou parametry

Důkaz:

$\hookrightarrow$ Volné proměnné se přejmenují na parametry $\mu_1, \dots, \mu_{n-r}$

$\hookrightarrow$ Necht y je řešení soustavy $Ax=b$ a x libovolné řešení $Ax=b$

$$\text{Pak } A(x-y) = b-b=0 \quad \bar{x} = x-y \quad A(\bar{x})=0$$

pro homogenní soustavu lze určit koeficienty $q_{1,1}, \dots, q_{n,n-r}$ a jako

funkci určit proměnné

$$\bar{x}_1 = q_{1,1} \mu_1 + \dots + q_{1,n-r} \mu_{n-r}$$

$\vdots$

$$\bar{x}_n = q_{n,1} \mu_1 + \dots + q_{n,n-r} \mu_{n-r}$$

lze vyjádřit

$$\bar{x}_1 = (q_{1,1}, \dots, q_{1,n-r}), \dots, \bar{x}_n = (q_{n,1}, \dots, q_{n,n-r})$$

Pak $\bar{x}_i$ lze vyjádřit pro $\beta_j \begin{cases} 1 & j=i \\ 0 & \text{jinak} \end{cases}$

$$a \quad x = y + \bar{x}$$

$$x = y + \beta_1 \bar{x}_1 + \beta_2 \bar{x}_2 + \dots + \beta_{n-r} \bar{x}_{n-r}$$

50) Vyslozte a dokašte vetu o ekvivalentních definicích regulárních matic

$A \in \mathbb{R}^{n \times n}$ matice je regulární pokud: (následující jsou ekvivalentní):

1. A je regulární, nebo-li $\exists B \in \mathbb{R}^{n \times n} : A \cdot B = I_n$

2. $\text{rank}(A) = n$

3. $A \sim I_n$

4. $Ax = 0$ má pouze triviální řešení $x = 0$

Důkaz:

Musíme dokázat $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4 \Rightarrow 1$ $2 \Leftrightarrow 4$ $3 \Leftrightarrow 1$

1. $\Rightarrow$ 2. (sporem) $1. \wedge \neg 2.$

A regulární $\wedge \text{rank}(A) < n$

$\hookrightarrow$ tím by se vynuloval poslední řádek u soustavy $Ax = 0$, protože by byl lineární kombinací, např. i -tý řádek

$\hookrightarrow Ax_i = e_i$ by nemělo řešení, spor, kde e_i je 1

2. $\Rightarrow$ 3.

$\hookrightarrow$ Gauss Jordanovy eliminace lze získat $A \sim I_n$ pokud je počet pivotů n u matice $A \in \mathbb{R}^{n \times n}$

3. $\Rightarrow$ 4.

$\hookrightarrow Ax = 0$ bude mít stejné řešení jako $I_n x = 0$ z předpokladu, že $A \sim I_n$, takže $x = 0$

4. $\Rightarrow$ 1. $\rightarrow \dim(\ker(A)) = 0$ a pomocí věty $\text{rank } A + \dim(\ker(A)) = n \rightarrow \text{rank}(A) = n$

51) Vyslovte a dokažte větu o znaménku složené permutace

Věta: pro libovolné $p, q \in S_n$ platí $\text{sgn}(q \circ p) = \text{sgn}(p) \cdot \text{sgn}(q)$

Důkaz:

Nechť p se dá rozložit na r_1 transpozic a q na r_2 transpozic,
tak $q \circ p$ lze rozložit na $r_1 + r_2$ transpozic $\text{sgn}(q \circ p) = (-1)^{r_1 + r_2}$

$$\text{sgn}(q \circ p) = (-1)^{r_1} \cdot (-1)^{r_2} \Rightarrow \text{sgn}(q \circ p) = \text{sgn}(p) \cdot \text{sgn}(q)$$

52) Uveďte a dokažte větu charakterizující, kdy $\mathbb{Z}_n$ je těleso

Věta: $\mathbb{Z}_n$ je těleso právě tehdy, když je n prvočíslo.

Důkaz: $\mathbb{Z}_n$ je těleso a n není prvočíslo.

(sporem) $\Rightarrow$ pokud by n bylo složené $n = a \cdot b$, kde $1 < a < n$ a $1 < b < n$,
kde $a, b \in \mathbb{N}$

$\hookrightarrow$ pokud by bylo složené, tak $a \cdot b \pmod{n} \equiv 0$, což implikuje, že

$a = 0$ nebo $b = 0$, což je spor

$\Leftarrow$ předpoklad, že n je prvočíslo, pak $\mathbb{Z}_n$ je těleso

$\hookrightarrow$ ověřit axiomy tělesa, platí všechny, ale třeba ověřit, že existují inverzní

prvky: $\forall a \in \{1, \dots, n-1\} : \exists a^{-1} \in \{1, \dots, n-1\} : a \cdot a^{-1} \equiv 1 \pmod{n}$

$$f_a(x) = a \cdot x \pmod{n}$$

Nechť $f_a(x) = f_a(y)$

$$ax = ay \pmod{n} \Rightarrow a(x-y) \equiv 0 \pmod{n}$$

protože $a \not\equiv 0 \pmod{n}$, tih:

$$x - y \equiv 0 \pmod{n}$$

$$x = y$$

$\Rightarrow$ funkce je tedy prostá a tím, že zobrazuje celou množinu na sebe sama, tak i surjektivní

$\exists a(x) \equiv 1 \pmod{n}$ existuje inverzní prvky

53) Vyslovte a dokažte malou Fermatovu větu

Věta: Pro prvočíslo p a každé $a \in \{1, \dots, p-1\} : a^{p-1} \equiv 1 \pmod{p}$
pro těleso $\mathbb{Z}_p$

Důkaz:

$\forall a \in \{1, \dots, p-1\} : \exists a^{-1} \in \{1, \dots, p-1\} : a \cdot a^{-1} \equiv 1$ $\leftarrow$ existence inverzního prvku v $\mathbb{Z}_p$ tělese

$f_a(x) = ax \pmod{p}$ $\leftarrow$ funkce zobrazení pomocí $\uparrow$

Nechť

$$f_a(x) = f_a(y)$$

$$ax = ay \pmod{p}$$

$$a(x-y) \equiv 0 \pmod{p}, \text{ protože } a \not\equiv 0 \pmod{p}, \text{ pak } x-y \equiv 0 \pmod{p}$$

$$x=y$$

$\hookrightarrow \mathbb{Z}_p$ je bijektivní $\rightarrow$ tedy prosté a na

Proto v $\mathbb{Z}_p$ platí:

$$\prod_{x=1}^{p-1} x = \prod_{x=1}^{p-1} f_a(x) = \prod_{x=1}^{p-1} ax = a^{p-1} \prod_{x=1}^{p-1} x$$

$$a^{p-1} \prod_{x=1}^{p-1} x = \prod_{x=1}^{p-1} x$$

$$\underline{\underline{a^{p-1} \equiv 1 \pmod{p}}}$$

54) Vysloďte a dokažte větu o průniku vektorových prostorů
— množina indexů

Věta: Necht' $(U_i : i \in I)$ je libovolný systém podprostorů prostoru V .

Průnik tohoto systému $\bigcap_{i \in I} U_i$ je také podprostorem V .

Důkaz:

Necht' $W = \bigcap_{i \in I} U_i$, ukažeme, že W je uzavřen na $+$ a $\cdot$:

$$\forall u, v \in W : \forall i \in I : u, v \in U_i \Rightarrow \forall i \in I : u, v \in U_i : u + v \in U_i \Rightarrow u + v \in W$$

$$\forall \lambda \in T : \forall v \in W : \forall i \in I : v \in U_i : \lambda \cdot v \in U_i \Rightarrow \lambda \cdot v \in W$$

pro prázdný průnik: $W = \bigcap_{i \in \emptyset} U_i = V$

55) Vysloste a dokašte větu o ekvivalenčních definicích lineárního obalu

Věta Necht' V je vektorový prostor nad tělesem T a $M \subseteq V$. Pak:

$$W_1 := \{ U \subseteq V \mid U \text{ je podprostor } V \text{ a } M \subseteq U \}$$

$$W_2 := \left\{ \sum_{i=1}^k a_i v_i \mid k \in \mathbb{N}; a_i \in T; v_i \in M \right\} = \text{span}(M)$$

Pak platí $W_1 = W_2$

Důkaz:

1) $W_1 \subseteq W_2$

W_2 je uzavřena skalární násobky a součet

$$u \in W_2 \Rightarrow u = \sum_{i=1}^k a_i v_i \Rightarrow t \cdot u = t \sum_{i=1}^k a_i v_i = \sum_{i=1}^k (t a_i) v_i \Rightarrow t \cdot u \in W_2$$

$$u, w \in W_2 \Rightarrow u + w = \sum_{i=1}^k a_i v_i + \sum_{j=1}^l b_j v_j = \sum_{i=1}^k a_i v_i + b_j v_j \Rightarrow u + w \in W_2$$

$$\left. \begin{array}{l} W_2 \subseteq V \\ M \subseteq W_2 \end{array} \right\} \text{ z toho plyne } W_1 \subseteq W_2$$

2) $W_2 \subseteq W_1$

Každý U obsahuje M , tedy všechny lineární kombinace M

$$\forall U: W_2 \subseteq U \Rightarrow W_2 \subseteq W_1$$

56) Vysloste a dokažte tvrzení o mohutnostech lineárně nezávislé množiny a generující množiny

Věta: Necht' V je vektorový prostor nad tělesem T

Je-li $B \subseteq V$ lineárně nezávislá množina

• $C \subseteq V$ konečná generující množina prostoru V

pak platí:

$$|B| \leq |C|$$

Důkaz:

Necht' $C = \{c_1, \dots, c_n\}$ $|C| = n$

↖ $|B| \leq |C|$ platí

sporem $|B| > |C|$ tedy $|B| \geq n+1$

↳ pak existují vektory $b_1, \dots, b_{n+1} \in B$

↳ každé b_i lze vyjádřit $b_i = \sum_{j=1}^n a_{ij} c_j$, kde $a_{ij} \in T$

↳ lze udělat matici $A = (a_{ij}) \in T^{(n+1) \times n}$

↳ tato matice má více řádků než sloupců a tedy její řádky jsou lineárně závislé

↳ proto existuje nenulový vektor $d = (d_1, \dots, d_{n+1}) \in T^{n+1} \setminus \{0\}$ a ten, když $d^T A = 0^T$, proto můžeme získat netriviální lineární kombinaci pro nulový vektor

$$\sum_{i=1}^{n+1} d_i b_i = \sum_{i=1}^{n+1} d_i \sum_{j=1}^n a_{ij} c_j = \sum_{j=1}^n \left(\sum_{i=1}^{n+1} d_i a_{ij} \right) c_j = \sum_{j=1}^n 0 \cdot c_j = 0$$

57) Uveďte a dokažte Steinitzovu větu o výměně (včetně lemmatu a jeho důkazu, pokud jej potřebujete)

Věta:

(Lemma o výměně): Necht' $C = \{c_1, \dots, c_n\}$ je systém generátorů vektorového prostoru V nad tělesem T . Pak $v \in V$ se vyjádří jako $v = \sum_{i=1}^n a_i c_i$, kde

$a_1, \dots, a_n \in T$ a $c_1, \dots, c_n \in C$. Pak pro libovolné $i \in \{1, \dots, n\}$, které

$a_i \neq 0$ je množina $C = C \cup \{v\} \setminus \{c_i\} = \{c_1, \dots, c_{i-1}, v, c_{i+1}, \dots, c_n\}$ opět

systém generátorů prostoru V $\text{span}((C \setminus c_i) \cup v) = V$

(Steinitzova věta): Necht' C je systém generátorů V a necht' B je konečná lineárně nezávislá množina $v \in V$. Pak existuje množina D taková, že:

$$\text{span}(D) = V$$

$$B \subseteq D$$

$$|D| = |C|$$

$$D \setminus B \subseteq C$$

Důkaz:

(Lemma o výměně) Vektorový prostor V nad tělesem T s množinou generátorů C

$$\forall w \in V: \exists \beta_1, \dots, \beta_n \in T: w = \sum_{i=1}^n \beta_i c_i$$

$$\forall v \in V: \exists \alpha_1, \dots, \alpha_n \in T: v = \sum_{i=1}^n \alpha_i c_i \Rightarrow v = \sum_{i \neq k} \alpha_i c_i + \alpha_k c_k \Rightarrow c_k = \frac{v}{\alpha_k} - \sum_{i \neq k} \frac{\alpha_i}{\alpha_k} c_i$$

$$w = \sum_{i=1}^n \beta_i c_i = \sum_{i \neq k} \beta_i c_i + \beta_k c_k = \sum_{i \neq k} \beta_i c_i + \beta_k \cdot \left(\frac{v}{\alpha_k} - \sum_{i \neq k} \frac{\alpha_i}{\alpha_k} c_i \right) =$$

$$w = \frac{\beta_k v}{\alpha_k} + \sum_{i \neq k} \left(\beta_i c_i - \frac{\alpha_i}{\alpha_k} c_i \right) \rightarrow \text{dostaneme vyjádření bez } c_k$$

(Steinitzova věta - znova): Necht V je vektorový prostor nad tělesem T . Necht

C je systém generátorů V a B konečná lineárně nezávislá množina. Pak

existuje množina D taková, že:

$$\text{span}(D) = V$$

$$B \subseteq D$$

$$|C| = |D|$$

$$D \setminus B \subseteq C$$

1. krok indukce:

Pokud $B \setminus C = \emptyset$, pak $D = C$ a platí $\text{span}(C) = V$

$$+ B \subseteq C$$

$$+ C \setminus B \subseteq C$$

$$+ |C| = |C|$$

2. krok:

zvolíme $b \in B \setminus C$, nové $B' = B \setminus b$, a protože množina B'

je znova lineárně nezávislá, dá se předpokládat $|B' \setminus C| < |B \setminus C|$.

existuje D' pro B' a C : $\text{span}(D') = V$

$$\cdot B' \subseteq D'$$

$$\cdot |D'| = |C|$$

$$\cdot D' \setminus B' \subseteq C$$

58) Vyslozte a dokažte větu o dimenzi průniku vektorových prostorů.

Věta: Jsou-li U, V podprostory konečně generovaného prostoru W ,

$$\text{pak } \dim(U) + \dim(V) = \dim(U \cap V) + \dim(\text{span}(U \cup V))$$

Důkaz:

↳ Vezmu bázi B prostoru $U \cap V$

↳ Rozšířím bázi B na $\rightarrow$ bázi C prostoru U
 $\rightarrow$ bázi D prostoru V

↳ množina $C \cup D$ generuje $U \cup V$

↳ proto $|C| + |D| = |B| + |C \cup D|$, kde $|C| = \dim U$

$$|D| = \dim V$$

$$|B| = \dim(U \cap V)$$

$$|C \cup D| = \dim(\text{span}(U \cup V))$$

59) Vyslovte a dokažte větu o vektorových prostorech souvisejících s maticí A (včetně lemmatu, které se týká součinu matic a jeho diskuzy, pokud jej potřebujete.)

Definice: Necht $A \in T^{m \times n}$

$\hookrightarrow$ jádro: $\ker A := \{x \in T^n \mid Ax = 0\}$

$\hookrightarrow$ sloupový prostor $S_A := \{Ac \mid c \in T^n\} = \{u \in T^m : \exists c \in T^n : u = A \cdot c\}$

$\hookrightarrow$ řádkový prostor: $R_A := \{v \in T^m : \exists d \in T^n : v = A^T d\}$

Lemma: Pro sloupové prostory A a AB platí $S_{AB} \subseteq S_A$

Důkaz: $A \in T^{m \times n}$, $B \in T^{n \times p}$

$$\{ABc : c \in T^p\} \subseteq \{Ad : d \in T^n\}, \text{ protože } \{Bc : c \in T^p\} \subseteq T^n$$

Věta: Pro každou $A \in T^{m \times n}$ platí $\dim(R_A) = \dim(S_A)$, čili $\text{rank}(A) = \text{rank}(A^T)$

Důkaz: $\dim R_A = \dim R_{A'} = \text{rank } A = \text{rank } A' = \dim S_A = \dim S_{A'}$

6.1) Vysloďte a dokažte větu o dimenzi jádra matice

Věta: Pro $A \in T^{n \times n}$ platí $\dim(\ker A) + \text{rank } A = n$

Důkaz:

$d = n - \text{rank } A$, d je počet volných proměnných $\rightarrow$ když jednu proměnnou nastavíme na 1

$\hookrightarrow$ každé volné proměnné odpovídá jeden vektor řešení homogenní

soustavy. tedy $\dim(\ker A) = n - \text{rank } A$

$\hookrightarrow$ tyto vektory jsou mezi sebou lineárně nezávislé $\rightarrow$ tvoří bázi

$$\underline{n = \text{rank } A + \dim(\ker A)}$$

62) Vysloďte a dokažte větu o jedinečnosti lineárního zobrazení

Věta: Necht U a V jsou vektorové prostory nad tělesem T a B je báse U .

Pak všechna zobrazení $f_0: B \rightarrow V$ mají jediné lineární zobrazení $f: U \rightarrow V$

$$\forall b \in B: f_0(b) = f(b)$$

Důkaz:

Pro jakéholi $u \in U$ existuje lineární kombinace pomocí $n \in \mathbb{N}_0$:

$$a_1, \dots, a_n \in T, b_1, \dots, b_n \in B \Rightarrow u = \sum_{i=1}^n a_i b_i$$

$$f(u) = f\left(\sum_{i=1}^n a_i b_i\right) = \sum_{i=1}^n a_i f(b_i) = \sum_{i=1}^n a_i f_0(b_i)$$

63) Vysloste a dokažte tvrzení, že převod na vektor souřadnic je lineární zobrazení

Věta: Necht' U je prostor nad T s bází $B = (b_1, \dots, b_n)$, potom zobrazení $f: U \rightarrow T^n$ je definované $f(u) = [u]_B$ a je lineární.

Důkaz:

Pro $u, v \in U$ lze vyjádřit $u = \sum_{i=1}^n a_i b_i$

$$v = \sum_{i=1}^n c_i b_i$$

Pak vektory souřadnic jsou $[u]_B = (a_1, \dots, a_n)^T$

$$[v]_B = (c_1, \dots, c_n)^T$$

Platí linearita součtu:

$$f(u+v) = [u+v]_B = \left[\sum_{i=1}^n a_i b_i + \sum_{i=1}^n c_i b_i \right]_B = \left[\sum_{i=1}^n (a_i + c_i) b_i \right]_B =$$

$$= (a_1 + c_1, \dots, a_n + c_n)^T = [u]_B + [v]_B = f(u) + f(v)$$

Platí linearita násobku $\lambda \in T$

$$f(\lambda \cdot u) = [\lambda \cdot u]_B = \left[\lambda \cdot \sum_{i=1}^n a_i b_i \right]_B = \left[\sum_{i=1}^n (\lambda \cdot a_i) b_i \right]_B = (\lambda \cdot a_1, \dots, \lambda \cdot a_n)^T =$$

$$= \lambda \cdot [u]_B = \lambda \cdot f(u)$$

$f(u) \leftrightarrow [u]_B$ je bijekce nebo-li isomorfismus

64) Uysloďte a dokažte pozorování o matici složeného zobrazení

Pozorování: Mějme vektorové prostory U, V a W s uspořádanými bázemi

B, C a D . Pak pro matice lineárních zobrazení $f: U \rightarrow V$

$$g: V \rightarrow W \text{ platí } [g \circ f]_{B,D} = [g]_{C,D} [f]_{B,C}$$

Důkaz:

$$\text{Pro všechny } u \in U \text{ platí } [(g \circ f)(u)]_D = [g \circ f]_{B,D} [u]_B$$

Pak platí i:

$$[(g \circ f)(u)]_D = [g(f(u))]_D = [g]_{C,D} [f(u)]_C = [g]_{C,D} [f]_{B,C} [u]_B$$

$$\text{porovnáním a zkrácením vektorů: } [g \circ f]_{B,D} = [g]_{C,D} [f]_{B,C}$$

65) Nyslovte a dokažte větu o charakterizaci isomorfismu mezi vektorovými prostory pomocí matic

Věta: Lineární zobrazení $f: U \rightarrow V$ mezi prostory U a V s bázemi B a C . f je isomorfismus právě tehdy, když je $[f]_{B,C}$ regulární

(prostorů)

Důkaz:

$\Leftarrow$

$$g: V \rightarrow U$$

$$[g]_{C,B} = ([f]_{B,C})^{-1}$$

$$[g \circ f]_{B,B} = [g]_{C,B} [f]_{B,C} = ([f]_{B,C})^{-1} [f]_{B,C} = I_{|B|} = [id]_{B,B}$$

$\downarrow$ jednotková matice

$\hookrightarrow f$ je prosté

$$[f \circ g]_{C,C} = [f]_{B,C} [g]_{C,B} = [f]_{B,C} ([f]_{B,C})^{-1} = I_{|C|} = [id]_{C,C}$$

$\hookrightarrow f$ je na

$$\Rightarrow f(U) = V \quad f^{-1}(V) = U, \text{ tak } \dim(U) = \dim(V)$$

$\hookrightarrow f$ je isomorfismus, takže splňuje

$$[f]_{B,C} \Rightarrow [f^{-1}]_{C,B} [f]_{B,C} = [id]_{B,B} = I_{|B|}$$

6b) Vyslozte a dokažite větu o řešení rovnice s lineárním zobrazením

Věta: Necht' $f: U \rightarrow V$ je lineární zobrazení, kde U, V jsou vektorové prostory nad stejným tělesem T .

Necht' $v \in V$

Pak rovnice $f(x) = v \rightarrow$ nemá žádné řešení
nebo $\rightarrow$ množina všech řešení má tvar $u + \ker(f)$,
kde u je řešení rovnice $f(x) = v$ $\downarrow$ tvoří afinní prostor

doplňm'
jádro lineární zobrazení $\ker(f) = \{w \in U : f(w) = 0\}$ _

Důkaz:

$f(x) = v$ má alespoň jedno řešení $u \in U \Rightarrow f(u) = v$

1. $x \in u + \ker(f) \rightarrow$ každý prvek $\in u + \ker f$ je řešením

pak existuje $w \in \ker f \Rightarrow x = u + w$

$$f(x) = f(u + w) = f(u) + f(w) = v + 0 = v$$

2. každé řešení leží v $u + \ker f$

$$f(x - u) = f(x) - f(u) = v - 0 = v$$

67) Yformulujte problém o počtu sudých podgrafů a vyřešte jej

↳ Problém: $G = (V, E)$ je souvislý graf. Kolik existuje sudých podgrafů? Tedy kolik množin hran $A \subseteq E$ má vrcholy takové, že náleží sudému počtu hran?

↳ Řešení:

$$A \Delta B := (B \setminus A) \cup (A \setminus B) \quad \leftarrow \text{hrany, které jsou právě v jedné z množin}$$

$$A \Delta B := |A| + |B| - |A \cap B|$$

↳ kde $|A|$ je sudé, $|B|$ je sudé, $|A \cap B|$ je sudé

$(A, \Delta, \cdot)$ tvoří vektorový prostor nad $\mathbb{Z}_2$

$$|A| = |T| \dim(A) \quad \leftarrow \text{platí pro prostory konečné dimenze, takže}$$

stačí najít velikost báze $A \rightarrow \dim(A)$

1. zvolíme libovolnou kostru K z grafu G

$$C = \{C_i : e_i \in E_G \setminus E_K\} \rightarrow \text{je lineárně nezávislá}$$

↳ $\rightarrow$ tvoří cykly C_i pomocí kostry a hran e_i ,
hrany grafu - hrany kostry které nejsou v kostře

↳ jeho dimenze je $|E| - |V| + 1$ Graf má $2^{|E| - |V| + 1}$ sudých podgrafů

68) Formulujte problém o množinových systémech s omezeními na
mohutnosti a vyřešte jej

Problém: Kolik podmnožin může mít n -prvková množina, aby
každá podmnožina měla lichou velikost a průnik
dvou podmnožin sudou velikost?

Formálně:

$$\max k: \exists A_1, \dots, A_k \subseteq \{1, \dots, n\}: \forall i \neq j: 2 \nmid |A_i| \wedge 2 \mid |A_i \cap A_j| \quad \rightarrow$$

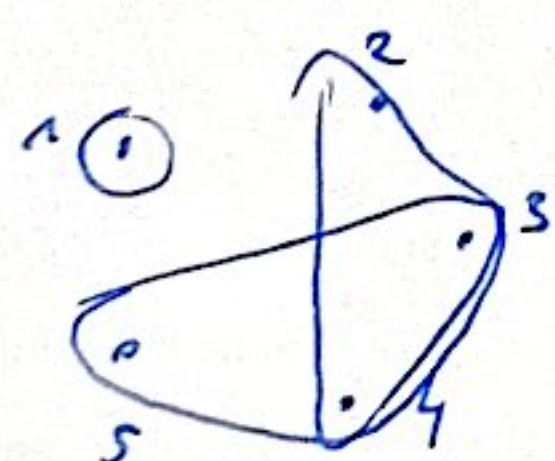
Řešení:

↳ platí: $k \leq n$, protože množin s danými vlastnostmi může být
nejvýše $n \rightarrow$ například samé jednoprvkové

matice incidence:

$$M \in \mathbb{Z}_2^{k \times n}, \text{ platí } m_{ij} = \begin{cases} 1 & \text{pokud } j \in A_i \\ 0 & \text{pokud } j \notin A_i \end{cases}$$

ukázka:



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

$$\begin{array}{c|c} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{array}$$

$$\text{platí: } MM^T = I_k \quad \leftarrow \text{protože } (MM^T)_{ij} = \begin{cases} 1 & \text{pro } i=j \\ 0 & \text{pro } i \neq j \end{cases}$$

$$k = \text{rank}(I_k) = \text{rank}(MM^T) \leq \text{rank}(M) \leq n$$

69) Zformulujte problém o dělení obdélníku na čtverce a vyřešte jej.

Problém: Lze čtverec s iracionálním poměrem stran
rozdělit na konečně mnoho čtverců?

- Základní tvrzení rozdělení neexistuje pro poměr stran $1/x \in \mathbb{R} \setminus \mathbb{Q}$

Řešení:

1 a x jsou lineárně nezávislé, protože $x \notin \mathbb{Q}$

Lineární zobrazení $\rightarrow f: \mathbb{R} \rightarrow \mathbb{R}$

$$f(1) = 1$$

$$f(x) = -1$$

plocha obdélníku:

$$v(A) := f(a) \cdot f(b)$$

$$v(A) = \sum_{i=1}^k v(B_i) \quad \leftarrow \text{protože se dále rozděluje na } B_1, \dots, B_k$$

$$f(a) \cdot f(b) = f(a_1 + a_2) \cdot f(b) = (f(a_1) + f(a_2)) \cdot f(b) = f(a_1) \cdot f(b) + f(a_2) \cdot f(b)$$

Sporem: Kdyby šel rozdělit na $A_1, \dots, A_k$ čtverců, tak by čtverce
jich rozdělit na obdélníky $B_1, \dots, B_l$

$\nwarrow$ celý obdélník s iracionálními poměry stran

$$-1 = f(1) \cdot f(x) = v(R) = \sum_{j=1}^l v(B_j) = \sum_{i=1}^k v(A_i) = \sum_{i=1}^k f(a_i) \cdot f(a_i) \geq 0$$

70) Píklkové sepište, co vře o elementárních řádkových operacích a Gaussově eliminaci

Matkový zápis $\swarrow$ m řádků a n sloupců

Necht' $A \in \mathbb{R}^{m \times n}$ je matice a $b \in \mathbb{R}^m$ vektor pravých stran a $x = (x_1, \dots, x_n)^T \in \mathbb{R}^n$ vektor neznámých pak

$Ax=b$ je soustava lineárních rovnic

$(A|b) \in \mathbb{R}^{m \times (n+1)}$ je rozšířená matice doplněná o vektor pravých stran

$Ax=0$ je homogenní soustava, kdy vektor pravých stran je nulový vektor $0_n = (0, \dots, 0)^T \in \mathbb{R}^n$, které má alespoň jedno triviální řešení

$(A)_{ij}$ je prvek matice

Řešením soustavy $Ax=b$ je vektor $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ právě tehdy, když splňuje všechny rovnice $\forall i \in \{1, \dots, m\}: \sum_{j=1}^n (a_{ij} x_j) = b_i$

1 rovnice o 2 neznámých: $(a_{11} \ a_{12}) \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \rightarrow$ řešení přímka

2 rovnice o 2 neznámých: $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \rightarrow$ bod v $\mathbb{R}^2$

1 rovnice o 3 neznámých $\rightarrow$ rovina

Elementární řádkové operace

↳ nemění množinu řešení

1. vynásobení ^(i-tý řádek) $t \in \mathbb{R} \wedge t \neq 0 \rightarrow a'_{kl} = \begin{cases} t a_{il} & \text{pro } k=i \\ a_{kl} & \text{pro } k \neq i \end{cases}$

2. přičtení j-tého řádku k i-tému $\rightarrow a'_{kl} = \begin{cases} a_{il} + a_{jl} & \text{pro } k=i \\ a_{kl} & \text{pro } k \neq i \end{cases}$

3. výměna 2 řádků $\rightarrow$ dá se odvodit z předchozích

4. přičtení $\lambda \in \mathbb{R} \wedge \lambda \neq 0$ násobek j-tého řádku k i-tému

$Ax=b$ a $A'x=b'$ jsou dvě soustavy splňující $(A|b) \sim (A'|b')$, tak
mají stejné množiny řešení
↳ provedeny řádkové operace

REF (řádkově odstupňovaný tvar)

1) nulové řádky jsou pod nenulovými

2) pivot v řádku je více vpravo než pivot v řádku nad ním
↳ první nenulový prvek v řádku $j(i) := \{j : a_{ij} \neq 0\}$

3) pod každým pivotem jsou sumy nuly

Gaussova eliminace

↳ algoritmus pro převedení matice do REF tvaru

1) výběr pivotu, případně zaměnit řádek, aby pivot nebyl nulový a vynulování prvků pod ním díky řádkovým operacím

2) přesun do dalšího řádku a sloupce

Zpětná substituce

- ↳ po převedení do REF tvaru jsou proměnné s pivotem báze a bez pivotu volné
- ↳ volné se dají změnit na parametry nebo volné zvolit
- ↳ je-li v $(A|b) \rightsquigarrow (A'|b')$ pivot ve vektoru pravých stran, tak soustava nemá řešení
- ↳ báze proměnné jsou určeny jednoznačně, REF tvar být nemusí

Hodnost

- ↳ je počet pivotů v REF tvaru matice A , značí se $\text{rank}(A)$
- ↳ Frobeniova věta: Gaussova $Ax=b$ má řešení právě tehdy, když se hodnost matice A rovná hodnosti rozšířené matice $(A|b)$
$$\text{rank}(A) = \text{rank}(A|b)$$

7) Přehledové sešity, co víte o řešení homogenních a nehomogenních soustav lineárních rovnic

Základní pojmy

matice $A \in \mathbb{R}^{m \times n}$ a vektor pravých stran $b \in \mathbb{R}^m$ a vektor řešení $x = (x_1, \dots, x_n) \in \mathbb{R}^n$

tak $Ax=b$ soustava lineárních rovnic o m řádcích a n proměnných

homogenní $\rightarrow$ pokud $b=0$

nehomogenní $\rightarrow$ pokud $b \neq 0$

(A|b) rozšířená matice soustavy

Homogenní a nehomogenní

- pokud x a y je řešením soustavy $Ax=b$, pak $\bar{x} = x - y$ je řešením homogenní soustavy $A\bar{x} = 0$ protože $A(x-y) = Ax - Ay = b - b = 0$
- pokud $\bar{x}$ je řešením $A\bar{x} = 0$ a y řešením $Ay=b$, pak $x = \bar{x} + y$ je řešením $Ax=b \Rightarrow A(\bar{x} + y) = A\bar{x} + Ay = 0 + b = b$
- Necht' y splňuje $Ay=b$. Pak zobrazení $\bar{x} = x - y$ je bijekce mezi množinami $\{\bar{x} : A\bar{x} = 0\}$ a $\{x : Ax=b\}$

Homogenní soustavy

- pokud $A \in \mathbb{R}^{m \times n}$ je matice hodnosti n , tak řešení lze popsat

$$A\bar{x} = 0 \text{ jako } \bar{x} = p_1 \bar{x}_1 + p_2 \bar{x}_2 + \dots + p_{n-n} \bar{x}_{n-n}$$

$\leftarrow n-n$ je počet volných proměnných

$\bar{x}_1, \bar{x}_2, \dots, \bar{x}_{n-n}$ vhodná řešení $A\bar{x} = 0$

$p_1, p_2, \dots, p_{n-n}$ parametry libovolné

- pokud má $A\bar{x} = 0$ hodnost $\text{rank}(A) = n \rightarrow$ má jen triviální řešení

Nehomogenní soustavy

Matice $A \in \mathbb{R}^{m \times n}$ hodnosti κ lze všechna řešení popsat:

$$X = \mu_1 \bar{x}_1 + \mu_2 \bar{x}_2 + \dots + \mu_{n-\kappa} \bar{x}_{n-\kappa} + y$$

• $\mu_1, \dots, \mu_{n-\kappa} \rightarrow$ libovolné parametry

• $\bar{x}_1, \dots, \bar{x}_{n-\kappa} \rightarrow$ vhodná řešení $A\bar{x} = 0$

• $y \rightarrow$ vhodné řešení $Ax = b$

↳ nehomogenní soustava může mít $\rightarrow$ 1 řešení $\text{rank}(A) = \text{rank}(A|b)$

$\rightarrow$ žádné řešení $\text{rank}(A) < \text{rank}(A|b)$

$\rightarrow$ nekonečně mnoho řešení $\text{rank}(A) < n$ a
matice $A \in \mathbb{R}^{m \times n}$

Gaussova eliminace

↳ algoritmus provádění elementárních řádkových operací až k REF tvaru

1) najde pivot, vynuluje řádky pod ním, případně výměnou řádků pivot nulový, pak postupuje na další řádky a sloupce

Ukážka

↳ ukážka se provede dosazením do původní soustavy, včetně parametrů

$$(A|I) \sim (A'|C) \quad (C|A') \sim (I_4|A) \quad A' = C \cdot A$$

RREF (redukovaný odstupňovaný tvar)

↳ protože tímto postupem lze
vypočítat inverzní matici

RREF : 1) nulové řádky pod nenulovými

2) pivoty nejsou ve stejném sloupci

3) pod každým pivotem jsou ve sloupci nuly

RREF doplnění : 1) pivot má hodnotu 1

4) přímo řešení

2) pod i nad pivotem jsou samé nuly

3) jednoznačný tvar od REF

↳ Gauss-Jordanova eliminace

72) Přehledové sešite, co víte o maticových operacích

Nulová matice: $O_{m,n} \in \mathbb{R}^{m \times n}$, pro libovolné $m, n \in \mathbb{N}$ platí: $\forall i, j: (O_{m,n})_{i,j} = 0$

Jednotková matice $I_n \in \mathbb{R}^{n \times n}$, pro libovolné $n \in \mathbb{N}$ platí: $(I_n)_{i,j} = 1 \iff i=j$
 $\hookrightarrow$ na hlavní diagonále $\rightarrow$ prvky $a_{i,i}$

Transponovaná matice: k matici $A \in \mathbb{R}^{m \times n}$ je transpozice $A^T \in \mathbb{R}^{n \times m}$

$\hookrightarrow$ splňuje $(A)_{i,j} = (A^T)_{j,i}$

$\hookrightarrow$ přechodím řádky a sloupce

Symetrická matice: Je u čtvercové matice $A \in \mathbb{R}^{n \times n}$, když platí

$$A^T = A$$

Sečtení matic: $A+B$, kde $A, B \in \mathbb{R}^{m \times n}$, platí: $(A+B)_{i,j} = a_{i,j} + b_{i,j}$

Násobek matice: Pro matici $A \in \mathbb{R}^{m \times n}$ a $t \in \mathbb{R}$ platí $(t \cdot A)_{i,j} = t a_{i,j}$

Loučení matic: Pro matici $A \in \mathbb{R}^{m \times n}$ a $B \in \mathbb{R}^{n \times p}$ je definováno

$$(A \cdot B) \in \mathbb{R}^{m \times p} \text{ jako } (AB)_{i,j} = \sum_{k=1}^n a_{i,k} b_{k,j}$$

$$\begin{array}{c|cc} & b_{11} & b_{12} \\ \hline a_{11} & a_{11}a_{12} & \\ a_{21} & a_{21}a_{12} & \end{array}$$

Pravidla pro počítání s maticemi

$$\bullet A + (B + C) = (A + B) + C$$

$$\bullet A + B = B + A$$

$$\bullet A + O = A$$

$$\bullet r(sA) = (rs)A$$

$$\bullet r(sA) = s(rA)$$

$$\bullet A + (-1)A = O$$

$$\bullet 1A = A$$

$$\bullet r(A+B) = rA + rB$$

$$\bullet (r+s)A = rA + sA$$

$$\bullet (r+s)(A+B) = rA + rB + sA + sB$$

$$\bullet (A^T)^T = A$$

$$\bullet (A+B)^T = A^T + B^T$$

$$\bullet (rA)^T = r(A^T)$$

$$\bullet (rA)B = A(rB)$$

$$\bullet (AB)^T = B^T A^T$$

$$\bullet (A^T + B)^T = A + B^T$$

$$\bullet (A^T B)^T = B^T A$$

$$\bullet A + tB = t(B + \frac{1}{t}A)$$

$$\bullet (A+B)^T C^T = (CB)^T + (CA)^T$$

$$\cdot A^T I = I A^T$$

$$\cdot (A^T)^n = (A^n)^T$$

$$\cdot (A^T)^{-1} = (A^{-1})^T$$

$$\cdot (ABC)^{-1} = C^{-1} B^{-1} A^{-1}$$

$$\cdot (A^{-1})^{-1} = A$$

$$\cdot (A^T B^T)^{-1} = (A^{-1} B^{-1})^T$$

pro libovolné $A \in \mathbb{R}^{m \times m}$ platí: $I_m A = A I_m = A$

$$\cdot (A + A^{-1})(A - A^{-1}) = A^2 - (A^2)^{-1}$$

$$\cdot I + A + A^2 + A^3 = (A - I)^{-1} (A^4 - I) \text{ pokud } (A - I) \text{ regulární}$$

$$\cdot (AB)^{-1} = B^{-1} A^{-1}$$

neplatí: $(A+B)^{-1} = A^{-1} + B^{-1}$ nelze jinak, nelze

$$\cdot (2A)^{-1} = \frac{1}{2} (A)^{-1}$$

$P^T = P^{-1} \rightarrow$ permutační matice: P

$A \in \mathbb{R}^{m \times n}$, $B \in \mathbb{R}^{n \times p}$, $C \in \mathbb{R}^{p \times q}$ platí $\begin{cases} A \cdot B \approx mn \text{ aritmetických operací} \\ (A \cdot B) \cdot C \approx mpq \text{ operací} \end{cases}$
celkem $mp(n+q)$

Elementární matice

vynásobení i -tý řádek $\underbrace{t \in \mathbb{R} \wedge t \neq 0}_{B = EA}$, kde $e_{ii} = t$

pr. $\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 4 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 9 \\ 4 & 4 \end{pmatrix}$

přičtení j -tého řádku k itému $B = EA$, kde $e_{ij} = 1$

pr. $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 4 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 7 \\ 4 & 4 \end{pmatrix}$

$B = EA \rightarrow$ elementární řádková operace

$B = AE \rightarrow$ elementární sloupková operace

73) Přehledové sešite, co víte o regulárních a singulárních maticích

Existují 4 ekvivalentní definice regulární matice:

1. Má inverzní matici, pro $A \in \mathbb{R}^{n \times n}$ platí, že $\exists B \in \mathbb{R}^{n \times n} : A \cdot B = I_n$
2. $\text{rank}(A) = n$ hodnost matice je rovna řádku matice
3. $A \sim I_n \rightarrow$ ekvivalentními řádkovými úpravami se lze dostat k jednotkové matici
4. $Ax=0$ má pouze triviální řešení $x=0$

↳ jinak je matice $A \in \mathbb{R}^{n \times n}$ singulární

↳ inverzní matice je jednoznačná

↳ inverzní matici získáme z rozšířené matice $(A|I)$ Gauss-Jordanovou eliminací na $(I|B)$ $\rightarrow$ pokud se zde najde singulární

↳ pokud R regulární, platí: $A=B \Leftrightarrow RA=RB \Leftrightarrow AR=BR \nRightarrow AR=RB$

↳ regulární matice je uzavřena na součin, transpozici, inverzi, ale ne součet, protože může vzniknout singulární matice

↳ pro regulární A, B platí: $A=B \Leftrightarrow A^{-1}=B^{-1}$

↳ invertování je ekvivalentní úprava

↳ $A^{-1}B \neq B^{-1}A$ nemohou se

Singulární

↳ má nekonečně mnoho řešení

↳ $\text{rank}(A) < n$

↳ nulový vektor, že $Ax=0$

↳ alespoň 1 řádek / sloupec je lineární kombinací ostatních

↳ nelze invertovat

řešení rovnice: $XA = B$ / A^{-1} zpráva, pro regulární A

$$X = B \cdot A^{-1}$$

↑ $A \in \mathbb{R}^{m \times n}$, pak rovnice $AX = I_m$ má řešení například.. $AX = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$
pokud $n < m$ můžeme mít $\text{rank}(AX) \leq \text{rank}(A) \leq \min\{m, n\}$

regulární matice se zachovávají: • násobení (součin matric) $\rightarrow$ obě regulární

• inverzí

• transpozice $\text{rank}(A) = \text{rank}(A^T)$

ne:

sčítání matric $\rightarrow$ nezachová regulárity, může být invertibilní

násobení singulární $\rightarrow$ zleva i zprava $\rightarrow$ vždy singulární AB singulární, kde
 A singulární
a B regulární

nelze vyřešit všechny lineární rovnice, např. $AX + XB = C$, X nelze
získnout ani nic jiného

74) Přehledové sešite, co víte o binárních operacích a jejich vlastnostech

↳ Binární operace na množině X je zobrazení $X \times X \rightarrow X$

↳ v definici zobrazení je přímo uvazňování, např. $\forall a, b \in X: a \circ b \in X$, když

a, b byli prvky X a $\circ$ operace definovaná $\circ: X \times X \rightarrow X$

↳ příklady $\rightarrow$ zároveň vždy platí jednoznačnost

↳ $(\mathbb{R}, +)$, $(\mathbb{R}, -)$, $(\mathbb{R}, \cdot)$, $(\mathbb{R} \setminus \{0\}, :)$ jsou různé binární operace

↳ $(\mathbb{N}, +)$ je, ale např. $(\mathbb{N}, -)$ není bin. operace, protože není uzavřena na odčítání

↳ $(a, b) \mapsto a$, $(p, q) \mapsto p + q$, sčítání matic stejného řádku nebo násobení čtvercových matic

↳ základní vlastnosti $\leftarrow$ obecně platit nemusí, Necht' $\circ$ je bin. operace na množině X

asociativita $\forall a, b, c \in X: a \circ (b \circ c) = (a \circ b) \circ c$

neutrální prvek $\exists e \in X: \forall a \in X: a \circ e = e \circ a = a$

komutativita $\forall a, b \in X: a \circ b = b \circ a$

inverzní prvek $\forall a \in X: \exists b \in X: a \circ b = b \circ a = e$ $\leftarrow$ kde e je neutrální

↳ algebraická struktura založená na bin. operaci

grupa $(G, \circ) \rightarrow$ množina G s bin. operací $\circ$

↳ platí asociativita, jednoznačnost neutrálních a inverzních prvků

15) Přehledové sešite, co víte o (obecných) grupách

↳ Grupa $(G, \circ)$ je množina G a binární operaci $\circ : G \times G \rightarrow G$

↳ platí následující axiomy:

$$\forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c) \rightarrow \underline{\text{asociační}}$$

$$\exists e \in G : \forall a \in G : a \circ e = e \circ a \rightarrow \underline{\text{neutrální prvek } e}$$

$$\forall a \in G : \exists b \in G : a \circ b = b \circ a = e \rightarrow \underline{\text{inverzní prvek } b}$$

↳ u Abelovské grupy:

$$\text{↳ platí komutativita : } \forall a, b \in G : a \circ b = b \circ a$$

↳ příklad : - nejmenší grupa je $(\{e\}, \circ)$, pro kterou platí $e \circ e = e$

- nejmenší neabelovská grupa je S_3 má 6 prvků

↳ neutrální prvek je jednoznačný pro všechny prvky $e = e \circ e' = e'$

↳ pro každý prvek je jednoznačný inverzní prvek

↳ příklady - aditivních grup : $(\mathbb{R}, +)$, ~~$(\mathbb{N}, +)$~~ není grupa, nemá inverzní prvek

- multiplikativních grup : $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q}^+, \cdot)$, $(\{-1, 1\}, \cdot)$

↳ ekvivalentní úpravy jsou : $a = b \Leftrightarrow a \circ c = b \circ c \Leftrightarrow c \circ a = c \circ b$

↳ pro uzavřenost, z definice binární operace : $\forall a, b \in G : a \circ b \in G$

$$(a^{-1})^{-1} = a \quad (a \circ b)^{-1} = b^{-1} \circ a^{-1} \quad a^n = \underbrace{a^{-1} \circ a^{-1} \circ \dots \circ a^{-1}}_{n \text{ krát}}$$

$$a^n := \underbrace{a \circ a \circ a \circ \dots \circ a}_{n \text{ krát}} \quad a^0 = e$$

$$a^{m+n} = a^m \circ a^n$$

76) Přehledově sepište, co víte o permutačních grupách

↳ permutační grupy jsou bijektivní zobrazení $p: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$
s bin. operací skládání $\circ$

↳ je to množina S_n všech permutací nad n prvky, která tvoří symetrickou grupu. $(S_n, \circ)$

↳ binární operace je skládání

↳ axiomy grupy: asociativita, neutrální prvek a inverzní prvek

↳ dají se zapsat pomocí cyklu, tabulky, grafu a permutační

matice $\rightarrow (p)_{ij} = \begin{cases} 1 & \text{když } p(i)=j \\ \text{jinak} \end{cases}$

↳ první bod je cyklus délky 1

↳ transpozice je cyklus délky 2

↳ každou permutaci lze zapsat jako složení transpozic

↳ znaménko permutace $\rightarrow$ udává zda je permutace sudá $\rightarrow +1$ nebo lichá $\rightarrow -1$

↳ dá se určit $\text{sgn}(p) = (-1)^{\# \text{inverzí}}$

$\text{sgn}(p) = (-1)^{\# \text{transpozic}}$

$\text{sgn}(p) = (-1)^{\# \text{sudých cyklů}}$

↳ kde inverze je $\{i, j : i < j \wedge p(i) > p(j)\}$, není to samé, co inverzní permutace

↳ rozklad na transpozice $(1, \dots, k) = (1, k) \circ (1, k-1) \circ (1, k-2) \circ \dots \circ (1, 2)$
↳ sudé cykly na lichý počet transpozic

↳ identita je složení permutace $\forall i: \text{id}(i) = i$

↳ znaménko při skládání permutací p q: $\text{sgn}(q \circ p) = \text{sgn}(q) \cdot \text{sgn}(p)$

↳ PA → Ranního řádky

↳ AP → Ranního sloupce

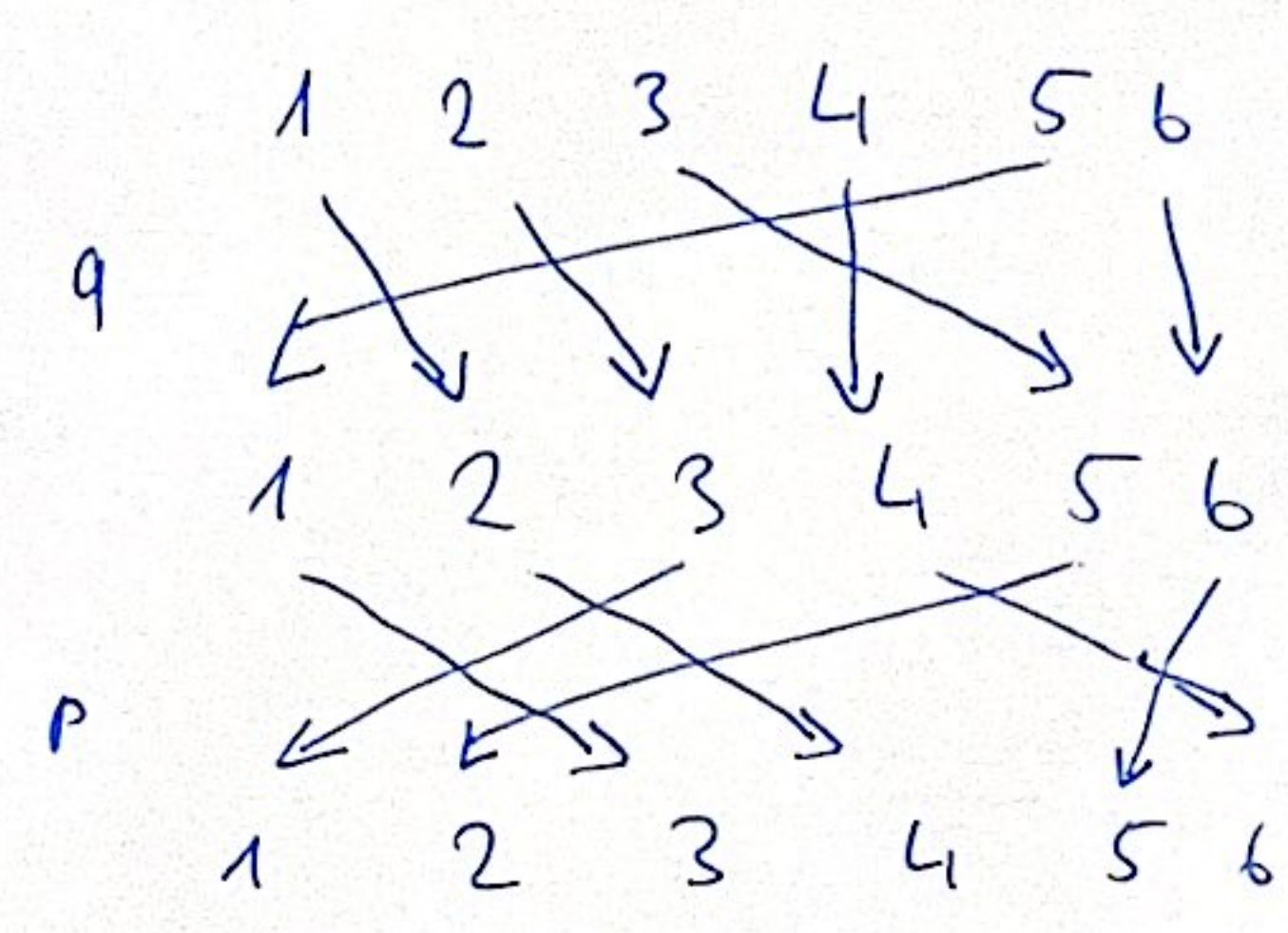
skládání permutací

↙ první: např. 2, na druhé pozici je 4

$p \circ q = (4, 1, 2, 6, 3, 5)$

$p = (3, 4, 1, 6, 2, 5)$

$q = (2, 3, 5, 4, 1, 6)$



invertování

↖ na které pozici je? 1, 2, 3, 4, ...

$p^{-1} = (3, 5, 1, 2, 6, 4)$

$q^{-1} = (5, 1, 2, 4, 3, 6)$

cykly

↖ co se stane na co

$p = (13)(2465)$

$q = (1235)(4)(6)$

Znaménka:

$\text{sgn}(p) = (-1)^{\# \text{ počet sudých cyklů}}$

$\text{sgn}(p) = -1$

$\text{sgn}(q) = -1$

mocniny

↖ posunuti v cyklech

$p^{15} = p^{12} \circ p^3 = (p^4)^3 \circ p^3 = (\text{id})^3 \circ p^3 = p^3$

$p^3 = (13)(2564) \quad p^3 = (3, 5, 1, 2, 6, 4)$

$q^{33} = (q^{32}) \circ q^1 = q = (1235)(4)(6) \quad q = (2, 3, 5, 4, 1, 6)$

- 2 → 5
- 5 → 6
- 6 → 4
- 4 → 2
- 3 → 1
- 1 → 3

77) Průhledově sepište, co víte o tělesech

↳ těleso je algebraická struktura s množinou T a dvěma binárními komutativními operacemi: $+$ a $\cdot$, kde $(T \setminus \{0\}, \cdot)$ a $(T, +)$ jsou Abelovské grupy, pro které platí axiomy:

↳ komutativita, asociativita, neutrální prvek a inverzní prvek $\rightarrow$ 8 axiomů?

$$\downarrow$$
$$\text{kde } 1 \text{ u } \cdot$$
$$0 \text{ u } +$$

$$\hookrightarrow a^{-1} \text{ u } \cdot$$

$$-a \text{ u } + \text{ (opaciny) }$$

+1 axiom distributivity: $\forall a, b, c \in T: a \cdot (b + c) = a \cdot b + b \cdot c$

↳ příklady: $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$

↳ $\mathbb{Z}_p \Leftrightarrow p$ je prvočíslo je těleso

↳ počítám v modulu p

↳ neutrální prvky 0 u $(T, +)$ a 1 u $(T \setminus \{0\}, \cdot)$ jsou jednoznačné

↳ pro každý prvek je jednoznačný inverzní prvek a^{-1} u $(T \setminus \{0\}, \cdot)$ a $-a$ pro $(T, +)$ Abelovské grupy

↳ řešitelnost rovnic

↳ korektnost ekvivalentních úprav

↳ charakteristika tělesa $\underbrace{1+1+\dots+1}_{n \text{ krát}} = 0$

$$\text{char}(\mathbb{Z}_p) = p$$

$$\text{char}(\mathbb{R}) = 0$$

↳ malá Fermatova věta pro prvočíslo p a $a \in \{1, \dots, p-1\}$: $a^{p-1} \equiv 1 \pmod{p}$

78) Přehledové sešite, co víte o vektorových prostorech a jejich podprostorech

↳ Vektorový prostor $(V, +, \cdot)$ nad tělesem $(T, +, \cdot)$ je množina V spolu s binárními operacemi $+$: $V \times V \rightarrow V$ a skalárním násobkem $\cdot$: $T \times V \rightarrow V$.

$(V, +)$ je Abelova grupa

↳ platí axiomy pro $(V, +)$

- komutativita $\forall u, v \in V: u + v = v + u$
- asociativita $\forall u, v, w \in V: u + (v + w) = (u + v) + w$
- neutrální prvek $\exists 0 \in V: \forall u \in V: u + 0 = 0 + u = u$
- inverzní prvek $\forall u \in V: \exists -u \in V: u + (-u) = 0$
- uzavřenost $+$: $V \times V \rightarrow V \quad \forall u, v \in V: u + v \in V$

další axiomy:

↳ distributivita vlevo: $\forall v, u \in V: \forall t \in T: t \cdot (u + v) = t \cdot u + t \cdot v$

↳ distributivita sprava: $\forall t, s \in T: \forall v \in V: (t + s) \cdot v = t \cdot v + s \cdot v$

↳ násobek s 1: $\forall v \in V: 1 \cdot v = v$

↳ asociativita: $\forall t, s \in T: \forall v \in V: (t \cdot s) \cdot v = t \cdot (s \cdot v)$

↳ prvky množiny V jsou vektory, prvky množiny T jsou skaláry

↳ příklady prostorů: - triviální prostor: $V = \{0\}$ nad libovolným tělesem T

- aritmetický $\rightarrow T^n$ dimenze n nad tělesem T .

$\rightarrow$ vektory jsou uspořádané n -tice

- polynomy omezeného stupně

↳ vlastnosti vektorových prostorů:

↳ jednorozměrnost vektoru 0

↳ jednorozměrnost opačného vektoru $-u$

↳ ekvivalentní úpravy $u + w \Leftrightarrow u + v = w + v$

Podprostor je vektorový prostor pro který platí, že množina vektorů $U \subseteq V$, kde U je množina vektorů U

↳ každý vektorový prostor má bázi a velikost báze je $\dim(U) \rightarrow$ dimenze vektorového prostoru, díky lineární kombinaci vektorů z báze lze mít každý vektor ^{prostoru}

↳ podprostor musí být uzavřen na vektorový součet a skalární

násobek: $\forall u, v \in U: u+v \in U$

$$\forall \lambda \in T: \forall u \in U: \lambda \cdot u \in U$$

↳ a podprostor U je neprázdná množina a obsahuje počátek

↳ průnik podprostorů U_i platí že tvoří taky podprostor $\bigcap_{i \in I} U_i$

↳ průnik podprostorů $U \subseteq V$, které obsahují M je lineární obal $\text{span}(M)$,

$$\text{span}(M) = \bigcap \{ U: M \subseteq U \text{ a } U \text{ je podprostor } V \}$$

příklad $\text{span}(\{(1,0,0)^T, (0,1,0)^T\})$ je rovina v $\mathbb{R}^3$ prostoru

↳ lineární kombinace $u = \sum_{i=1}^n a_i b_i \rightarrow$ vyjádření vektoru U pomocí LK z vektorů množiny B

$$\rightarrow a_1, \dots, a_n \in T \text{ a } b_1, \dots, b_n \in V$$

↳ lineární obal lze chápat jako průnik podprostorů a nebo lineární kombinace

79) Přehledově sepište, co víte o vektorových prostorech maticí A

$A \in T^{m \times n}$, kde T je těleso

Jádro matice (nulový prostor)

$\ker A := \{x \in T^n : Ax = 0\}$ $Ax = 0 \rightarrow$ množina řešení homogenní soustavy, kdy se

$\dim(\ker A) \rightarrow$ je počet volných proměnných

Sloupový prostor S_A $\boxed{\dim(\ker A) + \text{rank}(A) = n}$

$S_A := \{u \in T^m : \exists d \in T^n : u = A \cdot d\} \subseteq T^m$

$\hookrightarrow$ prostě najdu sloupové vektory a jejich kombinace pomocí LH

$Ax = b$ má řešení $\Leftrightarrow b \in S_A$, protože $(A|b)$

$\hookrightarrow$ a musím ten vektor sloupů z matice vyjádřit

$\hookrightarrow S_A$ je obraz lineárního zobrazení daného maticí A

$\hookrightarrow$ sloupce, kde jsou báze proměnné v REF matici $A \rightsquigarrow A'$, tak, když

vezmu sloupce stejných indexů z původní A , tak jsou báze S_A

$$\text{rank}(A^T) = \dim(S_{A'}) = \dim(R_{A'}) = \text{rank}(A) = \text{rank}(A') = \dim(S_A) = \dim(R_A)$$

Rádkový prostor R_A

$$R_A := \{u \in T^m : \exists d \in T^n : u = A^T \cdot d\}$$

$\hookrightarrow$ 0 podprostor generovaný řádky matice A

$\hookrightarrow$ Gaussova eliminace a elementární řádkové úpravy nemění rádkový prostor

Vztahy mezi reálnými prostorem a jádrem

Pro ^(každé) $\forall x \in \ker A$ a ^(každé) $\forall v \in R_A$ platí: $v^T x = 0$

$\hookrightarrow$ jinak řečeno $x \in T^m: (\forall v \in R_A: v^T x = 0) \Leftrightarrow x \in \ker A$

$v \in T^m: (\forall x \in \ker A: v^T x = 0) \Leftrightarrow v \in R_A$

$\hookrightarrow$ pro reálné matice A platí $R_A \cap \ker A = \{0\}$

$\hookrightarrow$ prošel přímkou všech vektorů, co se zobrazí na nulu

$\hookrightarrow V \subseteq T^m$

$\hookrightarrow$ Pro složené prostory A a AB platí $S_{AB} \subseteq S_A$

$\hookrightarrow$ Pro reálné prostory A a AB platí $R_{AB} \subseteq R_A$

$\hookrightarrow \text{rank}(AB) \leq \min \{ \text{rank} A, \text{rank} B \}$

$\hookrightarrow$ neplatí to pro A a BA

$\hookrightarrow$ pro ně platí jen $\dim S_{BA} \leq \dim S_A$

$\hookrightarrow$ pro libovolnou matici $A \in T^{m \times n}$ a regulární $R \in T^{n \times n}$ a

$R' \in T^{n \times n}$ platí $\text{rank}(A) = \text{rank}(RA) = \text{rank}(AR')$

$\hookrightarrow$ pokud $A=BC$ a C je regulární, pak $S_A = S_B$

$\hookrightarrow$ Každý $V \subseteq T^m$ je množinou řešení vhodné homogenní soustavy

8) Přehledně sepište, co víte o lineární závislosti

V je vektorový prostor nad tělesem T a $B = \{b_1, \dots, b_n\}$ je $B \subset V$
lineárně nezávislá množina, pro kterou platí:

↳ neexistuje netriviální lineární kombinace, kdy by výsledný vektor byl nulový, tedy platí $u = \sum_{i=1}^n a_i b_i = 0 \Leftrightarrow a_1 = \dots = a_n = 0$

↳ nelze vyjádřit vektory LN množiny ostatními vektory z téže množiny

↳ v ostatních případech je množina lineárně závislá a lze

vyjádřit vektor pomocí ostatních, např. pro $v_j = \sum_{i \neq j} -\frac{a_i}{a_j} v_i$, vyjádřeno z

$$0 = \sum_{i=1}^n a_i v_i \rightarrow \text{je jednoznačný}$$

↳ příklady:

↳ pokud $0 \in B$, pak je lineárně závislá

↳ řádky / sloupce v I_n jsou lineárně nezávislé

↳ nemulové řádky matice v REF tvaru jsou lineárně nezávislé

↳ $\emptyset \rightarrow$ lineárně nezávislá

↳ v $\mathbb{R}^2 \rightarrow B = \{b_1\}$ je LN $\Leftrightarrow b_1 \neq 0$

$\rightarrow C = \{c_1, c_2\}$ je LN $\Leftrightarrow c_1 \neq c_2$ a přímka z bodů c_1 a c_2 neobsahuje počátek

$\rightarrow D = \{d_1, d_2, d_3\}$ je lineárně závislá

↳ testování lineární závislosti

↳ 1) vektory do řádků a pokud se řádek vynuluje, tak ten vektor byl lineárně závislý

2) vektory do sloupců a pokud bude volná proměnná $\rightarrow$ netriviální řešení nuly

↳ Pokud je B lineárně nezávislá a $C \subseteq B$, pak C je LN

↳ Pokud je B lineárně závislá a $B \subseteq D$, pak D je lineárně závislá

↳ B je LN $\Leftrightarrow \forall b \in B : b \notin \text{span}(B \setminus b)$

↳ Jestliže je C konečná generující množina prostoru V a B je lineárně nezávislá množina v prostoru V , tak platí $|B| \leq |C|$

↳ důkaz: pro spor, že $|B| > |C|$, a proto je tam nějaký vektor lineární kombinací ostatních

vektor k dimenzí a báze

báze je množina lineárně nezávislých vektorů generující celý prostor V , např. pro $V = \mathbb{R}^3$, tak B je báze $B = \{(0, 1, 0)^T, (1, 0, 0)^T, (0, 0, 1)^T\}$
 $\text{span}(B) = V$

dimenze $\rightarrow \dim(V)$ je velikost báze, která má přesně danou mohutnost
např. pro $\dim(\mathbb{R}^3) = 3$

81) Přehledově sepište, co víte o bářích vektorových prostorů

V je vektorový prostor nad tělesem T , kde B je lineárně nezávislá množina ve vektorovém prostoru nebo-li platí:

to existuje jen lineární kombinace pro každý vektor

$$0 = \sum_{i=1}^n a_i b_i \Leftrightarrow b_1 = \dots = b_n = 0, \text{ where } a_1, \dots, a_n \in T \text{ and } b_1, \dots, b_n \in B$$

Báze je lineárně nezávislá množina, která generuje celý prostor V

$$\text{Span}(B) = V$$

$|B| = \dim(V) \rightarrow$ velikost baze je dimenzija vektorskega prostora

→ map: $\mathbb{R}^3 \rightarrow V$, take $B = \{(0, 1, 0)^T, (1, 0, 0)^T, (0, 0, 1)^T\}$, take

$$\dim(\mathbb{R}^3) = 3 \quad \text{a} \quad \text{span}(B) = V \quad \text{a} \quad |B| = 3$$

↳ příklad: v prostoru T^n tvoří sloupce I_n matice (jednotkové) tzv. standardní bázi E

✓ $\mathbb{R}^2 \rightarrow$ množina $B = \{b_1, b_2\}$ bází $\Leftrightarrow b_1 \neq b_2$ a přímka body b_1 a b_2 neobsahují počátek

↳ povišati $\rightarrow$ izog komprese

↳ báze je minimální generující množina V

↳ baze je maximální lineárně nezávislá množina generující V

↳ každý vektor lze tedy rozpsat jedinečným způsobem lineárně

combinação $u = \sum_{i=1}^n a_i b_i$ pro $u \in V$, bási $B \subset V$ e $a_1, \dots, a_n \in T$
 $\downarrow$
 $b_1, \dots, b_n \in B$

$\text{span}(B) = V$ a $\forall b \in B: b \notin \text{span}(B \setminus b) \rightarrow$ je báze

pro každých n vektorů existuje báze

82) Přehledové sešite, co víte o lineárních zobrazeních

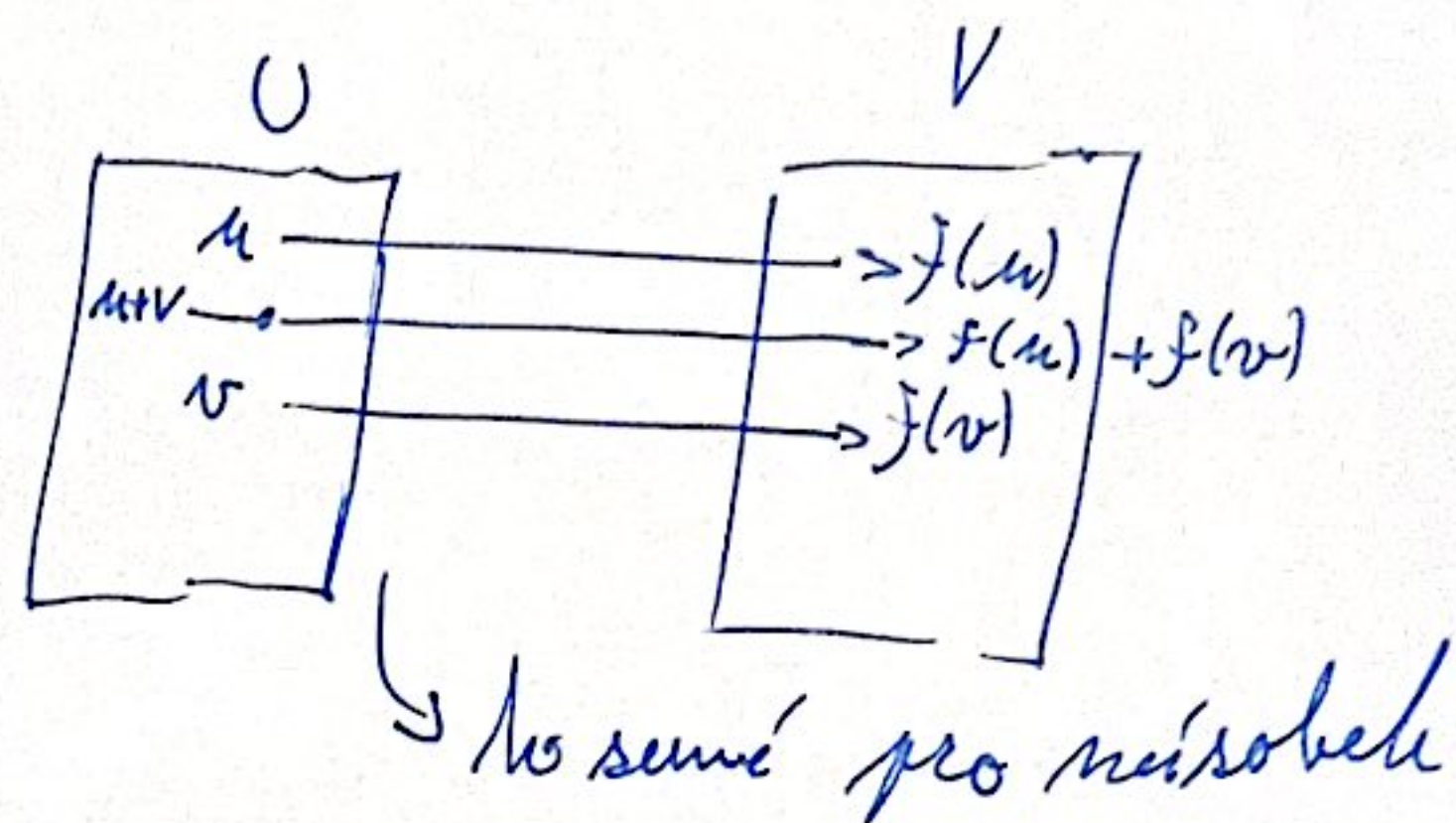
Necht' U, V prostory nad tělesem T . Zobrazení je $f: U \rightarrow V$

Pro $A \in T^{m \times n}$ je definované $f: T^n \rightarrow T^m$ jako $f(u) = A \cdot u$ → lineární zobrazení dané matricí

↳ zobrazení je lineární, tedy platí linearity součtu a násobku

$$\forall u, v \in U: f(u+v) = f(u) + f(v)$$

$$\forall u \in U: \forall \lambda \in T: f(\lambda \cdot u) = \lambda \cdot f(u)$$



platí: • $f(0) = 0$

• $f(-u) = -f(u)$

• $f\left(\sum_{i=1}^n t_i u_i\right) = \sum_{i=1}^n t_i f(u_i)$

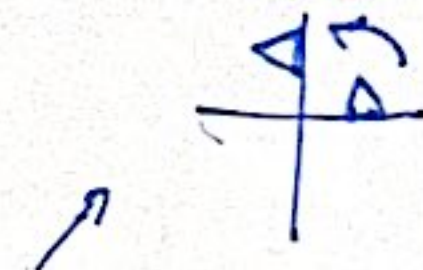
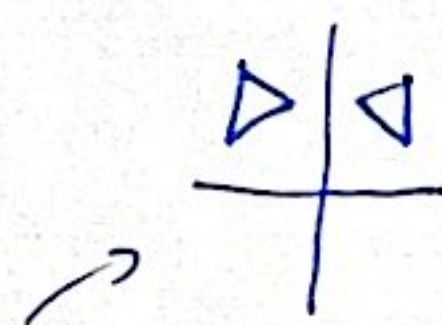
triviální

$$\forall u \in U: f(u) = 0$$

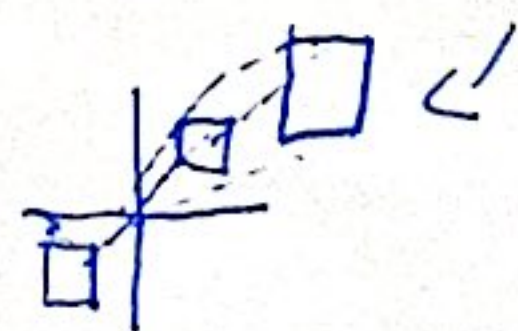
identita

$$\forall u \in U: f(u) = u \quad \text{nebo-li} \quad \forall u \in U: \text{id}(u) = u$$

příklady: - derivace na prostoru funkcí $f: X \rightarrow X'$



- geometrické lineární zobrazení → osová souměrnost, rotace kolem počátku, stejnoběžnost s středem v počátku



- projekce • $f(x, y) = x$

• $\pi_i((u_1, \dots, u_n)) = u_i$

• $f: T^n \rightarrow T$

↳ jestliže $f: U \rightarrow V$ a $g: V \rightarrow W$ obě lineární, pak $(g \circ f): U \rightarrow W$ je také lineární

↳ pokud je $f: U \rightarrow V$ ^(a lineární) bijektivní $\rightarrow$ prosté = každý vektor se neobrazí na jeden obraz dvakrát
 $\rightarrow$ na = pokrývá celou množinu vektorů

↳ pak je i $f^{-1}: V \rightarrow U$ lineární

↳ bijektivní lineární zobrazení se nazývá isomorfismus

Zobrazení na vektor souřadnic

Věta: Necht' V je vektorový prostor nad T s bází $B = (b_1, \dots, b_n)$,

pak je $f: U \rightarrow T^n$ definované jako $f(u) = [u]_B$ a je lineární.

↳ zobrazení $f(u) = [u]_B$ je také bijekce = isomorfismus

↳ každý konečně rozměrný vektorový prostor je isomorfní s T^n

Věta o rozšiřitelnosti (prodloužitelnosti)

Věta: Necht' U a V jsou prostory nad tělesem T a B je báze prostoru U ,

$B = (b_1, \dots, b_n)$, a $f: U \rightarrow V$ je lineární zobrazení a $f_0: B \rightarrow V$ je rozšířeno

$f: U \rightarrow V$, pak platí: $\forall b \in B: f(b) = f_0(b)$

↳ u $f: U \rightarrow V$, pokud $\dim(U) > \dim(V) \rightarrow$ není prosté

pokud $\dim(U) < \dim(V) \rightarrow$ není na

pokud $\dim(U) = \dim(V) \rightarrow$ je bijektivní

↳ platí $\dim(U) = \dim(\ker f) + \dim(\operatorname{Im} f)$ $f: U \rightarrow V$ sestavím matici $A \in \mathbb{R}^{\dim(V) \times \dim(U)}$

83) Přehledově sepište, co víte o maticích lineárních zobrazení

↳ Necht' U a V jsou vektorové prostory nad tělesem T a

$f: U \rightarrow V$ je lineární zobrazení, kde $B = (b_1, \dots, b_n)$ je báze prostoru U
a $C = (c_1, \dots, c_m)$ je báze prostoru V ,

pak $[f]_{B,C} \in T^{m \times n}$ je matice lineárního zobrazení

$$[f]_{B,C} = \begin{pmatrix} | & & | \\ [f(b_1)]_C & \dots & [f(b_n)]_C \\ | & & | \end{pmatrix}, \text{ kde } [f(b_i)]_C \text{ je vektor souřadnic}$$

obrazu báze B vůči bázi C

$$\hookrightarrow \text{platí } \forall u \in U: [f(u)]_C = [f]_{B,C} [u]_B$$

$$\hookrightarrow [f]_{E,E} [u_i]_E = [v_i]_E$$

$$\hookrightarrow \text{shládním } f: U \rightarrow V \quad g: V \rightarrow W, \text{ pak } \underline{[g \circ f]_{B,D} = [g]_{C,D} [f]_{B,C}}$$

↳ kde báze jsou B pro U , C pro V , D pro W

↳ matice přechodu

↳ existuje zobrazení jednoho vektoru vůči jiným bázím, např. B a C jednoho prostoru, např. U

$$[id]_{B,C}$$

$$\forall u \in U: [u]_C = [id(u)]_{B,C} [u]_B$$

$$[id]_{C,B} [id]_{B,C} = [id]_B = I \rightarrow \text{existuje tedy inverze, a proto je}$$

matice přechodu regulární

$$[id]_{B,C} = ([id]_{C,B})^{-1}$$

↳ výpočet $[id]_{B,C}$

$$\hookrightarrow B = (b_1, \dots, b_n)$$

$$\hookrightarrow C = (c_1, \dots, c_n)$$

}

$$u = B \cdot [u]_B$$

$$u = C \cdot [u]_C$$

$$\Rightarrow B[u]_B = C[u]_C$$

$$[u]_C = C^{-1} B [u]_B$$

$$[u]_C = [id]_{B,C} [u]_B$$

změna báze u matic zobrazení: $[f]_{D,E} = [id]_{C,E} [f]_{B,E} [id]_{D,B}$

↳ matice isomorfismu

Prostory U, V nad T a lineární zobrazení $f: U \rightarrow V$ s bázemi B a C ,

pak je zobrazení $f: U \rightarrow V$ isomorfní pokud $[f]_{B,C}$ je regulární, tj.

$$[f]_{B,C} = ([f]_{C,B})^{-1}$$

$$\text{přiči } [f^{-1}]_{C,B} = ([f]_{B,C})^{-1}$$

↳ pokud má matice $f: U \rightarrow V$ nulový sloupec $\rightarrow$ není prostá

84) Přehledově sepište, co víte o afinních prostorech

↳ Necht W je vektorový podprostor vektorového prostoru V nad tělesem T , pak

afinní prostor je množina $\{u+w : w \in W\}$, značí se $u+W$,

dimenze afinního prostoru je $\dim(W)$

↳ afinní prostor je určený: bodem $\rightarrow u$

• translačním prostorem $\rightarrow W$

↳ příklady: - nadrovina $\sim \mathbb{R}^m$

- přímka $\sim \mathbb{R}^2 \rightarrow u + \text{span}(v)$

- rovina $\sim \mathbb{R}^3 \rightarrow u + \text{span}(v_1, v_2)$

↳ lze definovat přesněji podle axiomů: $+: A \times W \rightarrow A$

$$\forall a \in A: \forall u, v \in W: a + (u + v) = (a + u) + v$$

$\rightarrow$ prostě vznikla posunutá množina A

$$\forall a, b \in A: \exists! v \in W: a + v = b$$

↳ prvky množiny A jsou body

↳ afinní prostor: $\rightarrow$ není obecný vektorový prostor

↳ nemá privilegovaný nulový prvek $\rightarrow$ platí je $\forall a \in A: a + 0 = a$

↳ nemá určen na sčítání bodů ani skalární násobek

Afinní prostory a lin. zobrazení

$$\ker f := \{x \in V: f(x) = 0\} \rightarrow \text{jádro lineárního zobrazení}$$

$$f: T^m \rightarrow T^m \text{ platí } (f(x) = Ax) \Rightarrow \ker f = \ker A$$

Věta o řešení rovnice s lineárním zobrazením:

↳ Nechť U, V jsou vektorové prostory a $v \in V$, nechť $f: U \rightarrow V$, nechť

$f(x) = v$ buď nemá řešení $v \notin f(U)$

• řešení tvoří afinní prostor $u + \ker f$, kde u je libovolné řešení rovnice

↳ protože $f(u+w) = f(u) + f(w) = v + 0 = v$

↳ kde $w \in \ker f$

↳ Afinní prostor obsahuje $0 \iff$ je vektorovým prostorem

↳ $0 + W$