Lineární zobrazení

- Matice složeného lin. zobrazení:

Buďte $f: U \to V$, $g: V \to W$ lin. zobrazení, buď B_U, B_V a B_W báze.

$$_{B_W}[g \circ f]_{B_U} = {}_{B_W}[g]_{B_V} \cdot {}_{B_V}[f]_{B_U}$$

$\forall x \in U$

$$[(g \circ f)(x)]_{B_W} = [g(f(x))]_{B_W} = {}_{B_W}[g]_{B_V} \cdot \underbrace{{}_{B_V}[f]_{B_U} \cdot [x]_{B_U}}_{[f(x)]_{B_V}}$$

- Jednoznačnost matice lin. zobrazení:

Buď $f: U \to V$ lin. zobrazení, B_U, B_V báze. Pak jediná matice A splňující matici zobrazení je $A = {}_{B_V}[f]_{B_U}$.

Nechť $B_U \{z_1 \dots z_n\}$, pro spor mějme $A \neq A'$ matice lin. zobrazení. Tudíž existuje vektor $s \in T^n$ takový, že $As \neq A's$.

$x := \sum_{i=1}^{n} s_i z_i$. Pak $[f(x)]_{B_V} = As \neq A's = [f(x)]_{B_V}$ $\boxed{\lightning}$

Spor s jednoznačností souřadnic.

Maticová reprezentace lin. zobrazení

Buď $f: U \to V$ lin. zobrazení, B_U a B_V báze daných prostorů.
Pak pro každé $x \in U$ je:

$$[f(x)]_{B_V} = {}_{B_V}[f]_{B_U} \cdot [x]_{B_U}$$

Nechť $A := {}_{B_V}[f]_{B_U}$. Buď $x \in U$, tedy $x = \sum_{j=1}^{n} \alpha_j x_j$,
tedy $[x]_{B_U} = (\alpha_1 \dots \alpha_n)^T$.

Pak $f(x) = f\left(\sum_{j=1}^{n} \alpha_j x_j\right) = \sum_{j=1}^{n} \alpha_j f(x_j) = \sum_{j=1}^{n} \alpha_j \left(\sum_{i=1}^{m} a_{ij} y_i\right) =$

$$\sum_{j=1}^{n} \sum_{i=1}^{m} \alpha_j a_{ij} y_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \alpha_j a_{ij}\right) y_i$$

Tedy výraz $\sum_{j=1}^{n} \alpha_j a_{ij}$ reprezentuje i-tou souřadnici vektoru $[f(x)]_{B_V}$,
ale jeho hodnota je $\sum_{j=1}^{n} \alpha_j a_{ij} = \left(A \cdot [x]_{B_U}\right)_i$, což je
i-tá složka vektoru ${}_{B_V}[f]_{B_U} \cdot [x]_{B_U}$.

O dimenzi jádra a obrazu

Buď $f: U \to V$ lin. zobrazení, B_U a B_V jeho báze.

$A := {}_{B_V}[f]_{B_U}$. Pak

Tohle tam nebude, jasný!

1) $\dim(\ker(f)) = \dim(\ker(A))$

2) $\dim(f(U)) = \dim(\mathcal{Y}(A)) = \operatorname{rank}(A)$

① Prakticky stačí sestrojit isomorfismus mezi $\operatorname{Ker}(f)$ a $\operatorname{Ker}(A)$.

Např.: zobrazení $x \in \operatorname{Ker}(f) \to [x]_{B_U}$. Takové zobrazení je prosté a lineární

Prostota plyne z jednoznačnosti souřadnic (definice), lineární proto, že každá souřadnice je lin. kombinací nějakého vektoru.

Stačí dokázat, že $x \in \operatorname{Ker}(A)$ a že je „na".

Nechť $x \in \operatorname{Ker}(f)$, pak:

$$0 = [0]_{B_V} = [f(x)]_{B_V} = {}_{B_V}[f]_{B_U} \cdot [x]_{B_U}$$

tedy $[x]_{B_U}$ náleží do $\ker(A)$.

Takže $\forall [x]_{B_U} \in \operatorname{Ker}(A)$ je $f(x) = 0$

② $\dim U = n$, $\dim V = m$. Sestrojme isomorfismus mezi $f(U)$ a $\mathcal{Y}(A)$ a takto $y \in f(U) \to [y]_{B_V}$. Opět je lineární a prosté. Dále pro $y \in f(U)$ existuje $x \in U$ takový, že $f(x) = y$, tedy $[y]_{B_V} = [f(x)]_{B_V} = A \cdot [x]_{B_U}$, tedy $[y]_{B_V} \in \mathcal{Y}(A)$. A naopak

pro každé $b \in \mathcal{Y}(A)$ existuje $a \in T^n$ takový, že $b = Aa$. Tedy pro $x \in U$ takové, že $[x]_{B_U} = a$, platí: $f(x) \in f(U)$ a zároveň $[y]_{B_V} = [f(x)]_{B_V} = A \cdot [x]_{B_U} = Aa = b \in \mathcal{Y}(A)$

- Isomorfismus n-dimenzionálních prostorů

Všechny n-dimenzionální prostory nad T jsou navzájem isomorfní.

Podle tvrzení * jsou všechny n-dimenzionální prostory nad T isomorfní s T^n nad T, tedy i navzájem mezi sebou.

Tvrzení *:

Buď V vektorový prostor nad T dimenze n s bází B.
Pak zobrazení $x \mapsto [x]_B$ je isomorfismus mezi V a T nad T^n

Nechť báze $B = \{v_1 \dots v_n\}$. Zobrazení je lin, prosté a na.

- Prostota plyne z jednoznačnosti souřadnic.
- „Na", protože každá n-tice $(\alpha_1 \dots \alpha_n) \in T^n$ představuje souřadnice nějakého vektoru.

Uvažte $x := \sum_{i=1}^{n} \alpha_i v_i$

Lineární zobrazení

$f: U \to V$ je lineární:

1) $f(U)$ je podprostorem V
2) $\ker(f)$ je podprostorem U
3) pro každé $x_1 \dots x_n \in U$ platí: $f(\mathrm{span}\{x_1 \dots x_n\}) = \mathrm{span}\{f(x_1) \dots f(x_n)\}$

1), 2) Stačí ověřit o a uzavřenost na sčítání násobení

3)

Inkluze $\subseteq$:

$W := \mathrm{span}\{x_1 \dots x_n\}$, $\forall w \in W$: $w = \sum_{i=1}^{n} \alpha_i x_i$ pro nějaká $\alpha_1 \dots \alpha_n \in T$.
Z linearity platí, že $f(w) = \sum_{i=1}^{n} \alpha_i f(x_i) \in \mathrm{span}\{f(x_1) \dots f(x_n)\}$

Inkluze 2:

Protože $x_1 \dots x_n \in W$, tak $f(x_1) \dots f(x_n) \in f(W)$.
$f(W)$ je podprostor, tedy s vektory $f(x_1) \dots f(x_n)$ obsahuje i jejich span.

- Zobrazení je „na":

$f: U \to V$ je na $\iff$ nějaký generátory prostoru U zobrazí na generátory prostoru V.

Zobrazení je „na", jakmile $f(U) = V$, tedy že pro každý vektor $x \in U$ existuje $y \in V$: $f(x) = y$

- vezmu tedy generátory U a ověřím, jestli jejich obrazy generují V.

- Zobrazení je prosté: $f(x) = f(y)$ jenom pro $x = y$

Buď $f: U \to V$ lin. zobrazení: Následující jsou ekvivalentní:

1) f je prosté
2) $\ker(f) = \{0\}$
3) Obraz LNZ množiny je LNZ množina

$1 \Rightarrow 2$: Protože $f(0) = 0$, tak $0 \in \ker(f)$. Vzhledem k tomu, že je prosté, už ale jiný neobsahuje.

$2 \Rightarrow 3$: Nechť $x_1 \dots x_n \in U$ a jsou LNZ a nechť $\sum_{i=1}^{n} \alpha_i f(x_i) = 0$
Pak $f\left(\sum_{i=1}^{n} \alpha_i x_i\right) = 0$, čili $\sum_{i=1}^{n} \alpha_i x_i \in \ker(f)$, tudíž $\sum_{i=1}^{n} \alpha_i x_i = 0$, což díky LNZ platí pro $\alpha_i = 0 \ \forall i$

$3 \Rightarrow 1$: Sporem: $x, y \in U$, $f(x) = f(y)$, $x \neq y$.
Potom $0 = f(x) - f(y) = f(x-y)$ 0 představuje LNZ množinu, tedy $x - y = 0 \to x = y$ $\boxed{\lightning}$

- Jednoznačnost lin. zobr. vzhledem k obrazům báze

Buďte U, V 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 lin. zobr. takové že $f(x_i) = y_i$ pro $i \_ n$

„Existence"

Buď $x \in U$ libovolné. Pak $x = \sum_{i=1}^{n} \alpha_i x_i$ pro $\alpha_1 \dots \alpha_n \in \mathbb{T}$.

$f(x) = \sum_{i=1}^{n} \alpha_i y_i$, protože lin. zobrazení musí splňovat:

$$f(x) = f\left(\sum_{i=1}^{n} \alpha_i x_i\right) = \sum_{i=1}^{n} \alpha_i f(x_i) = \sum_{i=1}^{n} \alpha_i y_i$$

„Jednoznačnost"

Mějme dvě různá zobrazení f a g: $f(x_i) = g(x_i) = y_i$

$x = \sum_{i=1}^{n} \alpha_i x_i$

$$f(x) = f\left(\sum_{i=1}^{n} \alpha_i x_i\right) = \sum_{i=1}^{n} \alpha_i f(x_i) = \sum_{i=1}^{n} \alpha_i y_i = \sum_{i=1}^{n} \alpha_i g(x_i) = g\left(\sum_{i=1}^{n} \alpha_i x_i\right) = g(x) \ \boxed{\text{↯}}$$

- O dimenzi jádra a hodnosti matice

Pro libovolnou matici $A \in \mathbb{T}^{m \times n}$ platí:

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

Nechť $\dim(\ker(A)) = k$. Pak $v_1 \dots v_k$ tvoří $\ker(A)$, tedy $Av_1 \dots Av_k = 0$.
Rozšíříme tyto vektory o $v_{k+1} \dots v_n$. Tyto vektory tvoří bázi $\mathcal{S}(A)$.

„Generujícnost": Buď $y \in \mathcal{S}(A)$, pak $y = Ax$ pro $x \in \mathbb{T}^n$. $x = \sum_{i=1}^{n} \alpha_i v_i$

$$y = Ax = A \sum_{i=1}^{n} \alpha_i v_i = \sum_{i=1}^{n} \alpha_i A v_i = \sum_{i=k+1}^{n} \alpha_i (Av_i)$$

„LNZ": Buď $\sum_{i=k+1}^{n} \alpha_i v_i = 0$. Pak platí, že $A\left(\sum_{i=k+1}^{n} \alpha_i v_i\right) = 0$, tedy $\in \ker(A)$ a proto $= \sum_{i=1}^{k} \beta_i v_i$ z toho vyplývá...

$\sum_{i=k+1}^{n} \alpha_i v_i + \sum_{i=1}^{k} -\beta_i v_i = 0$, což vzhledem k LNZ vektorů $v_1 \dots v_n$ znamená, že

$$\alpha_1 \dots \alpha_n = \beta_1 \dots \beta_k = 0$$

Dimenze spojení a průniku

Buďte U, V podprostory W. Pak platí:

$$\dim(U+V) + \dim(U\cap V) = \dim U + \dim V$$

Důkaz:

$U \cap V$ je podprostor W, tedy existuje konečná množina vektorů tvořící bázi $z_1 \dots z_p$.

Tu můžeme rozšířit na bázi U $(z_1 \dots z_p, x_1 \dots x_m)$ nebo na bázi V $(z_1 \dots z_p, y_1 \dots y_n)$.

Vektory $z_1 \dots z_p, x_1 \dots x_m, y_1 \dots y_n$ tak tvoří $U+V$.

„Generujícnost":

Buď $z = u+v$, $u \in U$, $v \in V$. Pak $u = \sum_{i=1}^{p} \alpha_i z_i + \sum_{j=1}^{m} \beta_j x_j$, $v = \sum_{i=1}^{p} \gamma_i z_i + \sum_{h=1}^{n} \delta_h y_h$.

Pak $z = \sum_{i=1}^{p} (\alpha_i + \gamma_i) z_i + \sum_{j=1}^{m} \beta_j x_j + \sum_{h=1}^{n} \delta_h y_h$, tedy je lineární kombinací všech ostatních!

„LNZ":

Buď $\sum_{i=1}^{p} \alpha_i z_i + \sum_{j=1}^{m} \beta_j x_j + \sum_{h=1}^{n} \gamma_h y_h = 0$ → chceme ukázat, že všechny koeficienty jsou nulové.

$z := \sum_{i=1}^{p} \alpha_i z_i + \sum_{j=1}^{m} \beta_j x_j = -\sum_{h=1}^{n} \gamma_h y_h$. Zřejmě $z \in U \cap V$, tedy $z = \sum_{i=1}^{p} \delta_i z_i$.

$\sum_{i=1}^{p} \delta_i z_i = -\sum_{h=1}^{n} \gamma_h y_h$

$\sum_{i=1}^{p} \delta_i z_i + \sum_{h=1}^{n} \gamma_h y_h = 0$

má pouze triviální řešení, tedy $\forall \delta_i$ a $\forall \gamma_h = 0$

Dosadím do původní rovnice

$\sum_{i=1}^{p} \alpha_i z_i + \sum_{j=1}^{m} \beta_j x_j = 0$,

tudíž má opět triviální řešení

$\forall \alpha_i$ a $\forall \beta_j = 0$

Rozšíření LNZ systému na bázi

Každý LNZ vektorového prostoru V lze rozšířit na bázi V.

Nechť $x_1 \dots x_m$ jsou LNZ a $z_1 \dots z_d$ báze prostoru. Podle Steinitze existují indexy $k_1 \dots k_{d-m}$ takové, že $x_1 \dots x_m, z_{k_1} \dots z_{k_{d-m}}$ jsou generátory V. Těchto generátorů je d, tedy $\dim(V)$.

O existenci báze

Každý vektorový prostor má bázi.

Každý prostor má své generátory. Pokud jsou LNZ, rovnou tvoří bázi. Pokud jsou LZ, můžu nějaký odebrat a pokud takový systém je LNZ, mám bázi, jinak pokračuji s odebíráním.

Malá Fermatova věta

Buď n prvočíslo a buď $0 \neq a \in \mathbb{Z}_n$. Pak $\underline{a^{n-1} = 1 \pmod n}$

Podle Lemma* je $\{0, 1 \dots n-1\} = \{0a, 1a, \dots, (n-1)a\}$.

$0 = 0a$, takže můžeme vynádit a dostáváme $\{1, 2 \dots, n-1\} = \{1a, 2a, \dots (n-1)a\}$.

Tedy $1 \cdot 2 \cdot \dots \cdot n-1 = 1a \cdot 2a \cdot \dots \cdot (n-1)a$

$$1 = \underbrace{a \cdot a \cdot a \cdot \dots \cdot a}_{n-1} \;\longrightarrow\; \underline{\underline{1 = a^{n-1}}}$$

Lemma*: Buď n prvočíslo a buď $0 \neq a \in \mathbb{Z}_n$. Při násobení modulo platí:

$$\{0, 1, \dots, n-1\} = \{0a, 1a, \dots, (n-1)a\}$$

Nechť $ka = la$, kde $k \neq l$ a $k, l \in \mathbb{Z}_n$. Z toho dostaneme, že $ka - la = 0$, tedy $a \cdot (k - l) = 0$, což znamená, že

$a = 0$ nebo $k - l = 0$

$\lightning$ $\qquad$ $\Downarrow$

$k = l$ $\lightning$

$\mathbb{Z}_n$ je těleso $\Leftrightarrow$ n je prvočíslo

Mějme n složené, tedy $n = p \cdot q$, pak $1 < p, q < n$.

Kdyby $\mathbb{Z}_n$ bylo těleso, pak $p \cdot q = 0$, tedy $p = 0$ nebo $q = 0$

$\lightning$ $\qquad$ $\lightning$

Mějme n prvočíslo:

Pak je třeba projít všechny axiomy o tělese.

Jediné těžší je inverz pro násobení. Z lemma*, nahlédneme, že vpravo někde musí být $ba = 1$, tedy $b = a^{-1}$

Každou permutaci lze rozložit na složení transpozic

Postupně permutaci $(u_1 \dots u_r)$ rozložme následovně:

$$(u_1,\dots,u_r) = (u_1,u_2)\circ(u_2,u_3)\circ\dots\circ(u_{r-1},u_r)$$

Takový rozklad není jednoznačný, pouze jeho parita je vždy stejná.

O znaménku složení permutace a transpozice

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

Permutace p se skládá z několika cyklů. Prvky i,j jsou buď:

1) uvnitř stejného cyklu
2) v odlišných cyklech

1) $(i,u_1,\dots,u_r,j,v_1\dots v_n)$.

Pak $(i,j)\circ(i,u_1,\dots,u_r,j,v_1\dots v_n) = (i,u_1,\dots,u_r),(j,v_1\dots v_n)$

tedy počet cyklů se zvětšil o 1, tedy $sgn(p)=(-1)^{r+1}$

2) $(i,u_1,\dots,u_r),(j,v_1\dots v_n)$

Pak $(i,j)\circ(i,u_1,\dots,u_r),(j,v_1\dots v_n) = (i,u_1,\dots,u_r,j,v_1\dots v_n)$.

tedy počet cyklů se zmenšil o 1, tedy $sgn(p)=(-1)^{r-1}$

Obojí změní znaménko

Znaménko permutace

$sgn(p) = (-1)^r$, kde r je počet transpozic.

$sgn(id) = 1$ $\quad$ $sgn(p) = (v_1,v_2)\circ(v_2,v_3)\circ\dots\circ(v_{n-1},v_n)\circ(id)$

$1 \quad 1 \quad r=0$

$-1 \quad r=1$

takže $(-1)^r$

$\dots \quad 1 \quad r=2$

Znaménko součinu permutace

Buď $p, q \in S_n$. Pak $\mathrm{sgn}(p \circ q) = (-1)^{r_1 + r_2}$, kde r_1 a r_2 jsou počty transpozic.

Nechť se permutace rozloží na r_1 a r_2 transpozic. Pak jednotlivé permutace mají znaménko $(-1)^{r_1}$, $(-1)^{r_2}$, tedy $\mathrm{sgn}(p) = (-1)^{r_1} \cdot (-1)^{r_2} = (-1)^{r_1 + r_2}$

Soustava rovnic a inverzní matice

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

Protože A je reg., má soustava pouze jedno řešení x. Platí, že

$$x = Ix = A^{-1} A x = A^{-1}(Ax) = A^{-1} b \checkmark$$

Tohle dělá jednoduchý...

Jedna rovnost stačí (regularita)

Buďte $A, B \in \mathbb{R}^{n \times n}$, je-li $BA = I_n$, pak jsou obě matice reg. a vzájemně inverzní.

Jelikož je I_n reg, musí být i A, B reg. Regularita je tedy splněna.

Jinak by jedna z matic posílala nějaké řešení na 0 a $Ax = 0$ by mělo netriviální řešení, tedy i $ABx = 0$

$$B = BI_n = B(AA^{-1}) = (BA)A^{-1} = I_n A^{-1} = A^{-1}$$

$$A = AI_n = A(BB^{-1}) = (AB)B^{-1} = I_n B^{-1} = B^{-1}$$

$\boxed{\checkmark}$

O existenci inverzní matice

Buď $A \in \mathbb{R}^{n \times n}$. Je-li A reg., pak k ní existuje inverz matice a je určená jednoznačně. Naopak, existuje-li A^{-1}, je A reg. $AA^{-1} = I$

$$(AA^{-1})_{*j} = A(A^{-1})_{*j} = Ax_j = e_j = I_{*j}$$

tohle je j-tý sloupec inv. matice

pokud je A reg, má to jen jediné řešení, a to je e_j, tedy sloupec matice I_n

$$A(A^{-1}A - I) = AA^{-1}A - A = IA - A = 0$$