Zpracování vybraných otázek ke zkoušce z LA1

Karel Velička, *(původně: Zdeněk Tomis)*

11-12-2022

1. ročník bc. informatika
doc. RNDr. Jiří Fiala, Ph.D.

Obsah

1 Definice (3 otázky) 1
1.1 Soustavy lineárních rovnic . . . 1
1.1.1 Definujte rozšířenou matici soustavy. . . . 1
1.1.2 Definujte elementární řádkové operace. . . . 1
1.1.3 Definujte odstupňovaný tvar matice. (REF) . . . 1
1.1.4 Napište pseudokód pro Gaussovu eliminaci. . . . 1
1.1.5 Definujte pivot a to slovně i formálně. . . . 1
1.1.6 Definujte volné a bázické proměnné. . . . 1
1.1.7 Definujte hodnost matice. . . . 1
1.2 Matice . . . 2
1.2.1 Jednotkovou matici. . . . 2
1.2.2 Definujte transponovanou matici. . . . 2
1.2.3 Definujte symetrickou matici. . . . 2
1.2.4 Definujte maticový součin. . . . 2
1.2.5 Definujte inverzní matici. . . . 2
1.2.6 Definujte regulární matici. . . . 2
1.2.7 Definujte singulární matici. . . . 2
1.2.8 Definujte binární operaci. . . . 2
1.2.9 Definujte komutativní a asociativní binární operace. . . . 2
1.2.10 Definujte neutrální prvek. . . . 2
1.2.11 Definujte inverzní prvek. . . . 3
1.3 Grupy a permutace . . . 3
1.3.1 Definujte grupu. . . . 3
1.3.2 Definujte permutaci. . . . 3
1.3.3 Definujte permutační matici, . . . 3
1.3.4 Definujte transpozici. . . . 3
1.3.5 Definujte inverzi v permutaci. . . . 3
1.3.6 Definujte znaménko permutace. . . . 3
1.4 Tělesa . . . 3
1.4.1 Definujte těleso. . . . 3
1.4.2 Definujte charakteristiku tělesa. . . . 3
1.5 Vektorové prostory . . . 4
1.5.1 Definujte vektorový prostor. . . . 4
1.5.2 Definujte podprostor vektorového prostoru. . . . 4
1.5.3 Definujte lineární kombinaci. . . . 4
1.5.4 Definujte lineární obal (podprostor generovaný množinou). . . . 4
1.5.5 Definujte řádkový prostor matice a to slovně i formálně pomocí maticového součinu. . . . 4
1.5.6 Definujte sloupcový prostor matice a to slovně i formálně pomocí maticového součinu . . . 4
1.5.7 Definujte jádro matice. . . . 4
1.5.8 Definujte lineárně nezávislé vektory. . . . 5
1.5.9 Definujte bázi vektorového prostoru. . . . 5
1.5.10 Definujte dimenzi vektorového prostoru. . . . 5
1.5.11 Definujte vektor souřadnic. . . . 5
1.6 Lineární zobrazení . . . 5
1.6.1 Definujte lineární zobrazení. . . . 5

1.6.2 Definujte matici lineárního zobrazení. . . . 5
1.6.3 Definujte jádro lineárního zobrazení. . . . 5
1.6.4 Definujte matici přechodu. . . . 5
1.6.5 Definujte izomorfismus vektorových prostorů. . . . 5
1.6.6 Definujte afinní prostor a jeho dimenzi. . . . 6

2 Věty **7**
2.1 Soustavy lineárních rovnic . . . 7
2.1.1 Uved'te a dokažte vztah mezi elementárními řádkovými operacemi a soustavami rovnic. . . . 7
2.1.2 Vyslovte a dokažte větu o jednoznačnosti volných a bázických proměnných. . . . 7
2.1.3 Vyslovte a dokažte Frobeniovu větu. . . . 7
2.2 Matice . . . 8
2.2.1 Vyslovte a dokažte větu o vztahu mezi řešeními Ax = b a Ax = 0. . . . 8
2.2.2 Uved'te a dokažte větu popisující všechna řešení Ax = b. . . . 8
2.2.3 Vyslovte a dokažte větu o ekvivalentních definicích regulárních matic. . . . 8
2.3 Grupy a permutace . . . 9
2.3.1 Vyslovte a dokažte větu o znaménku složené permutace. . . . 9
2.4 Tělesa . . . 9
2.4.1 Uved'te a dokažte větu charakterizující, kdy Z_p je těleso . . . 9
2.4.2 Vyslovte a dokažte malou Fermatovu větu. . . . 9
2.5 Vektorové prostory . . . 9
2.5.1 Vyslovte a dokažte větu o průniku vektorových prostorů. . . . 9
2.5.2 Vyslovte a dokažte větu o ekvivalentních definicích lineárního obalu. . . . 10
2.5.3 Vyslovte a dokažte tvrzení o mohutnostech lineárně nezávislé množiny a generující množiny. 10
2.5.4 Uved'te a dokažte Steinitzovu větu o výměně (včetně lemmatu, pokud jej potřebujete). . . . 10
2.5.5 Vyslovte a dokažte větu o dimenzi průniku vektorových prostorů. . . . 11
2.5.6 Vyslovte a dokažte větu o vektorových prostorech souvisejících s maticí A. . . . 11
2.5.7 Vyslovte a dokažte větu o dimenzi jádra matice. . . . 11
2.6 Lineární zobrazení . . . 11
2.6.1 Vyslovte a dokažte větu o jedinečnosti lineárního zobrazení. . . . 11
2.6.2 Vyslovte a dokažte větu o řešení rovnice s lineárním zobrazením. . . . 11
2.6.3 Vyslovte a dokažte pozorování o matici složeného lineárnıho zobrazení. . . . 11
2.6.4 Vyslovte a dokažte větu o charakterizaci izomorfismu mezi vektorovými prostory. . . . 12
2.7 Grafy a podgrafy . . . 12
2.7.1 Zformulujte problém o počtu sudých podgrafů a vyřešte jej. . . . 12
2.7.2 Zformulujte problém o množinových systémech s omezeními na mohutnosti a vyřešte jej. . . . 12
2.7.3 Zformulujte problém o dělení obdélníku na čtverce a vyřešte jej. . . . 12

3 Přehled **13**
3.1 Soustavy lineárních rovnic . . . 13
3.1.1 Přehledově sepište, co víte o elementárních řádkových operacích a Gaussově eliminaci. . . . 13
3.1.2 Přehledově sepište, co víte o řešení homogenních a nehomogenních soustav lineárních rovnic. 13
3.2 Matice . . . 13
3.2.1 Přehledově sepište, co víte o maticových operacích. . . . 13
3.2.2 Přehledově sepište, co víte o regulárních a singulárních maticích. . . . 13
3.3 Grupy a permutace . . . 14
3.3.1 Přehledově sepište, co víte o binárních operacích a jejich vlastnostech. . . . 14
3.3.2 Přehledově sepište, co víte o (obecných) grupách. . . . 14
3.3.3 Přehledově sepište, co víte o permutačních grupách. . . . 14
3.4 Tělesa . . . 14
3.4.1 Přehledově sepište, co víte o tělesech. . . . 14
3.5 Vektorové prostory . . . 14
3.5.1 Přehledově sepište, co víte o vektorových prostorech a jejich podprostorech. . . . 14
3.5.2 Přehledově sepište, co víte o vektorových prostorech určených s maticí A. . . . 15
3.5.3 Přehledově sepište, co víte o lineární závislosti. . . . 15
3.5.4 Přehledově sepište, co víte o bázích vektorových prostorů. . . . 15
3.6 Lineární zobrazení . . . 15
3.6.1 Přehledově sepište, co víte o lineárních zobrazeních a jejich maticích. . . . 15

1 Definice (3 otázky)

1.1 Soustavy lineárních rovnic

1.1.1 Definujte rozšířenou matici soustavy.

Pro soustavu $Ax = b$, kde $A \in \mathbb{R}^{m \times n}$ je matice soustavy, $x = (x_1, ..., x_n)^T$ je vektor neznámých a b je vektor pravých stran, je *rozšířená matice soustavy*:

$$A^{m \times n} = \left(\begin{array}{ccc|c} a_{1,1} & \cdots & a_{1,n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m,1} & \cdots & a_{m,n} & b_m \end{array} \right)$$

1.1.2 Definujte elementární řádkové operace.

Elementární řádkovou úpravou vznikne z matice A matice A' ($A \sim\sim A'$):

(i) vynásobením i-tého řádku $t \in \mathbb{R} \setminus \{0\}$

(ii) přičtením j-tého řádku k i-tému, když $i \neq j$

Z těchto úprav lze odvodit také:

(iii) přičtení t-násobku j-tého řádku k i-tému, když $j \neq i$

(iv) prohození dvou řádků

1.1.3 Definujte odstupňovaný tvar matice. (REF)

Matice A je v *REF*, pokud **(i)** nenulové řádky jsou seřazeny podle počáteřních nul a **(ii)** nulové řádky jsou pod nenulovými.
Označme $j(i) := min(\{j : a_{i,j} \neq 0\})$. Matice $A \in \mathbb{R}^{m \times n}$ je v *REF* právě tehdy, když $\exists r \in \{1, ..., m\}$:

(i) $j(1) < j(2) < ... < j(r)$

(ii) $\forall i > r, \forall j : a_{i,j} = 0$

1.1.4 Napište pseudokód pro Gaussovu eliminaci.

Pseudokód pro Gaussovu eliminaci

1. Seřaď řádky podle počtu počátečních nul.
2. Pokud mají dva nenulové řádky stejný počet počátečních nul (i-tý a $i+1$-ní), tak od $i+1$-ního odečteme $\frac{a_{i+1,j(i)}}{a_{i,j(i)}}$-násobek i-tého.
3. Opakuj, dokud nemají každé dva nenulové řádky různé počty počátečních nul.

Algoritmus je konečný, protože po kroku 2. vždy vzroste celkový počet počátečních nul alespoň o jedna.

1.1.5 Definujte pivot a to slovně i formálně.

První nenulový prvek $a_{i,j(i)}$ na i-tém řádku. V REF prvky na místech $(i, j(i))$, kde $j(i) = min\{j : a_{i,j} \neq 0\}$.

1.1.6 Definujte volné a bázické proměnné.

Nechť máme pro matici A' v *REF* soustavy $A'x = b'$, potom sloupcové proměnné s *pivoty* značíme jako *bázické*. *Volné* proměnné jsou všechny ostatní.

1.1.7 Definujte hodnost matice.

Hodnost matice A, značená jako *rank(A)*, je počet ***pivotů*** v libovolné matici A' v *REF* takové, že $A \sim\sim A'$.

1.2 Matice

1.2.1 Jednotkovou matici.

Pro $(\forall n \in \mathbb{N})$ je *jednotková matice* $I_n \in \mathbb{R}^{n\times n}$ definována vztahy:

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

1.2.2 Definujte transponovanou matici.

Transponovaná matice k matici $A \in \mathbb{R}^{m\times n}$ je taková matice $A^T \in \mathbb{R}^{n\times m}$, pro kterou platí:

$$A^T_{i,j} = A_{j,i}$$

1.2.3 Definujte symetrickou matici.

Symetrická matice je taková čtvercová matice $A \in \mathbb{R}^{n\times n}$, pro kterou platí:

$$A_{j,i} = A_{i,j}, \text{ neboli } A = A^T$$

1.2.4 Definujte maticový součin.

Pro *součin* dvou matic $A \in \mathbb{R}^{m\times n}$ a $B \in \mathbb{R}^{n\times p}$ platí $(AB) \in \mathbb{R}^{m\times p}$:

$$(AB)_{i,j} = \sum_{k=1}^{n} a_{i,k} \cdot b_{k,j}$$

1.2.5 Definujte inverzní matici.

Inverzní matice k čtvercové matici $A \in \mathbb{R}^{n\times n}$ je taková matice $A^{-1} \in \mathbb{R}^{n\times n}$, pro kterou platí:

$$A \cdot A^{-1} = I_n$$

1.2.6 Definujte regulární matici.

Regulární matice je taková matice, ke které existuje ***inverzní matice***.

1.2.7 Definujte singulární matici.

Singulární matice je taková matice, která není ***regulární***.

1.2.8 Definujte binární operaci.

Binární operace na množině X je zobrazení $X \times X \to X$.

1.2.9 Definujte komutativní a asociativní binární operace.

Nechť máme množinu X a binární operaci $\circ$, potom je

asociativní pokud platí:

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

komutativní pokud platí:

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

1.2.10 Definujte neutrální prvek.

Nechť máme množinu X a binární operaci $\circ$, potom je e *neutrální prvek*, když:

$$(\exists e \in X)(\forall x \in X) : x \circ e = e \circ x = x$$

1.2.11 Definujte inverzní prvek.

Nechť máme množinu X a binární operaci $\circ$, potom je b *inverzní* a e *neutrální prvek*, když:

$$(\forall a \in X)(\exists b \in X) : a \circ b = b \circ a = e$$

1.3 Grupy a permutace

1.3.1 Definujte grupu.

Množina $\mathbb{G}$ s binární operací $\circ$, je dvojice $(\mathbb{G}, \circ)$ splňující:

(i) existence *neutrálního prveku*

(ii) existence *inverzního prvku*

(iii) asociativitu

1.3.2 Definujte permutaci.

Permutace na množině $[n]$ je bijektivní zobrazení $p : [n] \to [n]$. $[n] = \{1, ..., n\}$)

1.3.3 Definujte permutační matici,

Permutační matice P je taková matice popisující permutaci, pro kterou platí:

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

1.3.4 Definujte transpozici.

Transpozice je permutace na množině o velikosti n, která má jeden netriviální cyklus délky 2 a $n-2$ *pevných bodů.*

1.3.5 Definujte inverzi v permutaci.

Inverze v permutaci je taková dvojice prvků (i, j), pro které platí $(i, j) : i < j$ a $p(i) > p(j)$.
Můžeme zapsat také $p(i) = j \iff p^{-1}(j) = i$.

1.3.6 Definujte znaménko permutace.

Znaménko permutace p je číslo $sgn(p) = (-1)^{\#\text{inverzí v } p}$.
Můžeme zapsat také: $(p \in S_n)$ a skládá se z k-cyklů, potom $sgn(p) = (-1)^{n-k}$.

1.4 Tělesa

1.4.1 Definujte těleso.

Nechť $\mathbb{K}$ je množina a $(\oplus, *)$ jsou binární operace na $\mathbb{K}$. Trojici $(T, \oplus, *)$ potom nazýváme *tělesem*, splňuje-li:

(i) $(K, \oplus)$ tvoří Abelovskou grupu s neutrálním prvkem 0

(ii) $(K \setminus \{0\}, *)$, tvoří Abelovskou grupu s neutrálním prvkem 1

(iii) platí *distributivita*, tedy $(\forall a, b, c \in K) : a * (b \oplus c) = a * b \oplus a * c$

1.4.2 Definujte charakteristiku tělesa.

Pokud $(\exists n \in N)$ takové, že v tělese $\mathbb{K}$ platí $\underbrace{1 + 1 + ... + 1}_{n\text{-krát}} = 0$, potom nejmenší takové n je $char(\mathbb{K})$ *tělesa* $\mathbb{K}$.

Jinak má *těleso* charakteristiku 0.

1.5 Vektorové prostory

1.5.1 Definujte vektorový prostor.

Vektorový prostor $(V, \oplus, *)$ nad tělesem $(\mathbb{K}, \oplus, *)$ je množina V spolu s binární operací $\oplus$ na V a binární operací *skalárního násobku* $* : \mathbb{K} \times V \to V$, kde:

(i) $(V, \oplus)$ tvoří Abelovskou grupu

(ii) $(\forall v \in V) : 1 * v = v$, *(kde 1 je neutrální prvek pro násobení v* $\mathbb{K}$*)*

(iii) $(\forall a, b \in \mathbb{K})(\forall v \in V) : (a * b) * v = a * (b * v)$ - asociatavita

(iv) $(\forall a, b \in \mathbb{K})(\forall v \in V) : (a \oplus b) * v = (a * v) \oplus (b * v)$ - distributivita

(v) $(\forall a \in \mathbb{K})(\forall u, v \in V) : a * (u \oplus v) = (a * u) \oplus (a * v)$ - distributivita

Prvky $\mathbb{K}$ se nazývají *skaláry* a prvky V *vektory.*

1.5.2 Definujte podprostor vektorového prostoru.

Nechť $(V, \oplus, *)$ je vektorový prostor nad $\mathbb{K}$, potom *podprostor* U je neprázdná podmnožina V splňující:
($U \subseteq V) \wedge (U \neq \emptyset$*):*

1. $(\forall u, v \in U) : u \oplus v \in U$, neboli: U je uzavřená na operaci $\oplus$,
2. $(\forall v \in U)(\forall a \in \mathbb{K}) : a * v \in U$, neboli: U je uzavřená na operaci $*$
3. obsahuje nulový vektor o.

1.5.3 Definujte lineární kombinaci.

Lineární kombinace vektorů $v_1, ..., v_n \in V$ nad $\mathbb{K}$ je libovolný vektor $u = a_1 \cdot v_1 + \cdots + a_n \cdot v_n$, kde $a_1, ..., a_n \in \mathbb{K}$.

1.5.4 Definujte lineární obal (podprostor generovaný množinou).

Lineární obal $\mathfrak{L}(X)$ množiny $X \subseteq V$, kde V je vektorový prostor nad $\mathbb{K}$, je průnik všech podprostorů U z V obsahující X.
Neboli: $span(X) = \mathfrak{L}(X) = \bigcap\{U : X \subseteq U, U \text{je podprostor} V\}$

1.5.5 Definujte řádkový prostor matice a to slovně i formálně pomocí maticového součinu.

Řádkový prostor matice je prostor generovaný jejími řádky. Pro matici $A \in \mathbb{K}^{m \times n}$

$$\mathcal{R}(A) = \mathcal{S}(A^T) = \sum_{j=1}^{m} x_j A_{j,*}$$
$$\mathcal{R}(A) = \{(v \in \mathbb{K}^n) : v = A^T y, y \in \mathbb{K}^m\}, \textit{všechny lineární kombinace řádků}$$

1.5.6 Definujte sloupcový prostor matice a to slovně i formálně pomocí maticového součinu

Sloupcový prostor matice je prostor generovaný jejími sloupci. t.j.: Pro matici $A \in \mathbb{K}^{m \times n}$:

$$\mathcal{S}(A) = \mathfrak{L}\{A_{*,1}, ..., A_{*,n}\} = \sum_{j=1}^{n} x_j A_{*,j}$$
$$\mathcal{S}(A) = \{(u \in \mathbb{K}^m) : u = Ax, x \in \mathbb{K}^n\}, \textit{všechny lineární kombinace sloupců}$$

1.5.7 Definujte jádro matice.

Jádro matice $A \in \mathbb{K}^{m \times n}$ je podprostor $\mathbb{K}^n$ tvořen řešeními homogenní soustavy $Ax = 0$.

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

1.5.8 Definujte lineárně nezávislé vektory.

Množina vektorů X ve vektorovém prostoru V je *lineárně nezávislá*, pokud nelze nulový vektor získat netriviální lineární kombinací vektorů z X.

Formálně: vektory $v,...,v_n$ jsou lineárně nezávislé $\iff \sum_{i=1}^{n} a_i v_i = 0$ má pouze triviální řešení $a_1 = ... = a_n = 0$.

1.5.9 Definujte bázi vektorového prostoru.

Báze vektorového prostoru V je lineárně nezávislá množina X, která generuje V.

1. $\mathfrak{L}(X) = V$, *každý vektor* V *je lineární kombinací vektorů báze* X
2. X je lineárně nezávislá, *proto je lin. kombinace unikátní pro každý vektor* V.

1.5.10 Definujte dimenzi vektorového prostoru.

Nechť má V konečnou bázi. Potom je *dimenze* V mohutnost jeho báze. Značíme $dim(V)$.

1.5.11 Definujte vektor souřadnic.

Nechť $X = (v_1, ..., v_n)$ je konečná uspořádaná báze vektorového prostoru V nad tělesem $\mathbb{K}$. *Vektor souřadnic* $u \in V$ vzhledem k bázi X je $[u]_X = (a_1, ..., a_n)^T \in \mathbb{K}^n$, kde $u = \sum_{i=1}^{n} a_i v_i$.

1.6 Lineární zobrazení

1.6.1 Definujte lineární zobrazení.

Nechť V a W jsou vektorové prostory nad stejným tělesem $\mathbb{K}$. Potom zobrazení $f : V \to W$ se nazývá *lineární zobrazení*, pokud splňuje:

1. $(\forall u, v \in V) : f(u + v) = f(u) + f(v)$
2. $(\forall u \in V), (\forall a \in \mathbb{K}) : f(a \cdot u) = a \cdot f(u)$

1.6.2 Definujte matici lineárního zobrazení.

Nechť V a W jsou vektorové prostory nad stejným tělesem $\mathbb{K}$ s bázemi $X = (v_1, ..., v_n), Y = (w_1, ..., w_m)$.
Matice lineárního zobrazení $f : V \to W$ vzhledem k bázím X a Y je $[f]_{X,Y} \in \mathbb{K}^{m \times n}$, jejíž sloupce jsou vektory souřadnic obrazů vektorů báze X vzhledem k bázi Y.

$$\text{Formálně: } [f]_{X,Y} = \begin{pmatrix} | & & | \\ [f(v_1)]_Y & ... & [f(v_n)]_Y \\ | & & | \end{pmatrix}$$

1.6.3 Definujte jádro lineárního zobrazení.

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

1.6.4 Definujte matici přechodu.

Nechť X a Y jsou dvě konečné báze vektorového prostoru V. *Matice přechodu* od X k Y je identické zobr. $[id]_{X,Y}$.

1.6.5 Definujte izomorfismus vektorových prostorů.

Bijektivní lineární zobrazení $f : V \to W$, nazýváme *izomorfismem prostorů* V a W.

1.6.6 Definujte afinní prostor a jeho dimenzi.

Nechť U je podprostor vektorového prostoru W a $w \in W$.
Afinní prostor $w + U$ je množina $\{w + u \mid u \in U\}$.
Dimenze afinního prostoru $w + U$ je $dim(w + U) = dim(U)$.

Můžeme také definovat jako:
Afinní prostor je množina A a zobrazení $+ : A \times W \to A$, spňující:

1. $(\forall a \in A) : a + 0 = a$
2. $(\forall a \in A), (\forall v, w \in W) : a + (v + w) = (a + v) + w$
3. Pro dvojice $(a, b \in A)(\exists! v \in W) : a + v = b$.

2 Věty

2.1 Soustavy lineárních rovnic

2.1.1 Uved'te a dokažte vztah mezi elementárními řádkovými operacemi a soustavami rovnic.

Nechť $Ax = b$ a $A'x = b'$ jsou dvě soustavy splňující $(A|b) \sim\sim (A'|b')$, potom obě tyto soustavy mají totožné množniny řešení.

Proof. Cílem je tedy ukázat $\{x \in \mathbb{R}^n \mid Ax = b\} = \{x \in \mathbb{R}^n \mid A'x = b'\}$, neboli ukázat $Ax = b \iff A'x = b'$.

1. Vynásobení i-tého řádku nenulovým skalárem t.
   (a) $Ax = b \implies A'x = b'$:
   $a'_{i,1}x_1 + ... + a'_{i,n}x_n = ta_{i,1}x_1 + ... + ta_{i,n}x_n = t(a_{i,1}x_1 + ... + a_{i,n}x_n) = tb_i = b'_i$
   (b) $Ax = b \impliedby A'x = b'$:
   $a_{i,1}x_1 + ... + a_{i,n}x_n = \frac{1}{t}(ta_{i,1}x_1 + ... + ta_{i,n}x_n) = \frac{1}{t}(a'_{i,1}x_1 + ... + a'_{i,n}x_n) = \frac{1}{t}b'_i = \frac{1}{t}tb_i = b_i$
2. Přičtení j-tého řádku k i-tému
   (a) $Ax = b \implies A'x = b'$: $a'_{i,1}x_1 + ... + a'_{i,n}x_n =$

$$= (a_{i,1} + a_{j,1})x_1 + ... + (a_{i,n} + a_{j,n})x_n = \underbrace{(a_{i,1}x_1 + ... + a_{i,n}x_n)}_{b_i} + \underbrace{(a_{j,1}x_1 + ... + a_{j,n}x_n)}_{b_j} = b_i + b_j = b'_i$$

   (b) $Ax = b \impliedby A'x = b'$: $a_{i,1}x_1 + ... + a_{i,n}x_n =$
   $= (a_{i,1}x_1 + ... + a_{i,n}x_n) + b_j - b_j = (a_{i,1}x_1 + ... + a_{i,n}x_n) + (a_{j,1}x_1 + ... + a_{j,n}x_n) - b_j =$
   $= (a_{i,1} + a_{j_1})x_1 + ... + (a_{i,n} + a_{j,n})x_n - b_j = (a'_{i,1}x_1 + ... + a'_{i,n}x_n) - b_j = b'_j - b_j = b_i + b_j - b_j = b_i$

3., 4. dokazovat nemusíme, jsou odvozeny od prvních dvou.

□

2.1.2 Vyslovte a dokažte větu o jednoznačnosti volných a bázických proměnných.

Pro $A'x = b'$ s $(A' \mid b')$ v REF a bez pivotu v b', lze jakoukoli volbu proměnných jednoznačně rozšířit na řešení.

Proof. : *Matematickou Indukcí podle* $i = r, r-1, ..., 1$ *v i-té rovnici:*

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

Hodnoty následujících bázických proměnných $x_{j(i+1)}, ..., x_{j(r)}$ jsou známy z *indukčního předpokladu*, proto je $x_{j(i)}$ jednoznačně: $x_{j(i)} = \frac{1}{a'_{i,j(i)}}(b'_i - a'_{i,j(i)+1}x_{j(i)+1} - ... - a'_{i,n}x_n)$.
Jednoznačnost řešení vychází z jednoznačnosti bázických a volných proměnných, protože ty to řešení tvoří.

□

2.1.3 Vyslovte a dokažte Frobeniovu větu.

Soustava $Ax = b$ má řešení právě tehdy, když se hodnost matice A rovná hodnosti rozšířené matice.

Proof. Zvolme libovolné $(A'|b')$ v REF, t. ž. $(A'|b') \sim\sim (A|b)$.
Potom $Ax = b$ má řešení $\iff$ $(A'|b')$ nemá pivot v b' $\iff$ pivoty A' se shodují s pivoty $(A'|b')$ $\iff$ $rank(A) = rank((A|b))$ □

2.2 Matice

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

Nechť x_0 splňuje $Ax_0 = b$. Potom zobrazení $\overline{x} \to \overline{x} + x_0$ je bijekce mezi množinami $\{\overline{x} : Ax = 0\}$ a $\{x : Ax = b\}$.

Proof. Označme $U = \{\overline{x} : Ax = 0\}$ a $V = \{x : Ax = b\}$.
Předpokládejme, že $f : U \to V$, t.ž. $f(\overline{x}) = \overline{x} + x_0$ a $g : V \to U$, t.ž. $g(x) = x - x_0$. Potom:

$$\left.\begin{array}{l} g \circ f \text{ je identita na } U \implies \text{je } \textit{prostá} \\ f \circ g \text{ je identita na } V \implies \text{je } \textit{na} \end{array}\right\} \implies \text{je } \textit{bijektivní}.$$

□

2.2.2 Uved'te a dokažte větu popisující všechna řešení Ax = b.

Je-li $A \in \mathbb{R}^{m\times n}$ matice hodnosti r, pak všechna řešení $Ax = 0$ lze popsat jako $x = p_1x_1 + p_2x_2 + ... + p_{n-r}x_{n-r}$, kde jsou $p_1, ..., p_{n-r}$ *libovolné reálné parametry* a $x_1, ..., x_{n-r}$ *vhodná řešení soustavy* $Ax = 0$. Soustava má pouze triviální řešení $x = 0$, právě když $rank(A) = n$.

Proof. Přejmenujeme volné proměnné na $p_1, ..., p_{n-r}$. Zpětnou substitucí můžeme vyjádřit každou složku řešení jako lineární funkci proměnných, t.j.

$$\begin{aligned} x_1 &= \alpha_{1,1}p_1 + ... + \alpha_{1,n-r}p_{n-r} \\ &\vdots \\ x_n &= \alpha_{n,1}p_1 + ... + \alpha_{n,n-r}p_{n-r} \end{aligned}$$

Zvolíme $x_1 = p_1(\alpha_{1,1}, ..., \alpha_{n,1})^T, ..., x_{n-r} = p_{n-r}(\alpha_{1,n-r}, ..., \alpha_{n,n-r})^T$
Tyto vektory řeší soustavu $Ax = 0$, protože každý takový x_i pochází z:

$$p_j = \begin{cases} 1, j = i \\ 0, j \neq i \end{cases}$$

Je-li $rank(A) = n$, proměnné jsou jen bázické a 0 je pak jediné řešení.

Důsledek: Obecné řešení soustavy $Ax = b$ lze vyjádřit ve tvaru $x = x_0 + p_1x_1 + ... + p_{n-r}x_{n-r}$, kde x_0 je libovolné řešení soustavy $Ax = b$.
Důsledek platí díky bijekci mezi řešeními $Ax = b$ a $Ax = 0$. *(věta 2.2.1)*

□

2.2.3 Vyslovte a dokažte větu o ekvivalentních definicích regulárních matic.

Pro čtvercovou matici $A \in \mathbb{R}^{n\times n}$ jsou následující podmínky ekvivalentní:

i $(\exists A^{-1}) : A \cdot A^{-1} = I_n$, *neboli A je regulární*

ii $rank(A) = n$, *neboli A má hodnost n*

iii $A \sim\sim I_n$, *neboli A lze převést na* I_n

iv Soustavy $Ax = 0$ má pouze triviální řešení $x = 0$.

Proof.

- $(ii) \iff (iv)$: *Z věty o řešení homogenních soustav 2.2.2.:*

  $$rank(A) = n \iff A' \sim A \text{ neobsahuje volné proměnné} \iff \text{existuje právě jedno řešení}$$

- $(ii) \implies (iii)$: Podle Gauss-Jordanovy eliminace $(iii) \implies (ii)$ triviálně.
- $(ii) \implies (i)$: Označme $I_n = (e_1|...|e_n)$, kde e jsou sloupce matice I_n. Pro $i = 1, ..., n$ uvažme soustavy $Ax_i = e_i$. Z $rank(A) = n$ dostaneme řešení $A^{-1} = (x_1|...|x_n)$.
- $(i) \implies (ii)$ *Sporem.* Pokud $rank(A) < n$, pak pro některé i může bát i-tý řádek matice A eliminován ostatními řádky, $Ax_i = e_i$ tedy nemá řešení, protože jedinou 1 na i-tém řádku v e_i nelze eliminovat nulami. *...spor s existencí* A^{-1}.

□

2.3 Grupy a permutace

2.3.1 Vyslovte a dokažte větu o znaménku složené permutace.

Věta: Pro libovolné $(p, q \in S_n)$, kde S_n je množina všech permutací na n prvcích, platí: $sgn(q \circ p) = sgn(q) \cdot sqn(p)$

Proof. Pro počet inverzí ve složené permutaci platí, že: *inverze v p a q se navzájem vyruší* a *inverze v $q \circ p$ odpovídá inverzi v p nebo v q.*

$$\#\text{ inverzí } (q \circ p) = \#\text{ inverzí } p + \#\text{ inverzí } q - 2|\{(i,j) : i < j \wedge p(i) > p(j) \wedge q(p(i)) < q(p(j))\}|$$

□

2.4 Tělesa

2.4.1 Uved'te a dokažte větu charakterizující, kdy Z_p je těleso

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

Proof.

- $\implies$: Pokud by p bylo složené $p = a \cdot b$, pak $a \cdot b \equiv 0 \mod p$, což je spor s pozorováním.
- $\impliedby$ Je potřeba ukázat platnost axiomů pro tělesa. Všechny axiomy plynou z vlastností + a $\cdot$ na $\mathbb{Z}$, kromě existence inverzních prvků, protože $\mathbb{Z}$ není uzavřená na dělení.:

  Ukažme existenci inverzního prvku v násobení $(\forall a \in [p-1])(\exists a^{-1} \in [p-1]) : a \cdot a^{-1} \equiv 1 \mod p$

  Definujeme pro každé a zobrazení $f_a : [p-1] \to [p-1]$ předpisem $f_a(x) = ax \mod p$

  Ukážeme, že f_a je *prosté*: Kdyby nebylo, $(\exists b, c, b \neq c) : f_a(b) = f_a(c) \implies 0 \equiv ab - ac \implies a(b-c) \equiv 0$. Ale víme, že $a \neq 0$ a $b \neq c$, takže jde o **spor**.

  f_a je prosté $\implies$ je na $\implies \exists a^{-1}$ splňující $f_a(a^{-1}) = 1$.

□

2.4.2 Vyslovte a dokažte malou Fermatovu větu.

Věta: Nechť $a \in \{1, ..., p-1\}$ a p je prvočíslo, potom platí: $a^{p-1} \equiv 1 \mod p$.

Proof. Pro každé a definujeme zobrazení $f_a : [p-1] \to [p-1]$ předpisem $f_a(x) = ax \mod p$.
Ukážeme, že f_a je *prosté*: Kdyby nebylo, $(\exists b, c, b \neq c) : f_a(b) = f_a(c) \implies 0 \equiv ab - ac \implies a(b-c) \equiv 0$. Ale víme, že $a \neq 0$ a $b \neq c$, takže jde o **spor**.
f_a je prosté $\implies$ je na $\implies$ je bijekcí na $[p-1]$, proto platí:

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

□

2.5 Vektorové prostory

2.5.1 Vyslovte a dokažte větu o průniku vektorových prostorů.

Nechť $(U_i, i \in I)$ je libovolný systém podprostorů prostoru V. Potom průnik $\bigcap_{i \in I} U_i$ je také podprostorem V.

Proof. Označme $W = \bigcap_{i \in I} U_i$ a ukažme uzavřenost na $\oplus$ a $*$:

1. Uzavřenost na $\oplus$:

$$(u, v \in W) \implies (\forall i \in I) : u, v \in U_i \implies (\forall i \in I) : u \oplus v \in U_i \implies u \oplus v \in W$$

2. Uzavřenost na $*$:

$$(\forall a \in \mathbb{K}), (u \in W) \implies (\forall i \in I) : u \in U_i \implies (\forall i \in I) : a * u \in U_i \implies a * u \in W$$

□

2.5.2 Vyslovte a dokažte větu o ekvivalentních definicích lineárního obalu.

1 Lineární obal množiny $X \subseteq V$ je průnik všech podprostorů U z V nad $\mathbb{K}$, které obsahují X.

2 Lineární obal množiny X je množina všech lineárních kombinací vektorů z X.

Proof. Označme:
$W_1 = \bigcap_{X \subseteq U_i \subseteq V} U_i$
$W_2 = \left\{ \sum_{i=1}^{n} a_i \cdot v_i : a_i \in \mathbb{K}, v_i \in X, n \in \mathbb{N} \right\}$
Dokažme $W_1 = W_2 = span(X)$:

1. $W_1 \subseteq W_2$
   Protože $X \subseteq W_2$, máme W_2 mezi protínajícími se podprostory U_i. Z toho plyne $W_1 \subseteq W_2$.
2. $W_2 \subseteq W_1$

$$\text{uavřenost na } \cdot : u \in W_2 \implies u = \sum_{i=1}^{k} a_i v_i \implies \alpha u = \alpha \sum_{i=1}^{k} a_i v_i = \sum_{i=1}^{k} (\alpha a_i) v_i \implies \alpha u \in W_2$$
$$\text{uzavřenost na } + : u, u' \in W_2 \implies ... \implies u + u' \in W_2$$

   Každý U_i obsahuje X a je uzavřen na $+$ a $\cdot$. Každý U_i tedy obsahuje všechny lineární komb. vektorů X. Proto $\forall U_i : W_2 \subseteq U_i \implies W_2 \subseteq W_1$.

□

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

Jestliže Y je konečná generující množina prostoru V a X je lineárně nezávislá ve V, potom $|X| \leq |Y|$.

Proof. Předpokládejme, že $Y = \{v_1, ..., v_n\}$ a že z X lze vybrat různá $u_1, ..., u_{n+1}$. Každé u_i vyjádříme jako $u_i = \sum_{j=1}^{n} a_{i,j} v_j$. Odpovídající matice A má $n+1$ řádků a n sloupců, proto je některy řádek lineární kombinací ostatních. Tato kombinace také potvrzuje lineární závislost $u_1, ..., u_{n+1}$. □

2.5.4 Uved'te a dokažte Steinitzovu větu o výměně (včetně lemmatu, pokud jej potřebujete).

Lemma o výměně Nechť X generuje vektorový prostor V nad $\mathbb{K}$. Jestliže pro vektor $(u \in V)$ existují $(v_1, ..., v_n \in X)$ a $(a_1, ..., a_n \in \mathbb{K})$ taková, že $u = \sum_{i=0}^{n} a_i v_i$, kde $a \neq 0$ pro nějaké i, potom $span((X \setminus v_i) \cup u) = V$.

Proof.

$$u = a_1 v_1 + ... + a_i v_i + ... + a_n v_n \implies v_i = \frac{1}{a_i} (u - \sum_{j \neq i} a_i v_i)$$

Jakékoli $w \in V$ můžeme zapsat jako lineární kombinaci prvků z X. Vyskytuje-li se v_i v této kombinaci, dosadíme za v_i výraz výše. Tím získáme w jako lineární kombinaci prvků z $(X \setminus v_i) \cup u$.
V konečném případě, je-li $X = \{v1, ..., v_n\}$ a $w = \sum_{j=1}^{n} b_j v_j$, dostaneme jmenovitě $w = \frac{b_i}{v_i} u + \sum_{j \neq i} \left(b_j - \frac{a_j b_j}{a_i} \right) v_j$.

□

Steinitzova věta o výměně Nechť X je konečná lineárně nezávislá množina vektorového prostoru V nad $\mathbb{K}$ a Y je systém generátorů V.
Potom platí $|X| \leq |Y|$ a existuje Z, taková že:

1. $\mathfrak{L}(Z) = V$
2. $X \subseteq Z$
3. $|Z| = |Y|$
4. $Z \setminus X \subseteq Y$

Proof. Indukcí dle $|X \setminus Y|$

- Základní krok $X \setminus Y = \emptyset$, potom $Z = Y$.
- Indukční krok $X \setminus Y \neq \emptyset$

  Zvolíme libovolné $u \in X \setminus Y$ a položíme $X' = X \setminus u$.

  Protože množina X' je lineárně nezávislá a $|X' \setminus Y| < |X \setminus Y|$, podle indukčního předpokladu pro X' a Y existuje Z' splňující $\mathfrak{L}(Z') = V$; $X' \subseteq Z'$; $|Z'| = |Y|$ a $Z' \setminus X' \subseteq Y$.

  Použijeme lemma o výměně pro $Z' = \{v_1, ..., v_n\}$ a u vyměníme za v_i, takové že $v_i \in Z' \setminus X$.

  Takové v_i existuje, protože jinak by byla X lineárně závislá. Potom $Z = Z' \cup u \setminus v_i$ splňuje *1-4*.

  neboli: množina Y umí vygenerovat u, ale množina X' to nemůže umět, jinak by $X' \cup u$ nebylo lin. nezavislé.

□

2.5.5 Vyslovte a dokažte větu o dimenzi průniku vektorových prostorů.

Jsou-li U, V podprostory konečně generovaného prostoru W, pak $dim(U)+dim(V) = dim(U \cap V)+dim(\mathfrak{L}(U \cup V))$.

Proof. Rozšíříme bázi X průniku $U \cap V$ na bázi Y prostoru U a také na bázi Z prostoru V.
Potom $|Y| + |Z| = |X| + |Y \cup Z|$ □

2.5.6 Vyslovte a dokažte větu o vektorových prostorech souvisejících s maticí A.

Jakákoli $A \in \mathbb{K}^{m \times n}$ splňuje: $dim(\mathcal{R}(A)) = dim(\mathcal{S}(A))$.

Proof. Nechť $A \sim\sim A'$ v REF, neboli existuje *regulární* R taková, že $A' = RA$.
Podle lemmatu určíme $dim(\mathcal{S}(A')) \leq dim(\mathcal{S}(A))$ a z $A = R^{-1}A'$ dostaneme $dim(\mathcal{S}(A')) \geq dim(\mathcal{S}(A))$, tudíž dostáváme jejich rovnost.
Dále pro matice A' v REF platí věta přímo: $dim(\mathcal{R}(A'))$ = počet pivotů $= rank(A') = dim(\mathcal{S}(A'))$.
Protože $\mathcal{R}(A) = \mathcal{R}(A')$, dostaneme $dim(\mathcal{R}(A)) = dim(\mathcal{R}(A')) = dim(\mathcal{S}(A')) = dim(\mathcal{S}(A))$.

Jinými slovy, počet pivotů v řádcích je roven počtu pivotů ve sloupcích.
(Lemma říká: vynásobíme-li A z leva maticí B, pak celková dimenze A' nevzroste). □

2.5.7 Vyslovte a dokažte větu o dimenzi jádra matice.

Pro libovolné $A \in \mathbb{K}^{m \times n} : dim(ker(A)) + rank(A) = n$.

Proof. Nechť $d = n - rank(A)$ je počet *volných proměnných* a $x_1, ..., x_d$ jsou řešení soustavy $Ax = 0$ daná zpětnou substitucí.
Tato řešení jsou lineárně nezávislá, protože pro každé i platí, že x_i je mezi $x_1, ..., x_d$ jediné, které má složku odpovídající i-té volné proměnné nenulovou.
Vektory $x_1, ..., x_d$ tudíž tvoří bázi $ker(A)$ a proto $dim(ker(A)) = d = n - rank(A)$.

□

2.6 Lineární zobrazení

2.6.1 Vyslovte a dokažte větu o jedinečnosti lineárního zobrazení.

Nechť U a V jsou prostory nad $\mathbb{K}$ a X je báze U.
Pak pro jakékoli zobrazení $f_0 : X \to V$ existuje jediné lineární zobrazení $f : U \to V$ rozšiřující f_0,
t.j. $(\forall u \in X) : f(u) = f_0(u)$.

Proof.
Pro jakékoli $w \in U$ existují jednoznačná $n \in \mathbb{N}_0$, $a_1, ..., a_n \in \mathbb{K} \setminus 0$ a $u_1, ..., u_n \in X$ taková, že $w = \sum_{i=1}^{n} a_i u_i$
Potom $f(w) = f\left(\sum_{i=1}^{n} a_i u_i\right) = \sum_{i=1}^{n} a_i f(u_i) = \sum_{i=1}^{n} a_i f_0(u_i)$. □

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

Proof. □

2.6.3 Vyslovte a dokažte pozorování o matici složeného lineárnıho zobrazení.

Proof. □

2.6.4 Vyslovte a dokažte větu o charakterizaci izomorfismu mezi vektorovými prostory.

Lineární zobrazení $f : U \to V$ je **isomorfismus** prostorů U a V s konečnými bázemi X a Y právě tehdy, když $[f]_{X,Y}$ je *regulární.*

Proof.

- $\Longleftarrow$: Uvažme $g : V \to U$ takové, že $[g]_{Y,X} = [f]^{-1}_{X,Y}$. Pak:

$$[g \circ f]_{X,X} = [f]^{-1}_{X,Y}[f]_{X,Y} = I_{|X|} = [id]_{X,X} \implies f \text{ je prosté}$$
$$[f \circ g]_{Y,Y} = [f]^{-1}_{X,Y}[f]_{X,Y} = I_{|Y|} = [id]_{Y,Y} \implies f \text{ je na.}$$

- $\Longrightarrow$:

$$\left.\begin{array}{l}[\mathrm{f}^{-1}]_{Y,X}[f]_{X,Y} = [id]_{X,X} = I_{|X|} \implies |Y| \geq |X| \\ [\mathrm{f}]_{X,Y}[f^{-1}]_{Y,X} = [id]_{Y,Y} = I_{|Y|} \implies |X| \geq |Y|\end{array}\right\} \implies |X| = |Y|.$$

□

2.7 Grafy a podgrafy

2.7.1 Zformulujte problém o počtu sudých podgrafů a vyřešte jej.

Kolik sudých podgrafů obsahuje G?

Proof. Symetricky rozdíl $\triangle$ zachovává sudé stupně, protože symetricky rozdíl dvou množin sudé mohutnosti, konkrétně hran incidentních s vrcholem, má také sudou mohutnost.

$$|A \triangle B| = |A| + |B| - 2|A \cap B|$$

Proto $(U, \triangle, \cdot)$ tvoří vektorový prostor $\mathbb{Z}_2$. Pro prostory konečné mohutnosti platí $|U| = |\mathbb{K}|^{dim(U)}$ □

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

Kolik množin může mít n-prvková množina, pokud každá podmnožina má mít lichou velikost, ale průnik každé dvojice různych podmnožin má mít sudou velikost?

Proof. □

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

Lze obdélník s iracionálním poměrem délek jeho stran rozdělit na konečně mnoho čtverců?
Pro iracionální poměr žádné takové rozdělení neexistuje.

Proof. □

3 Přehled

(U přehledových otázek uved'te definice, tvrzení, věty, příklady a souvislosti. Důkazy u přehledových otázek nejsou vyžadovány.)

3.1 Soustavy lineárních rovnic

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

- **Definice**: Elementární řádkové úpravy, Gaussova eliminace, Řádkově odstupňovaný tvar
- **Věta**: *(2.1.1)* Nechť $Ax = b$ a $A'x = b'$ jsou dvě soustavy splňující $(A|x) \sim\sim (A'|b')$, potom obě soustavy mají totožné množiny řešení.
- Zmínit Gauss-Jordanovu eliminaci

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

- **Definice**: Gaussova eliminace, REF, pivot, volné a bázické proměnné, hodnost matice
- Zpětnou substitucí lze získat každé řešení.
- **Věta**: *(2.1.3) Frobeniova věta*: Soustava $Ax = b$ má řešení $\iff rank(A) = rank(A|b)$
- **Věta**: *(2.1.2)* Pro $A'x = b'$ s $(A'|b')$ v REF a bez pivotu v b', lze jakoukoli volbu proměn. rozšířit na řešení.
- **Věta**: *(2.2.1)* Nechť x_0 splňuje $Ax_0 = b, ppotomzobr. \rightarrow \bar{x} + x_0$ je bijekce mezi $\{\bar{x} : Ax = 0\}$ a $\{x : Ax = b\}$.
- **Věta**: *(2.2.2)* Je-li $A \in \mathbb{R}^{m\times n}$ matice hodnosti r, pak všechna řešení $Ax = 0$ lze popsat jako $x = p_1x_1 + p_2x_2 + ... + p_{n-r}x_{n-r}$, kde jsou $p_1, ..., p_{n-r}$ *libovolné reálné parametry* a $x_1, ..., x_{n-r}$ *vhodná řešení soustavy* $Ax = 0$. Soustava má pouze triviální řešení $x = 0$, právě když $rank(A) = n$.

3.2 Matice

3.2.1 Přehledově sepište, co víte o maticových operacích.

- **Definice** nulová matice, jednotkové matice, transponovaná matice, symetrická matice
- **Definice** maticový součin, komutativita, asociativita, distributivita, neutrální prvek, inverzní prvek
- *Násobení skalárem* - komutativní, asociativní, ditributivní na sčítání, neutrální prvek je 1
- *Sčítání* - komutativní, asociativní, neutrální prvek je nulová matice.
- *Maticový součin* - asociativní, distributivní na sčítání, neutrální prvek je I_n, NENÍ komutativní

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

- **Definice**: regulární matice, singulární matice, inverzní matice
- **Věta** *(2.2.3)* Pro čtvercovou matici $A \in \mathbb{R}^{n\times n}$ jsou následující podmínky ekvivalentní:
  - $(\exists B) : A \cdot B = I_n \rightarrow$ A je regulární
  - $rank(A) = n$
  - $A \sim\sim I_n$
  - $Ax = 0 \implies x = 0$
- $(A^{-1})^{-1} = A$

  Proof. $(A^{-1})^{-1} = I_n(A^{-1})^{-1} = AA^{-1}(A^{-1})^{-1} = AI_n = A$ □
- $(A^T)^{-1} = (A^{-1})^T$

  Proof. Využijeme, že $X^TY^T = (YX)^T$: ; $(A^{-1})^T = (A^{-1})^TA^T(A^T)^{-1} = (AA^{-1})^T(A^T)^{-1} = I_n(A^T)^{-1} = (A^T)^{-1}$ □

3.3 Grupy a permutace

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

- **Definice**: Binární operace, relace, kartézsky součin, zobrazení na, prosté, bijektivní
- **Definice**: Asociativita, komutativita, distributivita, inverzní prvek, neutrální prvek
- Příklady - Grupa, Abelova grupa, Tělesa, ...

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

- **Definice**: Grupa, Abelovaká grupa
- Neutrální a inverzní prvky jsou určeny jednoznačně (Důkaz přičtením nuly/ násobením jedničkou)
- Platí ekvivalentní úpravy $a = b \iff c \circ a = c \circ b \iff a \circ c = b \circ c$
- $(a^{-1})^{-1} = a$
- $(ab)^{-1} = (b^{-1}a^{-1})$
- Příklady: aditivní grupy, multiplikativní, ostatní (symetrická - množina permutací na 1 až n)

3.3.3 Přehledově sepište, co víte o permutačních grupách.

- **Definice**: Permutace, permutační matice, transpozice, inverze, znaménko
- **Věta**: *(2.3.1)* Pro libovolné $(p, q \in S_n) : sgn(q \circ p) = sgn(q) \cdot sqn(p)$.

3.4 Tělesa

3.4.1 Přehledově sepište, co víte o tělesech.

- **Definice**: Tělesa, charakteristika tělesa
- **Věta** *(2.4.1)* $\mathbb{Z}_p$ je těleso právě tehdy, když p je prvočíslo
- **Věta** *(2.4.2)* Nechť $a \in [p-1]$ a p je prvočíslo, potom platí $a^{p-1} \equiv 1 \mod p$
- **Věta** Charakteristika tělesa je vždy 0 nebo prvočíslo (důkaz sporem)
- Vlastnosti:
  - $\forall a, a \times 0 = 0$
  - $ab = 0 \implies a = 0 \vee b = 0$

    Proof. Sporem: $\exists a^{-1}, b^{-1} : 1 = a^{-1}abb^{-1} = aba^{-1}b^{-1} = 0a^{-1}b^{-1} = 0$ □
  - $a(-1) = -a$

    Proof. $0 = 0a = (1-1)a = 1a + (-1)a \implies -a = (-1)a$ □
- Příklady: $\mathbb{R}, \mathbb{Q}, \mathbb{Z}_p$, racionální lomené funkce
- Tělesa nejsou $\mathbb{Z}_p$ kde p není prvočíslo

3.5 Vektorové prostory

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

- **Definice**: Vektorový prostor, podprostor, lineární kombinace, lineární obal,
- **Věta** *(2.5.1)* Průnik podprostorů je podprostor (ověří se uzavřenost na +,.)
- Pojem skalár, vektor
- Příklady: $\mathbb{K}^n$, posloupnosti, funkce, polynomy
- $a0 = 0u = 0$
- $au = 0 \implies a = 0 \vee u = 0$

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

- **Definice** Řádkový prostor, sloupcový prostor, jádro
- **Věta** o shodnosti dimenzí: $dim(\mathcal{R}) = dim(\mathcal{S})$
- Elementární řádkové úpravy zachovávají řádkový prostor, sloupcový zachovávat nemusí. (+ Jádro)
- $dim(\mathcal{R}) = rank(A)$, $dim(KerR) + rank(A) = n$

3.5.3 Přehledově sepište, co víte o lineární závislosti.

- **Definice**: Lineárně nezávislost
- Příklady:
  - $|X| = 1 \begin{cases} X = \{0\} & \text{závislá} \\ \text{jinak} & \text{nezávislá} \end{cases}$
  - $0 \in X \implies X$ je lineárně závislá.
  - Řádky/sloupce diagonální matice jsou lineárně nezávislé.
  - Nenulové řádky v matici v REF jsou lineárně nezávislé
- Y je lineárně nezávislá a $X \subseteq Y \implies X$ je lineárně nezávislá
- X je lineárně závislá a $X \subseteq Y \implies X$ je lineárně závislá
- X je lineárně nezávislá $\iff \forall u \in X : u \notin \mathfrak{L}(X \setminus u)$
- Asi je možné zmínit báze

3.5.4 Přehledově sepište, co víte o bázích vektorových prostorů.

- **Definice**: Báze, vektor souřadnic
- Pro libovolnou bázi platí: (předpoklady neuvádím) $[x]_B + [y]_B = [x + y]_B$, $[ax]_B = a[x]_B$
- Věta: $\mathfrak{L}(X) = V, \forall Y \subset X : \mathfrak{L}(Y) \neq V \implies X$ je báze.
- Důsledek: Každý prostor má bázi.
- Z každého systému generátorů lze vytvořit bázi
- Steinitzova věta o výměně (+ lemma)
- Pokud má prostor konečnou bázi, potom mají všechny báze stejnou mohutnost

3.6 Lineární zobrazení

3.6.1 Přehledově sepište, co víte o lineárních zobrazeních a jejich maticích.

- **Definice** Lineární zobrazení, matice lineárního zobrazení, matice přechodu,
- Příklady: nulové, identické
- Složení lineárních zobrazení je lineární
- $[f(u)]_Y = [f]_{XY} \cdot [u]_X$
- Skládání zobrazení vyjádříme součinem matic
- Zobrazení je isomorfismus, iff jeho matice je regulární,
- pak platí inverzní matice je maticí inverzního zobrazení
- Vektorový prostor dimenze n je isomorfní prostoru nad $\mathbb{K}^n$