Organizační úvod

Přednáška bude asi touto formou celý semestr.

Pozor
Bude důležitá zpětná vazba (přímo přes Zoom, kde bude snad nějaký cvičící, nebo přes diskuzi k předmětu v Moodle, či kvízy (od 5. 10.)).

Poznámka
Číst mail a popis předmětu na webu.

Poznámka (Organizace)
2krát týdně přednáška na Zoomu. K zápočtu jsou třeba 2 věci:

Průběžná práce (nejlépe přečíst skripta už před přednáškou, na dotazy bude přihlíženo) = kvízy (od 5. 10., 3 / 4 otázky a,b,c, za jeden kvíz až 2 body do bodovacího systému) + domácí úkoly (zadávány se zpožděním = další týden, odevzdává se ve středu, za jeden úkol až 8 bodů), počítá se 10 nejlepších kvíz + úkol (minimum pro zápočet je 60%).

Aktivní účast alespoň na 9 cvičeních. Je to záměrně trochu neurčité (optimálně připojit se na cvičení a počítat příklady a interagovat s cvičícím (v menších skupinkách)), dá se i bez toho (např. méně interaktivně) podle domluvy se cvičícími.

Odevzdávání bude elektronické, většinou v Moodle. Pro skenování přes mobil používat aplikace jako Adobe scan / Genius scan. Nepoužívejme aplikace na automatické výpočty (1. je potřeba i postup, 2. děláme to pro sebe), ale můžeme je používat pro experimenty, ověření nebo představu.

Sociální stránka, spolupracujme (viz cvičení, klidně si na cvičeních můžete skupinky domluvit), ale úkol zkusme vypracovat každý sám.

Zkouška je standardně nějakých 5 termínů + jeden záchranný v září?, kdy bude 3hodinový test, požadavky ke zkoušce budou na webu. Midtermy (konec listopadu a půlka prosince) budou takové menší zkoušky, které se možná budou počítat ke zkoušce (minimálně si to můžeme vyzkoušet nanečisto).

Poznámka (Materiály)

- Skripta (Barto & Tůma, na webu), kapitola 1-7
- Cvičení, přímočaré úlohy (nejen mechanicky řešit)
- Přednášky nejsou směrodatný studijní materiál!

Pozor
Přednášky nejsou směrodatný studijní materiál! (Protože jejich cílem je pomoci nám látku pochopit, ne přečíst skripta. Navíc matematiku musí pochopit každý sám (doporučit přečíst text J. Hrnčíře`https://msekce.karlin.mff.cuni.cz/~smid/pmwiki/uploads/Main/vzkazHrncir.pdf`).)

1 Opakování (?)

- Analytická geometrie
- Komplexní čísla
- Zobrazení (hlavně terminologie)

Poznámka (Co je lineární algebra)
Abstraktní studium rovných útvarů a hezkých zobrazení mezi nimi.

Rovný útvar: Přímka, rovina, 3D prostor $\mathbb{R}^3 \equiv \{(x, y, z) : x, y, z \in \mathbb{R}\}$.

Hezkých zobrazení:

$$\mathbb{R}^2 \longrightarrow \mathbb{R}^2 \tag{1}$$
$$(x, y) \longrightarrow \text{otočení } (x, y) \text{ o } \frac{\pi}{6} \tag{2}$$

$$\mathbb{R}^2 \longrightarrow \mathbb{R}$$

Abstraktní: Časem dojdeme k tomu, že nás zajímají pouze vlastnosti.

Poznámka (Proč lineární algebra)

- Často se vyskytuje na různých místech matematiky
- Geometrie
- Matematická analýza (na limitním okolí bodu jsou funkce většinou také rovné)
- Kvantová teorie (a celkově fyzika)
- Trisekce úhlu
- Z historie – nalezení planetky Ceres

- Moderní aplikace – komprese dat (JPEG, …), kódování a šifrování (samoopravné kódy, RSA)

1.1 Analytická geometrie

Poznámka (Názvosloví)
- Body vs. vektory: bod hranatou závorkou, vektor (jako rozdíl bodů) kulatou ← je to skoro to samé, budeme uvažovat jen vektory (body jsou dané polohovými vektory)
- Operace s vektory: sčítání (sečteme po složkách), násobení skalárem (vynásobíme po složkách).
- Souřadnicové systémy (často nejsou kartézské)

Poznámka (Jak zadat přímku v $\mathbb{R}^2$)
- Bod a směrový vektor (parametricky)
- 2 různé body
- Rovnicí přímky: $L = \{(x, y) \in \mathbb{R}^2 : ax + by = c\} \quad a, b, c \in \mathbb{R}$ (implicitně)

Poznámka (Jak zadat rovinu v $\mathbb{R}^3$)
- Bod a 2 vektory s jiným směrem (parametricky)
- 3 různé body
- přímka a bod, který na ní neleží
- Rovnicí roviny: $P = (x, y, z) \in \mathbb{R}^3 : ax + by + cz = da, b, c, d \in \mathbb{R}$ (implicitně)

Poznámka (Jak zadat rovinu v $\mathbb{R}^3$)
- Bod a směrový vektor
- 2 různé body
- 2 roviny (soustava 2 lineárních rovnic)

1.2 Zobrazení

X, Y množiny
$f : X \longrightarrow Y \; x \in X \longrightarrow |f| \longrightarrow f(x) \in Y$

Například

$$X = \{\text{Různé symboly}\}, Y = \{A, B, \ldots, Z\}$$

- Zadání pomocí definice: $f(x) :=$ První písmeno tvaru$x$

- Zadání pomocí tabulky: tabulka (jeden řádek symboly (x), druhý písmena $(f(x))$)
- Zadání pomocí grafu: Graf (jedna osa symboly, druhá písmena)

Definice 1.1 (Rovnost zobrazení)

$$f : X \longrightarrow Y = g : M \longrightarrow Y \Leftrightarrow$$

Definice 1.2 (Prosté (= injektivní))

$$\forall x, y \in X, x \neq y : f(x) \neq f(y)$$

Definice 1.3 (Na (= surjektivní))

$$\forall y \in Y \exists x \in X : f(x) = y$$

Definice 1.4 (Vzájemně jednoznačné (= bijektivní))

Prosté a na.

Definice 1.5 (Skládání)

$$X \overrightarrow{f} Y \overrightarrow{g} : X \overrightarrow{g \circ f} Z, g \circ f(x) = g(f(x))$$

Dále obraz zobrazení je množina NA kterou se zobrazuje, obraz množiny v zobrazení je množina, na kterou zobrazí zobrazení prvky dané množiny. Vzor obdobně (z které zobrazuje,).

Definice 1.6 (Inverze)

$f : X \longrightarrow Y$ má inverzi $g : Y \longrightarrow Y$, pokud $f \circ g = id_Y$ (identita na Y)

Věta 1.1

f má inverzi, právě když je bijektivní

Důkaz

Nechť má inverzi, když není na, tak v Y přebývají prvky, které se nikam nezobrazují, když není prosté, tak chybí (TODO zlepšit popis).

Nechť je bijektivní, pak zřejmě má inverzi. □

2 Soustavy lineárních rovnic

6 motivačních příkladů v části 2.1 skript

Definice 2.1 (lineární rovnice)

Lineární rovnice o n neznámých s reálnými koeficienty je rovnice tvaru $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$, kde $a_1, \ldots, a_n, b \in \mathbb{R}$ jsou koeficienty a $x_1, \ldots, x_n$ jsou neznámé.

Pozor (Jak vypadá definice)

- Psát celé věty!
- Vysvětlit použité symboly!
- Nezahlcovat definice balastem!

Definice 2.2 (Soustava lineárních rovnic (SLR))

Soustavou m lineárních rovnic o n neznámých (s reálnými koeficienty) je soustava tvaru:

$$\begin{aligned}
a_{11}x_1 + \ldots + a_{1n} \cdot x_n &= b_1 \\
a_{21}x_2 + \ldots + a_{2n} \cdot x_n &= b_2 \\
\ldots\ldots + \ldots + \ldots \cdot \ldots = \ldots a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn} \cdot x_n &= b_m,
\end{aligned}$$

kde každý řádek je ve smyslu předchozí definice.

Definice 2.3 (Aritmetické vektory (nad $\mathbb{R}$))

Aritmetickým vektorem rozumíme uspořádanou n-tici reálných čísel. Zapisujeme ho jako:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$$

Definice 2.4 (Množina řešení SLR)

Množina řešení SLR ve smyslu definice výše je množina:

$$\left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n : a_i1x_1 + \ldots + a_{in}x_n = b_i \forall 1 \leq i \leq m \right\}$$

Definice 2.5 (Operace s (aritm.) vektory (n fixní))

$v, w \in \mathbb{R}^n \longrightarrow v + w$ sčítání po složkách
$t \in \mathbb{R} \longrightarrow t \cdot w$ násobení po složkách
$-v := (-1) \cdot v$
$v - w := v + (-w)$
$0 = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{R}^n$

Definice 2.6 (Elementární úpravy SLR)

Elementární úpravy dané SLR jsou:

1. Prohození pořadí 2 rovnic
2. Vynásobíme jednu rovnici číslem $t \in \mathbb{R} - \{0\}$
3. Přičteme t-násobek jedné rovnice ($t \in \mathbb{R}$) k jiné rovnici.

Tvrzení 2.1

Elementární úpravy jsou ekvivalentními úpravami.

Důkaz
Skripta □

Poznámka
1. lze nahradit kombinací druhých dvou.

Pozor
V přednášce jsou tvrzení (věty, lemmata, ...). Typicky mají strukturu: Pokud platí ...předpoklad..., pak platí ...závěr....

Definice 2.7 (Gaussova eliminace)

Algoritmus na úpravu matice do odstupňovaného tvaru za pomoci elementárních úprav.

Definice 2.8 (Pivot)

První nenulový prvek v řádku v odstupňovaném tvaru.

Pokud je pivot až ve „vektoru“?, SLR nemá řešení.

Počet pivotů je počet bázových proměnných, počet neznámých - počet pivotů je počet volných proměnných (neboli parametrů).

Definice 2.9 (Odstupňovaný tvar matice)

Matice $m \times n$ je v odstupňovaném tvaru, jestliže

$$\exists r \in \mathbb{N}, r < m, \text{ že řádky } r+1, \dots, m \text{ jsou nulové a}$$

$$k_1 < k_2 < \cdots < k_r, \text{ kde } k_i \text{ je index prvního nenulového prvku v } i\text{-tém řádku.}$$

Definice 2.10 (Hodnost matice)

Buď $A = (a_{ij})_{m \times n}$ matice. Potom $\text{rank}(A) = \text{r}(A)$ je tzv. hodnost matice, tedy počet nenulových řádků v odstupňovaném tvaru matice.

Pozor
Počet nenulových řádků v odstupňovaném tvaru nezáleží na volbě algoritmu, kterým jsme se do OT dostali.

Poznámka
$\text{rank}(A) \leq m$ a $\text{rank}(A) \leq n$

Poznámka (Geometrický význam)
Řádky popisují jednotlivé rovnice, netriviální rovnice má za množinu řešení nadrovinu v $\mathbb{R}^n$, řádky popisují proměnné, významově jsou lineárními kombinacemi.

3 Tělesa

Otázka: V jakých číselných oborech můžeme řešit soustavy lineárních rovnic?

Poznámka (Těleso budeme zavádět jako)
Uvažujme množinu „čísel“ $\mathbb{T}$ s binárními operacemi $+, \cdot$. $+, \cdot : \mathbb{T} \times \mathbb{T} \to \mathbb{T}$.

Pak $(\mathbb{T}, +, \cdot)$ je těleso, pokud splňuje:...

Poznámka (Co musí splňovat?)
Uvažujme množinu $\mathbb{T}$ s jednou binární operací $\triangle : \mathbb{T} \times \mathbb{T} \to \mathbb{T}$.

Budeme požadovat tyto vlastnosti:
(H1) $\forall a, b, c \in \mathbb{T} : (a \triangle b) \triangle c = a \triangle (b \triangle c)$ (Asociativita)
(H2) $\exists 0 \in \mathbb{T} \forall a \in \mathbb{T} : 0 \triangle a = a = a \triangle 0$ (Existence neutrálního prvku)
(H3) $\forall a \in \mathbb{T} \exists (-a) \in \mathbb{T} : a \triangle (-a) = 0 = (-a) \triangle a$ (Existence opačného / inverzního prvku)

Tvrzení 3.1

Ať $(\mathbb{T}, \triangle)$ *splňuje axiomy (H1), (H2), (H3). Pak pro každé* $a \in \mathbb{T}$ *je prvek* (-1) *z (H3) určen jednoznačně.*

Důkaz

Předpokládejme, že pro prvek $a \in \mathbb{T}$ existují prvky $b, c \in \mathbb{T}$ splňující:

$$a\triangle b = 0 = b\triangle a \wedge a\triangle c = 0 = c = c\triangle a$$

Pak:

$$(b\triangle a)\triangle c \overset{\text{(H1)}}{=} b\triangle(a\triangle c)$$

$$c \overset{\text{(H2)}}{=} 0\triangle c = b\triangle 0 \overset{\text{(H2)}}{=} b$$

$$b = c$$

□

Poznámka (Ještě často doplňujeme)
(H4) $\forall a, b \in \mathbb{T} : a\triangle b = b\triangle a$

Definice 3.1 (Těleso)

Tělesem (angl. field) rozumíme množinu $\mathbb{T}$ s binárními operacemi $+, \cdot : \mathbb{T} \times \mathbb{T} \to \mathbb{T}$, které splňují tyto axiomy:
(S1) $\forall a, b, c \in \mathbb{T} : (a + b) + c = a + (b + c)$
(S2) $\exists 0 \in \mathbb{T} \forall a \in \mathbb{T} : a + 0 = a$
(S3) $\forall a \in \mathbb{T} \exists (-a) \in \mathbb{T} : a + (-1) = 0$
(S4) $\forall a, b \in \mathbb{T} L a + b = b + a$
(N1) $\forall a, b, c \in \mathbb{T} : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
(N2) $\exists 1 \in \mathbb{T} : a \cdot 1 = a$
(N3) $\forall a \in \mathbb{T}, a \neq 0 \exists a^{-1} \in \mathbb{T} : a \cdot a^{-1} = 1$
(N4) $\forall a, b \in \mathbb{T} : a \cdot b = b \cdot a$
(D) $\forall a, b, c \in \mathbb{T} : (a + b) \cdot c = a \cdot c + b \cdot c$
($\neg$T) $|\mathbb{T}| > 1$ (jinými slovy $0 \neq 1$)

Například
$(\mathbb{R}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{C}, +, \cdot), (\{0, 1\}, XOR, AND)$

Tvrzení 3.2 (Další vlastnosti těles)

Je-li $a, b \in \mathbb{T}, a \neq 0$, *pak* $a \cdot x + b = 0$ *má v* $\mathbb{T}$ *právě jedno řešení* ($x = \frac{-b}{a}$).

$$\forall a \in \mathbb{T} : a \cdot 0 = 0 \ (a \cdot 0 + a \cdot 0 \overset{(D)}{=} a \cdot (0 + 0) \overset{(S2)}{=} a \cdot 0, \textit{ odečteme dvakrát pomocí (S2)})$$

$$a \cdot b = 0 \implies a = 0 \vee b = 0$$

$0 \neq 1$ *(Vezměme libovolné* $a \in \mathbb{T}$*. Kdyby* $0 = 1$*, pak* $0 = 0 \cdot a = 1 \cdot a = a$ *)*

Například
Buď $n > 2$ a $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$. Uvažujme násobení a dělení modulo. Potom $\mathbb{Z}_n$ splňuje všechny axiomy kromě (4N), které splňuje pokud n je prvočíslo.

Definice 3.2 (Charakteristika tělesa)

Nechť $\mathbb{T}$ je těleso, čísly $1, 2, 3, 4, \dots$ budeme značit součty $1, 1+1, 1+1+1, 1+1+1+1, \dots$. Charakteristikou tělesa budeme značit nejmenší číslo z $1, 2, 3, 4, \dots$, které je rovno 0. Pokud takové neexistuje je charakteristika rovna 0.

Například
Char. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ je 0. Char. $\mathbb{Z}_p$ je p.

Tvrzení 3.3

Je-li $\mathbb{T}$ *těleso, pak charakteristika* $\mathbb{T}$ *je buď 0 nebo prvočíslo.*

Důkaz (Sporem)
Předpokládejme, že char. $\mathbb{T}$ je $n \neq 0$ a n je složené číslo, tj. $n = k \cdot l$, $1 < k, l < n$. Všimněme si[a] $(1 + \dots + 1) = (1 + \dots + 1) \cdot (1 + \dots + 1)$ $(n = k \cdot l$ v $\mathbb{T})$. Z předpokladu $n = 0$ v $\mathbb{T}$, tak $0 = k \cdot l$ v $\mathbb{T}$, $k, l \neq 0$ a z vlastnosti těles . $\square$

[a] n, k a l jedniček.

3.1 Matice a operace s nimi

Definice 3.3 (Matice nad tělesem)

Matice typu $m \times n$ nad tělesem $\mathbb{T}$ je obdélníhové schéma prvků $\mathbb{T}$, m řádků, n sloupců.

Poznámka (Speciální případy)
$n = 1$ – sloupcový aritmetický vektor.

$m = 1$ – řádkový vektor.

Poznámka (Operace)
Podobně jako vektory lze matice sčítat a násobit prvkem z $\mathbb{T}$.

Věta 3.4 (Vlastnosti operace)

$$(A+B)+C = A+(B+C) \text{Má-li jedna strana smysl } (A, b, c \text{ stejného typu})$$
$$A+B = B+A, 0+A = A$$
$$(s+t)\cdot A = s\cdot A + t\cdot A, (s\cdot t)\cdot A = s\cdot(t\cdot A), s\cdot(A+B) = s\cdot A + s\cdot B$$

Definice 3.4 (Čtvercová matice)

Matice je čtvercová, pokud je typu $n \times n$, $n \geq 1$.

Například

Jednotková matice $\mathcal{I} = \begin{pmatrix} 1 & 0 & \dots \\ 0 & 1 & \dots \\ \vdots & \vdots & \ddots \end{pmatrix}$.

Trojúhelníkové matice (horní tj. $a_{ij} = 0 \forall i > j$ a dolní tj. $a_{ij} = 0 \forall j > i$).

Diagonální (horní a dolní trojúhelníková zároveň) $a_{ij} = 0 \forall j \neq i$.

Permutační tj. v každém řádku a v každém sloupci je právě jedna 1, jinak 0.

Definice 3.5 (Transponovaná matice)

Je-li $A = (a_{ij})_{m\times n}$, pak $A^T = (b_{ij})_{n\times m}$, kde $b_{ij} := a_{ji}$, je matice transponovaná.

Definice 3.6 (Symetrická matice)

Matice A je symetrická, pokud je čtvercová a $A = A^T$.

Definice 3.7 (Násobení matic)

Ať A, B jsou matice nad tělesem $\mathbb{T}$, $A = (a_{ij})_{m\times n}, B = (b_{jk})_{n\times p})$. Potom $AB = (\sum_{j=1}^{n} a_{ij} \cdot b_{jk})_{m\times p}$

Poznámka (Proč násobení matic)
Uvažujme SLR. Dá se zapsat jako $Ax = b$

Poznámka (Další pohledy na součin matic)
Sloupcový: sloupce výsledné matice jsou lineární kombinace sloupců první matice s koeficienty ze sloupců v druhé matici.

Řádkový pohled: totéž transponovaně.

Blokové násobení: můžeme násobit matice v maticích!

Pozor

$$AB \neq BA$$

$$(AB)C = A(BC)\text{Má-li jedna strana smysl.}$$

$$(A+B)C = AC + BC, C(E+F) = CE + CF$$

$$\mathcal{I}A = A = A\mathcal{I}$$

$$s \in \mathbb{T}, s(AB) = (aA)B = A(sB)$$

3.2 Matice jako zobrazení

Budeme se zabývat speciálním případem maticového násobení, kdy druhá matice má šířku 1 (je to sloupcový vektor).

Definice 3.8 (Zobrazení určené maticí)

Buď A pevně zvolená matice typu $m \times n$ nad T. Zobrazením určeným maticí A rozumíme $f_A : T^n \to T^m$, $x \to A \cdot x$

Příklad
Jak popsat zobrazení rotace $r : \mathbb{R}^2 \to \mathbb{R}^2$.

Řešení
Nejdříve vyzkoušíme na speciálních vektorech, např. vektorech tzv. kanonické báze $\mathbb{R}^2$: $e_1 = (10)^T, e_2 = (01)^T$:

$$r_\alpha(e_1) = (\cos\alpha \;\; \sin\alpha)^T$$

$$r_\alpha(e_2) = (-\sin\alpha \;\; \cos\alpha)^T$$

Následuje pozorování, že r_α je tzv. lineární zobrazení:

$$\forall v \in \mathbb{R}^2 \forall t \in \mathbb{R} : r_\alpha(t \cdot v) = t \cdot r_\alpha(v)$$

$$\forall u, v \in \mathbb{R}^2 : r_\alpha(u+v) = r_\alpha(u) + r_\alpha(v)$$

Je-li $u = (u_1, u_2)^T \in \mathbb{R}$ obecný vektor, pak $u = u_1 \cdot e_1 + u_2 \cdot e_2$. Tedy $r_\alpha(u) = u_1 \cdot r_\alpha(e_1) + u_2 \cdot r_\alpha(e_2) = u_1 \cdot (\cos\alpha \;\; \sin\alpha)^T + u_2 \cdot (-\sin\alpha \;\; \cos\alpha) = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} (u_1 u_2)^T$

Tvrzení 3.5 (Vlastnosti zobrazení určeného maticí)

Buď A matice $n \times m$ nad T, $f_A : T^n \to T^m$ jako výše, $x, y \in T^n, s \in T$. Pak platí

$$f_A(s \cdot x) = s \cdot f_A(x),$$

$$f_A(x + y) = f_A(x) + f_A(y)$$

Důkaz

$$f_A(s \cdot x) \overset{\text{DEF}}{=} A \cdot (s \cdot x) = x \cdot (A \cdot x) \overset{\text{DEF}}{=} s \cdot f_A(x)$$

$$f_A(x + y) \overset{\text{DEF}}{=} A \cdot (x + y) = A \cdot x + A \cdot y \overset{\text{DEF}}{=} f_A(x) + f_A(y)$$

□

Definice 3.9 (Prvky kanonické báze T^n)

Prvky kanonické báze T^n jsou vektory $e_i = (0 \dots 010 \dots 0)^T \in T^n, i \in \{1, \dots, n\}$.

Důsledek

$$f_A((x_1 \dots x_n)^T) = x_1 \cdot f_A(e_1) + \dots + x_n \cdot f_A(e_n) = (f_A(e_1)| \dots |f_A(e_n)) \cdot (x_1 \dots x_n)^T$$

Tedy pro A, B matice $m \times n$ nad T platí $(f_A = f_B) \Leftrightarrow (A = B)$.

Poznámka (Další pozorování)

Splňuje-li nějaké zobrazení $f : T^n \to T^m$ vlastnosti zobrazení daného maticí, pak je to zobrazení určené maticí.

Tvrzení 3.6 (Skládání zobrazení určených maticí)

Mějme zobrazení $f_A : T^n \to T^m$ a $f_B : T^p \to T^p$, dané maticemi A a B. Potom zobrazení $f_A \circ f_B$ je dáno maticí $A \times B$.

Důkaz

Totiž pro libovolné $x \in T^p$ platí

$$f_A \circ f_B(x) = f_A(f_B(x)) = f_A(B \cdot x) = A \cdot (B \cdot x) = (A \cdot B) \cdot x = f_{A \cdot B}(x)$$

□

Příklad
Složení otočení o úhly α a β.

3.3 Soustavy lineárních rovnic podruhé (oddíl 4.5.1, skripta)

Zvolme těleso T.

Poznámka (Vztah dvou řešení SLR)
$Ax = b$, $Ay = b$, potom
$$A(x - y) = Ax - ay = b - b = 0$$

Definice 3.10 (Homogenní SLR)

Soustava rovnic tvaru $A \cdot x = o$ se nazývá homogenní.

Poznámka
SLR budeme řešit tak, že najdeme jedno řešení (nebo zjistíme, že žádné neexistuje) a poté budeme hledat řešení homogenní SLR, čímž můžeme podle poznámky výše už jednoduše získat všechna řešení původní rovnice.

Definice 3.11 (Jádro / nulový prostor)

Je-li A matice typu $m \times n$, pak
$$\{v \in T^n : A \cdot v = 0\} \left(= f_A^{-1}(0) = \{v : v \text{řeší} A \cdot x = 0\}\right)$$
se nazývá jádrem (anglicky Kerner), nebo též nulovým prostorem, a značí se $\operatorname{Ker} A$.

Věta 3.7

Máme-li SLR $A \cdot x = b$ a známe-li jedno řešení $v \in T^n$, pak množina všech řešení je tvaru $v + \operatorname{Ker} A := \{v + w : w \in \operatorname{Ker} A\}$.

Důkaz
Označme $S = \{u \in T^n : A \cdot u = b\}$. Chceme ukázat $S = \{v + w : w \in \operatorname{Ker} A\}$.

$S \subseteq v + \operatorname{Ker} A$: Vezměme libovolné $u \in S$, tj. $A \cdot u = b$. Pak $A \cdot (u - v) = 0$ (poznámka výše), $w := u - v \in \operatorname{Ker} A$, tj. $u = vv + w \in v + \operatorname{Ker} A$.

$v + \operatorname{Ker} A \subseteq S$: Vezměme libovolné $u \in v + \operatorname{Ker} A$, tj. $u = v + w, w \in \operatorname{Ker} A$. Pak $A \cdot u = A \cdot (v + w) = A \cdot v + A \cdot w = b + 0 = b$, tj. $u \in S$. $\square$

Příklad
Ukazovalo se jedno řešení SLR pomocí jádra. Jádro má tu výhodu, že má bázi (vektory s 1 v jedné proměnné a nulami jinde).

Definice 3.12 (Elementární matice)

SKRIPTA oddíl 4.2.3

3.4 Inverzní matice

Poznámka (Motivace)

$$A \cdot x = b \to x = A^{-1} \cdot b$$

Inverzní zobrazení (tedy f_A musí být prosté / na / bijekce).

Definice 3.13

Buď A matice typu $m \times n$ nad T. Pak:

- A je zprava invertovatelná, pokud $\exists X \in T^{n \times m} : A \cdot X = I_m$.
- A je zleva invertovatelná, pokud $\exists Y \in T^{n \times m} : Y \cdot A = I_n$.
- A je invertovatelná, pokud $n = m$ a existuje $X \in T^{n \times n} : A \cdot X = I_n = X \cdot A$.

Poznámka
V posledním případě značíme $X = A^{-1}$ a jednoduše se dokáže, že existuje nejvýše jedna A^{-1}.

Tvrzení 3.8 ((T4.67))

Buď A matice typu $m \times n$ nad T. Potom následující je ekvivalentní:

a) *A je zprava invertovatelná.*

b) *$f_A : T^n \to T^m$ je na.*

c) *Matice C, kterou dostaneme z A Gaussovou eliminací, má všechny řádky nenulové.*

d) $\operatorname{rank}(A) = m$

Důkaz
1 $\implies$ 2: Předpoklad $\exists X : A \cdot X = I_m$. Vezměme $b \in T^m$, pak $A(X \cdot b) = (AX)b = I_m \cdot b = b$

2 $\implies$ 3: Předpoklad f_A je na ($Ax = b$ má řešení $\forall b$). Kdyby C měla nulový i-tý řádek, pak $C \cdot x = e_i$ nemá řešení $\implies$ $Ax = e_i$ nemá řešení, .

3 $\implies$ 1: Předpokládáme (3). Hledáme X: $A \cdot X = I_m$, čili $A \cdot (x_1 | \dots | x_m) = (e_1 | \dots | e_m)$, čili řešíme SLR. SLR upravíme $(A|e_j) \sim \dots \sim (C|d_j) \implies C \cdot x_j = d_j$ má podle (3) řešení. □

Důsledek
Pokud je $A \in T^{m \times n}$ invertovatelná zprava, pak $n \geq \operatorname{rank} A = m$.

Pokud je navíc čtvercová, pak $(A|I_n) \sim \dots \sim (I_n|A^{-1})$, tedy A je invertovatelná.

Tvrzení 3.9 (Čtvercové matice a inverze)

Buď A čtvercová matice řádu n nad T. Pak následující je ekvivalentní: A je invertovatelná zprava, A je invertovatelná zleva, A je invertovatelná.

Důkaz
(1 $\implies$ 3): Viz důsledek výše.

(3 $\implies$ 2): Triviální.

(2 $\implies$ 1): Transpozice. (1 $\implies$ 3). A transpozice znovu. □

Poznámka (Jak najdeme inveri zleva)
Matici transponujeme a hledáme inverzi z prava. Nebo použijeme EŘÚ podobně jako u čtvercových.

Tvrzení 3.10 ((4.70))

Buď A matice typu $m \times n$ nad $\mathbf{T}$. pak NPJE (následující podmínky jsou ekvivalentní):

1 A je invertovatelná zleva,

2 $f_A : \mathbf{T}^n \to \mathbf{T}^m$ je prosté,

3 $Ax = 0$ má právě jedno řešení $x = 0$,

4 Matice C vzniklá z A Gaussovou eliminací má všechny sloupce bázové,

5 $\operatorname{rank}(A) = n$.

Důkaz
(1 $\implies$ 2): Předpoklad: $\exists Y : Y \cdot A = I_n$. Vezměme $x, y \in \mathbf{T}^n$ takové, že $f_A(x) = f_A(y)$. Vynásobíme Y zleva: $x = y$.

(2 $\implies$ 3): (3) je speciální případ (2).

(3 $\implies$ 4): Předpokládejme, že neplatí (4). Pak dostáváme více řešení $Ax = Cx = 0$ (pokud je i-tý sloupec nulový, pak za i-tou proměnnou lze dosadit cokoliv).

(4 $\implies$ 1(5)) C má čtvercovou „podmatici" řádu n, můžeme doupravovat tak, aby podmaticí C byla I_n. Součin elementárních matic měnících A na I_n je inverze zleva (s několika řádky navíc, je to přesně postup na hledání inverze zleva).

(5 $\implies$ 4) Necháno na rozmyšlení. □

3.5 Regulární matice

Definice 3.14 (Regulární matice)

Matice A nad $\mathbf{T}$ je regulární, pokud $f_A : \mathbf{T}^n \to \mathbf{T}^m$ je bijekce.

Věta 3.11 (V4.81 (+ T4.88))

10 (+1) ekvivalentních podmínek pro Regulární matice, viz skripta.

3.6 Inverzní matice k horním a dolním trojúhelníkovým maticím

Tvrzení 3.12 (T4.98)

Buď A dolní trojúhelníková matice (tj. čtvercová) s nenulovými prvky na diagonále. Pak A je regulární a A^{-1} je dolní trojúhelníková. Měla-li na diagonále samé 1, pak A^{-1}, pak A^{-1} je má také. Podobně pro horní trojúhelníkové rovnice.

4 Vektorové prostory

4.1 definice

Definice 4.1 (Vektorový prostor)

Buď $\mathbb{T}$ těleso. Vektorový prostor nad tělesem $\mathbb{T}$ je množina $\mathbf{V}$ (množina vektorů) s operací sčítání na $\mathbf{V}$ ($\mathbf{V} \times \mathbf{V} \to \mathbf{V}$) a operací násobení skalárem ($\mathbb{T} \times \mathbf{V} \to \mathbf{V}$), které splňují tyto axiomy:

vS1 $\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbf{V} : (\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$,

vS2 $\exists \mathbf{o} \in \mathbf{V} \forall \mathbf{v} \in \mathbf{V} : \mathbf{o} + \mathbf{v} = v$,

vS3 $\forall \mathbf{v} \in \mathbf{V} \exists (-\mathbf{v}) \in \mathbf{V} : \mathbf{v} + (-\mathbf{v}) = \mathbf{o}$,

vS4 $\forall \mathbf{u}, \mathbf{v} \in \mathbf{V} : \mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$,

vN1 $\forall a, b \in \mathbb{T} \forall \mathbf{v} \in \mathbf{V} : (a \cdot b) \cdot \mathbf{c} = a \cdot (b \cdot \mathbf{v})$,

vN2 $\forall \mathbf{v} \in \mathbf{V} : 1 \cdot \mathbf{v} = \mathbf{v}$,

vD1 $\forall a, b \in \mathbb{T} \forall \mathbf{v} \in \mathbf{V} : (a + b) \cdot \mathbf{v} = a \cdot \mathbf{v} + b \cdot \mathbf{v}$,

vD2 $\forall a \in \mathbb{T} \forall \mathbf{u}, \mathbf{v} \in \mathbf{V} : a \cdot (\mathbf{u} + \mathbf{v}) = a \cdot \mathbf{u} + a \cdot \mathbf{v}$.

Například
$\mathbb{T}$ těleso, $n \geq 0$, $\mathbf{V} = \mathbb{T}^n$ s běžnými operacemi na aritmetických vektorech tvoří vektorový prostor.

$\mathbb{T}$ těleso, $\mathbf{V} = \left\{(x, y, z)^T \in \mathbb{T}^3 : x + y + z = 0\right\} \subseteq \mathbb{T}^3$. Operace z $\mathbb{T}^3$ zúžené na $\mathbf{V}$.

Tvrzení 4.1 (Vlastnosti vektorových prostorů)

- *Nulový vektor je určen jednoznačně.*
- *Opačný vektor je určen jednoznačně.*
- *Vektorový prostor nikdy není prázdný, ale existuje tzv. nulový vektorový prostor.*
- *Pro* $\mathbf{v} \in \mathbf{V} : 0 \cdot \mathbf{v} = \mathbf{o}$.

Definice 4.2 (Vektorový podprostor)

Buď $\mathbb{T}$ těleso a $\mathbf{V}$ vektorový prostor nad $\mathbb{T}$. Podprostorem rozumíme množinu $\mathbb{U} \subseteq \mathbb{V}$ takovou, že operace lze zúžit na $\mathbf{U}$ a $\mathbf{U}$ s těmito operacemi tvoří samo V. P. nad $\mathbb{T}$.

Tvrzení 4.2 (T5.12)

Vezměme $\mathbb{T}$ *a* $\mathbf{V}$ *jako výše. Pak* $\mathbf{U} \subseteq \mathbf{V}$ *tvoří podprostor právě tehdy, když je uzavřený na sčítání a násobení skalárem.*

Poznámka
Prostor $\mathbf{U}$ je podprostorem $\mathbf{V}$ značíme $\mathbf{U} \leq \mathbf{V}$.

Nulový vektorový prostor a prostor sám sobě je podprostorem (tzv. triviální nebo nevlastní podprostory).

Například
Prostor všech polynomů stupně n je podprostor všech polynomů stupně $n+1$ je podprostor všech polynomů.

Prostor všech spojitých funkcí (spolu s bodovým sčítáním a násobením konstantou, $\mathbb{R}^2 \to \mathbb{R}$) je podprostorem všech zobrazení nad $\mathbb{R}$. Prostor polynomiálních funkcí je podprostorem spojitých funkcí…

$\mathbb{R} \leq \mathbb{C}$ se sčítáním na $\mathbb{C}$ a násobením zúženým na $\mathbb{R} \times \mathbb{C} \to \mathbb{C}$.

Definice 4.3

Buď $\mathbf{V}$ vektorový prostor nad $\mathbb{T}$. Vezměme $\mathbf{v}_1, \ldots, \mathbf{v}_k \in \mathbf{V}$, $t_1, \ldots, t_k \in \mathbb{T}$. Pak vektor

$$t_1 \cdot \mathbf{v} + \ldots + t_k \cdot \mathbf{v}_k$$

se nazývá lineární kombinace vektorů $\mathbf{v}_1, \ldots, \mathbf{v}_k$ (s koeficienty $t_1, \ldots, t_k$).

Definice 4.4

Buď $\mathbf{V}$ V.P. nad $\mathbb{T}$, vezměme $X \subseteq \mathbf{V}$. Pak

$$\mathrm{LO}\, X = \{t_1 \cdot \mathbf{v}_1 + \ldots + t_k \cdot \mathbf{v}_k : k \in \mathbb{N}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k \in X, t_1, \ldots, t_k \in T\} \subseteq \mathbf{V}$$

se nazývá lineární obal X (v prostoru $\mathbf{V}$).

Tvrzení 4.3

Buď $x \subseteq \mathbf{V}$. *Pak* $\mathrm{LO}\, X \leq \mathbf{V}$.

Definice 4.5

Buď $\mathbf{V}$ vektorový prostor nad $\mathbb{T}$ a $X \in \mathbf{V}$. pak řekneme, že X generuje $\mathbf{V}$ (X je množina generátorů $\mathbf{V}$), pokud $\mathrm{LO}\, X = \mathbf{V}$

4.2 Maticové VP

Pozor (MIDTERMY)
Budou! První bude 24. 11. 2020. Druhý 15. 12. 2020.

Definice 4.6 (S maticí A jsou spojeny 4 vektorové prostory)

Jádro: $\ker A$.

Jádro transponované: $\ker A^T$.

Obraz (= LO sloupců = sloupcový prostor matice): $\Im A$.

Obraz transponované (= LO řádků = řádkový prostor matice): $\Im A^T$.

Poznámka
Sloupcové úpravy nemění obraz, řádkové nemění jádro (u transponovaných opačně).

Tvrzení 4.4 (Prostory spojené s maticí a elementární úpravy)

A typu $m \times n$ nad $\mathbf{T}$. Posloupnost EŘÚ $A \sim \ldots \sim RA$. Posloupnost sloupcových úprav $A \sim \ldots \sim AQ$.

$$\ker A = \ker RA$$

Důkaz
f_R je lineární a bijekce, tedy zobrazuje nulu na nulu. Tedy $Ax = 0 \implies f_R(Ax) = 0$. Opačně $RAx = 0 \implies f_R^{-1}(RAx) = Ax = 0$. □

$$\Im AQ = \Im A$$

Důkaz
f_Q je bijekce, tedy $\exists \mathbf{x} : A\mathbf{x} = \mathbf{y} \implies AQ(Q^-1\mathbf{x}) = \mathbf{y} \implies \mathbf{y} \in \Im(AQ)$ a $\exists \mathbf{x} : AQ\mathbf{x} = \mathbf{y} \implies A(Q\mathbf{x}) = \mathbf{y} \implies \mathbf{y} \in \Im(A)$ □

$$(A = (\mathbf{a}_1 | \ldots | \mathbf{a}_n))$$
$$\Im RA = \mathrm{LO}\, R\mathbf{a}_1, \ldots, R\mathbf{a}_n$$

Důkaz
Přímo z maticového násobení. $RA\mathbf{x} = R\mathbf{a}_1 x_1 + \ldots + R\mathbf{a}_n x_n$ □

4.3 Lineární (ne)závislost

Definice 4.7 (Lineární (ne)závislost)

Buď $\mathbf{V}$ vektorový prostor nad $\mathbb{T}$ a $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ posloupnost vektorů z $\mathbf{V}$. Řekněme, že posloupnost vektorů je lineárně nezávislá, pokud žádný vektor $\mathbf{v}_i$ z posloupnosti nelze vyjádřit jako lineární kombinaci zbývajících. Tj. neplatí:

$$\mathbf{v}_i = t_1\mathbf{v}_1 + \ldots + t_{i-1}\mathbf{v}_{i-1} + t_{i+1}\mathbf{v}_{i+1} + \ldots + t_k\mathbf{v}_k$$

pro žádné $1 \leq i \leq k$ a žádná $t_i \in T$. Ekvivalentně lze psát

$$\forall 1 \leq i \leq k : v_i \notin \mathrm{LO}\left\{\mathbf{v}_1 + \ldots + \mathbf{v}_{i-1} + \mathbf{v}_{i+1} + \ldots + \mathbf{v}_k\right\}$$

V opačném případě je posloupnost lineárně závislá.

Poznámka
Lineární (ne)závislost se nezmění permutací posloupnosti.

Definice 4.8 (Zkratky)

LN = lineárně nezávislá, LZ = lineárně závislá.

Například
$k = 0$ je posloupnost LN. $k = 1$ je posloupnost vždy LN, pokud není nulovým vektorem. $k = 2$ je posloupnost LZ právě tehdy, když je jeden vektor násobkem druhého.

Podposloupnost LN posloupnosti je LN.

Posloupnost je vždy LZ, pokud je nějaký vektor nulový, nebo pokud se dva vektory rovnají, ale LZ je v mnoha dalších případech.

Tvrzení 4.5

$\mathbf{V}$ *vektorový prostor nad* $\mathbb{T}$, $()$ *posloupnost vektorů z* $\mathbf{V}$. *Pak NPJE:*

- $()$ *je LN.*
- $\forall 1 \leq i \leq k : \mathbf{v}_i \notin \mathrm{LO}\left\{\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}\right\}$
- $\mathbf{v}_1 \cdot t_1 + \ldots + \mathbf{v}_k \cdot t_k = 0$ *pouze triviálně (pro všechna* t_i *nulová).*
- *Máme-li* $\mathbf{b} \in \mathbf{V}$, *pak existuje nejvýše 1* k*-tice* $(t_1, \ldots, t_k)$ *prvků* $\mathbb{T}$ *taková, že*

$$\mathbf{b} = t_1 \cdot \mathbf{v}_1 + \ldots + t_k \cdot \mathbf{v}_k.$$

Důkaz
(1) $\implies$ (2) : Triviální.

(2) $\implies$ (3) : Předpokládejme negaci (3), tj. máme vyjádření $\mathbf{o} = t_1 \cdot \mathbf{v}_1 + \ldots + t_k \cdot \mathbf{v}_k$ takové, že $t_i \neq 0$ pro nějaké $1 \leq i \leq k$. Zvolíme největší takové i, tj. $\mathbf{o} = t_1 \cdot \mathbf{v}_1 + \ldots + t_i \cdot \mathbf{v}_i \implies v_i = (-t_i^{-1} t_1) \cdot \mathbf{v}_1 + \ldots + (-t_i^{-1} t_{i-1}) \cdot \mathbf{v}_{i-1} \implies$ negace (2).

(3) $\implies$ (4) : Předpokládejme negaci (4) 2 vyjádření b následně od sebe odečteme a dostaneme negaci (3).

(4) $\implies$ (3) : Speciální případ.

(3) $\implies$ (1) : Předpokládejme $\neg$(1), tj. posloupnost je LZ, tj. existuje $1 \leq i \leq k$, tak že $\mathbf{v}_i$ lze vyjádřit za pomoci lineární kombinace ostatních vektorů. Odečteme $\mathbf{v}_i$ a hned dostáváme netriviální LK rovnou 0, jelikož $t_i = -1$. $\square$

Tvrzení 4.6

Vezměme matici $A = (a_1| \ldots |a_n)$ typu $m \times n$ nad T. Buď R regulární matice řádu m a Q regulární matice řádu n. Pak NTJE: a) sloupce A jsou LN, b) sloupce $R \cdot A$ jsou LN, c) sloupce $A \cdot Q$ jsou LN.

Tvrzení 4.7

Buď A matice typu $m \times n$. Pak řádky A jsou LN, právě když matice C, která vznikne Gaussovou eliminací z A, má všechny řádky nenulové.

4.4 Báze, dimenze

Definice 4.9 (Báze)

$\mathbf{V}$ vektorový prostor nad $\mathbb{T}$. Pak posloupnost vektorů je báze $\mathbf{V}$, pokud je lineárně nezávislá a její lineární obal je $\mathbf{V}$.

Důsledek
Posloupnost vektorů je báze $\mathbf{V}$ právě tehdy, když každý vektor z $\mathbf{V}$ lze vyjádřit jako právě jednu lineární kombinaci této posloupnosti.

Definice 4.10 (Kanonická báze)

$\mathbb{T}$ těleso, $\mathbf{V} = \mathbb{T}^n (n \geq 1)$. Pak posloupnost vektorů $(e_1, e_2, \ldots, e_n)$ je báze $\mathbf{V}$.

Tvrzení 4.8

$\mathbf{V}$ *VP nad* $\mathbb{T}$*, pak minimální posloupnost generátorů je báze* $\mathbf{V}$*.*

Důkaz
Přímo z definice. □

Definice 4.11 (Konečně generovaný VP)

Vektorový prostor $\mathbf{V}$ nad tělesem $\mathbb{T}$ je konečně generovaný, pokud existuje $X \subseteq \mathbf{V}$ konečná taková, že $\mathbf{V} = \mathrm{LO}(X)$.

Například
$\mathbb{T}$ těleso, $n \geq 1$, $\mathbf{V} = T^n$ je konečně generovaný (kanonická báze). $\mathbb{T} = \mathbb{R}$, $\mathbf{V} = \mathbb{R}^\omega = \{(a_1, a_2, \ldots) : a_1, a_2, \ldots \in \mathbb{R}\}$ není konečně generovaný.

Tvrzení 4.9

$\mathbf{V}$ *vektorový prostor nad* $\mathbb{T}$*,() je posloupnost generátorů, která je minimální, pak () je báze* $\mathbf{V}$*.*

Důsledek
Z každé konečné posloupnosti, která generuje $\mathbf{V}$ lze vybrat bázi $\mathbf{V}$.

Speciálně platí, že každý konečně generovaný vektorový prostor má bázi.

Věta 4.10 (Steinitzova věta o výměně (5.60))

Buď $\mathbf{V}$ *vektorový prostor nad tělesem* $\mathbb{T}$*. Mějme* $N = (\mathbf{v}_1, \ldots, \mathbf{v}_k)$ *LN posloupnost vektorů* $\mathbf{V}$*,* $G = (\mathbf{w}_1, \ldots, \mathbf{w}_l)$ *generující posloupnost vektorů. Pak* $k \leq l$ *a navíc můžeme* G *přeuspořádat tak, aby po zaměnění prvních* k *prvků prvky z* N *stále generovala* $\mathbf{V}$*.*

Důkaz (Indukcí podle k)
Pro $k = 0$ je závěr věty triviální. Předpokládejme, že závěr věty platí pro LN posloupnost délky $k - 1$, kde $k \geq 1$. Použijeme tento indukční předpoklad na $N' := (\mathbf{v}_1, \ldots, \mathbf{v}_{k-1})$ a G. Tj. víme, že $k - 1 \leq l$ a můžeme přeuspořádat G na G'. Lineární obal G' s vyměněnými prvky za N', značme B, generuje $\mathbf{V}$, tedy speciálně v_k lze vyjádřit jako lineární kombinaci prvků B. Ale nedá se vyjádřit pomocí N', tedy $k - 1 < l$, a tudíž $k \leq l$. Zároveň mohu upravit vyjádření této lineární kombinace, aby byl nějaký prvek z B„ $\cap$ “G' vyjádřen za pomoci v_k a zbytku B. Takže je mohu vyměnit. □

Důsledek
V konečně generovaném VP mají všechny báze stejný počet prvků.

Definice 4.12

Dimenzí konečně generovaného VP $\mathbf{V}$ nad $\mathbb{T}$ rozumíme # prvků libovolné báze $\mathbf{V}$. Značíme $\dim(\mathbf{V})$.

Důsledek
$\mathbf{V}$ konečně generovaný VP a B je maximální LN posloupnost. Pak B je báze.

Obecněji, je-li G generující a N LN, pak lze N doplnit prvky G na bázi $\mathbf{V}$.

Tvrzení 4.11

Buď $\mathbf{V}$ konečně generovaný VP a $\mathbf{W}$ jeho podprostor. Pak

$$\dim(\mathbf{W}) \leq \dim(\mathbf{V}),$$

$$\dim(\mathbf{W}) = \dim(\mathbf{V}) \Leftrightarrow \mathbf{V} = \mathbf{W}$$

Důkaz
Krok 1: Ukážeme, že $\mathbf{W}$ je konečně generovaný vektorový prostor. Označme $n := \dim(\mathbf{V})$. Sporem $\dim(\mathbf{W}) < \omega_0$: předpokládejme, že $\mathbf{W}$ není konečně generovaný, tj. můžeme indukcí volit posloupnost vektorů z $\mathbf{W}$, $w_1, w_2, \ldots$, takovou, že $\forall i \geq 1 : w_i \notin \mathrm{LO}\{w_1, \ldots, w_{i-1}\}$ $(\leq \mathbf{W}, \neq \mathbf{W})$. Z T5.36 je $w_1, \ldots, w_n, w_{n+1}$ LN ve $\mathbf{W}$, tedy i ve $\mathbf{V}$, což je spor s tím, že $\dim(\mathbf{V}) = n$ (pozorování 5.67).

Krok 2: Argument z kroku 1 ukazoval, že posloupnost $(w_1, \ldots, w_k)$ z $\mathbf{W}$, která je LN ve $\mathbf{W}$, je LN i ve $\check{\mathbf{E}}$, tedy $k \leq \dim(\mathbf{V}) \implies \dim(\mathbf{W}) \leq \dim(\mathbf{V}) \wedge (\dim(\mathbf{W}) = \dim(\mathbf{V}) \implies \mathbf{V} = \mathbf{W})$. Poslední implikace druhým směrem je triviální (totožné prostory mají totožnou dimenzi). $\square$

4.5 Báze jako souřadnicový systém

Definice 4.13

Buď $\mathbf{V}$ VP nad tělesem $\mathbb{T}$, $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ báze $\mathbf{V}$, $\mathbf{v} \in \mathbf{V}$. Pak Souřadnicové (též vyjádření) vektoru $\mathbf{v}$ vzhledem k B je aritmetický vektor

$$[\mathbf{v}]_B = (a_1, a_2, \ldots, a_n)^T \in T^n$$

takový, že $\mathbf{v} = a_1 \cdot \mathbf{v}_1 + a_2 \cdot \mathbf{v}_2 + \ldots + a_n \cdot \mathbf{v}_n$. (Vizte pozorování 5.48 pro jednoznačnost.)

Tvrzení 4.12

Buď $\mathbf{V}$ VP nad $\mathbb{T}$ s bází B. Pak platí: a) $\forall \mathbf{v}, \mathbf{w} \in \mathbf{V} : [\mathbf{v} + \mathbf{w}]_B = [\mathbf{v}]_B + [\mathbf{w}]_B$ a b) $\forall \mathbf{v} \in \mathbf{V}, t \in \mathbb{T} : [t \cdot \mathbf{v}]_B = t \cdot [v]_B$.

Poznámka
V situaci T5.75 máme bijekci $f(\mathbf{v}) = [\mathbf{v}]_B$, která respektuje operace na VP, tzn. izomorfismus VP (tj. každý konečně generovaný VP je izomorfní aritmetickému).

Tvrzení 4.13 (Matice přechodu)

Mějme $\mathbf{V}$*, VP nad* $\mathbb{T}$*, s bázemi* $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ *a* $C = (\mathbf{w}_1, \dots, \mathbf{w}_n)$*. Potom existuje čtvercová matice* $[id]_C^B$ *řádu* n *taková, že*

$$\forall \mathbf{v} \in \mathbf{V} : [\mathbf{v}]_C = [id]_C^B \cdot [\mathbf{v}]_B.$$

Tuto matici nazýváme matice přechodu od báze B *k bázi* C*.*

Definice 4.14 (Matice přechodu (D5.78 + T5.79))

Matice z předchozího tvrzení je rovna

$$[id]_C^B = ([\mathbf{v}_1]_C | \dots | [\mathbf{v}_n]_C) \in \mathbb{T}^{n \times n}.$$

4.6 Hodnost a bázové sloupce matice podruhé

Tvrzení 4.14

Je-li $C = (c_1, \dots, c_n)$ *matice typu* $m \times n$ *nad* $\mathbb{T}$ *v odstupňovaném tvaru, pak* k*-tý sloupce* C_k *je bázový, právě když*

$$C_k \notin \mathrm{LO}\, c_1, \dots, c_{k-1}.$$

Důkaz
Pokud $k = k_i$ je bázový, pak má v i-tém řádku $\neq 0$ prvek, ale $c_1, c_2, \dots, c_{k-1}$ tam mají 0. Speciálně $c_{k_i} \notin \mathrm{LO}\,\{c_1, \dots c_{k_i - 1}\}$.

Naopak buď c_k nebázový, tj. $k_i < k < k_{i+1}$ (nebo $k < k_1$ nebo $k > k_2$). Všimněme si, že SLR odpovídající hledání lineární kombinace $c_1, c_2, \dots, c_{k-1}$ tak, aby byla rovna c_k, nemá pivot v posledním sloupci, tedy má řešení. □

Tvrzení 4.15

Buď A *libovolná matice typu* $m \times n$ *nad* $\mathbb{T}$*, buď* R *regulární matice řádu* m*, položme* $B = R \cdot A$*. Označme*

$$A = (a_1 | \dots | a_n), B = (b_1 | \dots | b_n).$$

Pak $\forall 1 \leq k \leq n$ *platí:*

$$a_k \in \mathrm{LO}\,\{a_1, \dots, a_{k-1}\} \Leftrightarrow b_k \in \mathrm{LO}\,\{b_1, \dots, b_{k-1}\}.$$

Důkaz
Přes asociativitu maticového násobení. $\square$

Důsledek
Buď A matice typu $m \times n$ nad T. Pak platí: a) k-tý sloupec A je bázový $\Leftrightarrow$ $a_k \notin \mathrm{LO}\{a_1, \ldots, a_{k-1}\}$ a b) $\mathrm{rank}(A) = \dim(\Im(A))$.

Poznámka (Pozorování)
Bázové sloupce matice A tvoří bázi $\Im(A)$.

Důkaz
Víme totiž, že bázové sloupce jsou lineárně nezávislé, jelikož nejdou vyjádřit jako lineární kombinace předchozích. Indukcí podle n se dá ukázat, že $\Im(A) = \mathrm{LO}\{\text{bázových vektorů}\}$
$\square$

Poznámka (Pozorování)
Hodnost matice A se nezmění řádkovými ani sloupcovými úpravami. Tj (a typu $m \times n$ nad $\mathbb{T}$, R regulární řádu m, Q regulární řádu n): $\mathrm{rank}(R \cdot A) = \mathrm{rank}(A) = \mathrm{rank}(A \cdot Q)$.

Důkaz
Použije se T5.86 (bázové sloupce zůstanou bázovými) a T5.32 ($\Im(A) = \Im(A \cdot Q)$). $\square$

Věta 4.16

(5.88) A matice typu $m \times n$ nad $\mathbb{T}$. Pak $\mathrm{rank}(A) = \mathrm{rank}(A^T)$.

Důkaz
Nechť $C = R \cdot A$ je odstupňovaný tvar.

$$\mathrm{rank}(A) = \mathrm{rank}(R \cdot A) = \mathrm{rank}(C) = \#\text{bázových sloupců} =$$

$$= \#\text{bázových řádků} = \mathrm{rank}(C^T) = \mathrm{rank}(A^T \cdot R^T) = \mathrm{rank}(A^T).$$

$\square$

Tvrzení 4.17

Buď A typu $m \times n$ a B typu $n \times p$. Pak $\mathrm{rank}(A \cdot B) \leq \min\{\mathrm{rank}(A), \mathrm{rank}(B)\}$.

Důkaz
Slupce $A \cdot B$ jsou lineární kombinace sloupců $A \implies \Im(A \cdot B) \leq \Im(A) \implies \mathrm{rank}(A \cdot B) \leq \mathrm{rank}(A)$. Dále totéž pro transponovaný součin: $\mathrm{rank}(A \cdot B) \leq \mathrm{rank}(B)$. $\square$

Poznámka
Ani v případě rovnosti $A = B$ nemusí nastat rovnost nerovnosti výše.

Poznámka (Pozorování 5.94 (variace na 4.81 – charakterizace regulárních matic))
Buď A čtvercová matice řádu n. Pak NPJE: a) A regulární, b) $\text{rank}(A) = n$, c) sloupce A jsou LN, d) sloupce A tvoří bázi T^n, e) sloupce generují T^n, c), d) a e) znovu pro řádky.

4.7 Gaussova-jordanova eliminace

Definice 4.15 (Redukovaný odstupňovaný tvar)

Matice A typu $m \times n$ nad $\mathbb{T}$ je v redukovaném (řádkově) odstupňovaném tvaru, pokud A je v odstupňovaném tvaru a navíc bázové sloupce A jsou kanonickými bázovými vektory.

Poznámka (Pozorování)
Každou matici můžeme pomocí EŘÚ dostat do redukovaného odstupňovaného tvaru. Postup se nazývá Gaussova-Jordanova eliminace.

Definice 4.16 (Skeletní rozklad matice)

Buď A typu $m \times n$ nad $\mathbb{T}$, $r := \text{rank}(A)$. Skeletní rozklad A je libovolné vyjádření $A = B \cdot C$, kde B je typu $m \times r$ a C je typu $r \times n$.

Věta 4.18 (Jakási ze skript)

Říká, jak počítat skeletní rozklad pomocí G-J eliminace.

4.8 SLR

Věta 4.19 (Frobeniova)

SLR $A \cdot \mathbf{x} = \mathbf{b}$ *je řešitelná, právě když* $\text{rank}(A) = \text{rank}(A|\mathbf{b})$.

Důkaz
$\text{rank}(A) = \text{rank}(A|\mathbf{b}) \Leftrightarrow b$ není bázový sloupec $(A|\mathbf{b}) \Leftrightarrow \mathbf{b} \in \Im(A) \Leftrightarrow A \cdot \mathbf{x} = \mathbf{b}$ má řešení. $\square$

Věta 4.20

Buď A matice typu $m \times n$ nad $\mathbb{T}$. Pak

$$\dim(\text{Ker}(A)) + \dim(\Im(A)) = n,$$

$$\dim(\text{Ker}(A^T)) + \dim(\Im(A^T)) = m.$$

Důkaz
Z algoritmu pro řešení SLR $A \cdot \mathbf{x} = 0$ víme, že # parametrů řešení $= n -$ # Bázových sloupců $= n - \text{rank}(A) = n - \dim(\Im(A))$. Navíc # parametrů řešení = # volných proměnných $= \dim(\text{Ker}(A))$ □

4.9 Průnik a součet podprostorů

Definice 4.17

Viz informatická lingebra.

Věta 4.21

Buď $\mathbf{W}$ *vektorový prostor a* $\mathbf{U}, \mathbf{V} \leq \mathbf{W}$*. Pak*

$$\dim(\mathbf{U}) + \dim(\mathbf{V}) = \dim(\mathbf{U} \cap \mathbf{V}) + \dim(\mathbf{U} + \mathbf{V}).$$

Důkaz
Prostor $\mathbf{U} \cap \mathbf{V}$ ($\leq \mathbf{W}$) má nějakou bázi $B = (\mathbf{w}_1, \ldots, \mathbf{w}_k)$ ($k = \dim(\mathbf{U} \cap \mathbf{V})$). B je LN v $\mathbf{U}$, tedy B můžeme rozšířit na bázi $C = (\mathbf{w}_1, \ldots, \mathbf{w}_k, \mathbf{u}_1, \ldots, \mathbf{u}_l)$ prostoru $\mathbf{U}$, tj. $\dim(\mathbf{U}) = k + l$, stejně tak můžeme B rozšířit na bázi $D = (\mathbf{w}_1, \ldots, \mathbf{w}_k, \mathbf{v}_1, \ldots, \mathbf{v}_m)$ prostoru $\mathbf{V}$, rj. $\dim(\mathbf{V}) = k + m$. Položíme $E = (\mathbf{w}_1, \ldots, \mathbf{w}_k, \mathbf{u}_1, \ldots, \mathbf{u}_l, \mathbf{v}_1, \ldots, \mathbf{v}_m)$. Stačí dokázat, že E je báze $\mathbf{U} + \mathbf{V}$ (pak totiž $\dim(\mathbf{U} + \mathbf{V}) = k + l + m = \dim(\mathbf{U}) + \dim(\mathbf{V}) - \dim(\mathbf{U} \cap \mathbf{V})$).

LO $\{\mathbf{w}_1, \ldots, \mathbf{w}_k, \mathbf{u}_1, \ldots, \mathbf{u}_l, \mathbf{v}_1, \ldots, \mathbf{v}_m\}$ = LO $\{\mathbf{w}_1, \ldots, \mathbf{w}_k, \mathbf{u}_1, \ldots, \mathbf{u}_l\}$+LO $\{\mathbf{w}_1, \ldots, \mathbf{w}_k, \mathbf{v}_1, \ldots, \mathbf{v}m\}$ = $\mathbf{U} + \mathbf{V}$ z definice součtu VP, tedy E generuje $\mathbf{U} + \mathbf{V}$. E je LN, jelikož když $\sum_{i=1}^{k} a_1 \mathbf{w}_i + \sum_{s=1}^{l} b_s \mathbf{u}_s + \sum_{t=1}^{m} c_t \mathbf{v}_t = 0$, kde $a_i, b_s, c_t \in \mathbb{T}$ správně přepíšeme, dostaneme prvky průniku, tedy budeme moci ukázat, že jsou koeficienty nulové. □

Definice 4.18

Mějme $\mathbf{V}$ VP nad $\mathbb{T}$ a $\mathbf{U}, \mathbf{W} \leq \mathbf{V}$. Pak $\mathbf{V}$ je direktní součet $\mathbf{U}$ a $\mathbf{W}$, pokud: a) $\mathbf{U} + \mathbf{W} = \mathbf{V}$ a b) $\mathbf{U} \cap \mathbf{W} = \{\mathbf{o}\}$. Značíme $\mathbf{V} = \mathbf{U} \oplus \mathbf{W}$.

Věta 4.22

Buď $\mathbf{V}$ *VP a* $\mathbf{U}, \mathbf{W} \leq \mathbf{V}$*. Pak NPJE:*

1. $\mathbf{V} = \mathbf{U} \oplus \mathbf{W}$,
2. $\forall \mathbf{v} \in \mathbf{V}\ \exists! \mathbf{u} \in \mathbf{U}, \mathbf{w} \in \mathbf{W} : \mathbf{V} = \mathbf{u} + \mathbf{w}$,
3. $\mathbf{V} = \mathbf{U} + \mathbf{W}$ *a* $\dim(\mathbf{V}) = \dim(\mathbf{U}) + \dim(\mathbf{W})$,
4. $\{\mathbf{o}\} = \mathbf{U} \cap \mathbf{W}$ *a* $\dim(\mathbf{V}) = \dim(\mathbf{U}) + \dim(\mathbf{W})$.

Důkaz
(1 $\implies$ 2): Předpokládejme 1 a buď $\mathbf{v} \in \mathbf{V} \implies \exists \mathbf{u} \in \mathbf{U}, \mathbf{v} \in \mathbf{W} : \mathbf{v} = \mathbf{u} + \mathbf{w}$. Pokud $\mathbf{u} + \mathbf{w} = \mathbf{v} = \mathbf{u}' + \mathbf{w}'$, pak $\mathbf{u} - \mathbf{u}' = \mathbf{w}' - \mathbf{w} \in \mathbf{U} \cap \mathbf{W} = \{\mathbf{o}\}$.

(2 $\implies$ 1): Předpokládejme 2. Pak určitě $\mathbf{U} + \mathbf{W} = \mathbf{V}$. Pokud $v \in \mathbf{U} \cap \mathbf{W}$, pak $\mathbf{v} \in \mathbf{U} + \mathbf{o} \in \mathbf{W} = \mathbf{o} \in \mathbf{U} + \mathbf{v} \in \mathbf{W} = \mathbf{v}$, tj. $\mathbf{v} = \mathbf{o}$. □

5 Lineární zobrazení

Definice 5.1 (Lineární zobrazení (homomorfismus))

Předpokládejme, že máme vektorové prostory $\mathbf{V}$, $\mathbf{W}$ nad stejným tělesem $\mathbb{T}$. Řekněme, že zobrazení $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení (též homomorfismus vektorových prostorů), pokud platí:

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

Například
Nad každým tělesem, mezi každými (každým) VP: Identita, Nulové zobrazení ($f(\mathbf{v}) = \mathbf{o}$), Zobrazení (dokonce bijekce) dané zapsáním (u konečně generovaných $\mathbb{T}^n$) v souřadnicích vzhledem k nějaké bázi, .

Tvrzení 5.1

Buďte $\mathbf{V}$, $\mathbf{W}$ VP nad $\mathbb{T}$ a buď $\mathbf{V}$ konečně generovaný s bází $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$. Vezmeme-li libovolnou posloupnost $(\mathbf{w}_1, \dots, \mathbf{w}_n)$ vektorů $\mathbf{W}$, pak $\exists!$ lineární zobrazení $f : \mathbf{V} \to \mathbf{W}$ takové, že $\forall i \in [n] : f(\mathbf{v}_i) = \mathbf{w}_i$.

Důkaz (Jednoznačnost)
Uvažujme lineární $f, g : \mathbf{V} \to \mathbf{W}$ taková, že $f(\mathbf{v}_i) = \mathbf{w}_i = g(\mathbf{v}_i) \forall i$. Vezměme libovolné $\mathbf{v} \in \mathbf{V}$, vyjádřeme jej jako $\mathbf{v} = t_1\mathbf{v}_1 + \ldots + t_m\mathbf{v}_m$. Pak platí

$$f(\mathbf{v}) = t_1 \cdot f(\mathbf{v}_1) + \ldots + t_n \cdot f(\mathbf{v}_n) = t_1 \cdot g(\mathbf{v}_1) + \ldots + t_n \cdot g(\mathbf{v}_n) = g(\mathbf{v}) \implies f = g.$$

□

Důkaz (Existence)
Definujeme $f : \mathbf{V} \to \mathbf{W}$ tak, že pro každé $\mathbf{v} \in \mathbf{V}$ vezmeme $(t_1, \dots, t_n)^T = [\mathbf{v}]_B$ a položíme $f(\mathbf{v}) := t_1 \cdot \mathbf{w}_1 + \ldots + t_n\mathbf{w}_n$. Následně ověříme, že $\forall i : f(\mathbf{v}_i) = \mathbf{w}_i$ a že f je lineární (např. z tvrzení 5.75, že zápis v souřadnicích daných bází je lineární). □

Definice 5.2 (Matice lineárního zobrazení)

$f : \mathbf{V} \to \mathbf{W}$, B báze $\mathbf{V}$, C báze $\mathbf{W}$. Maticí lineárního zobrazení f vzhledem k bázím B a C

rozumíme matici
$$[f]_C^B = \left([f(\mathbf{v}_1)]_C \,|\ldots|\, [f(\mathbf{v}_n)]_C\right).$$

Poznámka
Ve skriptech následují T6.6 a T6.7 neboli existence a jednoznačnost.

Tvrzení 5.2

Složení lineárních zobrazení je lineární zobrazení. Pokud jsou navíc konečně generované, pak matice složení je součin matic.

Důkaz

$$g \circ f(\mathbf{u}+\mathbf{v}) = g(f(\mathbf{u}+\mathbf{v})) = g(f(\mathbf{u})+f(\mathbf{v})) = g(f(\mathbf{u}))+g(f(\mathbf{v})) = g \circ f(\mathbf{u}) + g \circ f(\mathbf{v})$$

Analogicky $g \circ f(t \cdot \mathbf{v}) = t \cdot g \circ f(\mathbf{v})$.

$$[g \circ f]_D^B \cdot [v]_B = [g \circ f(\mathbf{v})][g]_D^C \cdot [f(\mathbf{v})]_C = \ldots$$

□

Tvrzení 5.3

Uvažujme VP $\mathbf{U}$, $\mathbf{V}$ *nad* $\mathbb{T}$ *a lineární bijekci* $f : \mathbf{U} \to \mathbf{V}$. *Pak* $f^{-1} : \mathbf{V} \to \mathbf{U}$ *je lineární.*

Jsou-li navíc VP konečně generované a B, C *jsou popořadě jejich báze, pak*
$$[f^{-1}]_B^C = ([f]_C^B)^{-1}.$$

Tvrzení 5.4

Buď $\mathbf{V}$ *konečně generovaný VP nad* $\mathbb{T}$, $f : \mathbf{V} \to \mathbf{V}$ *lineární zobrazení,* B, C *báze* $\mathbf{V}$. *Označme* $R = [id]_C^B$. *Pak*
$$[f]_B^B = R^{-1} \cdot [f]_C^C \cdot R.$$

Důkaz
Využijeme složení a inverzi lineárních zobrazení. Triviální. □

Definice 5.3 (Terminologie k lineárním zobrazením)

Buď $\mathbb{T}$ těleso a $\mathbf{V}$, $\mathbf{W}$ vektorové prostory a $f : \mathbf{V} \to \mathbf{W}$ homomorfismus. Pak f je

- monomorfismus (též vnoření), pokud f je prosté,
- epimorfismus, pokud f je na,
- isomorfismus, pokud f je bijekce,

- endomorfismus, pokud $\mathbf{V} = \mathbf{W}$,
- automorfismus, pokud $\mathbf{V} = \mathbf{W}$ a navíc f je bijekce,
- lineární forma, pokud $\mathbf{W} = \mathbb{T}$.

Definice 5.4

Buď $\mathbb{T}$ těleso, $\mathbf{V}$, $\mathbf{W}$ VP, $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak

- Jádro f je množina $\operatorname{Ker} f = \{\mathbf{v} \in \mathbf{V} : f(\mathbf{v}) = \mathbf{o}\}$
- Obraz f je množina $\Im f = \{f(\mathbf{v}) \in \mathbf{W} : \mathbf{v} \in \mathbf{V}\}$

Tvrzení 5.5 (Pozorování, část tvrzení)

$$\operatorname{Ker} f \leq \mathbf{V} \qquad \Im f \leq \mathbf{W}$$

Důkaz

$$\mathbf{u}, \mathbf{v} \in \operatorname{Ker} \varphi \Leftrightarrow f(\mathbf{u}) = \mathbf{o} = f(\mathbf{v}) \implies f(\mathbf{u} + \mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v}) = 0 \Leftrightarrow \mathbf{u} + \mathbf{v} \in \operatorname{Ker} f$$

Obdobně s násobením a obojím pro obraz. $\square$

Tvrzení 5.6

$f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení. Pak f je monomorfismus právě tehdy, když $\operatorname{Ker} f = \{\mathbf{o}\}$.

Důkaz

($\implies$) triviální. ($\impliedby$) $\forall \mathbf{u}, \mathbf{v} \in \mathbf{V} : f(\mathbf{u}) = f(\mathbf{v}) \Leftrightarrow f(\mathbf{u}) - f(\mathbf{v}) = \mathbf{o} \Leftrightarrow \mathbf{u} - \mathbf{v} \in \operatorname{Ker} f \Leftrightarrow \mathbf{u} - \mathbf{v} = \mathbf{o} \Leftrightarrow \mathbf{u} = \mathbf{v}$. $\square$

Definice 5.5 (Značení)

$\mathbf{V}$ konečně generovaný VP, B je báze $\mathbf{V}$, $X \subseteq v$ jeho podmnožina. Budeme značit $[X]_B = \{[\mathbf{v}]_B : \mathbf{v} \in X\} \subseteq \mathbb{T}^n (n = \dim \mathbf{V})$.

Tvrzení 5.7

Buďte $\mathbf{V}$, $\mathbf{W}$ konečně generované VP, B, C popořadě jejich báze, n, m popořadě jejich dimenze. Je-li $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak platí:

$$[\operatorname{Ker} f]_B = \operatorname{Ker}[f]^B_C \qquad [\Im f]_C = \Im [f]^B_C.$$

Tvrzení 5.8

Buďte $\mathbf{V}$, $\mathbf{W}$ *VP,* $\mathbf{V}$ *buďkonečně generovaný. Pak lineární zobrazení* $f : \mathbf{V} \to \mathbf{W}$ *je monomorfismus (epimorfismus, isomorfismus) právě tehdy, když* $\forall$ *LN (generující, bázi) posloupnost ve* $\mathbf{V}$ *je její obraz LN (generující, báze), což je právě tehdy, když* $\exists$ *báze prostoru* $\mathbf{V}$*, že její obraz je LN (generující, báze).*

Definice 5.6

Prostory $\mathbf{V}$, $\mathbf{W}$ nad $\mathbb{T}$ jsou isomorfní, pokud $\exists f : \mathbf{V} \to \mathbf{W}$ isomorfismus. Značíme $\mathbf{V} \cong \mathbf{W}$.

Věta 5.9

Buď $\mathbf{V}$, $\mathbf{W}$ *konečně generované VP nad* $\mathbb{T}$*. Pak* $\mathbf{V} \cong \mathbf{W} \Leftrightarrow \dim \mathbf{V} = \dim \mathbf{W}$.

Věta 5.10

Buď $\mathbf{V}$, $\mathbf{W}$ *konečně generované VP nad* $\mathbb{T}$*,* $f : \mathbf{V} \to \mathbf{W}$ *lineární zobrazení. Pak* $\dim(\operatorname{Ker} f) + \dim(\Im f) = \dim V$.

6 Determinanty a permutace

Definice 6.1

Buď A čtvercová matice řádu 2. Potom definujeme determinant jako

$$\det A := a_{11}a_{22} - a_{21}a_{12}.$$

Poznámka

Determinant počítá až na znaménko obsah rovnoběžníku daného obrazy kanonické báze.

Definice 6.2

Buď A čtvercová matice řádu 3. Potom definujeme determinant jako

$$\det A := a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}.$$

Poznámka

Determinant je roven orientovanému objemu rovnoběžnostěnu v $\mathbb{R}^3$.

Definice 6.3

Permutace množiny X je bijekce $\pi : X \to X$.

Množinu permutací na X značíme S_X.

Pro $X = \{1, \ldots, n\}$ značíme $S_n = S_{\{1,\ldots,n\}}$.

Poznámka (Vlastnosti a operace na permutacích)

- $\mathrm{id}_X : X \to X$ je permutace.
- $\pi, \varrho \in S_X$ můžeme složit na permutaci $\pi \circ \varrho \in S_X$.
- $\varrho \in S_X$, pak $\varrho^{-1} \in S_X$.
- $\forall \pi, \varrho, \sigma \in S_X : (\pi\varrho)\sigma = \pi(\varrho\sigma)$.
- $\forall \pi \in S_x : \mathrm{id}_X \pi = \pi = \pi \, \mathrm{id}_x$.
- $\forall \pi \in S_X : \pi^{-1}\pi = \mathrm{id}_X = \pi\pi^{-1}$.

(Poslední tři jsou vlastnosti operace skládání, které splňují grupové axiomy.)

Pozor

$$\pi\varrho \neq \varrho\pi!$$

Poznámka (Zápis permutace)
Tabulkou (např.: $\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 1 & 8 & 5 & 4 & 3 & 2 \end{matrix} \in S_8$). Obrázkem (orientovaný graf se smyčkami s $\deg_{out} = \deg_{in} = 1$).

Definice 6.4 (Cykly a transpozice)

Cyklus (délky a) je permutace, která obsahuje nejvýše jeden netriviální [Obrázek cyklu].

Cyklus zapisujeme jako $(x_1 x_2 \ldots x_k)$.

Cyklus délky 2, tj. $(x_1 x_2)$, se nazývá transpozice.

Tvrzení 6.1

Každou permutaci π na konečné množině X lze zapsat jako složení nezávislých cyklů. Tento zápis je až na pořadí a vynechání cyklů délky 1 jednoznačný.

Důkaz
Bez důkazu. (Důkaz ve skriptech.) □

Tvrzení 6.2

Každou permutaci na konečné množině lze zapsat jako složení transpozic (obecně nejednoznačně!).

Důkaz
Stačí dokázat pro cyklus (vzhledem k předchozímu tvrzení).

$$(x_1 \dots x_k) = (x_1 x_2) \circ (x_2 x_3) \circ (x_3 x_4).$$

□

Poznámka
Parita počtu transpozic, na které rozložím permutaci, je vždy stejná.

Tvrzení 6.3

Buď X konečna, $\pi = \pi_1 \circ \dots \circ \pi_l$ a $x \neq y$, $x, y \in X$. Pak počet cyklů v obdobném zápisu $(xy) \circ \pi$ je $l \pm 1$ a počty sudých cyklů v zápisu π a $(xy) \circ \pi$ se také liší o 1.

Důkaz
2 možnosti: x, y jsou ve stejném cyklu π_i. BÚNO $i = 1$,

$$\pi = (x_1, \dots, x_l, y_1, \dots, y_m) \implies (xy) \circ \pi = (x_1, \dots, x_l)\,(y_1, \dots, y_m)\pi_2, \dots, \pi_k.$$

Očividně se buď z lichého cyklu stal sudý a lichý, nebo ze sudého 2 liché, nebo ze sudého 2 sudé, tedy počet sudých cyklů se změní o 1.

Obdobně pokud byly v různých, tak se cykly spojí… □

Důsledek
Je-li X konečná množina a $\pi = (x_1 y_1) \circ \dots \circ (x_k y_k)$, pak nastane právě 1 z následujících možností: cyklický zápis π má sudý počet cyklů sudé délky a k je sudé, nebo cyklický zápis π má lichý počet cyklů sudé délky a k je liché.

Definice 6.5 (Znaménko permutace)

$\operatorname{sgn}(\pi)$ je 1 v prvním případě (a permutaci se říká sudá) a -1 v druhém (lichá).

Tvrzení 6.4

$\operatorname{sgn}(\mathrm{id}_X) = 1$, $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)$, $\operatorname{sgn}(\pi \circ \varrho) = \operatorname{sgn}(\pi) \cdot \operatorname{sgn}(\varrho)$.

Tvrzení 6.5

Počet sudých / lichých permutací na množině velikosti $n \in \mathbb{N} \setminus \{1\}$ je polovina všech.

6.1 Determinant

Definice 6.6 (Determinant)

Buď $A = (a_i j)$ čtvercová matice řádu n nad $\mathbb{T}$. Pak determinant A je následující prvek $\mathbb{T}$:

$$\det(A) = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \cdot a_{\pi(1),1} \cdot a_{\pi(2),2} \cdot \dots \cdot a_{\pi(n),n}.$$

Poznámka (Základní vlastnosti)
$\sum_{\pi \in S_n} \operatorname{sgn}(\pi) \cdot a_{1,\pi(1)} \cdot a_{2,\pi(2)} \cdot \dots \cdot a_{n,\pi(n)}$.

Tvrzení 6.6

Buď $\mathbb{T}$ těleso, $n \in \mathbb{N}$, $\mathbf{v}_1, \dots, \mathbf{v}_n, \mathbf{u} \in \mathbb{T}^n$, $t \in \mathbb{T}$. Pak platí:

$$\forall i : \det(\mathbf{v}_1|\dots|\mathbf{v}_{i-1}|\mathbf{v}_i + \mathbf{u}|\mathbf{v}_{i+1}|\dots|\mathbf{v}_n) = \det(\mathbf{v}_1|\dots|\mathbf{v}_{i-1}|\mathbf{u}|\mathbf{v}_{i+1}|\dots|\mathbf{v}_n) + \det(\mathbf{v}_1|\dots|\mathbf{v}_{i-1}|\mathbf{v}_i|\mathbf{v}_{i+1}|\dots|\mathbf{v}_n$$

$$\det(\mathbf{v}_1|\dots|\mathbf{v}_{i-1}|t\mathbf{v}_i|\mathbf{v}_{i+1}|\dots|\mathbf{v}_n) = t\det(\mathbf{v}_1|\dots|\mathbf{v}_{i-1}|\mathbf{v}_i|\mathbf{v}_{i+1}|\dots|\mathbf{v}_n),$$

$$\varrho \in S_n : \det\left(\mathbf{v}_{\varrho(1)}|\dots|\mathbf{v}_{\varrho(n)}\right) = \operatorname{sgn}(\varrho) \cdot \det(\mathbf{v}|\dots|\mathbf{v}_n),$$

$$v_i = v_j, i \neq j \implies \det(\mathbf{v}_1|\dots|\mathbf{v}_n) = 0,$$

$$i \neq j \implies \det(\mathbf{v}_1|\dots|\mathbf{v}_{i-1}|\mathbf{v}i + t\mathbf{v}_j|\mathbf{v}_{i+1}|\dots|\mathbf{v}_n) = \det(\mathbf{v}_1|\dots|\mathbf{v}_n) = 0.$$

Tvrzení 6.7

Je-li $A = (a_{ij})$ horní / dolní trojúhelníková, pak $\det(A) = a_{11} \cdot a_{22} \cdot \dots \cdot a_{nn}$.

Tvrzení 6.8

Buď A čtvercová matice nad $\mathbb{T}$. Pak A je regulární $\Leftrightarrow \det(A) \neq 0$.

Důkaz
Upravíme do odstupňovaného tvaru, tím se nulovost nezmění. Pak je nulovost ekvivalentní s tím, že na diagonále jsou prvky nenulové, což je ekvivalentní s tím, že A je regulární. $\square$

Definice 6.7

Buď A matice typu $m \times n$ nad $\mathbb{T}$. Pak minor matice A řádu $k \geq 1$ je determinant čtvercové matice řádu k, která vznikne z A vypuštěním některých řádků a sloupců.

Tvrzení 6.9

A matice typu $m \times n$ nad $\mathbb{T}$. Pak hodnost A je rovna největšímu $k \geq 1$ takovému, že nějaký minor řádu k je $\neq 0$.

Důkaz (Náznak)
Pro odstupňovaný tvar tvrzení zřejmě platí a hodnost ani nulovost determinantu (tedy ani k) se nemění EŘÚ. □

Poznámka (Determinanty elementárních úprav)
Determinant vynásobení řádku t je t, přičtení násobku řádku je 1 a prohození řádků je -1.

Tvrzení 6.10

Pokud A je čtvercová matice a E je elementární matice, obě řádu n. Pak $\det(EA) = \det(E) \cdot \det(A)$.

Důkaz
Jednoduše z předchozí poznámky. □

Tvrzení 6.11

Buďte A, B čtvercové matice řádu n nad $\mathbb{T}$. Pak $\det(A \cdot B) = \det(A) \cdot \det(B)$.

Důkaz
Pokud A je regulární, pak se dá podle tvrzení T4.88 rozepsat jako součin elementárních matic a indukcí roznásobit. Jinak ani $A \cdot B$ není regulární a tedy A i $A \cdot B$ mají nulový determinant. □

Důsledek
$\det(A^{-1}) = (\det(A))^{-1}$.

Věta 6.12 (Cramerovo pravidlo)

Buď A regulární matice řádu n. Buď $\mathbf{b} \in \mathbb{T}^n$ a $A\mathbf{x} = \mathbf{b}$. Pak

$$\forall j \in [n] : x_j = \frac{\det\left((\mathbf{a}_1 | \ldots | \mathbf{a}_{j-1} | \mathbf{b} | \mathbf{a}_{j+1} | \ldots | \mathbf{a}_n)\right)}{\det(A)}.$$

Důkaz
To, že $A\mathbf{x} = \mathbf{b}$, můžeme přepsat do tvaru $\mathbf{b} = x_1 \cdot \mathbf{a}_1 + \ldots + x_n \cdot \mathbf{a}_n$. Pak rozepíšeme determinant čitatele výše a dostaneme:

$$\det\left((\mathbf{a}_1|\ldots|\mathbf{a}_{j-1}|\mathbf{b}|\mathbf{a}_{j+1}|\ldots|\mathbf{a}_n)\right) = \det\left(\left(\mathbf{a}_1|\ldots|\mathbf{a}_{j-1}|\sum_{i=1}^{n} x_i \cdot \mathbf{a}_i|\mathbf{a}_{j+1}|\ldots|\mathbf{a}_n\right)\right) = \sum_{i=1}^{n} x_i \cdot \det\left((\mathbf{a}_1|\ldots|\mathbf{a}_j\right.$$

□

Definice 6.8

Algebraickým doplňkem (též kofaktorem) prvku a_{ij} rozumíme

$$A_{ij} = (-1)^{i+j} \cdot \det(M_{ij}),$$

kde M_{ij} je matice A bez i-tého řádku a j-tého sloupce.

Věta 6.13 (O rozvoji podle sloupce)

$$\det(A) = \sum_{i=1}^{n} a_{ij} \cdot A_{ij}, j \in [n].$$

Důkaz
1. speciální případ: $j = n, a_n = e_n$. Triviální.

2. speciální případ: $j, k, \in [n], a_j = e_k$. Permutace předchozího.

3. obecný případ: Součet předchozího. □

Věta 6.14 (O falešném rozvoji)

TODO

Definice 6.9

Adjungovaná matice (matice kofaktorů): $adj(A)$.

Poznámka
Můžeme si všimnout, že $A \cdot adj(A) = \det(A) \cdot I_n = adj(A) \cdot A$.

Věta 6.15

Tvrdí poznámku výše, speciální případ (A regulární) $A^{-1} = \frac{\det(adj(A))}{\det(A)}$.