

# Definice

## 2.2 Matice

Rálná matice typu  $m \times n$  je obdélníkové schema (tabulka)

## 2.3 Vektor

Reálný  $n$ -rozměrný aritmetický sloupcový vektor je matice typu  $m \times 1$

## 2.4 \* notace

$i$ -tý řádek matice  $A$  se značí:  $A_{i*} = (a_{i1}, a_{i2}, \dots, a_{in})$

## 2.5 Soustava lineárních rovnic

## 2.6 Matice soustavy

## 2.8 Elementární řádkové úpravy

### 2.12 Odstupňovaný tvar matice

### 2.13 Hodnost matice

### 2.18 Redukovaný odstupňovaný tvar matice

## 3.1 Rovnost

## 3.2 Součet

## 3.3 Násobek

## 3.7 Součin

### 3.11 Transpozice

### 3.14 Symetrická matice

### 3.23 Regulární matice

### 3.30 Inverzní matice

## 4.1 Grupa

Buď  $\circ : G^2 \rightarrow G$  binární operace na množině  $G$ . Pak grupa je dvojice  $(G, \circ)$  splňující:

1.  $\forall a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c$  (asociativita)
2.  $\exists e \in G \forall a \in G : e \circ a = a \circ e = a$  (existence neutrálního prvku)
3.  $\forall a \in G \exists b \in G : a \circ b = b \circ a = e$  (existence inverzního prvku)

### 4.5 Podgrupa

### 4.8 Permutace

### 4.9 Inverzní permutace

#### 4.1 Skládání permutací

#### 4.13 Znaménko permutace

#### 4.22 Těleso

Těleso je množina  $T$  spolu se dvěma komutativními binárními operacemi  $+$  a  $\cdot$  splňující:

1.  $(T, +)$  je Abelova grupa, neutrální prvek značíme  $0$  a inverzní k  $a$  pak  $-a$
2.  $(T \setminus \{0\}, \cdot)$  je Abelova grupa, neutrální prvek značíme  $1$  a inverzní k  $a$  pak  $a^{-1}$
3.  $\forall a, b, c \in T : a(b + c) = ab + ac$  (distributivita)

#### 4.35 Charakteristika tělesa

## 5.1 Vektorový prostor

Buď  $T$  těleso s neutrálními prvky  $0$  pro sčítání a  $1$  pro násobení. Vektorovým prostorem nad tělesem  $T$  rozumíme množinu  $V$  s operacemi sčítání vektorů  $+$  :  $V^2 \rightarrow V$ , a násobení vektoru skalárem  $\cdot$  :  $T \times V \rightarrow V$  splňující pro každé  $a, b \in T$  a  $u, v \in V$ :

1.  $(V, +)$  je Abelova grupa, neutrální prvek značíme  $0$  a inverzní k  $v$  pak  $-v$
2.  $a(bv) = (ab)v$  (asociativita)
3.  $1v = v$
4.  $(a + b)v = av + bv$  (distributivita)
5.  $a(u + v) = au + av$  (distributivita)

### 5.4 Podprostor

## 5.8 Lineární obal

### 5.11 Lineární kombinace

### 5.21 Lineární nezávislost

### 5.22 Lineární nezávislost nekonečné množiny

### 5.29 Báze

### 5.32 Souřadnice

### 5.42 Dimenze

### 5.49 Spojení podprostorů

### 5.55 Maticové prostory

## 6.1 Lineární zobrazení

### 6.6 Obraz a jádro

### 6.14 Matice lineárního zobrazení

### 6.20 Matice přechodu

### 6.29 Isomorfismus

### 6.41 Prostor lineárních zobrazení

## 7.1 Afinní podprostor

## 7.7 Dimenze afinního podprostoru

### 7.10 Afinní nezávislost

# Věty

## 1.1 Základní věta algebry

Každý polynom s komplexními koeficienty má alespoň jeden komplexní kořen.

**dukaz**

pres kruznici a její zmensovani v rovine komplexnich cisel. Snizujeme stupen polynomu az na nulu delenim keremem.

## 2.22 Frobeniova věta

Soustava  $(A|b)$  má (aspoň jedno) řešení právě tehdy, když  $\text{rank}(A) = \text{rank}(A|b)$

## 3.28 o regularni matici

Buď  $A \in R^{m \times n}$ . Pak  $RREF(A) = QA$  pro nějakou regulární matici  $Q \in Rm \times m$

**dukaz**

$RREF(A)$  získáme aplikací konečně mnoha elementárních řádkových úprav. Nechť jdou reprezentovat maticemi  $E_1, E_2, \dots, E_k$ . Pak  $RREF(A) = E_k \dots E_2 E_1 A = QA$ , kde  $Q = E_k \dots E_2 E_1$ . Protože matice  $E_1, E_2, \dots, E_k$  jsou regulární, i jejich součin  $Q$  je regulární

## 3.31 O existenci inverzní matice

Buď  $A \in R^{n \times n}$ . Je-li  $A$  regulární, pak k ní existuje inverzní matice, a je určená jednoznačně. Naopak, existuje-li k  $A$  inverzní, pak  $A$  musí být regulární

**dukaz**

Existence - Vytvořme matici  $A^{-1}$  tak, aby její sloupce byly vektory  $x_1, \dots, x_n$ , to jest,  $A^{-1} = (x_1|x_2|\dots|x_n)$   
Druhá rovnost -  $A(A^{-1}A - I) = AA^{-1}A - A = IA - A = 0$   
Jednoznačnost -  $B = BI = B(AA^{-1}) = (BA)A^{-1} = IA^{-1} = A^{-1}$

## 3.33 Jedna rovnost stačí

Buďte  $A, B \in Rn \times n$ . Je-li  $BA = I$ , pak obě matice  $A, B$  jsou regulární a navzájem k sobě inverzní, to jest  $B = A^{-1}$  a  $A = B^{-1}$

**dukaz**

vime ze  $I$  je regularni,  $B = BI = B(AA^{-1}) = (BA)A^{-1} = IA^{-1} = A^{-1}$  a obracene

## 3.34 Výpočet inverzní matice

Buď  $A, B \in R^{n \times n}$ . Nechť matice  $(A|I_n)$  typu  $n \times 2n$  má RREF tvar  $(I_n|B)$ . Pak  $B = A^{-1}$ . Netvoří-li první část RREF tvaru jednotkovou matici, pak  $A$  je singulární

**dukaz**

Je-li  $RREF(A|I_n) = (I_n|B)$ , potom existuje regulární matice  $Q$  taková, že  $(I_n|B) = Q(A|I_n)$ , neboli po roztržení na dvě části  $I_n = QA$  a  $B = QI_n$ . První rovnost říká  $Q = A^{-1}$  a druhá  $B = Q = A^{-1}$ .  
Netvoří-li první část RREF tvaru jednotkovou matici, pak  $RREF(A) \neq I_n$  a tudíž  $A$  není regulární.

## 3.37 Soustava rovnic a inverzní matice

Buď  $A \in R^{n \times n}$  regulární. Pak řešení soustavy  $Ax = b$  je dáno vzorcem  $x = A^{-1}b$ .

**dukaz**

Protože  $A$  je regulární, má soustava jediné řešení  $x$ . Platí  $x = Ix = (A^{-1}A)x = A^{-1}(Ax) = A^{-1}b$

### 3.41 Shermanova–Morrisonova formule

Buď  $A \in R^{n \times n}$  regulární a  $b, c \in R^n$ . Pokud  $c^T A^{-1} b = -1$ , tak  $A + bc^T$  je singulární, jinak

$$(A + bc^T)^{-1} = A^{-1} - \frac{1}{1 + c^T A^{-1} b} A^{-1} bc^T A^{-1}$$

**dukaz**

V případě  $c^T A^{-1} b = -1$  máme  $(A + bc^T)A^{-1}b = AA^{-1}b + bc^T A^{-1}b = b(1 + c^T A^{-1}b) = 0$ . Protože  $b \neq 0$  a vzhledem k regularitě  $A$  je  $A^{-1}b \neq 0$ , musí matice  $(A + bc^T)$  být singulární

### 3.43 Jednoznačnost RREF

RREF tvar matice je jednoznačně určen

**dukaz**

$$A = Q_1^{-1} A_1 = Q_2^{-1} A_2, \text{ a tedy } A_1 = Q_1 Q_2^{-1} A_2 \Rightarrow A_1 = A_2$$

### 4.15 O znaménku složení permutace a transpozice

Buď  $p \in S_n$  a buď  $t = (i, j)$  transpozice. Pak  $\text{sgn}(p) = -\text{sgn}(t \circ p) = -\text{sgn}(p \circ t)$

### 4.16 Každou permutaci lze rozložit na složení transpozic

### 4.27 $Z_n$ je těleso právě tehdy, když $n$ je prvočíslo

**dukaz**

Je-li  $n$  složené, pak  $n = pq$ , kde  $1 < p, q < n$ . Kdyby  $Z_n$  bylo těleso, pak  $pq = 0$  implikuje podle tvrzení 4.25 buď  $p = 0$  nebo  $q = 0$ , ale ani jedno neplatí

### 4.33 O velikosti konečných těles

Existují konečná tělesa právě o velikostech  $p^n$ , kde  $p$  je prvočíslo a  $n \geq 1$

### 4.38 Malá Fermatova věta

Buď  $p$  prvočíslo a buď  $0 \neq a \in Z_p$ . Pak  $a^{p-1} = 1$  v tělese  $Z_p$

### 5.15 o vektorovém prostoru a obalu

Buď  $V$  vektorový prostor nad  $T$ , a mějme  $v_1, \dots, v_n \in V$ . Pak  $\text{span}\{v_1, \dots, v_n\} = \{\sum_{i=1}^n a_i v_i; a_1, \dots, a_n \in T\}$

### 5.26 o vektorové závislosti

Buď  $V$  vektorový prostor nad  $T$ , a mějme  $v_1, \dots, v_n \in V$ . Pak vektory  $v_1, \dots, v_n$  jsou lineárně závislé právě tehdy, když existuje  $k \in 1, \dots, n$  takové, že  $v_k = P_i \neq k a_i v_i$  pro nějaké  $a_1, \dots, a_n \in T$ , to jest  $v_k \in \text{span}\{v_1, \dots, v_{k-1}, v_{k+1}, \dots, v_n\}$

### 5.31 o bazi

Nechť  $v_1, \dots, v_n$  je báze prostoru  $V$ . Pak pro každý vektor  $u \in V$  existují jednoznačně určené koeficienty  $a_1, \dots, a_n \in T$  takové, že  $u = \sum_{i=1}^n a_i v_i$

### 5.38 O existenci báze

Každý vektorový prostor má bázi

### dukaz

Buď  $v_1, \dots, v_n$  systém generátorů  $V$ . Jsou-li lineárně nezávislé, tak už tvoří bázi. Jinak podle důsledku 5.27 existuje index  $k$  tak, že

$$\text{span}\{v_1, \dots, v_n\} = \text{span}\{v_1, \dots, v_{k-1}, v_{k+1}, \dots, v_n\}$$

## 5.40 Steinitzova věta o výměně

Buď  $V$  vektorový prostor, buď  $x_1, \dots, x_m$  lineárně nezávislý systém ve  $V$ , a necht'  $y_1, \dots, y_n$  je systém generátorů  $V$ . Pak platí:

1.  $m \leq n$
2. existují navzájem různé indexy  $k_1, \dots, k_{n-m}$  takové, že  $x_1, \dots, x_m, y_{k_1}, \dots, y_{k_{n-m}}$  tvoří systém generátorů  $V$

### dukaz

indukci od  $m = 0$  předpoklad pro  $m - 1 \Rightarrow$  platí i pro  $m$

## 5.44 Vztah počtu prvků systému k dimenzi

Pro vektorový prostor  $V$  platí:

1. Necht'  $x_1, \dots, x_m$  jsou lineárně nezávislé. Pak  $m \leq \dim V$ . Pokud  $m = \dim V$ , potom  $x_1, \dots, x_m$  je báze.
2. Necht'  $y_1, \dots, y_n$  jsou generátory  $V$ . Pak  $n \geq \dim V$ . Pokud  $n = \dim V$ , potom  $y_1, \dots, y_n$  je báze

## 5.45 Rozšíření lineárně nezávislého systému na bázi

Každý lineárně nezávislý systém vektorového prostoru  $V$  lze rozšířit na bázi  $V$

## 5.46 Dimenze podprostoru

Je-li  $W \subseteq V$ , pak  $\dim W \leq \dim V$ . Pokud navíc  $\dim W = \dim V$ , tak  $W = V$

## 5.50 Spojení podprostorů

Buďte  $U, V$  podprostory vektorového prostoru  $W$ . Pak  $U + V = \text{span}(U \cup V)$

## 5.52 Dimenze spojení a průniku

Buďte  $U, V$  podprostory vektorového prostoru  $W$ . Pak platí  $\dim(U + V) + \dim(U \cap V) = \dim U + \dim V$

## 5.62 Maticové prostory a RREF

Buď  $A \in T^{m \times n}$  a buď  $A^R$  její *RREF* tvar s pivoty na pozicích  $(1, p_1), \dots, (r, p_r)$ , kde  $r = \text{rank}(A)$ . Pak:

1. nenulové řádky  $A^R$ , tedy vektory  $A_{1*}^R, \dots, A_{r*}^R$ , tvoří bázi  $R(A)$
2. sloupce  $A_{*p_1}, \dots, A_{*p_r}$  tvoří bázi  $S(A)$
3.  $\dim R(A) = \dim S(A) = r$

## 5.63 Pro každou matici $A \in T^{m \times n}$ platí $\text{rank}(A) = \text{rank}(A^T)$

## 5.66 O dimenzi jádra a hodnotě matice

Pro každou matici  $A \in T^{m \times n}$  platí  $\dim \text{Ker}(A) + \text{rank}(A) = n$

## 6.10 Prosté lineární zobrazení

Buď  $f: U \rightarrow V$  lineární zobrazení. Pak následující jsou ekvivalentní:

1.  $f$  je prosté
2.  $\text{Ker}(f) = \{0\}$
3. obraz libovolné lineárně nezávislé množiny je lineárně nezávislá množina

## 6.12 Lineární zobrazení a jednoznačnost vzhledem k obrazům báze

Buďte  $U, V$  prostory nad  $T$  a  $x_1, \dots, x_n$  báze  $U$ . Pak pro libovolné vektory  $y_1, \dots, y_n \in V$  existuje právě jedno lineární zobrazení takové, že  $f(x_i) = y_i, i = 1, \dots, n$

## 6.16 Maticová reprezentace lineárního zobrazení

Buď  $f : U \rightarrow V$  lineární zobrazení,  $B_1 = \{x_1, \dots, x_n\}$  báze prostoru  $U$ , a  $B_2 = \{y_1, \dots, y_m\}$  báze prostoru  $V$ . Pak pro každé  $x \in U$  je  $[f(x)]_{B_2} = {}_{B_2}[f]_{B_1} \cdot [x]_{B_1}$

## 6.18 Jednoznačnost matice lineárního zobrazení

Buď  $f : U \rightarrow V$  lineární zobrazení,  $B_1$  báze prostoru  $U$ , a  $B_2$  báze prostoru  $V$ . Pak jediná matice  $A$  splňující (6.16) je  $A = {}_{B_2}[f]_{B_1}$

## 6.24 Matice složeného lineárního zobrazení

Buďte  $f : U \rightarrow V$  a  $g : V \rightarrow W$  lineární zobrazení, buď  $B_1$  báze  $U$ ,  $B_2$  báze  $V$  a  $B_3$  báze  $W$ . Pak  ${}_{B_3}[g \circ f]_{B_1} = {}_{B_3}[g]_{B_2} \cdot {}_{B_2}[f]_{B_1}$

## 6.35 Isomorfismus $n$ -dimenzionálních prostorů

Všechny  $n$ -dimenzionální vektorové prostory nad tělesem  $T$  jsou navzájem isomorfní

## 6.37 O dimenzi jádra a obrazu

Buď  $f : U \rightarrow V$  lineární zobrazení,  $U, V$  prostory nad  $T$ ,  $B_1$  báze prostoru  $U$  a  $B_2$  báze prostoru  $V$ .

Označme  $A = {}_{B_2}[f]_{B_1}$ . Pak:

1.  $\dim \text{Ker}(f) = \dim \text{Ker}(A)$
2.  $\dim f(U) = \dim S(A) = \text{rank}(A)$ .

## 7.4 Charakterizace afinního podprostoru

Buď  $V$  vektorový prostor nad tělesem  $T$  charakteristiky různé od 2, a buď  $\emptyset \neq M \subseteq V$ . Pak  $M$  je afinní, tj. je tvaru  $M = U + a$  právě tehdy, když pro každé  $x, y \in M$  a  $a \in T$  platí  $ax + (1-a)y \in M$

## 7.5 Množina řešení soustavy rovnic

Množina řešení soustavy rovnic  $Ax = b$  je prázdná nebo afinní. Je-li neprázdná, můžeme tuto množinu řešení vyjádřit ve tvaru  $\text{Ker}(A) + x_0$ , kde  $x_0$  je jedno libovolné řešení soustav