Poznámky - lineární algebra I

Petr Chmel

Definice 1 (Matice, vektor, * notace)**.** Reálná matice $m \times n$ je obdélníkové schéma (tabulka) reálných čísel. Prvek na pozici (i, j) matice (tedy v i-tém řádku a j-tém sloupci) značíme a_{ij}. Množinu všech reálných matic typu $m \times n$ značíme $\mathbb{R}^{m \times n}$. Je-li $m = n$, nazýváme matici čtvercovou.
Reálný n-rozměrný sloupcový vektor je matice typu $n \times 1$, řádkový je matice typu $1 \times n$.
i-tý řádek matice značíme A_{i*}, j-tý sloupec matice značíme A_{*j}.

Definice 2 (Soustava lineárních rovnic a matice soustavy)**.** Mějme soustavu m lineárních rovnic o n neznámých:

$$a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1$$

$$a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2$$

$$\ldots$$

$$a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m$$

kde a_{ij}, b_i jsou dané koeficienty a x_i jsou neznámé. Řešením rozumíme každý vektor $x \in \mathbb{R}^n$ vyhovující všem rovnicím.
Matice soustavy je matice A, rozšířená matice soustavy je matice $(A|b)$.

Definice 3 (Elementární řádkové úpravy)**.** Elementární řádkové úpravy jsou

1. vynásobení i-tého řádku reálným číslem $\alpha \neq 0$,
2. přičtení α-násobku j-tého řádku k i-tému řádku, přičemž $i \neq j \wedge \alpha \in \mathbb{R}$,
3. výměna i-tého a j-tého řádku.

Tvrzení 1 (Elementární úpravy a množina řešení)**.** Elementární řádkové operace zachovávají množinu řešení soustavy.

Důkaz. Stačí ukázat, že ke každé operaci existuje inverzní operace. □

Definice 4 (Odstupňovaný tvar matice - REF)**.** Matice $A \in \mathbb{R}^{m \times n}$ je v řádkově odstupňovaném tvaru, pokud existuje r takové, že platí

- řádky $1, \ldots, r$ jsou nenulové
- řádky $r + 1, \ldots, m$ jsou nulové
- pro $p_i = \min\{j; a_{ij} \neq 0\}$ platí $p_1 < p_2 < \ldots < p_r$

Pozice $(1, p_1), \ldots, (r, p_r)$ se nazývají pivoty, sloupce $p_1, \ldots, p_r$ se nazývají bázické, ostatní sloupce jsou nebázické.

Definice 5 (Hodnost)**.** Hodností matice (značeno $\text{rank}(A)$) rozumíme počet nenulových řádků po převodu do odstupňovaného tvaru.

Věta 1 (Gaussova eliminace)**.** Cíl: REF tvar

Definice 6 (Redukovaný řádkově odstupňovaný tvar matice - RREF)**.** Matice je v RREF tvaru, pokud je v REF tvaru a navíc platí

- $a_{1p_1} = a_{2p_2} = \ldots = a_{rp_r}$
- pro každé $i \in [r]$ je $a_{1p_i} = a_{2p_i} = \ldots = a_{i-1,p_i} = 0$.

Věta 2 (Gauss-Jordanova eliminace)**.** Cíl: RREF tvar.

Důsledek 1 (Frobeniova věta)**.** Soustava $(A|b)$ má (aspoň jedno) řešení právě tehdy, když $\text{rank}(A) = \text{rank}(A|b)$

Definice 7 (Operace s maticemi)**.** Dvě matice se rovnají, pokud mají stejné rozměry a všechny prvky.
Součet dvou matic stejného typu je matice téhož typu s $c_{ij} = a_{ij} + b_{ij}$.
Násobek matice skalárem je matice stejného typu se všemi prvky vynásobenými týmž skalárem.
Součin matic $A \in \mathbb{R}^{m\times p}, A \in \mathbb{R}^{p\times n}$ je $(AB)_{ij} = \sum_{k=1}^{p} A_{ik}B_{kj}$.

Tvrzení 2 (Vlastnosti součtu, násobku a součinu)**.**

1. $A + B = B + A$
2. $(A + B) + C = A + (B + C)$
3. $A + 0 = A$
4. $A + (-1)A = 0$
5. $\alpha(\beta A) = (\alpha\beta)A$
6. $1A = A$
7. $\alpha(A + B) = \alpha A + \alpha B$
8. $(\alpha + \beta)A = \alpha A + \beta A$
9. $(AB)C = A(BC)$
10. $A(B + C) = AB + AC$
11. $(A + B)C = AC + BC$
12. $\alpha(AB) = (\alpha A)B = A(\alpha B)$
13. $0A = A0 = 0$
14. $I_m A = AI_n = A$, kde $A \in \mathbb{R}^{m\times n}$

Důkaz. Triviální □

Definice 8 (Transpozice)**.** Nechť $A \in \mathbb{R}n \times m$ je matice. Pak $A^T \in \mathbb{R}^{m\times n}$ je transponovaná matice s prvky $(A^T)_{ij} = aji$.

Tvrzení 3 (Vlastnosti transpozice)**.**

1. $(A^T)^T = A$
2. $(A + B)^T = A^T + B^T$
3. $(\alpha A)^T = \alpha A^T$
4. $(AB)^T = B^T A^T$

Důkaz. Triviální, technické cvičení. □

Definice 9 (Symetrická, diagonální, horní trojúhelníková a dolní trojúhelníková matice)**.** Matice $A \in \mathbb{R}^{n\times n}$ je symetrická, pokud $A^T = A$.
Matice $A \in \mathbb{R}^{n\times n}$ je diagonální, pokud $i \neq j \Rightarrow a_{ij} = 0$.
Matice $A \in \mathbb{R}^{m\times n}$ je horní trojúhelníková, pokud $i > j \Rightarrow a_{ij} = 0$.
Matice $A \in \mathbb{R}^{m\times n}$ je dolní trojúhelníková, pokud $j > i \Rightarrow a_{ij} = 0$.

Definice 10 (Regulární, singulární matice)**.** Matice $A \in \mathbb{R}^{n\times n}$ je regulární, pokud soustava $Ax = 0$ má právě jedno řešení. V opačném případě se matice nazývá singulární.

Tvrzení 4 (Charakterizace regulární matice)**.** Nechť $A \in \mathbb{R}^{n\times n}$. Pak NTJE:

1. A je regulární
2. $RREF(A) = I$
3. $\text{rank}(A) = n$

Důkaz. Plyne z rozboru Gaussovy-Jordanovy eliminace. □

Tvrzení 5 (Charakterizace regulární matice)**.** Nechť $A \in \mathbb{R}^{n\times n}$. Pak NTJE:

1. A je regulární
2. pro nějaké $b \in \mathbb{R}^n$ má soustava $Ax = b$ jediné řešení
3. pro každé $b \in \mathbb{R}^n$ má soustava $Ax = b$ jediné řešení

Důkaz. Plyne z rozboru Gaussovy-Jordanovy eliminace a předchozího tvrzení. □

Tvrzení 6 (O součinu dvou regulárních matic)**.** Nechť $A, B \in \mathbb{R}^{n\times n}$ jsou regulární matice. Pak AB je také regulární.

Důkaz. Buď x řešení $ABx = 0$. Označme $y = Bx$. Pak lze soustavu přepsat jako $Ay = 0$. Z regularity A plyne $y = 0$. Pak $Bx = 0$, tedy $x = 0$ z regularity B. □

Tvrzení 7 (O součinu regulárních a singulárních matic)**.** Nechť $A, B \in \mathbb{R}^{n\times n}$ jsou matice. Je-li alespoň jedna z nich singulární, pak AB je také singulární.

Důkaz. Uvažme dva případy: Nejprve B je singulární. Pak $\exists x \neq 0 : y = Bx = 0$. Pak $(AB)x = A(Bx) = Ay = 0$.
Nyní nechť A je singulární. Pak $\exists y \neq 0 : Ay = 0 \wedge \exists x \neq 0 : Bx = y$. Pak $(AB)x = A(Bx) = Ay = 0$. □

Poznámka (Matice elementárních řádkových úprav)**.** Vynásobení řádku $\alpha \neq 0$: Jednotková matice, jen s α na řádku.
Přičtení α-násobku: Jednotková matice, jenom s α na řádku, do nějž se píše a sloupci čísla násobeného řádku.
Výměna dvou řádků: Jednotková matice s prohozením dvou řádků.
Tyto matice jsou regulární (triv).

Tvrzení 8 (Rozklad RREF na součin regulární matice a původní matice)**.** Nechť $A \in \mathbb{R}^{m\times n}$. Pak $RREF(A) = QA$, kde $Q \in \mathbb{R}^{m\times m}$ je regulární matice.

Důkaz. $RREF(A)$ získáme aplikací konečně mnoha elementárních řádkových úprav. Nechť jdou reprezentovat maticemi $E_1, E_2, \dots, E_k$. Pak $RREF(A) = E_k \dots E_2E_1A = QA$, kde $Q = E_k \dots E_2E_1$. A protože jednotlivé matice E_i jsou regulární, i jejich součin Q je regulární. □

Tvrzení 9 (Rozklad na součin matic elementárních úprav)**.** Každá regulární matice $A \in \mathbb{R}^{n\times n}$ se dá vyjádřit jako součin konečně mnoha elementárních matic.

Důkaz. Pokud k úpravami jsem chopen upravit matici A na I_n, pak jinými k úpravami lze matici I_n převést na A. Jde o to, že každá elementární úprava má svoji inverzi. Tedy existují matice $E_1, E_2, \dots, E_k$ elementárních úprav tak, že $E_k \dots E_2E_1 = A$ □

Definice 11 (Inverzní matice)**.** Buď $A \in \mathbb{R}^{n\times n}$. Pak A^{-1} je inverzní matice k matici A, pokud splňuje $A^{-1}A = AA^{-1} = I_n$.

Věta 3 (O existenci inverzní matice)**.** Buď $A \in \mathbb{R}^{n\times n}$. Je-li A regulární, pak k ní existuje inverzní matice a je určena jednoznačně. Naopak, pokud má A inverzní matici, musí být regulární.

Důkaz. Existence: z regularity A plyne $Ax = e_j$ má jediné řešení pro každé $j \in [n]$, označme tato řešení x_j. Vytvořme matici A^{-1} se sloupci $x_1, \dots, x_j$. Nyní ukážeme $AA^{-1} = I_n$ po sloupcích: $(AA^{-1})_{*j} = A(A^{-1})_{*j} = Ax_j = e_j = (I_n)_{*j}$.
Druhou rovnost ukážeme trikem - uvažme výraz $A(A^{-1}A - I) = AA^{-1}A - A = IA - A = 0$. Matice $A(A^{-1}A - I)$ je tedy nulová a její j-tý sloupec je nulový vektor: $A(A^{-1}A - I)_{*j} = 0$. Z regularity A dostáváme $(A^{-1}A - I)_{*j} = 0$. To platí pro každé $j \in [n]$, tedy $A^{-1}A = I$.
Jednoznačnost: Nechť máme B: $AB = BA = I_n$. Pak $B = BI_n = BAA^{-1} = IA^{-1} = A^{-1}$, tedy B musí být rovno naší zkonstruované matici A^-1.
Inverze implikuje regularitu: Nechť pro A existuje inverzní matice. Pak x buď řešení soustavy $Ax = 0$. Pak $x = I_n x = (A^{-1}A)x = A^{-1}(Ax) = A^{-1}0 = 0$. Tedy A je regulární. □

Tvrzení 10 (O regularitě transponované matice)**.** Je-li A regulární, je i A^T regulární.

Důkaz. Je-li A regulární, existuje A^{-1}. Tedy $AA^{-1} = A^{-1}A = I$. Toto transponujme: $(AA^{-1})^T = (A^{-1}A)^T = I^T$, tedy $(A^{-1})^T A^T = (A^{-1})^T A^T = I$. Vidíme, že A^T má inverzní matici, a tedy je regulární. □

Věta 4 (Jedna rovnost stačí)**.** Nechť $A, B \in \mathbb{R}^{n \times n}$. Je-li $AB = I$, pak obě matice jsou regulární a navzájem k sobě inverzní.

Důkaz. Regularita plyne z tvrzení o součinu dvou regulárních matic a součinu regulární a singulární matice - I_n je regulární. Dále odvodíme: $B = BI = BAA^{-1} = A^{-1}$, $A = AI = ABB^{-1} = B^{-1}$. □

Věta 5 (Výpočet inverzní matice)**.** Buď $A \in \mathbb{R}^{n \times n}$. Nechť matice $(A|I_n)$ typu $n \times 2n$ má RREF tvar $(I_n|B)$. Pak $B = A^{-1}$. Netvoří-li první část RREF jednotkovou matici, je A singulární.

Důkaz. Je-li $RREF(A|I_n) = (I_n|B)$, potom dle věty o rozkladu RREF existuje regulární matice Q taková, že $(I_n|B) = Q(A|I_n)$, neboli po roztržení na dvě části: $I_n = QA$, $B = QI_n$. První rovnost říká $Q = A^{-1}$, druhá $B = Q = A^{-1}$.
Netvoří-li první část RREF I_n, pak A je singulární. □

Tvrzení 11 (Vlastnosti inverzní matice)**.** Buďte $A, B \in \mathbb{R}^{n \times n}$. Pak:

1. $(A^{-1})^{-1} = 1$
2. $(A^T)^{-1} = (A^{-1})^T$
3. $(\alpha A)^{-1} = \frac{1}{\alpha} A^{-1}$ pro $\alpha \neq 0$
4. $(AB)^{-1} = B^{-1}A^{-1}$

Důkaz.
1. Inverze k A^{-1} je A z $AA^{-1} = I$
2. Z věty o regularitě transponované matice
3. Plyne z $(\alpha A)(\frac{1}{\alpha}A^{-1}) = \frac{\alpha}{\alpha}AA^{-1} = I$
4. Plyne z $(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AIA^{-1} = AA^{-1} = I$.

□

Věta 6 (Jednoznačnost RREF - bez dk.)**.** RREF tvar matice je jednoznačně určen.

Grupy a tělesa

Definice 12 (Grupa)**.** Buď $\circ : G^2 \to G$ binární operace na 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. $\exists e \in G : \forall a \in G : e \circ a = a \circ e = a$ (neutrální prvek)
3. $\forall a \in G \, \exists b \in G : b \circ a = a \circ b = e$ (inverzní prvek)

Pokud je splněna následující podmínka, pak grupu nazveme Abelovou (komutativní) grupou:

4. $\forall a, b \in G : a \circ b = b \circ a$

Tvrzení 12 (Základní vlastnosti v grupě)**.** Pro prvky grupy $(G, \circ)$ platí následující vlastnosti:

1. $a \circ c = b \circ c$ implikuje $a = b$ (krácení)
2. neutrální prvek e je určen jednoznačně
3. pro každé $a \in G$ je jeho inverzní prvek určen jednoznačně
4. rovnice $a \circ x = b$ má právě jedno řešení $\forall a, b \in G$
5. $(a^{-1})^{-1} = a$
6. $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$

Důkaz. Triviální □

Definice 13 (Podgrupa)**.** Podgrupa grupy $(G, \circ)$ je grupa $(H, \diamond)$ taková, že $H \subseteq G$ a $\forall a, b \in H : a \circ b = a \diamond b$. Značíme $(H, \diamond) \leq (G, \circ)$

Definice 14 (Permutace, inverzní permutace, skládání permutací a znaménko permutace)**.** Permutace na konečné množině X je bijekce $p : X \to X$. Množina permutací na $[n]$ se značí S_n.
Transpozice je permutace s jedním cyklem (i, j) délky dva a ostatními cykly délky 1. Buď $p \in S_n$. Pak inverzní permutace k p je p^{-1} definovaná jako $p^{-1}(i) = j \Leftrightarrow p(j) = i$.
Nechť $p, q \in S_n$. Pak složená permutace $p \circ q$ je $(p \circ q)(i) = p(q(i))$.
Nechť se permutace $p \in S_n$ skládá z k cyklů. Pak znaménko permutace je číslo $\mathrm{sgn}(p) = (-1)^{n-k}$. Pokud je znaménko 1, řekneme, že permutace je sudá. Pokud je znaménko -1, jedná se o permutaci lichou.

Věta 7 (O znaménku složení permutace a transpozice)**.** Nechť $p \in S_n$ a $(i, j) = t \in S_n$ je transpozice. Pak $\mathrm{sgn}(p) = -\mathrm{sgn}(p \circ t) = -\mathrm{sgn}(t \circ p)$

Důkaz. Dokážeme jen $\mathrm{sgn}(p) = -\mathrm{sgn}(p \circ t)$, druhá rovnost je analogická. Pokud jsou i, j v témže cyklu: cyklus se rozpadne do dvou. Pokud jsou i, j ve dvou rozdílných cyklech, tyto dva cykly se spojí v jeden. Tedy znaménko se zaručeně změní, protože se změnil počet cyklů o 1. □

Definice 15 (Těleso)**.** Těleso je množina $\mathbb{T}$ spolu se dvěma komutativními binárními operacemi $+, \cdot$ splňující:

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

Z tohoto nutně vyplývá, že $1 \neq 0$.

Tvrzení 13 (Základní vlastnosti v tělese)**.** Pro prvky tělesa platí následující vlastnosti:

1. $0a = 0$
2. $ab = 0 \Rightarrow a = 0 \lor b = 0$
3. $-a = (-1)a$

Důkaz. Technické cvičení □

Lemma 1 (Násobky v tělese prvočíselné velikosti)**.** Nechť n je prvočíslo a $0 \neq a \in \mathbb{Z}_n$. Pak $\{0, 1, \dots, n-1\} = \{0a, 1a, \dots, (n-1)a\}$.

Sporem. Nechť $ak = al$ pro $k \neq l$. Pak ovšem $a(k - l) = 0$, tedy $a = 0 \lor k = l$, což je spor. □

Věta 8 (Těleso prvočíselné velikosti)**.** $\mathbb{Z}_n$ je těleso právě tehdy, když n je prvočíslo.

Důkaz. n není prvočíslo: Pak $n = kl : k, l \neq 0$, tedy v tělese $kl = 0 \wedge k \neq 0 \wedge l \neq 0$ - spor.
n je prvočíslo: ověříme všechny předpoklady z definice tělesa.. □

Definice 16 (Charakteristika tělesa)**.** Charakteristika tělesa je nejmenší n takové, že součet n jedniček dává nulu. Pokud takové n neexistuje, definujeme ji jako 0.

Tvrzení 14 (O charakteristice tělesa)**.** Charakteristika tělesa je buď nula nebo prvočíslo.

Důkaz. Charakteristika nemůže být 1 z netriviality tělesa. Dále nechť $n = pq$. Pak můžeme zapsat součet n jedniček jako součin součtů p a q jedniček. Z vlastností tělesa plyne, že $p = 0 \vee q = 0$, což je spor. □

Věta 9 (Malá Fermatova věta)**.** Nechť p je prvočíslo a buď $0 \neq a \in \mathbb{Z}_p$. Pak v $\mathbb{Z}_p$ platí: $a^{p-1} = 1$.

Důkaz. Dle lemmatu o násobcích v tělese prvočíslené velikosti platí $\{0, 1, \ldots, n-1\} = \{0a, 1a, \ldots, (n-1)a\}$. Dále víme, že $0 = 0a$, tedy $\{1, \ldots, n-1\} = \{1a, \ldots, (n-1)a\}$. Nyní všechny prvky vynásobíme: $1 \cdot 2 \cdot \ldots (n-1) = (1a)(2a) \ldots ((n-1)a)$. Po zkrácení $1 \cdot 2 \cdot \ldots (n-1)$ získáme $1 = a^{p-1}$. □

Vektorové prostory

Definice 17 (Vektorový prostor)**.** Nechť $\mathbb{T}$ je těleso s neutrálními prvky 0 pro $+$, 1 pro $\cdot$. Vektorovým prostorem nad tělesem $\mathbb{T}$ rozumíme množinu V s operacemi sčítání vektorů $+ : V^2 \to V$ a násobení vektoru skalárem $\cdot : \mathbb{T} \times V \to V$ splňující $\forall \alpha, \beta \in \mathbb{T}, u, v \in V :$

1. $(V, +)$ je Abelova grupa s neutrálním prvkem o a inverzním prvkem k v $-v$
2. $\alpha(\beta v) = (\alpha\beta)v$
3. $1v = v$
4. $(\alpha + \beta)v = \alpha v + \beta v$
5. $\alpha(u + v) = \alpha u + \alpha v$

Tvrzení 15 (Základní vlastnosti vektorů)**.** V prostoru V nad $\mathbb{T}$ platí

1. $\forall v \in V : 0v = o$
2. $\forall \alpha \in \mathbb{T} : \alpha o = o$
3. $\forall v \in V, \alpha \in \mathbb{T} : \alpha v = o \Rightarrow \alpha = 0 \vee v = o$
4. $\forall v \in V : (-1)v = v$

Důkaz. Triviální, technické cvičení □

Definice 18 (Podprostor)**.** Když V je vektorový prostor nad $\mathbb{T}$, pak $U \subseteq V$ je podprostorem V, pokud tovří vektorový prostor nad $\mathbb{T}$ se stejně definovanými operacemi.

Tvrzení 16 (O průniku podprostorů)**.** Nechť V je vektorový prostor nad $\mathbb{T}$ a mějme $V_i, i \in I$ jako libovolný systém podprostorů. Pak $\cap_{i \in I} V_i$ je opět podprostor V.

Důkaz. Stačí ověřit uzavřenost na sčítání, násobky a obsahování o. □

Definice 19 (Lineární obal)**.** Nechť V je vektorový prostor nad $\mathbb{T}$ a $W \subseteq V$. Pak lineární obal W značený span(W) je průnik všech podprostorů V obsahujících W, tedy span$(W) = \bigcap_{U : W \subseteq U \twoheadrightarrow V}$.

Definice 20 (Lineární kombinace)**.** Nechť V je vektorový prostor nad $\mathbb{T}$ a $v_1, \ldots, v_n \in V$. Pak lineární kombinací vektorů $v_1, \ldots, v_n$ rozumíme výraz typu $\sum_{i=1}^{n} \alpha_i v_i$, kde $\alpha_i \in \mathbb{T}$.

Věta 10 (Lineární obal jako množina lineárních kombinací)**.** Nechť V je vektorový prostor nad $\mathbb{T}$ a mějme $v_1, \ldots, v_n \in V$. Pak span$\{v_1, \ldots, v_n\} = \{\sum_{i=1}^{n} \alpha_i v_i : \alpha_i \in V\}$.

Důkaz. Inkluze zprava doleva: Lineární obal je uzavřený na sčítání a násobky, tedy musí obsahovat všechny lineární kombinace.
Inkluze zleva doprava: Množina lineárních kombinací obsahuje mj. všechny z vektorů, tedy musela být jednou z množin (vektorových prostorů), z nichž se dělal průnik. A všechny tyto prostory jsou uzavřené na sčítání a násobky, tedy obsahují všechny lineární kombinace. □

Definice 21 (Lineární nezávislost konečné a nekonečné množiny)**.** Nechť $v_1, \ldots, v_n \in V$, kde V je vektorový prostor nad $\mathbb{T}$. Pak vektory $v_1, \ldots, v_n$ jsou lineárně nezávislé pokud rovnost $\sum_{i=1}^{n} \alpha_i v_i = o$ nastane jen pro $\alpha_1 = \ldots = \alpha_n = 0$. V opačném případě jsou vektory lineárně nezávislé.
Pokud $M \subseteq V$ je nekonečná množina vektorů, je M lineárně nezávislá, pokud každá konečná podmnožina M je lineárně nezávislá. Jinak je lineárně závislá.

Věta 11 (Charakterizace lineárně nezávislých vektorů)**.** Nechť V je vektorový prostor nad $\mathbb{T}$ a $v_1, \ldots, v_n \in V$. Pak vektory $v_1, \ldots, v_n$ jsou lineárně závislé právě tehdy když existuje $k \in [n] : v_k = \sum_{i \neq k} \alpha_i v_i$ pro nějaké $\alpha_1, \ldots, \alpha_n \in \mathbb{T}$, tedy $v_k \in \operatorname{span}\{v_1, \ldots, v_k - 1, v_k + 1, \ldots, v_n\}$.

Důkaz. „$\Rightarrow$“: Jsou-li vektory lineárně závislé, existuje netriviální lineární kombinace rovna nule. Tedy pro $\beta_1, \ldots, \beta_n \, \exists k \in [n] : \beta_k \neq 0 \wedge \sum_{i=1}^{n} \beta_i a_i = o$. Pak upravíme do tvaru $\beta_k v_k = -\sum_{i \neq k} \beta_i v_i$, což po přepsání vyhovuje.
„$\Leftarrow$“: Máme rovnost $v_k = \sum_{i \neq k} \alpha_i v_i$, takže po úpravě na $o = \sum_{i \neq k} \alpha_i v_i - v_k$ máme požadovanou netriviální lineární kombinaci. □

Důsledek 2. Nechť V je vektorový prostor nad $\mathbb{T}$ a $v_1, \ldots, v_n \in V$. Pak vektory $v_1, \ldots, v_n$ jsou lineárně závislé právě tehdy, když existuje $k \in [n]$ takové, že: $\operatorname{span}\{v_1, \ldots, v_n\} = \operatorname{span}\{v_1, \ldots, v_k - 1, v_k + 1, \ldots, v_n\}$.

Důkaz. „$\Rightarrow$“: Vektory jsou LZ, tedy z předchozí věty plyne, že obaly jsou stejné.
„$\Leftarrow$“: Platí rovnost, tedy $\exists k \in [n] : v_k \in \operatorname{span}\{v_1, \ldots, v_k - 1, v_k + 1, \ldots, v_n\}$. □

Definice 22 (Báze vektorového prostoru)**.** Nechť V je vektorový prostor nad $\mathbb{T}$. Pak bází rozumíme libovolný systém generátorů V.

Věta 12 (O jednoznačnosti souřadnic)**.** Nechť $v_1, \ldots, v_n \in V$ je báze V. Pak pro každý vektor existují jednoznačně určené koeficienty $\alpha_1, \ldots, \alpha_n \in \mathbb{T}$ takové, že $u = \sum_{i=1}^{n} \alpha_i v_i$.

Důkaz. Vektory tvoří bázi, takže existence vyjádření je z definice. Jednoznačnost ukážeme sporem: Ať existují dvě rozdílná vyjádření s koeficienty α_i, β_i. Pak ovšem $u = \sum_{i=1}^{n} \alpha_i v_i = \sum_{i=1}^{n} \beta_i v_i$. Tedy $o = u - u = \sum_{i=1}^{n} \alpha_i v_i - \sum_{i=1}^{n} \beta_i v_i = \sum_{i=1}^{n} (\alpha_i - \beta_i) v_i$, tedy z lineární nezávislosti $\alpha_i = \beta_i \forall i \in [n]$. □

Definice 23 (Souřadnice)**.** Nechť $B = v_i : i \in [n]$ je báze vektorového prostoru V nad $\mathbb{T}$ a vektor $v \in V$ má vyjádření $v = \sum_{i=1}^{n} \alpha_i v_i$. Pak souřadnicemi vektoru u vzhledem k bázi B rozumíme koeficienty $\alpha_1, \ldots, \alpha_n$ a vektor souřadnic značíme $[u]_B = (\alpha_+, ldots, \alpha_n)^T$.

Věta 13 (O existenci báze)**.** Každý vektorový prostor má bázi.

Důkaz. Důkaz provedeme jen pro konečně generovaný prostor. Nechť $v_1, \ldots, v_n$ je systém generátorů V. Jsou-li lineárně nezávislé, již tvoří bázi. Nejsou-li, pak můžeme najít vektor takový, že je lineární kombinací ostatních vektorů. Tento postup můžeme opakovat, dokud nezredukujeme dostatečně. □

Věta 14 (Steinitzova věta o výměně)**.** Nechť V je vektorový prostor s lineárně nezávislým systémem $x_1, \ldots, x_m$ a systémem generátorů $x_1, \ldots, x_n$. Pak platí:

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

Indukcí podle m. 1.IK: $m = 0$ - triviální.
2.IK: Uvažme vektory $x_1, \ldots, x_{m-1}$ - ty jsou lineárně nezávislé - a podle IP: $m - 1 \leq n$. Kdyby $n - 1 = m$, pak vektory $x_1, \ldots, x_{m-1}$ jsou generátory V a dostáváme $v_m \in \text{span} x_1, \ldots, x_{m-1}$, což je spor s lineární nezávislostí. Tím máme dokázáno první tvrzení.
Nyní druhá část: Uvažme lineární kombinace $x_m = \sum_{i=1}^{m-1} \alpha_i x_i + \sum_{j=1}^{n-m+1} \beta_j y_{l_j}$, což si můžeme dovolit díky tomu, že vektory v sumě generují V. Kdyby všechny β_i byly nulové, jednalo by se o spor s lineární nezávislostí. Proto existuje k takové, že $\beta_k \neq 0$. Pak dle lemmatu o výměně lze vyměnit tyto y_{l_k} za x_m a pak budou vektory $x_1, \ldots, x_m, y_{l_1}, \ldots, y_{l_{k-1}}, y_{l_{k+1}}, \ldots, y_{l_{n-m+1}}$ opět generovat V. □

Důsledek 3 (O velikosti báze)**.** Všechny báze konečně generovaného vektorového prostoru jsou stejně velké.

Důkaz. Mějme dvě odlišné báze. Ze Steinitzovy věty o výměně: můžeme prohodit jejich vlastnosti, tedy $m \leq n \wedge n \leq m \Rightarrow m = n$. □

Definice 24 (Dimenze)**.** Dimenze nějakého konečně generovaného prostoru je velikost nějaké jeho báze, dimenze nekonečně generovaného prostoru je ∞. Značíme $\dim V$.

Věta 15 (Vztah počtu prvků systému k dimenzi)**.** Pro vektorový prostor V platí:

1. Nechť $x_1, \ldots, x_m$ jsou lineárně nezávislé. Pak $m \leq \dim V$. Pokud si jsou rovny, pak $x_1, \ldots, x_m$ je báze V.

2. Nechť $y_1, \ldots, y_n$ jsou generátory V. Pak $n \geq \dim V$. Pokud si jsou rovny, pak $y_1, \ldots, y_n$ je báze V.

Důkaz. Nechť $d = \dim V$ a $z_1, \ldots, z_d$ je báze V.

1. $x_1, \ldots, x_m$ jsou lineárně nezávislé, tedy dle Steinitzovy věty je $m \leq d$. Pokud $m = d$, tak ze stejné věty lze systém doplnit o $m - d = 0$ vektorů na systém generátorů V, tedy na bázi.

2. $y_1, \ldots, y_n$ jsou generátory V, tedy dle Steinitzovy věty je $n \geq d$. Když $n = d$, pak pokud $y_1, \ldots, y_n$ jsou LN, tvoří bázi. Kdyby ovšem byly závislé, pak lze jeden vynechat a získat systém generátorů o velikosti $n - 1$, což je spor - protože pak by platilo $d \leq n - 1$ dle Steinitzovy věty, což vede ke sporu.

□

Věta 16 (Rozšíření lineárně nezávislého systému na bázi)**.** Každý lineárně nezávislý systém vektorového prostoru V lze rozšířit na bázi V.

Důkaz. Nechť $x_1, \ldots, x_m$ jsou lineárně nezávislé a $z_1, \ldots, z_d$ je báze V. Podle Steinitzovy věty lze doplnit vektory x pomocí vektorů z na bázi. □

Definice 25 (Spojení podprostorů)**.** Nechť U, V jsou podprostory W. Pak spojení podprostorů U, V je definováno jako $U + V := \{u + v : u \in U, v \in V\}$.

Věta 17 (Spojení podprostorů jako lineární obal jejich sjednocení)**.** Nechť U, V jsou podprostory W. Pak $U + V = \text{span}(U \cup V)$.

Důkaz. Inkluze zleva doprava je triviální: $\text{span}(U \cup V)$ je uzavřený na součty.
Inkluze zprava doleva: Stačí ukázat, že $U + V$ obsahuje U, V a je podprostorem W. První část je zřejmá, pro druhou uvažme $x_1, x_2 \in U + V$. Vektory umíme vyjádřit jako $x_1 = u_1 + v_1, x_2 = u_2 + v_2 : u_1, u_2 \in U, v_1, v_2 \in V$. Pak $x_1 + x_2 = u_1 + v_1 + u_2 + v_2 = (u_1 + u_2) + (v_1 + v_2) \in U + V$, tedy je uzavřený na sčítání. Pro uzavřenost na násobky uvažme $x = u + v \in U + V, u \in U, v \in V, \alpha$ skalár. Pak $\alpha x = \alpha(u + v) = \alpha u + \alpha v \in U + V$, tedy jsme uzavřeni i na násobky. □

Věta 18 (O dimenzi spojení a průniku)**.** Nechť U, V jsou podprostory W. Pak $\dim(U + V) + \dim(U \cap V) = \dim U + \dim V$.

Důkaz. $U \cap V$ je podprostor W, tedy má konečnou bázi $z_1, \dots, z_p$. Podle věty o rozšíření lineárně nezávislého systému na bázi U tvaru $z_1, \dots, z_p, x_1, \dots, x_m$. Podobně ji můžeme rozšířit na bázi V tvaru $z_1, \dots, z_p, y_1, \dots, y_n$. Stačí ukázat, že vektory $z_1, \dots, z_p, x_1, \dots, x_m, y_1, \dots, y_n$ tvoří bázi $U+V$. Nejprve ukážeme, že jsou generátory, pak, že jsou lineárně nezávislé.
„Generujícnost“: Pro $z \in U + V : z = u + v, u \in U, v \in V$. Tedy $u = \sum \alpha_i z_i + \sum \beta_j x_j$, stejně $v = \sum \gamma_i z_i + \sum \delta_k y_k$. Potom $z = \sum(\alpha_i + \gamma_i) z_i + \sum \beta_j x_j + \sum \delta_k y_k$, tedy z je lineární kombinací našich vektorů.
„Lineární nezávislost“: Buď $\sum \alpha_i z_i + \sum \beta_j x_j + \sum \gamma_k y_k = o$. Chceme ukázat, že všechny koeficienty musí být nulové. Označme $z := \sum \alpha_i z_i + \sum \beta_j x_j = -\sum \gamma_k y_k$. Zjevně $z \in U \cap V$, tedy $z = \sum \delta_i z_i$. Tím dostáváme $z = \sum \delta_i z_i = -\sum \gamma_k y_k$, neboli $\sum \delta_i z_i + \sum \gamma_k y_k = o$. Jediná lineární kombinace je triviální (z toho, že to je báze V). Z toho už plyne, že všechny koeficienty musí být nulové. □

Definice 26 (Maticové prostory: sloupcový, řádkový, jádro)**.** Nechť $A \in \mathbb{T}^{m \times n}$. Pak definujeme

1. sloupcový prostor $\mathcal{S}(A) := \operatorname{span}\{A_{*1}, \dots, A_{*n}\}$
2. řádkový prostor $\mathcal{R}(A) := \mathcal{S}(A^T)$
3. jádro matice $\operatorname{Ker}(A) := \{x \in \mathbb{T}^n : Ax = o\}$

Věta 19 (Maticové prostory a RREF)**.** Nechť $A \in T^{m \times n}$ a A^R její RREF tvar s pivoty na pozicích $(1, p_1), \dots, (r, p_r)$, kde $r = \operatorname{rank}(A)$. Pak

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

Důkaz. Z věty o rozkladu RREF na součin regulární a původní matice víme, že $A^R = QA$.

1. Podle tvrzení o prostorech a násobení regulární maticí zleva je $\mathcal{R}(A) = \mathcal{R}(QA) = \mathcal{R}(A^R)$. Nenulové řádky A^R jsou lineárně nezávislé, tedy tvoří bázi.
2. Nejprve ukážeme, že sloupce A^R tvoří bázi $\mathcal{S}(A^R)$. Protože jsou jednotkové, jsou jistě nezávislé a generují celý prostor, neboť libovolný nebázický sloupec lze vyjádřit za pomoci těch bázických. Nyní dle tvrzení o prostorech a násobení regulární maticí zleva máme jistotu, že i sloupce A tvoří bázi (tedy jsou LN a generují ostatní sloupce).
3. Zjevné.

□

Věta 20 (O dimenzi jádra a hodnosti matice)**.** Pro každou matici $A \in \mathbb{T}^{m \times n}$ platí $\dim \operatorname{Ker}(A) + \operatorname{rank}(A) = n$.

Důkaz. Nechť $\dim \operatorname{Ker}(A) = k$ a vektory $v_1, \dots, v_k$ jsou báze jádra. Pak $Av_1 = \ldots = Av_k = o$. Pak rozšíříme bázi o vektory $v_{k+1}, \dots, v_n$. Pak stačí ukázat, že vektory $Av_{k+1}, \dots, Av_n$ tvoří bázi $\mathcal{S}(A)$, protože hodnost je rovna dimenzi sloupcového prostoru (tedy $n - k$).
„Generujícnost“: Mějme $y \in \mathcal{S}(A)$. Pak $y = Ax$ pro nějaké $x \in \mathbb{T}^n$. Toto x lze vyjádřit jako $\sum \alpha_i v_i$. Dosazením: $y = Ax = A(\sum \alpha_i v_i) = \sum \alpha_i A v_i = \sum_{i=k+1}^n \alpha_i (Av_i)$.
„Lineární nezávislost“: Buď $\sum_{i=k+1}^n \alpha_i A v_i = o$. Pak platí $A(\sum_{i=k+1}^n \alpha_i v_i) = o$, čili $\sum_{i=k+1}^n \alpha_i v_i$ je v jádru matice. Proto $\sum_{i=k+1}^n \alpha_i v_i = \sum_{i=1}^k \beta_i v_i$ pro nějaké skaláry β. Přepisem dostaneme, že alfy a bety jsou nulové. □

Lineární zobrazení

Definice 27 (Lineární zobrazení)**.** Nechť U, V jsou vektorové prostory nad $\mathbb{T}$. Zobrazení $f : U \to V$ je lineární, pokud $\forall x, y \in U, \alpha \in \mathbb{T}$ platí:

1. $f(x + y) = f(x) + f(y)$

2. $f(\alpha x) = \alpha f(x)$

Tvrzení 17 (Vlastnosti lineárních zobrazení)**.** Nechť $f : U \to V$ je lineární zobrazení. Pak

1. $f(\sum \alpha_i x_i) = \sum \alpha_i f(x_i) \forall \alpha_i \in \mathbb{T}, x_i \in U, i \in [n]$.
2. $f(o) = o$

Důkaz. 1 z definice + rozšíření indukcí.
2 $f(o) = f(0o) = 0f(o) = o$. □

Definice 28 (Obraz a jádro lineárního zobrazení)**.** Nechť $f : U \to V$ je lineární zobrazení. Pak

1. obraz je $f(U) := \{f(x) : x \in U\}$
2. jádro je $\mathrm{Ker}(f) := \{x \in U : f(x) = o\}$

Věta 21 (O prostém lineárním zobrazení)**.** Nechť $f : U \to V$ je lineární zobrazení. Pak NTJE:

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

Důkaz. Ukážeme $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$: „$1 \Rightarrow 2$“: $f(o) = o \Rightarrow o \in \mathrm{Ker}(f)$. Ale f je prosté, tedy jádro jiný prvek neobsahuje.
„$2 \Rightarrow 3$“: Nechť $x_1, \dots, x_n \in U$ lineárně nezávislé a nechť $\sum \alpha_i f(x_i) = o$. Pak $f(\sum \alpha_i x_i) = o$, tedy $\sum \alpha_i x_i$ náleží do jádra zobrazení, které ovšem obsahuje jen nulový vektor, tedy máme z lineární nezávislosti $a_i = 0 \forall i \in [n]$.
„$3 \Rightarrow 1$“: Sporem předpokládejme, že existují $x, y \in U : f(x) = f(y)$. Potom $o = f(x) - f(y) = f(x - y)$. Vektor o ovšem představuje lineárně závislou množinu, tedy $x - y$ musí být z 3 také lineárně závislá, tedy $x - y = 0 \Rightarrow x = y$, což je spor. □

Věta 22 (Jednoznačnost lineárního zobrazení vzhledem k obrazům báze)**.** Nechť U, V jsou prostory nad $\mathbb{T}$ 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 $f(x_i) = y_i \forall i \in [n]$.

Důkaz. „Existence“. Mějme $x \in U$. Pak $x = \sum \alpha_i x_i$. Pak $f(x) = f(\sum \alpha_i x_i) = \sum \alpha_i f(x_i) = \sum \alpha_i y_i$. Pak jen ověříme linearitu.
„Jednoznačnost“. Mějme $f, g : f(x_i) = g(x_i) = y_i \forall i \in [n]$. Pak pro libovolné $x \in U : f(x) = f(\sum \alpha_i x_i) = \sum \alpha_i f(x_i) = \sum \alpha_i y_i = \sum \alpha_i g(x_i) = g(\sum \alpha_i x_i) = g(x)$. Tedy $\forall x \in U : f(X) = g(x)$, tedy tato zobrazení musí být stejná. □

Definice 29 (Matice lineárního zobrazení)**.** Nechť $f : U \to V$ je lineární zobrazení, $B_1 = \{x_1, \dots, x_n\}$ báze U nad $\mathbb{T}$, $B_2 = \{y_1, \dots, y_m\}$ báze V nad $\mathbb{T}$. Nechť $f(x_j) = \sum a_{ij} y_i$. Potom matice $A \in \mathbb{T}^{m \times n}$ s prvky a_{ij} se nazývá matice lineárního zobrazení vzhledem k bázím B_1, B_2 a značí se ${}_{B_2}[f]_{B_1}$

Věta 23 (Maticová reprezentace lineárního zobrazení)**.** Nechť $f : U \to V$ je lineární zobrazení, $B_1 = \{x_1, \dots, x_n\}$ báze U, $B_2 = \{y_1, \dots, y_m\}$ báze V. Pak $\forall x \in U : [f(x)]_{B_2} = {}_{B_2}[f]_{B_1} \cdot [x]_{B_1}$.

Důkaz. Označme $A := {}_{B_2}[f]_{B_1}$. Buď $x \in U$, tedy $x = \sum \alpha_i x_i$, tedy $[x]_{B_1} = (\alpha_1, \dots, \alpha_n)^T$. Pak $f(x) = f(\sum \alpha_j x_j) = \sum \alpha_j f(x_j) = \sum \alpha_j (\sum a_{ij} y_i) = \sum \sum \alpha_j a_{ij} y_i = \sum(\sum \alpha_j a_{ij}) y_i$. Tedy $\sum \alpha_j a_{ij}$ reprezentuje i-tou souřadnici vektoru $[f(x)]_{B_2}$, ale jeho hodnota je $(A[x]_{B_1})_i$, což je i-tá složka vektoru ${}_{B_2}[f]_{B_1} \cdot [x]_{B_1}$. □

Věta 24 (Jednoznačnost matice lineárního zobrazení)**.** Nechť $f : U \to V$ je lineární zobrazení, B_1 je báze U, B_2 je báze V. Pak jediná matice A splňující $[f(x)]_{B_2} = A \cdot [x]_{B_1}$ je ${}_{B_2}[f]_{B_1}$.

Důkaz. Nechť se báze B_1 sestává z vektorů $x_1, \dots, x_n$. Pro spor předpokládejme, že f má dvě maticové reprezentace pomocí matic $A \neq A'$. Tedy existuje vektor $s \in \mathbb{T}^n$ takový, že $As \neq A's$. Takový vektor lze volit například jako jednotkový s jedničkou na takové pozici, ve kterém sloupci se matice liší. Definujme $x := \sum s_i x_i$. Pak $[f(x)]_{B_2} = As \neq A's = [f(x)]_{B_2}$, což se spor s jednoznačností souřadnic. □

Definice 30 (Matice přechodu)**.** Nechť V je vektorový prostor a B_1, B_2 dvě jeho báze. Pak maticí přechodu od B_1 k B_2 nazveme matici ${}_{B_2}[id]_{B_1}$.

Tvrzení 18 (O složeném lineárním zobrazení)**.** Nechť $f : U \to V, g : V \to W$ jsou lineární zobrazení. Pak složené zobrazení $g \circ f$ je opět lineární zobrazení.

Důkaz. Ověřit z definice. □

Věta 25 (O matici složeného lineárního zobrazení)**.** Nechť $f : U \to V, g : V \to W$ jsou lineární zobrazení, B_1 báze U, B_2 báze V, B_3 báze W. Pak ${}_{B_3}[g \circ f]_{B_1} = {}_{B_3}[g]_{B_2} \cdot {}_{B_2}[f]_{B_1}$.

Důkaz. $\forall x \in U : [(g \circ f)(x)]_{B_3} = [g(f(x))]_{B_3} = {}_{B_3}[g]_{B_2} \cdot [f(x)]_{B_2} = {}_{B_3}[g]_{B_2} \cdot {}_{B_2}[f]_{B_1} \cdot [x]_{B_1}$. Díky jednoznačnosti matice lineárního zobrazení je součin hledaná matice. □

Definice 31 (Izomorfismus)**.** Izomorfismus mezi prostory U, V je bijekce $f : U \to V$. Pokud mezi U a V existuje izomorfismus, říkáme, že U, V jsou izomorfní.

Tvrzení 19 (Vlastnosti izomorfismu)**.**

1. Je-li $f : U \to V$ izomorfismus, pak i inverzní funkce existuje a je izomorfismus.
2. Jsou-li $f : U \to V, g : V \to W$ izomorfismy, pak $g \circ f : U \to W$ je také izomorfismus.
3. Je-li $f : U \to V$ izomorfismus, pak libovolná báze U se zobrazuje na bázi V.
4. Je-li $f : U \to V$ izomorfismus, pak $\dim U = \dim V$.

Důkaz.

1. Vzájemná jednoznačnost je dána, stačí ověřit linearitu.
2. Plyne z tvrzení o složeném lineárním zobrazení.
3. Mějme bázi B_1 prostoru U, která je nutně LN. Pak i $f(B_1)$ je LN a navíc každý vektor $x \in U$ je těmito vektory generovaný, takže je to báze.
4. Plyne z 3.

□

Tvrzení 20 (Izomorfismus $\mathbb{T}^n$ a n-dimenzionálního prostoru nad $\mathbb{T}$)**.** Nechť V je vektorový prostor nad $\mathbb{T}$ s dimenzí n a bází B. Pak zobrazení $x \mapsto [x]_B$ je izomorfismus mezi V a $\mathbb{T}^n$.

Důkaz. Nechť báze sestává z vektorů $v_1, \ldots, v_n$. Snadno nahlédneme, že je to lineární zobrazení a že je prosté (z jednoznačnosti souřadnic). Surjekce plyne z toho, že každá n-tice představuje souřadnice nějakého vektoru. Linearitu dokážeme triviální úpravou. □

Věta 26 (Izomorfismus n-dimenzionálních prostorů)**.** Všechny n-dimenzionální prostory nad $\mathbb{T}$ jsou navzájem izomorfní.

Důkaz. Všechny prostory jsou izomorfní s $\mathbb{T}^n$ a z vlastností izomorfismu plyne, že jsou tedy všechny izomorfní. □

Věta 27 (O dimenzi jádra a obrazu)**.** Nechť $f : U \to V$ je lineární zobrazení, U, V prostory nad $\mathbb{T}$, B_1 báze U, B_2 báze V. Označme $A = {}_{B_2}[f]_{B_1}$. Pak:

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

Důkaz. 1: Podle 4. vlastnosti izomorfismu stačí sestrojit izomorfismus mezi jádry. Izomorfismem může být např. zobrazení $x \in \mathrm{Ker}(f) \mapsto [x]_{B_1}$. Z izomorfismu $\mathbb{T}^n$ a n-dimenzionálního prostoru nad $\mathbb{T}$ víme, že je lineární a prostá. Stačí ukázat, že je na. Pro $x \in \mathrm{Ker}(f) : o = [o]_{B_2} = [f(x)]_{B_2} = {}_{B_2}[f]_{B_1} \cdot [x]_{B_1}$, tedy $[x]_{B_1}$ náleží do jádra matice A. Stejně i naopak.
2: Mějme $\dim U = n, \dim V = m$. Opět sestrojíme izomorfismus mezi $f(U)$ a $\mathcal{S}(A)$, a to takto: $y \in f(U) \mapsto [y]_{B_2}$. A opět je zobrazení lineární a prosté. Dále pro $y \in f(U)$ existuje $x \in U$ takové, že $f(x) = y$. Nyní $[y]_{B_2} = [f(x)]_{B_2} = A[x]_{B_1}$, tedy $[y]_{B_2}$ náleží do sloupcového prostoru $\mathcal{S}(A)$. A naopak, pro každé $b \in \mathcal{S}(A)$ existuje $a \in \mathbb{T}^n$ takové, že $b = Aa$. Tedy pro vektor $x \in U$ takový, že $[x]_{B_1} = a$ platí $y := f(x) \in f(U) \wedge [y]_{B_2} = [f(x)]_{B_2} = A[x]_{B_1} = Aa = b \in \mathcal{S}(A)$. □

Definice 32 (Lineární funkcionál a duální prostor)**.** Nechť V je vektorový prostor nad $\mathbb{T}$. Pak lineární funkcionál je libovolné lineární zobrazení z V do $\mathbb{T}$. Duální prostor, též značený $V*$, je vektorový prostor všech lineárních funkcionálů.

Afinní podprostory

Definice 33 (Afinní podprostor)**.** Buď V vektorový prostor nad $\mathbb{T}$. Pak afinní podprostor je jakákoliv množina $M \subseteq V$ tvaru $M = U + a\{v + a : v \in V\}$, kde $a \in V$ a U je vektorový podprostor V.

Věta 28 (Charakterizace afinního podprostoru)**.** Nechť V je vektorový podprostor nad $\mathbb{T}$ charakteristiky různé od 2, a buď $\emptyset \neq M \subseteq V$. Pak M je afinní, tj. je tvaru $M = U + a$ právě tehdy, když $\forall x, y \in M, a \in \mathbb{T}$ platí $\alpha x + (1 - \alpha)y \in M$.

Důkaz. Implikace „$\Rightarrow$“: Mějme $x, y \in M$, tedy jsou tvaru $x = u + a, y = v + a : u, v \in U$. Pak $\alpha x + (1 - \alpha)y = \alpha u + \alpha a + (1 - \alpha)v + (1 - \alpha)a = \alpha u + (1 - \alpha)v + a$, což odpovídá.
Implikace „$\Leftarrow$“: Ukážeme, že stačí zvolit libovolné $a \in M$ pevně a $U := M - M = x - y : x, y \in M$. Tedy ukážeme, že $M = (M - M) + a$.
Inkluze zleva doprava: $x \in M : x = x - a + a \in (M - M) + a = U + a$.
Inkluze zprava doleva: Mějme $x - y + a \in (M - M) + a$. Protože $x, y, a \in M$, dostáváme, že afinní kombinace $a/2 + x/2 \in M$ a také $2(a/2 + x/2) - (1 - 2)y = x - y + a \in M$. □

Věta 29 (O afinních podprostorech a řešení soustav lineárních rovnic)**.** Množina řešení soustavy $Ax = b$ je prázdná nebo afinní. Je-li neprázdná, můžeme tuto množinu řešení vyjádřit ve tvaru $\mathrm{Ker}(A) + x_0$, kde x_0 je libovolné řešení soustavy.

Důkaz. Pokud x_1 je řešením, pak lze psát $x_1 = x_1 - x_0 + x_0$. Stačí ukázat, že $x - 1 - x_0 \in \mathrm{Ker}(A)$. Dosazením $A(x_1 - x_0) = Ax_1 - Ax_0 = b - b = 0$. Tedy $x_1 \in \mathrm{Ker}(A) + x_0$. Naopak, je-li $x_2 \in \mathrm{Ker}(A)$, pak $x_2 + x_0$ je řešením soustavy, jelikož $A(x_2 + x_0) = Ax_2 + Ax_0 = 0 + b = b$. □

Definice 34 (Dimenze afinního podprostoru)**.** Dimenze afinního podprostoru $M = U + a$ je definována jako $\dim(M) := \dim(U)$.

Definice 35 (Afinní nezávislost)**.** Vektory $x_0, \ldots, x_n$ jsou afinně nezávislé, pokud vektory $x_1 - x_0, \ldots, x_n - x_0$ jsou lineárně nezávislé. V opaném případě vektory nazýváme afinně závislé.

Seznam témat