1. přednáška z lineární algebry

2. říjen 2007

Osnova

1) Vektorové prostory: základní pojmy
2) Matice a linearní zobrazení
3) Vektorové prostory se skalárním součinem
4) Řešení lineárních rovnic
5) Determinanty
6) Vlastní čísla, vlastní vektory
7) Exponenciály matic a jiné speciální matice

1. Vektorové prostory: základní pojmy

Geometrická představa: $\mathbb{R}$, $\mathbb{R}^2$, $\mathbb{R}^3$, $\ldots$, $\mathbb{R}^n$, $\{n \in \mathbb{N}\}$.
Ale můžou být i jiného typu. Např prostory funkcí.

Definice 1.1. $(V, +, \cdot)$ nazvu vektorovým prostorem (v.p.) nad tělesem $\mathbb{R}(\mathbb{C})$ pokud $V \neq \emptyset$ a:

(1) $+$ je operace: $V \times V \to V$

(2) $\cdot$ je operace: $\mathbb{R}(\mathbb{C}) \times V \to V$

které splňují:

I.1 $\forall v, w, x \in V : v + (w + x) = (v + w) + x$ (asociativita)

I.2 $\forall v, w \in V : v + w = w + v$ (komutativita)

I.3 $\exists n \in V \; \forall v \in V : v + n = v$ (existence neutrálního prvku)

I.4 $\forall v \in V \; \exists v' \in V : v + v' = n$ (existence inverzního prvku)

II.1 $\forall r, s \in \mathbb{R}(\mathbb{C}) \; \forall v \in V : (rs) \cdot v = r \cdot (s \cdot v)$

II.2 $\forall v \in V : 1 \cdot v = v$

II.3 $\forall r \in \mathbb{R}(\mathbb{C}) \; \forall v, w \in V : r \cdot (v + w) = r \cdot v + r \cdot w$

II.4 $\forall r, s \in \mathbb{R}(\mathbb{C}) \; \forall v \in V : (r + s) \cdot v = r \cdot v + s \cdot v$

Poznámka 1.1.

1) Geometrická představa splňuje definici. (Například sčítání vektorů a násobení vektorů reálným číslem)
2) Neutrální prvek je jediný. Pro spor mějme n, n' dva různé neutrální prvky. Pak platí

$$n' = n' + n = n$$

přičemž druhá rovnost je oprávněná proto, že n' (a obecně jakýkoli neutrální prvek) se chová „neutrálně“ z obou stran.

3) Pro jakýkoli prvek $v \in V$ existuje jen jediná inverze. Pro spor mějme $v', v'' \in V$ inverzní k v. Pak

$$\begin{aligned} v + v' = n \quad \& \quad v + v'' &= n \\ v + v' &= v + v'' \qquad / + v' \\ v' + (v + v') &= v' + (v + v'') \\ (v + v') + v' &= (v + v') + v'' \\ n + v' &= n + v'' \\ v' &= v'' \end{aligned}$$

což je spor s předpokladem. Inverzy (jedinou) budeme značit $-v$. □

4) Čemu se rovná $0 \cdot v$? Použijme $v = 1 \cdot v = (1+0) \cdot v = 1 \cdot v + 0 \cdot v = v + 0 \cdot v$ (užili jsme axiómu II.2: $1 \cdot v = v$) a podle definice neutrálního prvku snadno nahlédneme, že $0 \cdot v$ je neutrální prvek n a budeme jej značit 0 (přičemž z kontextu bude vždy jasné, jedná-li se o nulu nebo o nulový vektor).

   Zkusme $1 \cdot v + (-1) \cdot v = (1 + (-1)) \cdot v = 0 \cdot v = 0$. Čímž jsme ukázali, že $(-1) \cdot v$ je jistě inverzním prvkem k v. Tedy podle našeho značení píšeme $(-1) \cdot v = -v$.

5) Prostor splňující vlastnosti I.1, I.2, I.3, I.4 nazýváme abelovská grupa. $(V, +)$

6) Pojem "těleso $\mathbb{R}(\mathbb{C})$" je pro nás zatím jen sousloví, definice tělesa bude později.

7) Při násobení už nadále nebudeme psát tečku tam, kde to nebude zapotřebí.

8) místo $(V, +, \cdot)$ budeme stručně psát V

9) Vektorový prostor nad tělesem $\mathbb{R}$ nazýváme reálný vektorový prostor, v.p. nad tělesem $\mathbb{C}$ nazýváme komplexní v.p.

Příklad 1.1.

1) Ukažme, že $(\mathbb{R}^n, +, \cdot)$ je vektorový prostor:

$$(v_1, \ldots, v_n) + (w_1, \ldots, w_n) = (v_1 + w_1, \ldots, v_n + w_n) \quad v, w \in \mathbb{R}^n$$

$$r(v_1, \ldots, v_n) = (rv_1, \ldots, rv_n) \quad r \in \mathbb{R};\ v, w \in \mathbb{R}^n$$

2) $\mathbb{C}^n$ analogicky

3) Prostor všech funkcí F na otevřeném intervalu I v $\mathbb{R}$

$$(f + g)(x) = f(x) + g(x)$$

$$(rf)(x) = rf(x)$$

4) $\mathcal{C}^0(I) = \{f : I \to \mathbb{C} : f \text{ je spojitá na } I\}$ kde I je otevřený v $\mathbb{R}$. Pak ale $\mathcal{C}^0(I)$ tvoří vektorový prostor. Např.: když $f \in \mathcal{C}^0(I)$, tak f je spojitá, pak ale také $(-f)(x) = -(f(x))$ je spojitá. Určitě platí $(f + (-f))(x) = f(x) + (-f)(x) = f(x) + (-(f(x))) = 0$ tj. $\mathcal{C}^0(I)$ má inverzní prvek, kde neutrální prvek je nulová funkce. Další axiomy ověřit za domácí úkol.

5) $\Psi(\langle 0, 1\rangle) = \{f : \langle 0, 1\rangle;\ f(0) = 0 \wedge f(1) = 1\}$ Není vektorový prostor, protože není splněno, že $\cdot : \mathbb{R} \times \Psi \to \Psi$

Definice 1.2. (Vektorový podprostor) $(V, +, \cdot)$ je vektorový prostor, neprázdnou množinu $W \subseteq V$ nazvu vektorový podprostor prostoru V, pokud $\forall v, w \in W : v + w \in W$ a $\forall v \in W; r \in \mathbb{R}(\mathbb{C}) : r \cdot v \in W$.

Poznámka 1.2. Vektorový podprostor je i zřejmě vektorový prostor, protože také splňuje axiomy v.p., neboť je jeho podmnožinou. Ověřme například existenci neutrálního prvku: $W \subseteq V$ a je podprostor $V \Rightarrow W \neq \emptyset \Rightarrow \exists v \in W$ pak $0 \cdot v \in W$ z definice podprostoru je totiž uzavřený na násobení a $0 \cdot v = 0 \in W$ což je neutrální prvek.

Příklad 1.2.

1) $W = \{(r, 0, 0)\ r \in \mathbb{R}\} \cup \{(0, r, 0)\ r \in \mathbb{R}\}$ není vektorový podprostor $(\mathbb{R}^3, +, \cdot)$ neboť $(1, 0, 0) + (0, 1, 0) = (1, 1, 0) \notin W$

2) Rovina určená osami x a y je zřejmě vektorový podprostor vektorového prostoru $(\mathbb{R}^3, +, \cdot)$ nebo taky osa z je vektorový podprostor tohoto prostoru.

3) Vypište všechny podprostory prostoru $\mathbb{R}^2$

   a) celý prostor $\mathbb{R}^2$ je také podprostorem

   b) všechny přímky procházející počátkem - musí obsahovat neutrální prvek

   c) $\{0\}$ - triviální vektorový podprostor

Definice 1.3.

* Nechť V je vektorový prostor a $M \subseteq V$ je jeho podmnožina. Pak $\mathcal{L}(M) = \{\sum_{i=1}^{k} r_i v_i |\ r_i \in \mathbb{R}, v_i \in M, k \in \mathbb{N}_0\}$ nazveme lineární obal M.

* $v \in V$ je lineární kombinací prvků $\{v_1, \ldots, v_n\}$ pokud $\exists r_i \in \mathbb{R}$, že $v = \sum_{i=1}^{n} r_i v_i$

* $M \subseteq V$ nazvu lineárně závislou pokud $\exists k \in \mathbb{N}$, $\exists v_1 \ldots v_k \in M$, $\exists r_1 \ldots r_k \in \mathbb{R}$ kde alespoň jedno r je nenulové, tak že: $\sum_{i=1}^{k} r_i v_i = 0$

* M nazvu lineárně nezávislou, pokud není lineárně závislá.

Příklad 1.3.

1) Mějme $(1, 2), (2, 4) \in \mathbb{R}^2$ pak platí: $2(1, 2) + (-1)(2, 4) = (2, 4) + (-2, -4) = 0$. Tj. $\{(1, 2), (2, 4)\}$ je lineárně závislá. Navíc $(2, 4) = 2(1, 2)$ tedy je lineární kombinací $(1, 2)$.

2) Pokud $0 \in M \Rightarrow M$ je lineárně závislá.

   Nechť $\{0\} = M$ pak $1 \cdot 0 = 0$ což je lineární závislost. Nechť M obsahuje ještě jeden prvek $v \in M, v \neq 0$ pak $1 \cdot 0 + 0 \cdot v = 0$ zase je lineárně závislá.

3) Jestliže M je lineárně závislá, lze pak všechny $n \in M$ vyjádřit jako lineární kombinaci prvků z M?

   Neplatí! Př.: množina $\{(0, 0), (1, 2)\}$ je lineárně závislá, ale určitě nelze $(1, 2)$ vyjádřit jako lineární kombinaci prvků $(0, 0)$: $(1, 2) \neq r(0, 0)$

Lemma 1.1. Nechť $\{v_1, \ldots, v_k\} \subseteq V$, kde V je v.p., je lineárně nezávislá.
Pokud $\{v_1, \ldots, v_k, v_{k+1}\}$ je lineárně závislá pak v_{k+1} lze zapsat jako lineární kombinaci $\{v_1, \ldots, v_k\}$.

Důkaz. Předpokládejme tedy, že $\{v_1, \ldots, v_k\}$ je l.n. a $\{v_1, \ldots, v_k, v_{k+1}\}$ je l.z. Z definice lineární závislosti potom platí, že $(r_1, \ldots, r_k, r_{k+1})$ nejsou samé nuly (t.j. alespoň jedno r_i je nenulové)

Ukážeme-li, že r_{k+1} je nutně nenulové, důkaz bude téměř hotov.

Pro spor vezmeme r_{k+1} nulové. Tedy $0 = r_1v_1 + \cdots r_kv_k + 0v_{k+1} = r_1v_1 + \cdots r_kv_k$ přičemž nutně $(r_1, \ldots, r_k)$ nejsou samé nuly. Pak je ale tato množina lineárně závislá, což je spor s předpokladem. Víme tedy, že r_{k+1} je nenulové.

Algebraickou úpravou potom dostáváme: $v_{k+1} = -\frac{1}{r_{k+1}}(r_1v_1 + \cdots + r_kv_k)$, t.j v_{k+1} je lineární kombinaci vektorů $\{v_1 \ldots v_k\}$. □

Poznámka 1.3.

a) Platí tedy lemma pro $M = \{(0,0),(1,2)\}$? Množina ale není lineárně nezávislá, takže nesplňuje předpoklad lemmatu, ale množina $\{(1,2)\}$ už lineárně nezávislá je. Také platí, že $\{(1,2),(0,0)\}$ je linárně závislá. Pak opravdu umíme vektor $(0,0)$ zapsat jako lineární kombinaci, tedy $(0,0) = 0(1,2)$.

b) Mějme množinu $M = \{v_1, \ldots, v_k\}$ a nech $\exists i \in \{1 \ldots k\} : v_i = \sum_{j=1\ j\neq i}^{k} \alpha_j v_j$. Pak M je lineárně závislá. Důkaz: $\sum_{j=1\ j\neq i}^{k} \alpha_j v_j - v_i = 0$ což je netriviální lineární kombinace (před v_i je -1) takže M je linárně závislá.

2. přednáška z lineární algebry

Steinitzova věta

9. říjen 2007

Zopakujme

LEMMA 1.2. Nechť $\{v_1, \ldots, v_k\}$ je l.n. Pokud $\{v_1, \ldots, v_k, v_{k+1}\}$ je l.z., pak v_{k+1} je l.k. množiny $\{v_1, \ldots, v_k\}$.

DŮKAZ. viz přednášku. □

Obměna implikace $a \Rightarrow b$ je $\neg b \Rightarrow \neg a$ a je jí ekvivalentní. Výroku před implikační spojkou se říká antecedent a výroku za ní konsekvent.

Obměna lemmatu 1.1. říká: Nechť $\{v_1, \ldots, v_k\}$ je l.n. Pokud není v_{k+1} l.k. $\{v_1, \ldots, v_k\}$, potom je $\{v_1, \ldots, v_k, v_{k+1}\}$ l.n.

Uvažme relace $R(x, y)$ dvou prvků x, y (binární relaci) jako jsou např. relace "x rovnoběžné s y," "x dělí y," popř. "x zná y". Řekneme, že R je reflexivní, pokud $R(x, x)$ platí pro všechny uvažované x. Řekneme, že je symetrická, pokud platí $R(x, y)$, právě tehdy když platí $R(x, y)$ pro všechny uvažované x, y. Nakonec řekneme, že R je tranzitivní, pokud z $R(x, y)$ a $R(y, z)$ plyne $R(x, z)$ opět pro všechny x, y, z, pro něž má relace R smysl. Relaci, která je reflexivní, symetrická a tranzitivní, říkáme ekvivalence. Relace rovnoběžnosti je zřejmě ekvivalencí. Relace dělitelnosti není, neboť není symetrická: jednotka dělí dvojku, ale dvojka nedělí jednotku. Pojem známosti zase není tranzitivní - a chceme-li filozofovat, tak možná ani není reflexivní (znáte sami sebe? ;-).)

VĚTA 1.3. (Steinitz): Nechť $M := \{v_1, \ldots, v_r\}$ a $N := \{w_1, \ldots, w_s\}$ jsou konečné l.n. množiny a nechť platí

(1) $\forall i \in \{1, \ldots, r\}$ je v_i l.k. $\{w_1, \ldots, w_s\}$ a

(2) $\forall j \in \{1, \ldots, s\}$ je w_j l.k. $\{v_1, \ldots, v_r\}$.

Potom $r = s$.

DŮKAZ. Splňují-li dvě konečné l.n. množiny relaci (1) a (2), budeme psát $\{v_1, \ldots, v_r\} \simeq \{w_1, \ldots, w_s\}$. Zřejmě platí, že $\simeq$ je symetrická, reflexivní a tranzitivní, tj. je to relace ekvivalence (jak jsme ukázali na přednášce nebo snadno sami). Dokažme jako část důkazu Steinitzovy věty násl. pozororvání. Potom se k důkazu věty vrátíme.

POZOROVÁNÍ: Pokud M, N tvaru výše splňují $M \simeq N$, potom pro každé v_i, $i = 1, \ldots, r$ (v dalším bude stačit existence pro $i = r$), existuje w_{j_r}, $j_r \in \{1, \ldots, s\}$, že $\{v_1, \ldots, v_{r-1}, w_{j_r}\} \simeq \{w_1, \ldots, w_s\}$. Tj. element v_r jsme vyměnili za element w_{j_r}, aniž bychom porušili relaci.

DŮKAZ. Při prvním čtení můžete pro jednoduchost důkaz tohoto Pozorování vypustit a číst text začínající až po něm (pracovat jako by bylo pozorování dokázáno), ale pak se k němu vrátit.

a) Zřejmě $\{v_1, \ldots, v_{r-1}\} \not\simeq \{w_1, \ldots, w_s\}$, neboť předpokládejme pro spor, že $\{v_1, \ldots, v_{r-1}\} \simeq \{w_1, \ldots, w_s\}$. Potom ale kvůli tomu, že $\{w_1, \ldots, w_s\} \simeq \{v_1, \ldots, v_r\}$, plyne z tranzitivity relace $\simeq$, že $\{v_1, \ldots, v_{r-1}\} \simeq \{v_1, \ldots, v_r\}$, odkud však plyne, že v_r je l.k. $\{v_1, \ldots, v_{r-1}\}$, tj. $\{v_1, \ldots, v_r\}$ by byla l.z. (podle Poznámky 1.3.), čímž bychom dostali spor s pp. tohoto Pozorování.

b) Nyní tedy víme, že $\{v_1, \ldots, v_{r-1}\} \not\simeq \{w_1, \ldots, w_s\}$. Co to znamená podle definice relace $\simeq$? Víme z předpokladu Pozorování, že v_i je l.k. $\{w_1, \ldots, w_r\}$ pro $i = 1, \ldots, r$ a tím spíše i pro $i = 1, \ldots, r-1$, a proto zřejmě nějaký element w_j z $\{w_1, \ldots, w_s\}$ není l.k. elementů z $\{v_1, \ldots, v_{r-1}\}$, aby mohlo platit

$$\{v_1, \ldots, v_{r-1}\} \not\simeq \{w_1, \ldots, w_s\}.$$

Vezměme tento element a položme $w_{j_r} := w_j$. Tvrdíme, že je to vhodný kandidát. Definujme $M' = \{v_1, \ldots, v_{r-1}, w_{j_r}\}$ a snažme se tedy dokázat, že $M' \simeq N$, tj. že je splněn konsekvent Pozorování pro tohoto kandidáta.

(1) Ukažme, že M' je l.n. Jelikož $\{v_1, \ldots, v_{r-1}\}$ je l.n. a $w_{j_r} = w_j$ není l.k. množiny $\{v_1, \ldots, v_{r-1}\}$ (z definice w_{j_r}), je pak $M' = \{v_1, \ldots, v_{r-1}, w_j\}$ l.n. dle obměny Lemmatu 1.1., což bylo dokázat.

(2) Nyní ukažme, že každý element z $M' = \{v_1, \ldots, v_{r-1}, w_j\}$ je l.k. $N = \{w_1, \ldots, w_s\}$ a naopak každý element z N je l.k. M', tj. zbylé podmínky pro platnost relace $M' \simeq N$. Zřejmě každý element $v_i, i = 1, \ldots, r-1$ je l.k. $\{w_1, \ldots, w_s\}$ dle pp. Pozorování. Element w_j je také l.k. mny $N = \{w_1, \ldots, w_s\}$, neboť $w_j \in N$, ale zda naopak můžeme každý $w_i \in N$ napsat jako l.k. mny M', nevíme. Zkusme nejdříve dokázat, že

$$M' = \{v_1, \ldots, v_{r-1}, w_j\} \simeq M = \{v_1, \ldots, v_r\} \, (*),$$

odtud totiž by již plynulo že, $M' \simeq N$, neboť víme dle pp., že $M \simeq N$, což dohromady s $(*)$ dává dík tranzitivitě $M' \simeq N$. Zkusme tedy, zda podle definice relace $\simeq$ platí $(*)$, tj. $\{v_1, \ldots, v_{r-1}, w_j\} \simeq \{v_1, \ldots, v_r\}$. Za prvé v_i jsou l.k. M pro $i = 1, \ldots, r-1$ a w_j je také l.k. elementů z M, neboť $w_j \in N = \{w_1, \ldots, w_s\}$ a každý element z N lze psát jako l.k. elementů z $M = \{v_1, \ldots, v_r\}$ dle pp. Pozorování. Zbývá tedy ověřit, zda každý element z M je l.k. elementů z M'. Pro v_i, $i = 1, \ldots r-1$ je to opět snadné, neboť jsou obsaženy v obou těchto množinách (M i M'). Zbývá toto ověřit pro v_r. Zkusme následující. Jistě platí (dle pp. pozorování), že w_j je l.k. elementů z $M = \{v_1, \ldots, v_r\}$, tj. platí

$$w_j = c_1 v_1 + \ldots c_{r-1} v_{r-1} + c_r v_r \, (**)$$

pro $c_i \in \mathbb{R}$, $i = 1, \ldots, r$. Zkusme dokázat, že $c_r \neq 0$. Kdyby pro spor $c_r = 0$, potom předchozí rovnost přechází na $w_j = c_1 v_1 + \ldots c_{r-1} v_{r-1}$, tj. w_j je l.k elementů z $\{v_1, \ldots, v_{r-1}\}$, což je však spor s volbou w_j, neboť jsme jej volili tak, aby nebylo l.k. uváděných prvků (tato volba je klíčovou částí idey důkazu). Je tedy $c_r \neq 0$ a mohu rovnost $(**)$ převést na $v_r = -\frac{1}{c_r}(w_j - c_1 v_1 - \ldots - c_{r-1} v_{r-1})$, tj. i v_r je l.k. elementů z M', c.b.d. Tím je pozororvání dokázáno. □

Pokračujme v důkazu Steinitzovy věty.

Iterujemu-li proces v Pozorování, dostaneme, že $\{v_1, \ldots, v_{r-1}, w_{j_r}\} \simeq \{w_1, \ldots, w_s\}$, $\{v_1, \ldots, v_{r-2}, w_{j_{r-1}}, w_{j_r}\} \simeq \{w_1, \ldots, w_s\}$, a nakonec $\{w_{j_1}, \ldots, \ldots, w_{j_r}\} \simeq \{w_1, \ldots, w_s\}$. Dokažme, že $\{w_{j_1}, \ldots, w_{j_r}\} = \{w_1, \ldots, w_s\}$ jako množiny. Jistě $\{w_{j_1}, \ldots, w_{j_r}\} \subseteq \{w_1, \ldots, w_s\}$. Předpokládejme pro spor ostrou inkluzi, tj. $\{w_{j_1}, \ldots, w_{j_r}\} \subsetneq \{w_1, \ldots, w_s\}$, a proto existuje $w_i \in \{w_1, \ldots, w_s\}$, že $w_i \notin \{w_{j_1}, \ldots, w_{j_r}\}$. Jelikož $w_i \in \{w_1, \ldots, w_r\}$ a $\{w_1, \ldots, w_r\} \simeq \{w_{j_1}, \ldots w_{j_r}\}$, jak jsme dokázali, je tedy w_i l.k. elementů z $\{w_{j_1}, \ldots, w_{j_r}\}$, tj. existují reálná $d_i \in \mathbb{R}$, $i = 1, \ldots, r$, že $w_i = \sum_{k=1}^{r} d_k w_{j_k}$. Odtud ekvivalentní rovnost: $w_i - \sum_{k=1}^{r} d_k w_{j_k} = 0$, která je zjevně netriviální l.k. Nnetrivialita plyne z toho, že koeficient u w_i (který dle toho, co nyní předpokládáme, není v sčítanci se sumou $\sum$) je roven $+1$. To však poskytuje spor s tím, že N je l.n. (Našli jsme podmnožinu $\{w_i, w_{j_1}, \ldots, w_{j_r}\} \subseteq N$, která je l.z., tj. formálně spor s Tvrzením 1.2 o tom, že podmnožina l.n. mny (mny N) je také l.n.) Celkem tedy

$$\{w_{j_1}, \ldots, w_{j_r}\} = \{w_1, \ldots, w_s\}.$$

Jelikož prvky množiny nalevo od rovnosti jsou vesměs různé a prvky množiny napravo od rovnosti jsou také vesměs různé (jinak by byly l. z), dostávám dík rovnosti množin, že $r = s$ (stejné mny mají stejný počet prvků), čímž je důkaz ukončen. □

Poznámka 1.4.

(1) Klíčovou ideou bylo nalezení w_{j_r} a zbytek důkazu jsme jen ověřovali, že tento element existuje a po jeho nalezení jsme dokazovali, že splňuje naše požadavky (konsekvent Pozorování).

(2) V přednášce se objevil drobný přepis, který jistě odhalíte, totiž za větou "Pokračujeme-li tento proces dále, dostaneme $\{v_1, \ldots, v_{r-1}, w_{j_{r-1}}, w_{j_r}\} \simeq \{w_1, \ldots, w_s\}$, $\{v_1, \ldots, v_{r-2}, w_{j_{r-2}} w_{j_{r-1}}, w_{j_r}\} \simeq \{w_1, \ldots, w_s\}$..." mají být posunuté indexy. Tj. má být správně: "... $\{v_1, \ldots, v_{r-2}, w_{j_{r-1}}, w_{j_r}\} \simeq \{w_1, \ldots, w_s\}$, $\{v_1, \ldots, v_{r-3}, w_{j_{r-2}}, w_{j_{r-1}}, w_{j_r}\} \simeq \{w_1, \ldots, w_s\}$..."

(Vždy odzadu nahrazuji/vyměňuji v_i pomocí členů w_{j_i}. Steinitzově větě se někdy říká věta o nahrazení/výměně.)

(3) Význam Steinitzovy věty spočívá v tom, že nám umožní pro konečně dimenzionální (bude později) vektorový prostor dokázat, že počet prvků l.n. mny, která takovýto prostor generuje, je nezávislý na volbě takovéto množiny. Tj. počet prvků báze (l.n. mny generující celý v.p.) je pro všechny báze daného v.p. stejný, konstantní.

3. prednáška z lineárnej algebry

16. október 2007

PRIPOMENUTIE. Niekedy minule sme si zaviedli internú reláciu $\simeq$ medzi dvomi množinami vektorov. Ak platilo $\{v_1, \ldots, v_r\} \simeq \{w_1, \ldots, w_s\}$, potom obe množiny boli l.n. a $\forall i \in \{1, \ldots, r\}$ platí, že v_i je l.k. $\{w_1, \ldots, w_s\}$ a obdobne naopak. Dokonca sme si ukázali, že ak sú dve množiny v danej relácii, potom nutne $r = s$ (Steinitzova veta).

DEFINÍCIA 1.4. (dôležitá!!!) Nech $M \subseteq V$. Ak M je l.n. & M generuje V (t.j. $\mathcal{L}(M) = V$), tak M nazveme **bázou** priestoru V.

PRÍKLAD 1.4. Uvažujme vektorový priestor $\mathbb{R}^2 := \mathbb{R} \times \mathbb{R} = \{(x, y) | x \in \mathbb{R}, y \in \mathbb{R}\}$ s obvyklým sčítaním a násobením reálnym číslom a jeho podmnožinu $M = \{(1, 0), (0, 1)\}$. Je M jeho bázou?

Riešenie: Podľa definície báze stačí ukázať, že M je l.n. a že generuje $\mathbb{R}^2$. Nech $\exists r_1, r_2 \in \mathbb{R}$ také, že $r_1(1, 0) + r_2(0, 1) = (0, 0)$. Potom máme

$$(0, 0) = r_1(1, 0) + r_2(0, 1) = (r_1, 0) + (0, r_2) = (r_1, r_2) \Rightarrow r_1 = r_2 = 0$$

takže sa jedná o triviálnu lineárnu kombináciu a teda M je l.n. Teraz ukážeme, že každé $(a, b) \in \mathbb{R}^2$ patrí do $\mathcal{L}(M)$

$$(a, b) = a(1, 0) + b(0, 1) \in \mathcal{L}(M)$$

a teda $\mathbb{R}^2 \subseteq \mathcal{L}(M)$, čo zrejme platí aj opačne, čo potom dáva $\mathbb{R}^2 = \mathcal{L}(M)$ a teda sa jedná o generátor. Ako cvičenie to samé overte pre $M = \{(1, -1), (1, 2)\}$ (návod: budete riešiť raz homogénnu a raz „normálnu" sústavu dvoch rovníc o dvoch neznámych)

Príklad nám ilustruje dôležitý fakt a to ten, že báza daného priestoru nie je jedna (ale dokonca ich je nekonečne mnoho), čo sa ukáže ako kľúčový „problém" celej tejto časti.

TVRDENIE 1.4. Nech $M, N \in V$ sú konečné a M i N sú báze V. Potom $\#M = \#N$ ($\#$ značí počet prvkov).

DÔKAZ. Stačí dokázať, že z predpokladov platí $M \simeq N$ (potom už len užijeme Steinitzovu vetu a dôkaz je hotový). No nie je nič ľahšie. Ak $v \in M$ tak v je l.k. N, lebo tiež $v \in V$ a N generuje V. Množina M je tiež l.n. lebo je to báza. Podone ak $w \in N$ tak v je l.k. M, lebo tiež $w \in V$ a M generuje V. Množina N je znova l.n. lebo je to báza. Toto sú podmienky, ktoré keď sú splnené, tak môžme písať $M \simeq N$. □

TVRDENIE 1.5. Nech M je konečná báza V, nech N je báza V. Potom N je konečná.

Poznámka: Možno sa môžte nazdávať, že toto je (taktiež ako tvrdenie 1.4) triviálny dosledok S.v. ale tak to nie je, lebo S.v. bola formulovaná za predpokladu konečnosti oboch množín.

DÔKAZ. Podobne ako v dôkaze predchádzajúceho tvrdenia môžme zistiť, že $M \simeq N$. Teraz budeme postupovať chvíľu veľmi podobne ako pri dôkaze S.v. Označme $M = \{v_1, \ldots, v_r\}$, $N = \{w_1, \ldots\}$ a pre spor predpokladajme, že N je nekonečná (preto sme ju formálne neukončili nejakým w_s). Podobne ako v dôkaze S.v. (odporúčam si ho znova prečítať, ak sa vám zdá, že robíme niečo neoprávnene) platí $\{v_1, \ldots, v_{r-1}, w_{j_r}\} \simeq N$, kde $w_{j_r} \in N$ a w_{j_r} sa nedá zapísať ako l.k. $\{v_1, \ldots, v_{r-1}\}$ (takýto vektor nájsť vieme). Iterovaním nakoniec dostaneme $\{w_{j_1}, \ldots, w_{j_r}\} \simeq N$. Postupujeme v dôkaze ďalej. Určite platí, že $\exists w \in N$ také, že $w \notin \{w_{j_1}, \ldots, w_{j_r}\}$. To platí, pretože keby tomu tak nebolo, tak by $N \subseteq \{w_{j_1}, \ldots, w_{j_r}\}$ a teda by nemohla byť nekonečná, čo by bol spor s predpokladom sporu. Nakoľko ale $w \in N$ a $\{w_{j_1}, \ldots, w_{j_r}\} \simeq N$, tak w je l.k. $\{w_{j_1}, \ldots, w_{j_r}\}$, takže sme potom schopní nájsť netriviálnu lineárnu kombináciu vektorov $\{w, w_{j_1}, \ldots, w_{j_r}\}$ rovnajúcu sa nule ($0 = -1w + \sum_{i=1}^{r} r_i w_{j_i}$, pričom nenulový koeficient je minimálne pred w, keďže sme našli w tak, že ho nenájdeme v množine vektorov v sume) a tým získame l.z. množinu, ktorá je podmnožinou N a podľa vety, že ak množina obsahuje l.z. podmnožinu, tak je l.z, je i N l.z. To je ale v spore s predpokladom tvrdenia, že N je bázou. □

Definícia 1.5. Nech M je konečná báza V, potom V nazveme vektorový priestor **konečnej** dimenzie. Ak neexistuje M báza V, ktorá je konečná, potom nazveme V vektorový priestor **nekonečnej** dimenzie. Ak V je konečnej dimenzie a M je báza V, označíme $\dim V = \#M$.

Poznámka 1.5. Definícia 1.5 je korektná! Popravde povedané, celé toto snaženie bolo vyvinuté len kôli tomu, aby sme boli schopní odôvodniť túto poznámku. Tak to teda s radosťou spravme. Podľa predchádzajúcich tvrdení môžme povedať, že ak nájdeme M bázu V, ktorá je konečná s počtom prvkov $\#M$, tak všetky ostatné bázy, ktoré nájdeme (ako sme už naznačili, že ich vieme nájsť nekonečne mnoho), majú konečný a dokonca aj rovnaký počet prvkov. Tým pádom je $\dim V$ dobre (korektne/jednoznačne) definované. A taktiež ak nájdeme čo i len jednu nekonečnú bázu V, tak si môžme byť istí, že konečnú bázu nenájdeme a môžme so spokojnosťou prehlásiť, že V je nekonečnej dimenzie.

Príklad 1.5.

a) $\dim \mathbb{R} = 1$, lebo množina $\{1\}$ je báza $\mathbb{R}$, lebo je lineárne nezávislá ($\forall r \in \mathbb{R}$ platí $r \cdot 1 = 0 \Rightarrow r = 0$) a generuje celý priestor ($\forall r \in \mathbb{R}$ platí $r = r \cdot 1$).

   $\dim \mathbb{R}^2 = 2$, lebo množina $\{(1,0),(0,1)\}$ je báza, ako sme si ukázali v prechádzajúcom príklade. Teraz už ale vieme, že každá iná báza, ktorú sme schopní nájsť, ma rovnaký počet prvkov, čiže 2.

   $\dim \mathbb{R}^n = n$, lebo množina $\{(1,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,\ldots,0,1)\}$ je báza (a má teda n prvkov). Túto bázu budeme nazývať **kanonickou** bázou.

b) Označme $\mathcal{P} = \mathbb{R}[x] = \{\sum_{i=0}^{n} a_i x^i | a_i \in \mathbb{R}, n \in \mathbb{N}_0\}$ priestor polynómov. Môžte si uvedomiť, že $\mathcal{P}$ je vektorový priestor (teda spĺňa axiómy vektorového priestoru). Ďalej si definujme $\mathcal{P}_k := \{\sum_{i=0}^{k} a_i x^i | a_i \in \mathbb{R}\}$, pričom $k \in \mathbb{N}_0$, čo je vektorový priestor polynómov najviac k-tého stupňa.

   Tvrdenie príkladu. Tvrdíme, že $\dim \mathcal{P}_k = k+1$ a že $\mathcal{P}$ je nekonečnej dimenzie.

   Dôkaz tvrdenia príkladu. Najskôr dokážme, že $\dim \mathcal{P}_k = k+1$. Podľa toho, čo sme sa doteraz naučili, stačí nájsť ľubovolnú bázu tohto priestoru, spočítať (napr. aj na prstoch) jej prvky a máme vyhrané. Ukážme teda, že množina $M := \{x^0, x^1, \ldots, x^k\}$ je bázou $\mathcal{P}_k$. Nepochybne M generuje celý vektorový priestor, čo je jasné z jeho definície (pozrite si ju znova). Stačí teda ukázať, že M je l.n. Pred tým, ako to spravíme, si pripomeňme čosi o delení polynómu polynómom.

   Označme polynóm, ktorý chceme deliť P a nenulový polynóm, ktorým chceme deliť Q. Potom platí, že existuje polynóm S a R, pričom $\operatorname{st} R < \operatorname{st} Q$ (st je stupeň) tak, že $P = SQ + R$. Vráťme sa späť k dôkazu.

   Pre spor predpokladajme, že M je l.z., t.j. $\exists (b_0,\ldots,b_k) \neq (0,\ldots,0)$ také, že $b(x) := \sum_{i=0}^{k} b_i x^i = 0$. Nula na pravej strane je nulový polynom, čo potom znamená, že suma na strane lavej je identická nula, teda sa rovná nule pre všetky $x \in \mathbb{R}$. To ale v normálnej reči znamená, že polynom, má nekonečne veľa koreňov. Pre konkrétnosť si vyberme množinu koreňov $\{0,1,\ldots,k\}$ pomocou ktorej ukážeme, že polynom pomocou koeficientov $(b_0,\ldots,b_k)$ vytvorený, musí byť stupňa minimálne $k+1$, čo je spor s tým, čo sme už ukázali, a síce M generuje $\mathcal{P}_k$ (t.j. $\mathcal{L}(M) = \mathcal{P}_k$). Tak to teda ukážme: Vydelme náš polynom $b(x)$ polynomom $(x-0)$, teda to zapíšme pomocou spmínaného vzťahu $P = QS + R$. Čiže $b(x) = (x-0)s_0(x) + r_0(x)$, kde $\operatorname{st} r_0(x) < \operatorname{st}(x-0)=1$, teda polynóm $r_0(x)$ je obyčajné číselko, označme ho r_0. Keďže 0 je koreň polynómu $b(x)$, tak dosadením dostaneme $0 = (0-0)s_0(0) + r_0$, z čoho dostávame $r_0 = 0$, teda môžme písať $b(x) = (x-0)s_0(x)$. Vydelme teraz polynóm $s_0(x)$ polynómom $(x-1)$. Znova dostaneme $s_0(x) = (x-1)s_1(x) + r_1$. No tak isto ako 0, tak aj 1 je koreňom polynómu $b(x)$, teda dosadením do vzťahu pre $b(x)$ dostaneme $0 = (1-0)s_0(1)$, z čoho jasne vyplýva, že 1 je koreňom $s_0(x)$, z čoho potom podobným postupom dostaneme $r_1 = 0$, teda

$s_0(x) = (x-1)s_1(x)$. Iterovaním tohto procesu dostaneme výsledok $b(x) = s_k(x)\prod_{i=0}^{k}(x-i)$. O polynóme $s_k(x)$ vieme len to (a to nám stačí), že nie je 0 (nulový polynóm). Keby bolo $s_k(x) = 0$, tak môžme vidieť, že by všetky koeficienty β_i, stojace u x^i po roznásobení súčinu na pravej strane, boli nulové, čo ale vzhľadom na to, že rovnica $P = QS + R$ je identita nie len funkcií, ale aj v zmysle, že koeficient u x_i napravo je rovnaký, ako koeficient u x_i naľavo, dáva rovnosť $b_i = \beta_i$, čo by bolo potom v spore s predpokladom sporu. Takže z toho konečne máme, že $\operatorname{st} b(x) \geq k+1$ a máme vytúžený spor.□

Dokážme ešte chytro druhú časť tvrdenie, teda že vektorový priestor $\mathcal{P}$ je nekonečnej dimenzie. Znova pre spor predpokladajme, že jeho dimenzia je konečná, t.j. existuje množina M, ktorá je jeho báza a je konečná. Zrejme môžme nájsť maximum množiny $\{\operatorname{st} p | p \in M\}$ a označme ho m. Potom tiež zrejme $\mathcal{L}(M) \subseteq \mathcal{P}_m \subsetneq \mathcal{P}$. To ale potom znamená, že M negenuruje $\mathcal{P}$, čo je v spore s predpokladom, že M je báza $\mathcal{P}$. □

c) Označme symbolom $\mathcal{C}^0(\mathbb{R})$ priestor všetkých (reálnych či komplexných) spojitých funkcií na $\mathbb{R}$ definovaných (0 znakčí, že ich 0-tá derivácia je spojitá). Priestor je nekonečnej dimenzie, čo môžme ľahko nahliadnuť z $\mathcal{P} \subseteq \mathcal{C}^0(\mathbb{R})$.

Veta 1.6. Nech V je vektorový priestor konečnej dimenzie a označme $n := \dim V$. Platí, že ak množina M generuje V, tak $\#M \geq n$.

Dôkaz. Pred tým ako formulujeme dôkaz, ukážme si jeden algoritmus (chápte ako súčasť dôkazu).

Algoritmus 1.1. Tento algoritmus má ako vstup IN: $M := \{v_1, \ldots, v_r\}$ a výstup OUT: $N \subseteq M$ množina taká, že N je l.n. a $\mathcal{L}(N) = \mathcal{L}(M)$. Teda algoritmus z množiny vyberie nezávislú podmnožinu tak, že lin. obal sa nezmení. Napíšeme jednotlivé kroky algoritmu:

1. Zvoľ 1. nenulový vektor z M a daj ho do N. Nech je to j_1-tý vektor, čiže potom $N = \{v_{j_1}\}$. Ak sa ti to nepodarí, tak skonči a prehlás, že sa jedná o nezaujímavý a triviálny prípad. Inak choď na ďalší krok.
2. Zvoľ 1. vektor z M, ktorý nie je l.k. vektorov z množiny N. Nech je to j_2-tý vektor. Polož $N = \{v_{j_1}, v_{j_2}\}$. Ak sa ti to nepodarí, tak skonči a prehlás, že N je výsledok. V opačnom prípade choď na ďalší krok.
3. a.t.ď.

Poznámka 1.6. Algoritmus je správny. Dokážeme to: To znamená, že overíme, či množina N je l.n. a či $\mathcal{L}(N) = \mathcal{L}(M)$. To, že množina N je l.n. je triviálny dôsledok obmeny lemmatu, ktorý hovorí, že máme l.n. množinu vektorov a ak po pridaní nejakého vektoru vznikne množina l.z., tak tento vektor je l.k. pôvodnej množiny. Overme teraz, či naozaj platí pre algoritmom nájdenú množinu N, že $\mathcal{L}(N) = \mathcal{L}(M)$. Určite môžme povedať, nakoľko $N \subseteq M$, že platí $\mathcal{L}(N) \subseteq \mathcal{L}(M)$. Ukážme teraz aj opačnú inklúziu. Nech vektor $w \in \mathcal{L}(M)$. Potom môžme vektor zapísať ako l.k., t.j $w = \sum_{i=1}^{r} c_i v_i$. Otázka je, či platí i $w \in \mathcal{L}(N)$. Definujme si dve množiny.

$$M_{w1} := \{v_i \in M | c_i \neq 0, v_i \in N\}$$
$$M_{w2} := \{v_i \in M | c_i \neq 0, v_i \notin N\}$$

Pre všetky vektory $x \in M$ podľa algoritmu platí, že ak $x \notin N$, tak x sa dá zapísať ako l.k. vektorov z N. Takže ako prvky z M_{w1}, tak prvky z M_{w2} vieme zapísať ako l.k. vektorov z N (pre prvky z M_{w1} je to moc jasné na to, aby sme tomu venovali poznámku v zátvorke, takže robíme teraz zbytočnosť), čo potom znamená, že $w = \sum_{i=1}^{r} c_i v_i = \sum_{i=1}^{r}\sum_{k=1}^{s} c_i \alpha_{ij_k} v_{j_k}$, kde α_{ij_k} je koeficient stojaci pri vektore v_{j_k} pri rozpise vektoru v_i ako l.k. vektorov z N. No ale vidíme, že dvojitá suma je vlastne sumou vektorov z N, takže $w \in \mathcal{L}(N)$, čím sme dokázali $\mathcal{L}(N) \supseteq \mathcal{L}(M)$.

Teraz by sme mali pokračovať v dôkaze Vety 1.6, ale prednáška práve v tomto bode skončila (no to vás ale nemusí odradiť od toho, že si ho skúsite dokázať sami, keďže všetko potrebné máte už teraz k dispozícii).

4. prednáška z lineárnej algebry

23. október 2007

PRIPOMENUTIE. Minule sme si ukázali algoritmus, ktorý z množiny M vyberie jej podmnožinu M', takú, že M je l.n. a $\mathcal{L}(M') = \mathcal{L}(M)$. Aplikovanie algoritmu budeme písať $M = \{v_1, \ldots, v_k\} \rightsquigarrow M' = \{v_{j_1}, \ldots, v_{j_r}\}$, kde $1 \leq j_i \leq k$ pre $i = 1, \ldots, r$. Vrhnime sa teraz na dôkaz vety 1.6 (ktorej znenie ak si presne nepamätáte, tak si ho ešte raz prečítajte), ktorý sme si odložili práve na teraz.

DÔKAZ. Najskôr uvážme prípad, že M je nekonečná. V tomto prípade je určite počet jej prvkov väčší ako konečná dimenzia V. Takže v prípade M je konečná označme jej prvky $\{m_1, \ldots, m_q\}$. Označme ešte nejakú bázu nášho priestoru ako B, pričom $\#B = \dim V = n$. Aplikujme algoritmus na M a dostaneme $M' = \{m_{j_1}, \ldots, m_{j_r}\}$, kde znova pre istotu explicitne napíšeme $1 \leq j_i \leq q$ pre $i = 1, \ldots, r$. Nie je ťažké si uvedomiť, že M' je bázou V a preto podľa tvrdenia 1.4 (dve báze majú rovnaký počet prvkov) máme $r = \#M' = \#B = n$. Taktiež, keďže $M' \subseteq M$, máme $\#M = q \geq r = n$. □

VETA 1.7. Nech V je v.p.k.d. a $\dim V = n$. Nech ďalej $M \subseteq V$ je l.n. Potom $\#M \leq n$. Veta je v istom zmysle podobná ako predchádzajúca, viď potom Poznámku 1.7.

DÔKAZ. Najskôr vyšetrime prípad M je konečná. Označme $M = \{m_1, \ldots, m_q\}$ a prvky nejakej bázy $B = \{b_1, \ldots, b_n\}$. Aplikujme algoritmus na

$$M \cup B = \{m_1, \ldots, m_q, b_1, \ldots, b_n\} \rightsquigarrow M' = \{m_1, \ldots, m_q, b_{j_1}, \ldots, b_{j_r}\}, \quad 1 \leq j_i \leq n,\ i = 1, \ldots, r$$

Je dôležité si teraz uvedomiť, čo sa stalo. Stalo sa to, že algoritmus vybral a musel vybrať všetky vektory z M, pretože M je l.n. a algoritmus ide zľava. Potom podľa toho, či M generuje V alebo nie (rozmyslite) vybral ešte nejaké vektory naviac z B. Uvedomením si, že $\mathcal{L}(M \cup B) = V$ (uvedomťe si obe inklúzie) znova dostaneme, že M' je báza a preto $\#M' = \#B = n$ a tiež platí $q + r = \#M'$, z čoho konečne máme $\#M = q \leq n$.

Pre M je nekonečná postupujeme podobne a skončime pri konštatovaní, že M' je báza. No keďže M' obsahuje celú M, tak musí byť nekonečná, čo ale podľa tvrdenia 1.5 (nemôžme mať zároveň konečnú a nekonečnú bázu) dáva spor. Takže sme dokázali, že M je konečná s počtom prvkov $\#M \leq n$. □

Hĺbavý čitateľ teraz istotne ostáva znepokojený (poznamenám len, že autor tohto textu ním nie je), keďže ak by nekonečná množina M bola nespočetná, t.j. nejde ju bijektívne zobraziť na $\mathbb{N}$, tak by sme algoritmus vôbec použiť nemohli, nakoľko algoritmus, tak ako bol definovaný, vyžaduje oindexovanie prvkov vstupujúcej množiny a hlavne zoradenie do rady, čo by v prípade nespočetnej množiny evidentne nešlo. Takže sme podvádzali, ale keďže sme si toho vedomí, tak celkom korektný dôkaz poskytneme teraz. Nech je teda M l.n. a nekonečná (či už spočetná alebo nespočetná). Potom z nej určite môžme vybrať $n+1$ prvkovú podmnožinu, označíme N. Aplikujeme algoritmus na mn. $N \cup B$ a dostaneme $n + 1 + r$ prvkovú mn. o ktorej vieme, že je bázou. Potom ale dostávame $n+1+r = n$, z čoho musí byť r záporné, čo je spor s tým, že podľa algoritmu je kladné. Môžme teraz tiež „korektnejšie" dokázať tvrdenie 1.5 hovoriace, že v.p.k.d má všetky báze konečné. Stačí si pri dôkaze uvedomiť, že ak v.p. je aj k.d., tak existuje z definície konečná báza, nech má n prvkov. Každá iná báza musí mať ale podľa vety, ktorú sme práve korektne dokázali, maximálne n prvkov (báza je tiež l.n!).

POZNÁMKA 1.7.

a) Z Vety 1.6 vyplýva, že báza B vektorového priestoru V je najmenšia generujúca množina. Nemysíme tým ale to, že ak M generuje V, tak by nutne $B \subseteq M$ (teda najmenším myslíme s najmenším počtom prvkov).

b) Z Vety 1.7 vyplýva, že báza B vektorového priestoru V je najväčšia l.n. množina. Nemysíme tým ale to, že ak M je l.n. tak by nutne $M \subseteq B$ (teda najväčším myslíme s najväčším počtom prvkov).

Definícia 1.6. Nech V je v.p.k.d., $\dim V = n$, označme bázu $B = \{b_1, \ldots, b_n\}$, nech ešte $v \in V$. n-ticu $(v^1, \ldots, v^n) \in \mathbb{R}^n$ nazveme súradnice vektoru v vočí bázi B, ak

$$v = \sum_{i=1}^{n} b_i v^i$$

Poznámka: Vedzte, že súradnice budeme indexovať hornými indexami. Robíme to pre vaše dobro, v záujme vašej budúcnosti. Ak vám to ale z nejakých príčin vadí, predstavujte si ich dole.

Lemma 1.8. Ako si môžte všimnúť, predchádzajúca definícia súradníc nehovorí nič o tom, že daný vektor má len jedny súradnice voči nejakej pevnej bázi. No pravdou je, že ich má len jedny. A táto (večná (?)) pravda je náplňou tohto lemmatu (a my sa teda v príslušnom dôkaze presvedčíme, že to naozaj pravda je). Ale tak to ešte dáko sformulujme: Buď V v.p.k.d. s $\dim V = n$ a bázou B. Nech $v \in V$. Potom ak sú $(v^1, \ldots, v^n)$ súradnice v voči B a zároveň $(w^1, \ldots, w^n)$ sú súradnice v voči B, tak nutne $v^i = w^i$ pre $i = 1, \ldots, n$.

Dôkaz. Nech teda $v = \sum_{i=1}^{n} b_i v^i$ a zároveň $v = \sum_{i=1}^{n} b_i w^i$. Potom ale máme

$$\sum_{i=1}^{n} b_i v^i = \sum_{i=1}^{n} b_i w^i \;\Rightarrow\; \sum_{i=1}^{n} b_i (v^i - w^i) = 0 \;\Rightarrow\; v^i - w^i = 0, \quad i = 1, \ldots, n$$

Posledná implikácia platí, lebo vektory báze sú l.n. □

Lemma 1.9. Nech W_1 a W_2 sú vektorové podpriestory priestoru V. Potom aj $W_1 \cap W_2$ je vektorový podpriestor. Lemma moc nesúvisí s ničím, o čom sme teraz hovorili, ale vy ste určite radi, že sa zas dozviete niečo nové.

Dôkaz. Z definície vektorového podpriestoru stačí ukázať, že $W_1 \cap W_2$ je uzavreté na sčítanie a násobenie $r \in \mathbb{R}$. Ukážme teda, že ak $v \in W_1 \cap W_2$ a $w \in W_1 \cap W_2$, tak $v + w \in W_1 \cap W_2$ a taktiež $\forall r \in \mathbb{R} : rv \in W_1 \cap W_2$.

$$v \in W_1 \cap W_2 \;\Rightarrow\; v \in W_1 \;\&\; v \in W_2$$
$$w \in W_1 \cap W_2 \;\Rightarrow\; w \in W_1 \;\&\; w \in W_2$$

potom ale

$$\left.\begin{array}{l} v \in W_1 \;\&\; w \in W_1 \;\Rightarrow\; v + w \in W_1 \\ v \in W_2 \;\&\; w \in W_2 \;\Rightarrow\; v + w \in W_2 \end{array}\right\} \;\Rightarrow\; v + w \in W_1 \cap W_2$$

keďže W_1 a W_2 sú v.p. a teda sú na sčítanie uzavreté. Obdobne môžme dokázať zvyšok.

$$v \in W_1 \cap W_2 \;\Rightarrow\; v \in W_1 \;\&\; v \in W_2 \;\Rightarrow\; \forall r \in \mathbb{R} : rv \in W_1 \;\&\; rv \in W_2 \;\Rightarrow\; rv \in W_1 \cap W_2. \quad \square$$

Tvrdenie 1.10. Nech $W \subseteq V$ je podpriestor v.p.k.d V. Nech B' je báza W. Potom existuje množina M taká, že $B' \cap M = \emptyset$ a $B' \cup M$ je báza V.

Poznámka 1.8. Ľudsky povedané, vieme rozšíriť bázu podpriestoru B' na bázu celého V.

Dôkaz. Označme prvky báze vektorového priestoru W ako $B' = \{b'_1, \ldots, b'_m\}$. Nech B je nejaká (celkom ľubovolná) báza V s prvkami $B = \{b_1, \ldots, b_n\}$. Aplikujme náš algoritmus na

$$B' \cup B = \{b'_1, \ldots, b'_m, b_1, \ldots, b_n\} \rightsquigarrow \{b'_1, \ldots, b'_m, b_{j_1}, \ldots, b_{j_r}\}, \quad 1 \leq j_i \leq n,\ i = 1, \ldots, r$$

Stalo sa to isté, ako pri dôkaze Vety 1.7. Označme $M = \{b_{j_1}, \ldots, b_{j_r}\}$ a tvrdíme, že toto je hľadaná množina. No vskutku je. Z algoritmu jasne plynie, že $B' \cap M = \emptyset$ a taktiež si môžte uvedomiť, že $B' \cup M$ je bázou V (ak rozmýšľania a uvedomovania ešte nemáte dosť, tak si uvedomte, že kebyže zvolíme inú bázu B, tak dostaneme inú množinu M, ale vždy s rovnakým počtom prvkov, a taktiež že pre jednu bázu B nemusíme dostať vždy len jednu množinu M). □

Poznámka 1.9. Platí zaujímavá vec, a to, že $\mathcal{L}(B') \cap \mathcal{L}(M) = 0$ (tá nula napravo je nula), ktorá platí i obecne, teda ak máme nejakú bázu, ktorú rozdelíte na dve množiny, tak ich lineárne obaly budú mať spoločnú tiež len nulu. Mimochodom si uvedomme ešte, že v žiadnom prípade neplatí rovnosť $\mathcal{L}(B' \cup M) \neq \mathcal{L}(B') \cup \mathcal{L}(M)$ (toto teda platí, a platí to napríklad aj preto, že $\mathcal{L}(B') \cup \mathcal{L}(M)$ vôbec nie je vektorový priestor).

Dokážme ale prvú časť poznámky. Pre spor predpokladajme, že $\exists v \neq 0$ také, že $v \in \mathcal{L}(B') \cap \mathcal{L}(M)$. Potom v môžme napísať ako l.k. množiny B' a tiež ako l.k. množiny M. Teda

$$v = \sum_{i=1}^{m} c_i b'_i \;\&\; v = \sum_{i=1}^{r} d_i b_{j_i} \;\Rightarrow\; 0 = \sum_{i=1}^{m} c_i b'_i - \sum_{i=1}^{r} d_i b_{j_i}$$

No keďže $B' \cap M = \emptyset$, musí $c_i = 0$, $d_k = 0$, $i = 1, \ldots, m$, $k = 1, \ldots, r$. No potom ale $v = 0$, čo je spor s predpokladom. No a že 0 je v oboch lin. obaloch je hádam každému zrejmé.

2. Matice a lineárne zobrazenia

(Meta)Definícia 2.7. Nech $m, n \in \mathbb{N}$. Maticou $m \times n$ rozumieme „schéma“ o m riadkoch a n stĺpcoch vyplnené elementami z $\mathbb{R}$ resp. $\mathbb{C}$. (i, j)-tý element $(1 \leq i \leq m, 1 \leq j \leq n)$ tejto matice je na i-tom riadku a j-tom stĺpci.

Poznámka 2.10.

a) Ak sa pýtate, prečo to je práve tak, a nie naopak (teda prečo matica 2×3 má dva **R**iadky a tri **S**tĺpce), tak vedzte, že preto, lebo **R** je v abecede skôr ako **S**. Anglicky hovoriaci kolegovia ale majú namiesto riadku '**R**ow' a namiesto stĺpca '**C**olumn', no využívajú podobnú argumentáciu: riadky idú skôr, lebo **R** je v abecede neskôr.

b) Matice $m \times n$ značíme $M(m, n, \mathbb{R})$ resp. $M(m, n, \mathbb{C})$. Matice môžme napríklad označovať veľkými latinskými písmenami (napr. A). (i, j)-tý element matice označujeme $a^i_{\ j}$, pričom vždy platí, že index viac napravo označuje v ktorom stĺpci sa daný element nachádza. Píšeme

$$A = \left(a^i_{\ j}\right)^{i=1,\ldots,m}_{j=1,\ldots,n}, \quad (A)^i_{\ j} = a^i_{\ j}$$

Matice vieme sčítavať a dokonca aj násobiť číslom (keď si to definujeme nasledovne): Nech $A, B \in M(m, n, \mathbb{R})$ a $r \in \mathbb{R}$. Potom súčet $A + B = C$ je tiež matica, patriaca do $M(m, n, \mathbb{R})$ taká, že

$$c^i_{\ j} := a^i_{\ j} + b^i_{\ j}, \quad \forall (i, j) \in \{1, \ldots, m\} \times \{1, \ldots, n\}$$

Podobne $rA = D$ je matica v $M(m, n, \mathbb{R})$ taká, že

$$d^i_{\ j} := r a^i_{\ j}, \quad \forall (i, j) \in \{1, \ldots, m\} \times \{1, \ldots, n\}$$

c) Matice s takto definovaným sčítaním a násobením číslom tvoria vektorový priestor (t.j. spĺňajú axiómy vektorového priestoru, čo si môžte overiť). Je evidentné, že nulový prvok (označme $\mathbb{O}$) je matica

$$\begin{pmatrix} 0 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 0 \end{pmatrix}$$

Dimenzia $\dim M(m, n, \mathbb{R}) = mn$, napríklad aj preto, že množina

$$\{{}^{ij}E | i = 1, \ldots, m,\ j = 1, \ldots, n\}$$

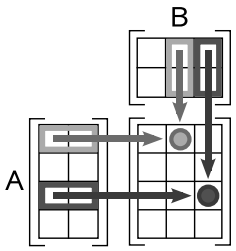
je bázou, kde ${}^{ij}E$ je matica, ktorá má všade okrem prvku na i-tom riadku a j-tom stĺpci, ktorý je jednička, samé nuly.

Definícia 2.8. Teraz si definujeme ešte súčin matíc. Nech $A \in M(r,s,\mathbb{R})$ a $B \in M(s,t,\mathbb{R})$. Potom súčin $AB = C$ je matica typu $r \times t$, pričom

$$c^i_{\ j} := \sum_{k=1}^{s} a^i_{\ k} b^k_{\ j}, \quad \forall (i,j) \in \{1,\dots,r\} \times \{1,\dots,t\}$$

Treba poznamenať, že násobenie je veľmi sugestívne definované!

Poznámka 2.11. Takto definované násobenie odpovedá násobeniu podľa obrázka.



Tvrdenie 2.11. Z takto definovaných operácií plynú tieto vlastnosti: $\forall A, B, C \in M(r,s,\mathbb{R})$:

1) komutatívnosť sčítania: $A + B = B + A$ a vlastnosť nulovej matice: $A + \mathbb{O} = A$
2) asociativita sčítania: $(A + B) + C = A + (B + C)$
3) distributívnosť násobenia voči sčítaniu napravo: $A(M+N) = AM+AN$, $\forall M, N \in M(s,t,\mathbb{R})$
4) distributívnosť násobenia voči sčítaniu naľavo: $(A + B)M = AM + BM$
5) asociativita násobenia: $(AM)P = A(MP)$, $\forall P \in M(t,u,\mathbb{R})$

Dôkaz. Prvé dve vlastnosti plynú triviálne a dokazovať ich nebudeme. Ďalšie tri plynú tiež triviálne ale dokážeme si ich. Označme ľavú stranu rovnosti 3) L, pravú R, potom

$$(L)^i_{\ j} = \sum_{k=1}^{s} a^i_{\ k}(m^k_{\ j} + n^k_{\ j}) = \sum_{k=1}^{s} a^i_{\ k} m^k_{\ j} + a^i_{\ k} n^k_{\ j} = \sum_{k=1}^{s} a^i_{\ k} m^k_{\ j} + \sum_{k=1}^{s} a^i_{\ k} n^k_{\ j} = (AM)^i_{\ j} + (AN)^i_{\ j} = (R)^i_{\ j}$$

Podobne sme chopní dokázať aj rovnosť 4) a nakoniec teda rovnosť 5):

$$(L)^i_{\ j} = \sum_{k=1}^{t} (AM)^i_{\ k} p^k_{\ j} = \sum_{k=1}^{t} \left(\sum_{l=1}^{s} a^i_{\ l} m^l_{\ k} \right) p^k_{\ j} = \sum_{l=1}^{s} a^i_{\ l} \left(\sum_{k=1}^{t} m^l_{\ k} p^k_{\ j} \right) = \sum_{l=1}^{s} a^i_{\ l} (MP)^l_{\ j} = (R)^i_{\ j}. \quad \square$$

5. přednáška z lineární algebry

30. říjen 2007

Poznámka 2.12. (k Tvrzení 2.11 z předchozí přednášky)

1) Strukturu, splňující vlastnosti z tvrzení 2.11 výše nazveme komutativním okruhem (angl. ring)

2) !POZOR! Násobení matic není komutativní, tj. $AB \neq BA$.
Např.

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$
$$\not\parallel$$
$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

3) Relace $(AB)C = A(BC)$ "naznačuje" že $M(n, n; \mathbb{R})$ by mohla být grupa, ale jelikož zatím nevíme, co to je, nastává čas tento pojem zavést.

Grupa. $(G, \cdot, ^{-1}, e)$, $e \in G$ je množina, na které je definována binární operace

$$G \times G \to G, \quad (a, b) \mapsto a \cdot b$$

a platí:

1) $\forall a, b, c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (asociativita)
2) $\exists e \in G \, \forall a \in G : a \cdot e = e \cdot a = a$ (existence neutrálního prvku)
3) $\forall a \in G \, \exists a' \in G : a \cdot a' = e$ (a' se nazývá inverze a)

Vektorové prostory, jak jsme je definovali kdysi dávno v první přednášce, jsou rovněž grupa, dokonce Abelova (t.j. komutativní grupa pro všechna $a, b \in G$ splňující $a \cdot b = b \cdot a$), ale vzhledem ke sčítání. Matice (vzhledem k násobení) Abelova grupa nejsou, protože jejich násobení není komutativní. Další nekomutativní grupou je multiplikativní grupa kvaternionů $(\mathbb{H} \setminus \{0\}, \cdot, ^{-1}, 1)$. To, že kvaterniony obecně nekomutují, možno vidět už jenom na $ij = k \neq ji = -k$. Tedy i kvaterniony mají inverzy, kterou skonstrujujeme podobně jako u komplexních čísel.
Inverze je pro každé a jen jedna, pro spor nechť a', a'' jsou inverze k a. Pak $a \cdot a' = e = a \cdot a''$. Po vynásobení a' zleva a přezávorkování $(a' \cdot a) \cdot a' = (a' \cdot a) \cdot a''$, tudíž $a' = a''$. Stačí už jenom dokázať, že levé a pravé inverze se rovnají:

$$\begin{aligned} a \cdot a_R &= e \quad / a_L \cdot \\ a_L \cdot (a \cdot a_R) &= a_L \cdot e \\ (a_L \cdot a) \cdot a_R &= a_L \\ a_R &= a_L \qquad \square. \end{aligned}$$

e je pro matice zřejmě jednotková matice $\mathbb{1} = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$ protože $\mathbb{1} \cdot A = A \cdot \mathbb{1} = A$

Inverze k nulové matici $\mathbb{O} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$ neexistuje, protože by muselo platit $\mathbb{O}' \cdot \mathbb{O} = \mathbb{1} \Rightarrow \mathbb{O} = \mathbb{1}$, což je spor. Nula krát cokoliv zkrátka zůstane nulou.

pokračování poznámky

4) Zavedeme množinu $GL(n;\mathbb{R})$ jako množinu všech matic $n \times n$, které mají inverzi, tj. $GL(n;\mathbb{R}) = \{A \in M(n,n;\mathbb{R}), A \text{ má inverzi}\}$. Z vlastností v tvrzení výše je zřejmé, že $GL(n;\mathbb{R})$ je grupa, říkáme jí **obecná lineární grupa** (angl. general linear group).

Definice 2.9. Nechť V je vektorový prostor konečné dimenze, $B = \{b_1, \cdots, b_n\}$ a $B' = \{b'_1, \cdots, b'_n\}$ jsou báze V. Pak matici $M \in M(n,n;\mathbb{R})$, sestrojenou postupem níže nazveme **maticí přechodu** od báze B k bázi B'.

postup: B je báze, takže každé $b'_j \in B'$ lze vyjádřit jako l.k. $\{b_1, \cdots, b_n\}$, tj.

$$b'_j = \sum_{i=1}^{n} b_i m^i{}_j, \quad j = 1, \ldots, n$$

Matice $M = (m^i_j)^{i=1,\cdots,n}_{j=1,\cdots,n}$ je pak matice přechodu. Všimněte si, že každému b'_j odpovídá sloupec matice.

MiniPoznámka: samozřejmě jsme si mohli matici přechodu zavést „opačně", t.j. $b'^j = \sum_{i=1}^{n} m^j_i b^i$, přičemž by jsme museli také změniť našu konvenci psaní indexů u vektorů báze dolů, resp. u vektorů souřadnic nahoru. Výsledkem by bylo, že vektoru b'^j by v matici přechodu odpovídal j-tý řádek.

Poznámka 2.13.

1) Matice přechodu je určena jednoznačně, jelikož a protože souřadnice vektoru vůči dané bázi jsou podle Lemmatu 1.8 jednoznačné.

   Příklad 2.6. Jaká je matice přechodu v $\mathbb{R}^2$ od báze $B = \{(0,2),(1,0)\}$ k $B' = \{(1,2),(0,1)\}$? Podle postupu výše má být

$$(1,2) = (0,2)m^1_1 + (1,0)m^2_1 = (m^2_1, 2m^1_1) \Rightarrow m^1_1 = 1, m^2_1 = 1$$
$$(0,1) = (0,2)m^1_2 + (1,0)m^2_2 = (m^2_2, 2m^2_1) \Rightarrow m^1_2 = \frac{1}{2}, m^2_2 = 0.$$
$$\text{Tedy } M = \begin{pmatrix} 1 & \frac{1}{2} \\ 1 & 0 \end{pmatrix}.$$

2) Z definice nahoře plyne, že $(b'_1, \ldots, b'_n) = (b_1, \ldots, b_n) \cdot \begin{pmatrix} m^1_1 & \cdots & m^1_n \\ \vdots & \ddots & \vdots \\ m^n_1 & \cdots & m^n_n \end{pmatrix}$ Pozor, používáme maticové násobení, přičemž tentokát jsou maticovými elementy nejen čísla, ale také vektory. Také si dejtě do paměti, že maticí přechodu v tomhle případě násobíme zprava.

3) Buď V v.p.k.d., $\dim V = n$, $v \in V$ a B báze V. Pak $v = \sum_{i=1}^{n} b_i v^i$ a $(v^1, \cdots, v^n)$ jsou souřadnice v vůči B. Podle úmluvy budeme souřadnice napsané do sloupce značit

$$[v]_B = \begin{pmatrix} v^1 \\ \vdots \\ v^n \end{pmatrix}.$$

Definice 2.10. Nechť A je matice $A \in M(n,n;\mathbb{R})$. A^{-1} nazvu inverzí k A, pokud $AA^{-1} = \mathbb{1}$.

Poznámka 2.14. Tj. $(AA^{-1})^i_j = \mathbb{1}^i_j = \delta^i_j$ (to je funkce **Kroneckerovo delta**, je rovna 0 pro $i \neq j$ a 1 pro $i = j$). Jinak řečeno

$$\sum_{k=1}^{n} a^i_k (a^{-1})^k_j = \delta^i_j.$$

Tvrzení 2.12. Buď V v.p.k.d., B a B' báze V, $M = (m^i_{\ j})^{i=1,\cdots,n}_{j=1,\cdots,n}$ je matice přechodu od B k B', $v \in V$. Pak $[v]_{B'} = M^{-1}[v]_B$. Tj. pokud $[v]_B = \begin{pmatrix} v^1 \\ \vdots \\ v^n \end{pmatrix}$ a zároveň $[v]_{B'} = \begin{pmatrix} v'^1 \\ \vdots \\ v'^n \end{pmatrix}$, potom $v'^i = (M^{-1})^i_{\ j} v^j$ (tady násobíme inverzní maticí zleva).

Důkaz. Podle definice $b'_j = \sum_{i=1}^{n} b_i m^i_{\ j}$. Zároveň $\sum_{j=1}^{n} b'_{\ j} v'^j = v = \sum_{i=1}^{n} b_{\ i} v^i$, takže $\sum_{j=1}^{n}\sum_{i=1}^{n} b_i m^i_{\ j} v'^j = \sum_{i=1}^{n} b_i v^i \Rightarrow \sum_{i=1}^{n} b_i \left(\sum_{j=1}^{n} m^i_{\ j} v^j - v^i \right) = 0$, neboli l.k prvků B je nulová. Jelikož je ale B báze (a tedy l.n.), musí být její nulová l.k. nutně triviální. Takže

$$v^i = \sum_{j=1}^{n} m^i_{\ j} v'^j,$$

tedy $[v]_B = M[v]_{B'}$ a po vynásobení obou stran M^{-1} zleva vychází, že opravdu

$$[v]_{B'} = M^{-1}[v]_B. \qquad \square$$

Poznámka 2.15. Matice přechodu má inverzní matici. Označme M matici přechodu od B k B' a N matici přechodu od B' k B. Tvrdíme, že matice NM je matice přechodu od B' k B'. Vskutku, zřejmě platí $(b'_1, \ldots, b'_n) = (b_1, \ldots, b_n)M$ a $(b_1, \ldots, b_n) = (b'_1, \ldots, b'_n)N$. Dosadením matice („řádku“) $(b_1, \ldots, b_n)$ z druhé rovnosti do první, dostaneme $(b'_1, \ldots, b'_n) = ((b'_1, \ldots, b'_n)N)\,M$ a konečně použitím asociativity násobení matic $(b'_1, \ldots, b'_n) = (b'_1, \ldots, b'_n)(NM)$. Matice NM je tedy z definice maticí přechodu od B' k B'. Zřejmě jednotková matice je taky matice přechodu od B' k B'. Odtud $NM = \mathbb{1}$, neboť definice matice přechodu je jednoznačná. Celkově M a N jsou inevzrní.

Definice 2.11. Nechť V a W jsou v.p. Zobrazení L z $V \to W$ nazvu **linearní zobrazení** z V do W, pokud

$$\begin{aligned} \forall v, v' \in V: \quad & L(v + v') = L(v) + L(v') \\ \forall r \in \mathbb{R}: \quad & L(rv) = rL(v). \end{aligned}$$

Příklad 2.7.

1) V je v.p., $c \in \mathbb{R}$ je pevně dané číslo. Zobrazení $L : V \to V, L(v) := cv \quad \forall v \in V$ je evidentně lineární, protože $L(v + v') = c(v + v') = cv + cv' = L(v) + L(v')$ a $L(rv) = c(rv) = r(cv) = rL(v)$.

2) Rotace r_φ vektorů $v_1 = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$ a $v_2 = \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$ kolem počátku v rovině $\mathbb{R}^2$ je rovněž lineární:

$$r_\varphi \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \end{pmatrix} = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \left[\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \right],$$

což je podle bodu 3) Tvrzení 2.11. rovno $r_\varphi \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + r_\varphi \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = r_\varphi(v_1) + r_\varphi(v_2)$.

3) Předchozí případ lze zobecnit na libovolné zobrazení $\mathcal{A}$ z $\mathbb{R}^n \to \mathbb{R}^n$, které vynásobí vzor maticí $A \in M(n, n; \mathbb{R})$. Důkaz opět trivialně plyne z Tvrzení 2.11.

4) I derivace polynomu $\frac{d}{dx} : \mathcal{P} \to \mathcal{P}$ je lineární, což plyne z věty o aritmetice derivací z analýzy.

5) A jako příklad NElineárního (t.j. zobrazení, které NEní lineární) zobrazení jím je třeba translace v $\mathbb{R}^2$. Když $T_t(v) = v + t$, kde $t = \begin{pmatrix} t_1 \\ t_2 \end{pmatrix} \in \mathbb{R}^2$, pak zřejmě

$$\begin{gathered} T_t(v+w) = v + w + t \\ \nparallel \\ T_t(v) + T_t(w) = v + t + w + t \end{gathered}$$

Poznámka 2.16. Každé l.z. musí nulu zobrazovat opět na nulu, neboť podle definice l.z.

$$L(0 \cdot v) = 0 \cdot L(v) = 0.$$

Definice 2.12. Buď L l.z. z $V \to W$, V a W v.p.k.d., $\dim V = n$, $\dim W = m$, $\mathcal{B}$ báze V a $\mathcal{C}$ báze W. **Maticí lineárního zobrazení** L vůči $\mathcal{B}$ a $\mathcal{C}$ nazveme matici takových $(l_i^j)_{i=1,\cdots,n}^{j=1,\cdots,m}$, že

$$L(b_i) = \sum_{j=1}^{m} c_j l_i^j$$

Tuto matici budeme označovat $[L]_{\mathcal{C}}^{\mathcal{B}} \in M(m, n; \mathbb{R})$.

Poznámka 2.17. Jinak řečeno, $(L(b_1), \ldots, L(b_n)) = (c_1, \ldots, c_m) \cdot [L]_{\mathcal{C}}^{\mathcal{B}}$, tj.

$$\begin{gathered} L(b_1) = \sum_{i=1}^{m} c_i l_1^i \\ \vdots \\ L(b_n) = \sum_{i=1}^{m} c_i l_n^i \end{gathered}$$

Příklad 2.8.

1) Jaká je matice l.z. $L : \mathbb{R}^n \to \mathbb{R}^n; L(v) = cv,\ \forall v \in V$, $\mathcal{B} = \{(1, \cdots, 0), \cdots, (0, \cdots, 1)\}$? Podle poznámky nahoře má být

$$\left.\begin{gathered} L((1,\cdots,0)) = (c,\cdots,0) \\ \vdots \\ L((0,\cdots,1)) = (0,\cdots,c) \end{gathered}\right\} \Rightarrow \begin{pmatrix} c & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & c \end{pmatrix} = [L]_{\mathcal{B}}^{\mathcal{B}}$$

2) Jaká je matice l.z. derivace polynomu 2. stupně - $\frac{d}{dx} : P_2 \to P_2$ (ve skutečnosti derivace zobrazuje na polynomy prvního stupně, ale budeme se zatím tvářit, že to nevíme). Báze jsou $\mathcal{B} = \mathcal{C} = \{1, x, x^2\}$.

$$\left.\begin{aligned} \frac{d}{dx}1 = 0 &= 0 \cdot 1 + 0 \cdot x + 0 \cdot x^2 \\ \frac{d}{dx}x = 1 &= 1 \cdot 1 + 0 \cdot x + 0 \cdot x^2 \\ \frac{d}{dx}x^2 = x &= 0 \cdot 1 + 2 \cdot x + 0 \cdot x^2 \end{aligned}\right\} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

A opravdu vidíme, že matice má nulový poslední řádek, tedy odpovídá polynomu 1. stupně.

Tvrzení 2.13. Nechť jsou V, W v.p.k.d., $\dim V = m$, $\dim W = n$, $\mathcal{B}$ báze V a $\mathcal{C}$ báze W, $L : V \to W$ l.z. a $v \in V$. Pak

$$[L(v)]_{\mathcal{C}} = [L]_{\mathcal{C}}^{\mathcal{B}} [v]_{\mathcal{B}}$$

Důkaz tvrzení. Stačí nám ukázat, že $\left([L(v)]_{\mathcal{C}}\right)^i = \left([L]_{\mathcal{C}}^{\mathcal{B}} [v]_{\mathcal{B}}\right)^i$, kde $i = 1, \cdots, m$. $([L(v)]_{\mathcal{C}})^i$ můžeme rozepsat jako $\left(\left[L\left(\sum_{j=1}^{m} b_j v^j\right)\right]_{\mathcal{C}}\right)^i$ což je díky linearitě L rovno $\left(\left[\sum_{j=1}^{m} L(b_j) v^j\right]_{\mathcal{C}}\right)^i$ a to je zase podle definice matice l.z. $\left(\left[\sum_{j=1}^{m}\sum_{k=1}^{n} c_k l_j^k v^j\right]_{\mathcal{C}}\right)^i$, kde $\left(l_j^k\right)_{j=1,\cdots,m}^{k=1,\cdots,N}$ je zmiňovaná matice $[L]_{\mathcal{C}}^{\mathcal{B}}$. Prohozením sum dostaneme $\left(\left[\sum_{k=1}^{n} c_k \left(\sum_{j=1}^{m} l_j^k v^j\right)\right]_{\mathcal{C}}\right)^i = \sum_{j=1}^{m} l_j^i v^j = \left([L]_{\mathcal{C}}^{\mathcal{B}} [v]_{\mathcal{B}}\right)^i$. □

6. přednáška z lineární algebry

6. listopad 2007

PŘIPOMENUTÍ. V minulé, či předminulé přednášce jsme si zavedli matici. Matice „je“ v istém zmyslu lineární zobrazení. Pokud $L : V \to W$ je l.z., $\mathcal{B}$, $\mathcal{C}$ báze V resp. W, vektor $v \in V$, pak $[L(v)]_{\mathcal{C}} = [L]_{\mathcal{C}}^{\mathcal{B}}[v]_{\mathcal{B}}$, kde $[L]_{\mathcal{C}}^{\mathcal{B}}$ je matice lineárního zobrazení vůči bázím $\mathcal{B}$ a $\mathcal{C}$.

Dále pokud M je matice přechodu od nejaké báze $\mathcal{B}$ k bázi $\mathcal{B}'$, tj. $(b'_1, \ldots, b'_n) = (b_1, \ldots, b_n)M$, potom složky $v \in V$ transfromujeme podle „zákona“ $[v]_{\mathcal{B}'} = M^{-1}[v]_{\mathcal{B}}$. Nyní si odvodíme, jak se mění matice linearního zobrazení pri změne bází.

VĚTA 2.14. Nechť V, W jsou vektorové prostory konečné dimenze. $\mathcal{B}$, $\mathcal{B}'$ jsou báze V. $\mathcal{C}$, $\mathcal{C}'$ jsou báze W. β je matice přechodu od $\mathcal{B}$ k $\mathcal{B}'$. γ je matice přechodu od $\mathcal{C}$ k $\mathcal{C}'$. dim V = m. dim W = n. $L : V \to W$ je lineární zobrazení. Potom[1]:

$$[L]_{\mathcal{C}'}^{\mathcal{B}'} = \gamma^{-1}[L]_{\mathcal{C}}^{\mathcal{B}}\beta$$

Poznámka: situaci můžeme naznačít následujícím schématem: $\begin{array}{ccc} V & \xrightarrow{L} & W \\ \mathcal{B}\xrightarrow{\beta}\mathcal{B}' & & \mathcal{C}\xrightarrow{\gamma}\mathcal{C}' \end{array}$
Jednoduše řečeno, máme zadán vektor vzhledem k bázi $\mathcal{B}'$ a chceme jej zobrazit pomocí lineárního zobrazení L a vyjádřit ho v bázi $\mathcal{C}'$, přičemž poznáme matici lineárního zobrazení vůči bazím $\mathcal{B}$ a $\mathcal{C}$. A právě tato věta nám říká, jak si poradit, pokud známe matice přechodu β mezi bázemi $\mathcal{B} \to \mathcal{B}'$ a matici přechodu γ mezi $\mathcal{C} \to \mathcal{C}'$.

DŮKAZ. Důkaz provedeme přímo upravením rovnic. Z definice matice přechodu můžeme psát: $L(b'_i) = \sum_{j=1}^{n} c'_j \hat{\mathcal{L}}^j{}_i$ pro $i = 1, \ldots, m$, kde jsme si označili $\hat{\mathcal{L}}^j{}_i = \left([L]_{\mathcal{C}'}^{\mathcal{B}'}\right)^j{}_i$, dále si označím $\mathcal{L}^j{}_i = \left([L]_{\mathcal{C}}^{\mathcal{B}}\right)^j{}_i$. Nyní začnu upravovat levou strany původní rovnice: $L(b'_i) = L\Big(\sum_{k=1}^{m} b_k \beta^k_i\Big) = \sum_{k=1}^{m} L\left(b_k\right)\beta^k_i =$ $\sum_{k=1}^{m}\Big(\sum_{r=1}^{n} c_r \mathcal{L}^r{}_k\Big)\beta^k_i = \sum_{r=1}^{n} c_r\Big(\sum_{k=1}^{m} \mathcal{L}^r{}_k\beta^k_i\Big)$. Teď upravíme pravou stranu původní rovnice: $\sum_{j=1}^{n} c'_j\hat{\mathcal{L}}^j{}_i =$ $\sum_{j=1}^{n}\Big(\sum_{r=1}^{n} c_r\gamma^r{}_j\Big)\hat{\mathcal{L}}^j{}_i = \sum_{r=1}^{n} c_r\Big(\sum_{j=1}^{n}\gamma^r{}_j\hat{\mathcal{L}}^j{}_i\Big)$. Tedy dostáváme: $\sum_{r=1}^{n} c_r\Big(\sum_{j=1}^{n}\gamma^r{}_j\hat{\mathcal{L}}^j{}_i\Big) = \sum_{r=1}^{n} c_r\Big(\sum_{k=1}^{m}\mathcal{L}^r{}_k\beta^k_i\Big)$. Protože $\mathcal{C}$ je báze, proto z predchozí rovnosti vyplývá: $\sum_{j=1}^{n}\gamma^r{}_j\hat{\mathcal{L}}^j{}_i = \sum_{k=1}^{m}\mathcal{L}^r{}_k\beta^k_i$, pro $r = 1, \ldots, n$. Výraz zapíšeme pomocí maticového násobení: $\left(\gamma[L]_{\mathcal{C}'}^{\mathcal{B}'}\right)^r{}_i = \left([L]_{\mathcal{C}}^{\mathcal{B}}\beta\right)^r{}_i \Rightarrow \gamma[L]_{\mathcal{C}'}^{\mathcal{B}'} = [L]_{\mathcal{C}}^{\mathcal{B}}\beta \Rightarrow [L]_{\mathcal{C}'}^{\mathcal{B}'} = \gamma^{-1}[L]_{\mathcal{C}}^{\mathcal{B}}\beta$. První implikace je oprávnená, jelikož výraz nám platí pro všechna i, j. Druhá implikace platí proto, že matice γ je invertovatelná, což jsme si ukázali v poznámke v minulé přednáške. □

POZNÁMKA 2.18. Jak souvisí skládání lineárního zobrazení s násobením matic?

TVRZENÍ 2.15. Nechť U, V, W jsou v. p. k. d., $L : U \to V$ je lineární zobrazení, $M : V \to W$ je lineární zobrazení, $\mathcal{B}, \mathcal{C}, \mathcal{D}$ jsou pořadě báze U, V, W a $\dim U = m$, $\dim V = n$, $\dim W = q$. Potom platí:

$$[M \circ L]_{\mathcal{D}}^{\mathcal{B}} = [M]_{\mathcal{D}}^{\mathcal{C}}[L]_{\mathcal{C}}^{\mathcal{B}}$$

DŮKAZ. Označme $\mathcal{B} = \{b_1, \ldots, b_m\}$, $\mathcal{C} = \{c_1, \ldots, c_n\}$, $\mathcal{D} = \{d_1, \ldots, d_q\}$. Pro všechna $i =$

[1] Uvědomme si, že matici přechodu mezi dvěma bázemi $\mathcal{B}$ a $\mathcal{B}'$ můžme chápat jako identické zobrazení vůčí bazím $\mathcal{B}'$ a $\mathcal{B}$ a jeho matici vůči temhle bazím zonačme $[P]_{\mathcal{B}}^{\mathcal{B}'}$ (písmenko P pre identické zobrazení volíme podle slova „Přechod“). Nasledující vztah mezi lineárním zobrazením vyjadřeným v různých bázích můžme psát elegantńeji jako $[L]_{\mathcal{C}'}^{\mathcal{B}'} = [P]_{\mathcal{C}'}^{\mathcal{C}}[L]_{\mathcal{C}}^{\mathcal{B}}[P]_{\mathcal{B}}^{\mathcal{B}'}$ co potom, jako přečtetě následující tvrzení o skládání lineárních zobrazení bude vidět ještě lépe.

$1, \ldots, m$ platí:

$$(M \circ L)(b_i) \equiv M(L(b_i)) = M\Big(\sum_{j=1}^{n} c_j \left([L]_{\mathcal{C}}^{\mathcal{B}}\right)^j{}_i\Big) =$$
$$= \sum_{j=1}^{n} M(c_j) \left([L]_{\mathcal{C}}^{\mathcal{B}}\right)^j{}_i = \sum_{j=1}^{n}\Big(\sum_{k=1}^{q} d_k \left([M]_{\mathcal{D}}^{\mathcal{C}}\right)^k{}_j\Big) \left([L]_{\mathcal{C}}^{\mathcal{B}}\right)^j{}_i = \sum_{k=1}^{q} d_k\Big(\sum_{j=1}^{n} \left([M]_{\mathcal{D}}^{\mathcal{C}}\right)^k{}_j \left([L]_{\mathcal{C}}^{\mathcal{B}}\right)^j{}_i\Big),$$

což v maticovém zápisu dává $\sum_{k=1}^{q} d_k \left([M]_{\mathcal{D}}^{\mathcal{C}}[L]_{\mathcal{C}}^{\mathcal{B}}\right)^k{}_i$. Tady vidíme definici matice lineárního zobrazení (ktorá je mimochodem jednoznačně určená), takže dostáváme: $[M \circ L]_{\mathcal{D}}^{\mathcal{B}} = [M]_{\mathcal{D}}^{\mathcal{C}}[L]_{\mathcal{C}}^{\mathcal{B}}$. □

Definice 2.13. Nechť L je lineární zobrazení $L : V \to W$ a V, W jsou vektorové prostory. Pak nazveme Image (Obraz) lineárního zobrazení L takovou podmnožinu W, na kterou se zobrazuje V. To můžeme zapsat jako: $\operatorname{Im} L = \{w \in W | \exists v \in V : L(v) = w\}$. A dále nazveme Kernel (Jádro) lineárního zobrazení L takovou množinu prvků z V, která se zobrazí na nulu. Což lze zapsat jako: $\operatorname{Ker} L = \{v \in V \mid L(v) = 0\}$.

Poznámka 2.19.

1) $\operatorname{Im} L$ je vektorový podprostor prostoru V. Mějme dva vektory $w, w' \in \operatorname{Im} L$, ptáme se jestli $w + w' \overset{?}{\in} \operatorname{Im} L$. Z definice obrazu určitě $\exists v, v' \in V$ takové, že $w = L(v)$ a $w' = L(v')$. Nyní můžeme uvážit: $w + w' = L(v) + L(v') = L(v + v')$. Určitě $v + v' \in V$, z čeho dostáváme $w + w' \in \operatorname{Im} L$. Nyní ověříme násobení reálnými čísly: Mějme $w \in \operatorname{Im} L, r \in \mathbb{R}$, ptáme ser $rv \overset{?}{\in} \operatorname{Im} L$. Znova $\exists v \in V : L(v) = w$. Potom $L(rv) = rL(v) = rw$.

2) $\operatorname{Ker} L$ je vektorový podprostor prostoru V. Nejdříve se podíváme na sčítání: Nech $v, v' \in \operatorname{Ker} L$. Plyne z toho, že $v + v' \overset{?}{\in} \operatorname{Ker} L$? Skusme $L(v + v') = L(v) + L(v') = 0 + 0 = 0$. Obdobně bude postupovat i u násebení reálnými čísly: $v \in \operatorname{Ker} L, r \in \mathbb{R}$. Jestli $rv \overset{?}{\in} \operatorname{Ker} L$? Z definice jádra ovšem plyne: $L(rv) = rL(v) = r0 = 0$.

3) Definice 2.14. Mějme lineární zobrazení $L : V \to W$. Toto lineární zobrazení nazveme **surjektivní** pokud $\operatorname{Im} L = W$. Lineární zobrazení $L : V \to W$ nazvu **injektivní** pokud je L prosté, tj. $\forall v, v' \in V : L(v) = L(v') \Rightarrow v = v'$.

4) Věta 2.16. $\operatorname{Ker} L = \{0\} \Leftrightarrow L$ je injektivní.

   Důkaz. Nejdříve ukážeme implikaci „doprava“: Nechť $\operatorname{Ker} L = \{0\}$ a $v, v' \in V$ tak, že $L(v) = L(v')$. Pak stačí ukázat, že $v = v'$. Jelikož $L(v) = L(v')$, tudíž platí $0 = L(v) - L(v') = L(v - v')$, tedy $v - v' \in \operatorname{Ker} L = \{0\} \Rightarrow v - v' = 0 \Rightarrow v = v'$.

   Teď dokážeme obrácenou implikaci: Nechť L je injektivní, tedy pro všechny $v, v' \in V$ platí $L(v) = L(v') \Rightarrow v = v'$. Pak nechť $v \in \operatorname{Ker} L$. Aby byl důkaz proveden chci ukázat, že nutně $v = 0$. Víme, že platí $L(0) = 0 = L(v)$, takže z injektivity dostáváme, že $v = 0$. □

Věta 2.17. Nechť V, W jsou v. p. k. d. a L je lineární zobrazení $L : V \to W$. Pak

$$\dim \operatorname{Im} L + \dim \operatorname{Ker} L = \dim V$$

Důkaz. Označme $\dim V = m$, dále označíme $\dim \operatorname{Ker} L = m - n$. Zřejmě $0 \leq n \leq m$. Nechť $\{b_{n+1}, \ldots, b_m\}$ buď báze $\operatorname{Ker} L$ (Kdyby $m = n$, chápme že báze neexistuje a vtedy zřejmě $\operatorname{Ker} L = \{0\}$). Dle Tvrzení 1.10 lze tuhle bázi doplnit do celé báze prostoru V. Označme toto doplnění $\{b_1, \ldots, b_n\}$ (Znova kdyby $n = 0$, chápme, že jsme bázu doplnili o 0 vektorov. V tomhle případě zřejmě $\operatorname{Ker} L = V$, tedy $\operatorname{Im} L = \{0\}$ a věta je dokázaná už teď. Proto nasledující řádky uvažujeme jenom v případe $n \neq 0$.). A nyní ak dokážeme, že $\{L(b_1), \ldots, L(b_n)\}$ je báze $\operatorname{Im} L$, bude důkaz hotov.

1. Nejdříve dokážme, že daná množina vektorov $\operatorname{Im} L$ generuje.

   a) Platí $\mathcal{L}(\{L(b_1), \ldots, L(b_n)\}) \subseteq \operatorname{Im} L$, neboť ak w patří do lineárního obalu, potom existují koeficienty c_i, $i = 1, \ldots, n$, tak, že $w = \sum_{i=1}^{n} c_i L(b_i)$. No zřejmě platí, že $w = L(v)$, kde $v \in V$ a $v = \sum_{i=1}^{n} c_i b_i$, tedy $w \in \operatorname{Im} L$.

   b) Tak isto ukážeme, že platí $\operatorname{Im} L \subseteq \mathcal{L}(\{L(b_1), \ldots, L(b_n)\})$. Mějme $w \in \operatorname{Im} L$. Potom existuje vektor $v \in V$ takový, že $L(v) = w$. Ale protože $v \in V$, tak existují i koeficienty rozkladu v do báze d^i, $i = 1, \ldots, m$, tedy $v = \sum_{i=1}^{m} b_i d^i$. Můžeme psát $w = L(v) = L\Big(\sum_{i=1}^{m} b_i d^i\Big) = \sum_{i=1}^{m} L(b_i) d^i = \sum_{i=1}^{n} L(b_i) d^i \in \mathcal{L}(\{L(b_1), \ldots, L(b_n)\})$. Předposledná rovnost platí, protože platí $\sum_{i=n+1}^{m} L(b_i) d^i = 0$.

2. Nyní ukážeme, že $\{L(b_1), \ldots, L(b_n)\}$ je lineárě nezávislá. Nechť existují koeficienty c_i takové, že $\sum_{i=1}^{n} c_i L(b_i) = 0$. Potom ale i $L\Big(\sum_{i=1}^{n} c_i b_i\Big) = 0$, tedy $\sum_{i=1}^{n} c_i b_i \in \operatorname{Ker} L$. Jelikož jsme si na záčátku zvolili bázi $\operatorname{Ker} L$ jako $\{b_{n+1}, \ldots, b_m\}$, potom existují koeficienty c_i, $i = n+1, \ldots, m$ rozkladu sumy do báze, tedy $\sum_{i=1}^{n} c_i b_i = \sum_{i=n+1}^{m} c_i b_i \Rightarrow \sum_{i=1}^{m} c_i b_i = 0 \Rightarrow c_i = 0,\ i = 1, \ldots, m$. Ak by $n = m$, tak rozklad do báze neuvažujeme (žádná neexistuje) ale potom nutně $\sum_{i=1}^{n=m} c_i b_i = 0$, což dá znova $c_i = 0,\ i = 1, \ldots, m$. Takže jedině triviální lineární kombinace vektorů $\{L(b_1), \ldots, L(b_n)\}$ se rovná nule, a tým sme dokázali, že sú lineárně nezávislé.

   Takže dostáváme, že $\{L(b_1), \ldots, L(b_n)\}$ je báze $\operatorname{Im} L$ a tedy $\dim \operatorname{Im} L = n$. Odtud snadno $\dim \operatorname{Ker} L + \dim \operatorname{Im} L = m - n + n = m = \dim V$. □

PŘÍKLAD 2.9. Uvažujme $V = \mathcal{P}_2 = \Big\{\sum_{i=0}^{2} a_i x^i, a_i \in \mathbb{R}\Big\}$ s bází $\mathcal{B} = 1, x, x^2$, tedy $\dim \mathcal{P}_2 = 3$. Mějme lineární zobrazení $\frac{\mathrm{d}}{\mathrm{d}x} : \mathcal{P}_2 \to \mathcal{P}_2$. Jeho matice vůči basím $\mathcal{B}$ vypadá

$$\left[\frac{\mathrm{d}}{\mathrm{d}x}\right]_{\mathcal{B}}^{\mathcal{B}} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

Ako vypadá jádro a obraz zobrazení? Zřejmě $\operatorname{Ker} \frac{\mathrm{d}}{\mathrm{d}x} \equiv \big\{f \in \mathcal{P}_2 | \frac{\mathrm{d}}{\mathrm{d}x} f = 0\big\} = \mathcal{P}_0$. Trochu méně snáze najdeme obraz. Definice praví $\operatorname{Im} \frac{\mathrm{d}}{\mathrm{d}x} \equiv \big\{f \in \mathcal{P}_2 | \exists g \in \mathcal{P}_2 : \frac{\mathrm{d}}{\mathrm{d}x} g = f\big\} = \big\{f \in \mathcal{P}_2 | \int f \in \mathcal{P}_2\big\}$.

Z analýzy víme, že integrál polynomu je znova polynom, jenom o stupeň vyšší. Tedy $\forall f \in \mathcal{P}_1 : \int f \in \mathcal{P}_2$. Taktiež $\forall f \in \mathcal{P}_2 \backslash \mathcal{P}_1 : \int f \notin \mathcal{P}_2$. Keďže $\mathcal{P}_1 \subseteq \mathcal{P}_2$, tak $\operatorname{Im} \frac{\mathrm{d}}{\mathrm{d}x} = \mathcal{P}_1$.

Vidíme, že $\dim \operatorname{Im} \frac{\mathrm{d}}{\mathrm{d}x} + \dim \operatorname{Ker} \frac{\mathrm{d}}{\mathrm{d}x} = \dim \mathcal{P}_1 + \dim \mathcal{P}_0 = 2 + 1 = 3 = \dim \mathcal{P}_2$. Ověřili jsme tedy předchozí větu.

7. prednáška z lineárnej algebry

13. november 2007

MINULE. Minule sme si definovali jadro a obraz lineárneho zobrazenia, ukázali si, že jadro ako aj obraz tvoria vektorové (pod)priestory a tiež dokázali veľmi užitočné tvrdenie

$$\dim \operatorname{Ker} L + \dim \operatorname{Im} L = \dim V,$$

kde V je priestor, z ktorého zobrazujeme a L je lineárne zobrazenie.

TVRDENIE 2.18. Nech V je vektorový priestor konečnej dimenzie a $L : V \to V$ je lineárne zobrazenie. Potom L je injektívne (tj. prosté) práve vtedy keď je surjektívne (tj. na) a tým pádom je aj bijektívne (tj. vzájomne jednoznačné). Teda

$$\text{injektívne} \Leftrightarrow \text{surjektívne} \Leftrightarrow \text{bijektívne}.$$

DÔKAZ.

1.) Ak L je injektívne, tak podľa Vety 2.16, ktorá zaznela minule, je nutne $\operatorname{Ker} L = \{0\}$ a preto $\dim \operatorname{Im} L = \dim V$ (keďže $\dim \operatorname{Ker} L = 0$). Ale tiež $\operatorname{Im} L \subseteq V$, no nutne platí i rovnosť, teda $\operatorname{Im} L = V$ a to je definícia surjektivity. Prečo platí nutne rovnosť? Keby rovnosť neplatila, tak by existoval vektor $v \in V$ & $v \notin \operatorname{Im} L$ a teda by sa dala minimálne jedným vektorom doplniť báza $\operatorname{Im} L$ na bázu celého V (pozri dôkaz Tvrdenia 1.10), čo by ale znamenalo, že existujú dve báze V s rôznym počtom prvkom, čo je ale spor so Steinitzovou vetou.

1.) Ak L je surjektívne, tak z definície surjektivity $\operatorname{Im} L = V$ a teda aj $\dim \operatorname{Im} L = \dim V$, z čoho $\operatorname{Ker} L = \{0\}$, čo je ale ekvivalentné s tým, že L je injektívne.

3.) Ak je L surjektivne resp. injektívne, tak podľa toho, čo sme si už dokázali, je L i injektívne resp. surjektívne a teda je bijektívne. Ak je L bijektívne, tak je z definície surjektívne a injektívne. □

DEFINÍCIA 2.15. (Homomorfizmy vektorových priestorov) Aby sme si trocha pripomenuli stredoškolké praktiky učenia sa memorovacou metódou, zavedieme si nejeden nový pojem:

Nech V, W sú vektorové priestory a $L : V \to W$ lineárne zobrazenie. L sa tiež nazýva **homomorfizmus** V do W.[2] Ak je L tiež surjektívne, hovoríme o **epimorfizme**, ak je injektívne, tak o **monomorfizme**, ak je surjektívne aj injektívne, teda bijektívne, tak L je **izomorfizmus**. Zobrazenia do seba (teda ak $W = V$) sa nazývajú **endomorfizmy** a tie, ktoré su naviac izomorfizmy sa označujú **automorfizmy**.

MiniOdbočka: Slovom homomorfizmus všeobecne označujeme zobrazenie medzi algebraickými štruktúrami, ktoré v istom zmysle zachováva ich štruktúru. Napríklad grupový homomorfizmus zachováva grupovú operáciu skladania, ako aj operáciu inverse a tiež nulový prvok. Keď hovoríme, že zachováva operáciu skladania, tak tým myslíme to, že obraz prvku vzniknutého zložením dvoch prvkov musí tiež vzniknúť zložením obrazov týchto dvoch prvkov. Lineárne zobrazenie medzi vekt. priestormi je teda tiež homomorfizmus! Zachováva sčítanie vektorov a tiež násobenie prvkom z $\mathbb{R}(\mathbb{C})$.

Ak existuje izomorfizmus medzi dvoma štruktúrami, tak hovoríme, že sú izomorfné. Izomorfné štruktúry sú vlastne algebraicky identické (až na jemnosti, ktoré neprenášame). Konečnedimenzionálne vektorové priestory sú všetky izomorfné s $\mathbb{R}^n$, teda napríklad oproti grupám sú omnoho „chudnobnejšie“.

Uvedieme teraz jeden veľmi zaujímavý príklad izomorfizmu: Overte, že komplexné čísla $a + ib$ sú izomorfné s maticami tvaru $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$, kde sčítaniu komplexných čísel zodpovedá sčítanie matíc a násobedniu násobednie matíc. Tento fakt sa dá nahliadnúť tiež tak, že platí $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Tým pádom matice zapísatelné v tvare: $a\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) + b\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ sa vďaka pravidlám pre násobenie a sčítanie matíc naozaj „správajú“ ako komplexné čísla. Všimnite si, že komplexne združenému číslu zodpovedá matica transponovaná a veľkosť komplexného čísla sa rovná determinantu príslušnej matice.

[2] Prípadné pochybnosti o zmysluplnosti definície tohto a nasledujúcich pojmov si odložte až po poznámke na konci definície.

Podobným spôsobom môžme pomocou matíc reprezentovať i kvaternióny. Matice $\sigma_1\sigma_2$, $\sigma_3\sigma_1$ a $\sigma_2\sigma_3$ spĺňajú tie isté vlastnosti ako kvaterniónové jednotky: $i^2 = j^2 = k^2 = ijk = -1$, kde matice σ_i sú Pauliho matice, ktoré majú tvar $\sigma_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $\sigma_2 = \left(\begin{smallmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{smallmatrix}\right)$ a $\sigma_3 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Môžte ľahko overiť, že platí $\sigma_1\sigma_2 = \mathrm{i}\sigma_3$, pričom čísla môžte cyklicky zameniť. Potom sa dá kvaternión $a+ib+jc+kd$ zapísať maticou ako $\left(\begin{smallmatrix} a+\mathrm{i}b & c+\mathrm{i}d \\ -c+\mathrm{i}d & a-\mathrm{i}b \end{smallmatrix}\right)$. Ak maticu transponujeme a komplexne združíme, resp. spočítame determinant, znovu dostaneme združený kvaternión, resp. jeho veľkosť.

Definícia 2.16. Nech V a W sú vektorové priestory konečnej dimenzie a $L : V \to W$ lineárne zobrazenie. **Rankom** lineárneho zobrazenia, značíme $\mathrm{rank}(L)$, budeme rozumieť

$$\mathrm{rank}(L) := \dim \mathrm{Im}\, L.$$

Niekedy sa môžme namiesto ranku stretnúť i s pojmom hodnosť lineárneho zobrazenia, značíme $h(L)$.

Poznámka 2.20. Vieme, že matica $A \in M(m, n, \mathbb{R})$ definuje lineárne zobrazenie $\mathcal{A} : \mathbb{R}^n \to \mathbb{R}^m$ s predpisom $x \mapsto Ax$. Aký je $\mathrm{rank}(\mathcal{A})$? Ak si uvedomíme, ako súvisí $\mathrm{Im}\,\mathcal{A}$ s maticou A, tak na otázku ľahko zodpovieme. Ak označíme stĺpce matice:

$$\begin{pmatrix} | & & | \\ a_1 & \dots & a_n \\ | & & | \end{pmatrix},$$

tak si už ľahko uvedomíme, že obraz $\mathcal{A}$ definovaný, ako $\mathrm{Im}\,\mathcal{A} = \{y \in \mathbb{R}^m | \exists x \in \mathbb{R}^n : y = Ax\}$ sa dá zapísať tiež $\mathrm{Im}\,\mathcal{A} = \{y \in \mathbb{R}^m | \exists x \in \mathbb{R}^n : y = \sum_{i=1}^n a_i x^i\} \equiv \mathcal{L}(\{a_1, \dots, a_n\})$. To ale znamená, že $\mathrm{rank}(\mathcal{A}) = \dim \mathcal{L}(\{a_1, \dots, a_n\})$. Z istých dôvodov si zadefinujeme tiež rank matice ako

$$\mathrm{rank}(A) := \dim \mathcal{L}(\{a_1, \dots, a_n\}),$$

a teda platí $\mathrm{rank}(\mathcal{A}) = \mathrm{rank}(A)$. Toto minitvrdenie (ku ktorému sme postupne došli) neplatí iba pre zobrazenia $\mathcal{A} : \mathbb{R}^n \to \mathbb{R}^m$, ale všeobecne pre akékolvek lin. zobrazenie L medzi dvomi v.p. (s bázami $\mathcal{B}$ a $\mathcal{C}$), teda platí: (rozmyslite)

$$\mathrm{rank}(L) = \mathrm{rank}\left([L]_{\mathcal{C}}^{\mathcal{B}}\right)$$

Vidíme, že ak zobrazenie vyjadríme voči rôznym bázam, príslušné matice budú mať rovnaký rank. To je ale celkom zrejmé, lebo ak vynásobíme maticu regulárnou maticou, vzniknutá matica zodpovedá matici zloženého zobrazenia, pričom skladáme s bijekciou.

Ako spočítame rank matice (a teda aj rank ľubovolného li. zobrazenia)? Stačí nám nájsť bázu lin. obalu stĺpcov matice, čo docielime buď zdĺhavým algoritmom 1.1 (pripomenieme, že tento algoritmus vedel vybrať z množiny vektorov lin. nezávislú podmnožinu, ktorá generovala ten samý priestor), alebo sofistikovaným Gaussovým algoritmom (ktorý určite pozná azda už každý stredoškolák), ktorý nám dokáže pomocou stĺpcových úprav[3] upraviť maticu na Gaussovský tvar, v ktorom stĺpce matice budú lin. nezávislé, ale stĺpcové úpravy nám zaručia, že budú generovať ten samý priestor!

3. Vektorové priestory so skalárnym súčinom.

Definícia 3.17. Nech V je vektorový priestor nad telesom $\mathbb{R}(\mathbb{C})$ a b je zobrazenie $b : V \times V \to \mathbb{R}(\mathbb{C})$. Dvojicu (V, b) nazývame vektorový priestor so skalárnym súčinom práve vtedy keď sú splnené nasledujúce axiómy:

[3] Alebo pre niekoho možno príjemnejších úprav riadkových, ktoré použijeme na maticu transponovanú. Ak sa ale nebodaj pomýlime a maticu transponovať zabudneme a tým riadkovými úpravami spočítame rank matice transponovanej, výsledok bude aj napriek tomu vždy správny! Onedlho si naozaj dokážeme vetu, že rank matice je rovný ranku matice transponovanej.

1. $\forall x, y, z \in V:\ b(x+y, z) = b(x, z) + b(y, z)$,
2. $\forall x, y \in V, \forall r \in \mathbb{R}(\mathbb{C}):\ b(rx, y) = rb(x, y)$,
3. $\forall x, y \in V:\ b(x, y) = \overline{b(y, x)}$,
4. $\forall x \in V:\ b(x, x) \geq 0$,
5. $\forall x \in V:\ b(x, x) = 0 \Rightarrow x = 0$.

Poznámka 3.21. V prípade reálneho skalárneho súčinu (vtedy je nutne V nad $\mathbb{R}$) je axióm 3. splnený práve vtedy keď $b(x, y) = b(y, x)$. V prípade komplexného skalárneho súčinu si treba uvedomiť, že $b(x, x) \in \mathbb{R}$ lebo z 3. axiómu máme $b(x, x) = \overline{b(x, x)}$, takže môžme hovoriť o **nezápornosti**. Piaty axióm nazývame tiež **nedegenerovanosť**. Z prvých troch axiómov vyplýva istá linearita. Zvolme si pevné $y \in V$ a označme zobrazenie $b_y : V \to \mathbb{R}(\mathbb{C})$ definované ako $x \mapsto b(x, y)$. Vidíme, že sa jedná o lineárne zobrazenie. Hovoríme, že b je **lineárne** v prvej premennej. Zo symetrie v reálnom prípade vyplýva

$$b(x, y + rz) = b(y + rz, x) = b(y, x) + rb(z, x) = b(x, y) + rb(x, z),$$

teda b je lineárne v oboch premených hovoríme o **bilinearite**. Pozrime sa na to, čo sa deje v druhej zložke v komplexnom prípade

$$b(x, y + rz) = \overline{b(y + rz, x)} = \overline{b(y, x) + rb(z, x)} = \overline{b(y, x)} + \overline{r}\overline{b(z, x)} = b(x, y) + \overline{r}b(x, z).$$

Zobrazenie skonštruované ako $y \mapsto b(x, y)$ nazývame potom **antilineárne** a teda hovoríme, že b je antilineárne v druhej premennej a to všetko preto, lebo číslo vytýkame s pruhom. Komplexný skalárny súčin je teda v prvej premmennej lineárny a v druhej antilineárny a túto vlastnosť nazývame **sesqiulinearita**.

Aby sme v tom mali väčší poriadok, tak uvažujme zobraznie

$$F : V_1 \times V_2 \times \cdots \times V_k \to \mathbb{R}(\mathbb{C}),$$

ktoré je lineárne vo všetkých premenných. Takéto zobrazenie nazývame **multilineárna forma**. Slovíčko „forma“ značí to, že sa jedná o zobrazenie do $\mathbb{R}(\mathbb{C})$. Ak zobrazujeme z V, tak hovorím o lineárnej forme, ak z $V \times V$ (či obecne $V_1 \times V_2$), tak sa jedná o formu bilineárnu. Ako uvidíme, má zmysel hovoriť špeciálne i o formách sesquilineárnych, ktoré sú v prvej premmennej lineárne a v druhej antilineárne. Reálny skalárny súčin je teda bilineárnou formou (komplexný sesquilineárnou), ale splňuje i ďalšie vlastnosti, ktoré bilineárne formy splňovať nemusia.

Uvažujme teda bilineárnu formu $B : V \times V$, a nech $\{b_1, \ldots, b_n\}$ je báza konečnedimenzionálneho V. Potom tvrdíme, že zobrazenie B je určené sadou čísel $a_{ij} = B(b_i, b_j)$ a maticu $A = (a_{ij})$ nazývame maticu danej bilineárnej formy. Je to vskutku pravda, lebo nech si zoberieme ľubovolné prvky $v, w \in V$ so súradnicami $(v^1 \ldots v^n)$, resp. $(w^1 \ldots w^n)$, tak z linearity dostávame $B(v, w) = \sum_{ij} v^i a_{ij} w^j$. Pre všeobecnú bil. formu môžu byť prvky a_{ij} ľubovolné. Ak ale okrem bilinearity formy požadujeme napríklad symetričnosť, tak musí nutne platiť i $a_{ij} = a_{ji}$, teda $A = A^T$ (matica A je teda symetrická). Nakoľko i skalárny súčin je bilineárna forma (uvažujme zatiaľ len reálny prípad), tak i ten je tak isto určený sadou (reálnych) čísel $m_{ij} = b(b_i, b_j)$. No skalárny súčin spĺňa okrem bilinearity a symetričnosti i pozitivitu $\forall x \neq 0 : b(x, x) > 0$, a teda reálna matica $M = (m_{ij})$ musí byť v istom zmysle špeciálna. Triedu matíc, ktoré takto definujú skalárny súčin, nazývame pozitívne definitné matice (tieto matice definujú obecne komplexný skalárny súčin, o čom si povieme zachvíľu, takže my teraz uvažujeme reálne pozitívne definitné matice). Ako takáto špeciálna matica vyzerá? Platí, že M sa dá zapísať ako $M = A^T A$, kde A je matica, ktorej stĺpce sú lineárne nezávisle vektory, čo platí aj opačne, teda matica tvaru $A^T A$ definuje skalárny súčin. Prečo tomu tak je nie je asi celkom triviálne, uvádzame to len preto, aby ste mali akúsi predstavu o tom, ako vyzerá skalárny súčin v najširšom slova zmysle. Teda reálny skalárny súčin sa dá vždy zapísať ako $b(v, w) = \sum_{ij} v^i m_{ij} w^j$.

Príklad 3.10. Uvažujme vektorový priestor $\mathbb{R}^n$. Je zobrazenie $b : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ s predpisom $b(x, y) := \sum_{i=1}^{n} x^i y^i$ skalárnym súčinom? *Podľa predchádzajúceho textu teda stačí zistiť, či jednotková matica je pozitívne definitná.*

Overme teda axiómy skalárneho súčinu.
Linearita:

$$b(x, y + rz) = \sum_{i=1}^{n} x^i (y + rz)^i = \sum_{i=1}^{n} x^i (y^i + rz^i) = \sum_{i=1}^{n} x^i y^i + r \sum_{i=1}^{n} x^i z^i = b(x, y) + rb(x, z).$$

Symetričnosť:

$$b(x, y) = \sum_{i=1}^{n} x^i y^i = \sum_{i=1}^{n} y^i x^i = b(y, x).$$

Pozitívnosť:

$$\forall x \neq 0 : \; b(x, x) = \sum_{i=1}^{n} x^i x^i > 0.$$

Príklad 3.11. Uvažujme vektorový priestor $\mathbb{C}^n$. Nájdeme na ňom nejaký podobný skalárny súčin, ako v reálnom prípade? Čo by sa stalo, keby sme volili $b(x, y) := \sum_{i=1}^{n} x^i y^i$?

Skúsme bez toho, aby sme vyskúšali overovať jednotlivé axiómy, prísť k tomu, že by to fungovať nemohlo. Vyššie sme došli k tomu, že komplexný skalárny súčin je sesquilineárna forma, čo je de facto bilineárna forma s vytýkaním s pruhom v druhej zložke. Uvažujme teda V konečnej dimenzie s bázou $\{b_i\}$ a dva vektory v a w so súradnicami (v^i) a (w^i). Zo sesqulinearity skalárneho súčinu ale dostávame, že $b(v, w) = \sum_{ij} v^i b(b_i, b_j) \overline{w^j}$. Nemáme ale plnú volnosť pri definovaní zložiek $b(b_i, b_j)$ a musíme ich znova voliť tak, aby boli splnené i ostatné (okrem sesquilinearity) axiómy skal. súčinu, čo nás znova vedie k pozitívne definitnej matici. Teda $b(u, v)$ je skalárny súčin práve keď matica $M = (m_{ij})$, kde $m_{ij} = b(b_i, b_j)$, je pozitívne definitná. Ak by ste si chceli takúto maticu skonštruovať, tak skúste maticu v tvare $M = A^* A$, kde A má lin. nezávislé stĺpce a $*$ značí hermitovské združenie ($A^* := \overline{A^T}$). Uvážte, že pozitívne definitná matica musí byť hermitovská ($m_{ij} = \overline{m_{ji}}$), čo je istá analógia symetrickej matice v reálnom prípade. Všimnite si, že nami skonštruovaná poz. definitná matica hermitovská je.

Jasne teraz vidíme, že hore navrhnutá definícia skal. súčinu nebere ohľad na antilinearitu v druhej zložke. Vskutku $b(x, ry) = \sum_{i=1}^{n} x^i r y^i = rb(x, y)$. Jedná sa teda o spor s tretím axiómom. Ako sme už spomenuli, tretí axióm je esenciálny, ak chceme vôbec hovoriť o nejakej pozitívnosti, lebo inak nemáme zaručené, že výraz tvaru $b(x, x)$ je reálny, ako vidíme aj na nasledujúcom príklade.

Vskutočnosti takto zavedený skal. súčin by mal fatálne dôsledky. Zoberme si príklad $\mathbb{C}^2$ a vektoru $x = (1, \mathrm{i})$. Spočítajme $b(x, x) = 1 - 1 = 0$. Taktiež by sme mohli dostať napríklad pre vektor $y = (1 + \mathrm{i}, 0)$ komplexnú „veľkosť“ vektora.

No už krajšie by vyzeral skalárny súčin definovaný ako $b(x, y) := \sum_{i=1}^{n} x^i \overline{y^i}$. *Tí z nás, čo čítajú (či píšu) tieto minipoznámky už vedia, že takto definovaná sesquilineárna forma je skalárny súčin, lebo sme sa už presvedčili, že jednotková matica je pozitívne definitná.*

Overme ale posledné tri axiómy (je to poučné!):
(Kvázi)Symetričnosť:

$$b(x, y) = \sum_{i=1}^{n} x^i \overline{y^i} = \sum_{i=1}^{n} \overline{y^i \overline{x^i}} = \overline{b(y, x)}.$$

Pozitívnosť:

$$\forall x \neq 0 : \; b(x, x) = \sum_{i=1}^{n} x^i \overline{x^i} = \sum_{i=1}^{n} |x^i|^2 > 0.$$

Poznámka 3.22. Našli sme teda jeden skalárny súčin v reálnom i komplexnom prípade (ktorý je natoľko štandardný, že sa oplatí ho vnímať). No v skutočnosti ich existuje nekonečne mnoho (toľko, koľko je pozitívne definitných matíc, ak stále hovoríme o konečnedimenzionálnych priestroch). Zanedlho si ukážeme, že nech máme skalárny súčin akýkoľvek, vždy sa nám podarí nájsť bázu takú, že ak voči nej vyjadríme súradnice vektorov, skalárny súčin nadobudne toho jednoduchého (štandardného) tvaru.

VETA 3.19. (Cauchy-Schwartzova nerovnosť v reálnom prípade) (V, b) buď vektorový priestor so skalárnym súčinom nad $\mathbb{R}$. Potom platí

$$\forall u, v \in V : \ |b(u, v)| \leq \|u\|\|v\|$$

kde symbolom $\|\cdot\|$ značíme $\|u\| = \sqrt{b(u, u)}$. Neskôr uvidíme, že takto môžme definovať normu indukovanú skalárnym súčinom.

DÔKAZ. Je dobré si uvedomiť, že táto vlastnosť je (okrem iného aj) dôsledkom pozitívnosti. Teda ak by sme nemali túto podmienku, niekedy by sa nám skutočne podarilo definvať skal. súčin tak, že napríklad pre nejaké $u, v \in V$ by platilo $b(u, v) = 2$ a $b(u, u) = b(v, v) = 1$. Takže teraz už vieme, čo určite pri dôkaze použijeme :-). Platí:

$$\forall t \in \mathbb{R} : \ 0 \leq b(u + tv, u + tv) = b(u, u) + 2tb(u, v) + t^2 b(v, v).$$

Pokiaľ $v \neq 0$, tak sa jedná o kvadratickú nerovnicu, lebo potom nutne $b(v, v) \neq 0$. V opačnom prípade síce o kvadratickú nerovnicu nejde, ale CS nernosť je splnená triviálne, lebo $b(u, v) = b(u, 0) = 0$ (to, že posledné rovnítko platí, si rozmyslite, ak chcete). Kvadratická nerovnica, nakoľko $b(v, v) > 0$, môže byť splnená pre všetky $t \in \mathbb{R}$, ale iba v prípade, že diskriminant je nekladný. Teda

$$0 \geq 4b(u, v)^2 - 4b(v, v)(u, u),$$

čo je splnené práve vtedy, ak platí CS nerovnosť. □

8. přednáška z lineární algebry
Cauchy-Schwartzova věta
20. listopad 2007

Zopakujme vzorečky $Re(z) = \frac{z+\overline{z}}{2}$ a $Im(z) = \frac{z-\overline{z}}{2i}$ pro všechna $z \in \mathbb{C}$.

Nechť (V, b) je komplexní vektorový prostor se skalárním součinem. Připomeňme, že $b(u,v) = \overline{b(v,u)}$ pro každé $u, v \in V$. Odtud plyne pro každé $r \in \mathbb{C}$ je $b(u, rv) = \overline{b(rv, u)} = \overline{rb(v,u)} = \overline{r}\overline{b(v,u)} = \overline{r}b(u,v)$, tj. z pravé složky se vytýká sdružené číslo, tj. b je lineární v první a „anti-linearní" v druhé složce, tj. sesquilineární, jak jsme jej nazývali na přednášce. Definujme normu $||\cdot||$ indukovanou skalárním součinem b. Pro $v \in V$ položme $||v|| := \sqrt{b(v,v)}$. Zřejmě platí $||rv|| = \sqrt{b(rv,rv)} = \sqrt{r\overline{r}b(v,v)} = \sqrt{r\overline{r}}||v|| = |r|\,||v||$ pro každé $r \in \mathbb{C}$ a $v \in V$. Tj. z normy se vytýká absolutní hodnota.

Věta 3.20. Nechť (V, b) je komplexní vektorový prostor se skalárním součinem. Potom pro každé $u, v \in V$ platí

$$|b(u,v)| \leq ||u||\,||v||.$$

Navíc rovnost nastává právě tehdy, když $\{u, v\}$ je lineárně závislá.

Důkaz.

A. Nejprve dokažme první část.Uvažme ve větě zmíněné dva vektory $u, v \in V$ a pro každé $\lambda \in \mathbb{R}$ se zabývejme $\lambda u + v$. Z vlastnosti 4) sk. s. plyne, že $0 \leq b(\lambda u + v, \lambda u + v)$. Upravujme pravou stranu. Z linearity sk. s. v levé složce a z vlastnosti, že z pravé složky se sice vytýká opruhované (komplexně sdružené) komplexní číslo, ale v našem případě $\lambda = \overline{\lambda}$, dostáváme

$$\begin{aligned} 0 &\leq b(\lambda u + v, \lambda u + v) = b(\lambda u, \lambda u + v) + b(v, \lambda u + v) \\ &= b(\lambda u, \lambda u) + b(\lambda u, v) + b(v, \lambda u) + b(v, v) \\ &= \lambda^2 ||u||^2 + \lambda b(u,v) + \lambda b(v,u) + ||v||^2 \\ &= \lambda^2 ||u||^2 + \lambda(b(u,v) + \overline{b(u,v)}) + ||v||^2 \\ &= \lambda^2 ||u||^2 + 2\lambda Re(b(u,v)) + ||v||^2 \end{aligned}$$

Celkem máme

$$0 \leq \lambda^2 ||u||^2 + 2\lambda Re(b(u,v)) + ||v||^2. \tag{1}$$

Dostali jsme tedy nerovnost platnou pro všechna reálná λ. Všimněte si, že v případě sk. s. nad reálným v.p. se předchoí nerovnost redukuje na tu, kterou jsme dostali v důkazu minulé věty, tj. při důkazu Cauchy-Schwartzovy nerovnosti pro reálný v.p., neboť $b(u,v) = Re(b(u,v))$, neboť v reálném případě je $b : V \times V \to \mathbb{R}$.

Napišme ještě rovnost přidruženou k nerovnici (1)

$$0 = \lambda^2 ||u||^2 + 2\lambda Re(b(u,v)) + ||v||^2. \tag{2}$$

Rozlišme dva případy

1. $u = 0$. Tehdy nerovnost (1) není kvadratická nerovnost. Ale $b(0,v) = 0 = ||0||\,||v||$, tj. dokazovaná nerovnost platí.
2. $u \neq 0$. Z toho, že sk. s. dvou stejných vektorů je nula (tehdy a) jen tehdy, když je tento vektor nula, plyne, že nerovnost (1) je kvadratická. Ze střední školy je známo, že kvadratická nerovnost je splněna pro všechna reálná čísla λ právě tehdy, když je její diskriminant nekladný. Tj. $0 \geq D = 4Re(b(u,v))^2 - 4||u||^2||v||^2$, odkud dostáváme $|Re(b(u,v))| \leq ||u||\,||v||$, čímž spíše

$$Re(b(u,v)) \leq ||u||\,||v||, \tag{3}$$

neboť pokud je inkriminovaná část nezáporná, je rovna své abolutní hodnotě, a pokud je záporná, dostáváme nerovnici triviální, totiž že záporné číslo je menší nebo rovno nezápornému součinu norem napravo.
My však máme dokázat $|b(u,v)| \leq ||u||\,||v||$. Bude tedy nutné přijít s rafinovaným (ale pouze pomocným) ζ – viz níže. Rozlišme v rámci naší volby $u \neq 0$ ještě následující podmožnosti.

a) $b(u,v) = 0$. Zde opět není co dokazovat, neboť Cauchy-Schwartzova nerovnost platí triviálně.

b) Pro $b(u,v) \neq 0$ definujme $\zeta := \frac{b(u,v)}{|b(u,v)|}$. Zřejmě

$$1 = |\zeta|^2 = \zeta\overline{\zeta}. \tag{4}$$

Zkusme spočítat: $b(\overline{\zeta}u, v) = \overline{\zeta}b(u,v) = \frac{\overline{b(u,v)}}{|b(u,v)|}b(u,v) \in \mathbb{R}$, neboť obecně platí $\overline{z}z \in \mathbb{R}$ pro každé komplexní číslo z. Shrnuto dostáváme $Re(b(\overline{\zeta}u, v)) = b(\overline{\zeta}u, v)$, neboť se jedná o reálné číslo. Pišme $|b(u,v)| = \frac{b(u,v)\overline{b(u,v)}}{|b(u,v)|} = \overline{\zeta}b(u,v) = b(\overline{\zeta}u, v) = Re(b(\overline{\zeta}u, v))$. Tj. celkem

$$|b(u,v)| = Re(b(\overline{\zeta}u, v)). \tag{5}$$

O tomto výrazu však již nějaké informace máme. Nerovnost (3), kde namísto u pišme $\overline{\zeta}u$, dostává tvar $Re(b(\overline{\zeta}u, v)) \leq ||\zeta u||||v|| = |\zeta|||u||||v|| = ||u||||v||$, kde jsem užili rovnosti (4). Dosadíme-li do (5) za levou stranu právě získanou nerovnost, dostaneme

$$|b(u,v)| \leq ||u||\,||v||,$$

čímž je první část důkazu hotova.

B. Nyní se věnujme druhé části.

1) Jedna implikace je zřejmá, a sice: pokud je $\{u,v\}$ l.z., potom platí rovnost. Zkusme toto dokázat explicitně. Nechť $\{u,v\}$ je l.z. Jsou dvě možnosti $u = 0$, a tehdy dokazovaná rovnost zjevně platí, nebo $u \neq 0$. Tehdy ovšem lineární závislost uvažované množiny implikuje, že existuje $\lambda \in \mathbb{C}$, že $\lambda u + v = 0$. Spočtěme $|b(u,v)| = |b(u,-\lambda u)| = |\overline{\lambda}|\,||u||^2 = |\lambda|||u||\,||u|| = ||u||\,|| - \lambda u|| = ||u||\,||v||$, kde jsme užili, že norma komplexního čísla je stejná jako norma čísla sdruženého a opačného (s opačným znaménkem). Navíc jsme ještě užili, jak se vytýká z normy.

2) Nyní dokažme, že platí-li v Cauchy-Schwartzově nerovnosti rovnost, potom je uvažovaná množina l.z. Postupujme obráceně vzhledem k důkazu první části věty (část A). Nejprve si všimněme, že $b(u,v) = 0$ je opět nezajímavá, neboť díky tomu, že předpokládáme rovnost dostneme, že $||u||\,||v|| = 0$, což implikuje $u = 0$ nebo $v = 0$, tj. v obou případech je $\{u,v\}$ l.z. Nyní se zabývejme situací, kdy je $b(u,v) \neq 0$, tj. je možné definovat pomocné ζ jako výše. Připomeňme, že v průběhu části (A) jsme dostali $|b(u,v)| = Re(b(\overline{\zeta}u, v)) \geq ||\overline{\zeta}u||\,||v|| = ||u||\,||v||$. Má-li platit rovnost, dostáváme, že

$$Re(b(\overline{\zeta}u, v) = ||\overline{\zeta}u||\,||v||. \tag{6}$$

Napišme nyní místo (2) rovnici $\lambda^2||\overline{\zeta}u||^2 + 2Re(b(\overline{\zeta}u, v))\lambda + ||v||^2 = 0$. Diskriminant v tomto případě je $D = 4Re(b(\overline{\zeta}u, v))^2 - 4||\overline{\zeta}u||^2||v||^2$. Vzhledem k rovnosti (6) dostáváme, že diskriminant je nula, a proto nyní uvažovaná rovnice má alespoň jeden kořen (dokonce právě jeden, ale to není důležité). Uvědomme si, že uvažovaná rovnice je nic jiného než $b(\lambda\overline{\zeta}u + v, \lambda\overline{\zeta}u + v) = 0$. Jelikož jme právě dokázali, že rovnice má řešení, můžeme psát, že existuje λ_1, že $b(\lambda_1\overline{\zeta}u + v, \lambda_1\overline{\zeta}u + v) = 0$. Pokud skalární součin stejných vektorů je nula, je uvažovaný vektor nula, tj. dostáváme

$$(\lambda_1\overline{\zeta})u + v = 0,$$

tj. $\{u,v\}$ je l.z., c.b.d.

□

9. přednáška z lineární algebry

27. listopad 2007

Poznámka 3.23. V reálném případě navíc platí, že rovnost $|b(u,v)| = \|u\|\|v\|$ implikuje lineární závislost (důkaz stejně jako v komplexním případě). Vycházíme z toho, že reálný případ splňuje „stejné“ axiomy jako komplexní.

$$b(u,v) = b(v,u) = \overline{b(v,u)}$$

Definice 3.18. V je vektorový prostor. $b : V \times V \to \mathbb{R}$ je skalární součin. Zobrazení $\| \ \| : V \to \mathbb{R}$ definované $\|u\| = \sqrt{b(u,u)}$ nazvu normou indukovanou skalárním součinem.

Definice 3.19. $\| \ \|$ nazvu **normou** pokud $\forall u, v \in V, r \in \mathbb{R}$ platí:

1) $\|u + w\| \leq \|u\| + \|v\|$
2) $\|rv\| = |r|\|v\|$
3) $\|v\| = 0 \ \Rightarrow \ v = 0$

Tvrzení 3.21. (Trojúhelníková nerovnost) V je vektorový prostor. $b : V \times V \to \mathbb{R}$ je skalární součin. $\| \ \| : V \to \mathbb{R}$ je norma indukovaná skalárním součinem. Pak:

$$\|u + w\| \leq \|u\| + \|v\|$$

Důkaz. $b(u+v, u+v) = b(u, u+v)+b(v, u+v) = b(u,u)+2b(u,v)+b(v,v) = \|u\|^2+2b(u,v)+\|v\|^2$
Z Cauchy-Schwarzovy nerovnosti víme, že: $b(u,v) \leq \|u\|\|v\|$ Takže pro celý výraz dostáváme:

$$\begin{aligned} b(u+v, u+v) &\leq \|u\|^2 + 2\|u\|\|v\| + \|v\|^2 \\ \|u+v\|^2 &\leq (\|u\| + \|v\|)^2 \\ \|u+v\| &\leq \|u\| + \|v\| \end{aligned}$$ □

Stejně zní věta i pro komplexní skalárny součin a dokazuje se taky stejně, akorát je potřeba si uvědomit, že pro $z \in \mathbb{C}$ platí: $Re(z) \leq |z|$.

Tvrzení 3.22. V je vektorový prostor. $b : V \times V \to \mathbb{R}$ skalární součin. Pak norma $\| \ \| : V \to \mathbb{R}$ indukovaná skalárním součinem je norma.

Důkaz.

1) $\|u + v\| \leq \|u\| + \|v\|$ už bylo dokázáno. Viz trojúhelníková nerovnost.
2) $\|rv\| = |r|\|v\|$ dokážeme úplně snadno: $\|rv\| = \sqrt{b(rv, rv)} = \sqrt{r^2 b(v,v)} = |r|\|v\|$
3) $0 = \|v\| = \sqrt{b(v,v)} \Rightarrow b(v,v) = 0$ a z vlastnosti 4 skal. součinu pak platí, že $v = 0$ □

Poznámka 3.24.

1) $\| \ \|$ je norma indukovaná skalárním součinem b, pak skalární součin jde v reálném případě spočítat z normy podle **polarizační formule**:

$$b(u,v) = \frac{1}{2}(\|u+v\|^2 - \|u\|^2 - \|v\|^2)$$

neboť $\frac{1}{2}(b(u+v,u+v) - b(u,u) - b(v,v)) = \frac{1}{2}(b(u,u) + 2b(u,v) + b(v,v) - b(u,u) - b(v,v)) = \frac{1}{2}(2b(u,v)) = b(u,v)$.

2) Existují normy, které nejsou indukované skalárním součinem. Např $\| \ \| : \mathbb{R}^2 \to \mathbb{R} \quad \|(x,y)\| = |x| + |y|$

a) Dokážeme, že se opravdu jedná o normu. Tedy ověříme vlastnosti normy.

$$\|(x,y)+(x',y')\| = \|(x+x',y+y')\| = |x+x'|+|y+y'|$$

a po užití trojúhelníkové nerovnosti můžeme psát:

$$\|(x,y)+(x',y')\| \leq |x|+|x'|+|y|+|y'| = \|(x,y)\|+\|(x',y')\|$$

Nyní ověřme druhou vlastnost:

$$\|r(x,y)\| = \|(rx,ry)\| = |rx|+|ry| = |r|(|x|+|y|) = |r|(\|(x,y)\|)$$

A konečně třetí vlastnost:

$$0 = \|(x,y)\| = |x|+|y| \;\Rightarrow\; |x| = |y| = 0$$

b) Předpokládáme, že norma je indukovaná nějakým skalárním součinem a chceme odvodit spor. Pokud je norma indukovaná skalárním součinem, bude pro ni platit polarizační formule. Tedy:

$$b((1,-1),(2,1)) = \frac{1}{2}(\|(3,0)\|^2 - \|(1,-1)\|^2 - \|(2,1)\|^2) = \frac{1}{2}(3^2-2^2-3^2) = -2$$

$$b((2,2),(2,1)) = \frac{1}{2}(\|(4,3)\|^2 - \|(2,2)\|^2 - \|(2,1)\|^2) = \frac{1}{2}(7^2-4^2-3^2) = 12$$

$$b((3,1),(2,1)) = \frac{1}{2}(\|(5,2)\|^2 - \|(3,1)\|^2 - \|(2,1)\|^2) = \frac{1}{2}(7^2-4^2-3^2) = 12$$

Ale z linearity skalárního součinu by mělo platit, že: $b((1,-1),(2,1))+b((2,2),(2,1)) = b((3,1),(2,1))$, což očividně splněno není a máme vytoužený spor.

Definice 3.20.

* Buď (V,b) vektorový prostor se skalárním součinem. Potom $\{f_i, i \in I\} \subseteq V$ nazvu **ortogonální systém** pokud $\forall i,j \in I, i \neq j$ platí $b(f_i,f_j) = 0$ a pro $\forall i \in I:\ b(f_i,f_i) \neq 0$
* $\{f_i,\ i \in I\}$ nazvu **ortogonální bází**, pokud je ortogonálním systémem a zároveň bází.
* $\{f_i,\ i \in I\}$ nazvu **ortonormální bází**, pokud je ortogonální bazí a pro $\forall i \in I$ platí, že $b(f_i,f_i) = 1$.

Tvrzení 3.23. V je vektorový prostor $\{f_i,\ i \in I\}$ je ortogonální systém. Pak $\{f_i,\ i \in I\}$ je lineárně nezávislá.

Důkaz. Pro spor mějme $\{f_i,\ i \in I\}$ lineárně závislou, takže $\exists\{c_1,\ldots,c_k\} \in \mathbb{R}^k\backslash\{0,\ldots,0\}$ taková, že:

$$c_1f_1 + c_2f_2 + \ldots + c_kf_k = 0$$

A teď vezmeme postupně všechna $j \in \{1,\ldots,k\}$ a vynásobíme předchozí rovnost vektorem f_j. Dostaneme:

$$c_1b(f_1,f_j) + \ldots + c_jb(f_j,f_j) + \ldots + c_kb(f_k,f_j) = 0$$

Podle definice ortogonality ihned vidíme, že skalární součiny ve všech členech kromě $b(f_j,f_j)$ vyjdou nulové, takže se nám rovnice zredukuje na tvar:

$$c_jb(f_j,f_j) = 0$$

kde skalární součin je nenulový, takže abychom dostali nulu musí být nutně nulové c_j. Jelikož jsme toto prováděli pro všechna $j \in \{1,\ldots,k\}$ (jak je zmíněné výše), dostáváme triviální lineární kombinaci a vektory jsou tedy lineárně nezávislé, což je spor s předpokladem □

Tvrzení 3.24. (Pythagorova věta) (V, b) je vektorový prostor se skalárním součinem a $\| \ \|$ je norma indukovaná skalárním součinem. $\{f_i\}_{i\in I}$ je ortonormální bází tohoto vektorového prostoru $(\forall v \in V : v = \sum_{i=1}^{n} f_i v^i)$. Pak

$$\|v\|^2 = \sum_{i=1}^{n} (v^i)^2$$

Důkaz.

$$\|v\|^2 = b(v, v) = b\Big(\sum_{i=1}^{n} f_i v^i, \sum_{j=1}^{n} f_j v^j\Big) = \sum_{i=1}^{n}\sum_{j=1}^{n} b(f_i, f_j) v^i v^j$$

Dle definice ortonormální báze je $b(f_i, f_j) = \delta_{ij}$ (Kroneckerovo delta), takže:

$$\|v\|^2 = \sum_{i=1}^{n}\sum_{j=1}^{n} \delta_{ij} v^i v^j = \sum_{i=1}^{n} v^i v^i = \sum_{i=1}^{n} (v_i)^2 \quad \square$$

Definice 3.21. (V, b) je vektorový prostor se skalárním součinem $M \subseteq V$ je jeho podmnožina. Pak

$$M^\perp = \{v \in V | \, \forall m \in M : \, b(v, m) = 0\}$$

nazvu **ortogonální doplněk** množiny M.

Např.: Ortogonální doplněk množiny $M = \{(1, 0, 0)\}$ vybrané z vektorového prostoru $\mathbb{R}^3$ je $M^\perp = \{(0, y, z) | \ y \in \mathbb{R}, \ z \in \mathbb{R})\}$. Jinými slovy řečeno, hledáme všechny vektory z daného vektorového prostoru kolmé na množinu M.

Tvrzení 3.25. (V, b) je vektorový prostor se skalárním součinem. $M, N \subseteq V$. Pak

1) $M^\perp$ je vektorový podprostor V
2) $M \subseteq N \Rightarrow N^\perp \subseteq M^\perp$
3) $\mathcal{L}(M)^\perp = M^\perp$

Důkaz.

1) $v \in M^\perp$, $w \in M^\perp$, $r \in R$ a chceme, aby $v + w \in M^\perp$, $rv \in M^\perp$. Pre všechny $m \in M$ platí:
   a) $b(v + w, m) = b(v, m) + b(w, m)$ oba sčítance jsou dle definice ortogonálního doplňku nulové, takže pak musí i $v + w \in M^\perp$
   b) $b(rv, m) = rb(v, m) = r \cdot 0 = 0 \Rightarrow rv \in M^\perp$
2) Chci aby každý vektor z $N^\perp$ byl obsažen i v $M^\perp$. To, že vektor $v \in N^\perp$ znamená, že $b(v, n) = 0, \ \forall n \in N$. Ale množina M je podmnožinou množiny N, takže tím spíš $b(v, m) = 0$ pro $\forall m \in M$ a tedy vektor $v \in M^\perp$.
3) Musíme dokázat dvě inkluze
   a) $M \subseteq \mathcal{L}(M) \Rightarrow \mathcal{L}(M)^\perp \subseteq M^\perp$ viz výše.
   b) Je $M^\perp \subseteq \mathcal{L}(M)^\perp$? Když $v \in M^\perp$, tak chceme, aby $v \in \mathcal{L}(M)^\perp$, čím myslíme, že $\forall w \in \mathcal{L}(M) : b(v, w) = 0$. Z definice lineárního obalu:

$$w \in \mathcal{L}(M) \Rightarrow \exists c_1, \ldots, c_k \in \mathbb{R} \text{ také, že } w = \sum_{i=1}^{k} c_i m_i, \text{ kde } m_i \in M, \ i = 1 \ldots k$$

   Směle dosadíme:

$$b(v, \sum_{i=1}^{k} c_i m_i) = \sum_{i=1}^{k} c_i b(v, m_i) = \sum_{i=1}^{k} c_i \cdot 0 = 0 \quad \square$$

ALGORITMUS 3.2. (Gramm-Schmidtova ortonormalizace)
INPUT: $\{v_1, \ldots, v_k\} \subseteq V$
OUTPUT: $\{f_1, \ldots, f_l\}$, že $\{f_i\}_{i=1}^{l}$ je ortonormální systém a dále platí:

$$\mathcal{L}(\{f_i, \ldots, f_l\}) = \mathcal{L}(\{v_1, \ldots, v_k\})$$

Bez újmy na obecnosti můžeme předpokládat, že $\{v_1, \ldots, v_k\}$ je linárně nezávislá, protože si takovou množinu můžeme z té původní vždy připravit aniž bychom změnili lineární obal (Například pomocí Gaussovy eliminace nebo Algoritmu 1.1).
POSTUP:

1) $f_1' = v_1$
2) $f_2' = v_2 + \lambda_2^1 f_1'$
   ale čemu se rovná λ_2^1? Požadujeme, aby skalární součin $b(f_2', f_1') = 0$

$$0 = b(v_2 + \lambda_2^1 f_1', f_1') = b(v_2, f_1') + \lambda_2^1 b(f_1', f_1') \Rightarrow \lambda_2^1 = -\frac{b(v_2, f_1')}{b(f_1', f_1')}$$

3) $f_3' = v_3 + \lambda_3^1 f_1' + \lambda_3^2 f_2'$
   a opět chceme, aby byl třetí vektor kolmý na všechny předcházející. Máme tedy dvě podmínky:

$$\left.\begin{matrix} b(f_3', f_1') = 0 \\ b(f_3', f_2') = 0 \end{matrix}\right\} \quad \Rightarrow \quad \lambda_3^1 = -\frac{b(v_3, f_1')}{b(f_1', f_1')} \quad \text{a také} \quad \lambda_3^2 = -\frac{b(v_3, f_2')}{b(f_2', f_2')}$$

   Postup je stejný jako v předcházejícím případě, jen předpokládáme ortogonálnost čárkovaných vektorů (Tedy, že např.: $b(f_2', f_1') = 0$).

4) Opakujeme dále algoritmus, přičemž obecné vyjádření:

$$f_j' = v_j + \sum_{i=1}^{j-1} \lambda_j^i f_i', \quad \text{kde} \quad \lambda_j^i = -\frac{b(v_j, f_i')}{b(f_i', f_i')}$$

5) Provedeme normalizaci:

$$f_j = \frac{f_j'}{\|f_j'\|}$$

VĚTA 3.26. (Správnost Gramm-Schmidtovy ortogonalizace)
Dokážeme, že výstup algoritmu, tj.: $\{f_i\}_{i=1}^{r}$ je ortonormální báze prostoru $\mathcal{L}(\{v_1 \ldots v_r\})$. Ještě před tým, než začneme cokoliv dokazovat si uvedomme, že vektory $\{f_i\}_{i=1}^{r}$ vůbec umíme zestrojit. Na konci ortogolizačního procesu jsme vektory f_i' nanormovali na jedničku, co umíme jenom tehdy, když ich velikost je nenulová, tedy když jsou nenulové. Jelikož předpokládáme lineární nezávislost množiny $\{v_1 \ldots v_r\}$ kterou ortogonalizujeme, nemůže nastat, že některý z vektorů f_i' by byl nulový. Z konštrukce těchto vektorů by to znamenalo, že jsme našli netriviální lineárni kombinaci (minimálně jednička před v_i) vektorů $\{v_1 \ldots v_r\}$.

a) Ukažme, že náš systém $\{f_i\}_{i=1}^{r}$ je ortonormální, což znamená že všechnu dva různé vektory v systému sou na sebe kolmé, a že norma každého vektoru je jednička.

   (i) Pokusíme se nejdříve dokázat, že systém je ortogonální. Ortogonální je právě tehdy, když i jejich libovolný nenulový násobek je ortogonální. Tedy speciálně když vektory $\{f_i'\}_{i=1}^{r}$ jsou ortogonální. No z konštrukce je naprosto zrejmé, že ortogonalizační relace vektory spňují (tak jsme ich předce zestrojovali). No pro úplnost to ještě dokážeme matematickou indukci:

1) Ověření indukčního předpokladu pro $k = 1$: $f'_1 = v_1 \neq 0 \Rightarrow \{f'_1\}$ je ortogonální systém.
2) Dokážeme, že $\{f'_i\}_{i=1}^{k+1}$ je ortogonální systém, když předpokládáme, že $\{f'_i\}_{i=1}^{k}$ jsou ortogonální. Dokážeme to pro $k = 1, \ldots, r-1$. Takže pro $i \leq k$ můžeme psát:

$$b(f'_{k+1}, f'_i) = b(v_{k+1} - \sum_{j=1}^{k} \frac{b(v_{k+1}, f'_j)}{b(f'_j, f'_j)} f'_j, f'_i) =$$

$$= b(v_{k+1}, f'_i) - \sum_{j=1}^{k} \frac{b(v_{k+1}, f'_j)}{b(f'_j, f'_j)} b(f'_j, f'_i) = b(v_{k+1}, f'_i) - \sum_{j=1}^{k} b(v_{k+1}, f'_j)\delta_{ij}$$

neboť podle indukčního předpokladu platí $b(f'_j, f'_i) = b(f'_j, f'_j)\delta_{ij}$, takže vztah přepíšeme na:

$$b(v_{k+1}, f_i) - b(v_{k+1}, f_i) = 0$$

čímž jsme dostali přesně to, co jsme chtěli, tedy, že vektor f'_{k+1} je vskutku kolmý na všechny vektory jemu předešlé, které jsou taky podle indukčního předpokladu kolmé mezi sebou. Ostáva už jenom dodat, že $b(f'_j, f'_j) \neq 0$, na čemž jsme se už dohodli.

(ii) Teď si zostává ještě uvědomit, že normovací proces v pátém kroku Gramm-Schmidtově ortogonalizace nám vektory nanormoval. Z vlastností normy platí

$$\|f_i\| = \left\| \frac{f'_i}{\|f'_i\|} \right\| = \frac{\|f'_i\|}{\|f'_i\|} = 1$$

Takže celkem můžeme psát:

$$b(f_i, f_j) = \delta_{ij},\ i, j = 1, \ldots, r \quad \Rightarrow \quad \{f_i\}_{i=1}^{r} \text{ je ON systém}$$

b) Chceme dokázat, že náš systém je báze prostoru $\mathcal{L}(\{v_1 \ldots v_r\})$, tedy, že je lineárně nezávislý a prostor generuje. Lineární nezávislost plyne triviálně z právě dokázané ortogonality. Dokažme tedy, že prostor doopravdu generuje:

(i) $\mathcal{L}(\{f_1 \ldots f_r\}) \subseteq \mathcal{L}(\{v_1 \ldots v_r\})$ plyne triviálně, protože $f_i \in \mathcal{L}(\{v_1 \ldots v_r\})$.

(ii) Jelikož vektory sou lineárně nezávislé, tak platí $\dim \mathcal{L}(\{f_1 \ldots f_r\}) = r$, což je ale také rovno dimenzi $\dim \mathcal{L}(\{v_1 \ldots v_r\})$. Tedy s ohledem na (i) zřejmě platí $\mathcal{L}(\{f_1 \ldots f_r\}) = \mathcal{L}(\{v_1 \ldots v_r\})$.

Tedy jsme celkem dokázali, že $\{f_i\}_{i=1}^{r}$ tvorí ortonormální bázi prostoru $\mathcal{L}(\{v_1 \ldots v_r\})$.

10. přednáška z lineární algebry

4. prosince 2007

Definice 3.22. Nechť V je v.p. a W', W'' jeho podprostory. Definujeme $W' + W'' := \{x \in V | \exists x' \in W', \exists x'' \in W'' : x = x' + x''\}$ a vzniklému vektorovému prostoru (proč jde vůbec o vektorový prostor?) budeme říkat **součet** v.p.p. W' a W''. Pokud navíc $W' \cap W'' = \{0\}$, tak píšeme $W' \oplus W''$ a říkáme tomu **direktní součet**.

Lemma 3.27. Nechť $V := W \oplus W'$. Potom všechny $v \in V$ se dají zapsat jako $v = w + w'$, kde $w \in W$ a $w' \in W'$ právě jedným způsobem.

Důkaz. Z definice určitě existuje minimálně jeden rozklad v. Když $v = w + w' = u + u'$, potom platí $w - u = u' - w'$, přičemž ale $w - u \in W$ a $u' - w' \in W'$, tedy $w - u = u' - w' = 0 \Rightarrow w = u \;\&\; w' = u'$. $\square$

Příklad 3.12.

1) $V := \mathbb{R}^3$, $W' := \{(x, 0, 0) | x \in \mathbb{R}\}$, $W'' := \{(0, y, 0) | y \in \mathbb{R}\}$, tj. W' a W'' jsou osy x a y, takže mají společnou jen nulu. Jejich direktním součtem je překvapivě rovina xy - $W' \oplus W'' = \{(x, y, 0) | x, y \in \mathbb{R}\}$.

2) $V := \mathbb{R}^3$, $W' := \{(x, 0, 0) | x \in \mathbb{R}\}$, $W'' := \{(a, b, 0) | a, b \in \mathbb{R}\}$, tj. osa x a rovina xy. Jejich součtem, který není direktní, vznikne $W' + W'' = \{(a + x, b, 0) | a, b, x \in \mathbb{R}\} = W''$.

Poznámka 3.25. Součet dvou podprostorů je stejný, jako lineární obal jejich sjednocení, tj. $W' + W'' = \mathcal{L}(W' \cup W'')$, neboť:

i) $x \in W' + W'' \Rightarrow x = x' + x''; x' \in W', x'' \in W'' \Rightarrow x = x' + x'' \in \mathcal{L}(W' \cup W'')$

ii) Stejně tak $x \in \mathcal{L}(W' \cup W'')$ jde zapsat jako

$$x = \sum_{i=1}^{k} c_i x'_i + \sum_{j=1}^{l} d_j x''_j,\ x'_i \in W', x''_j \in W'' \Rightarrow$$

$$\sum_{i=1}^{k} c_i x'^i =: x' \in W' \;\&\; \sum_{j=1}^{l} d_j x''^j =: x'' \in W''$$

Věta 3.28. 3Nechť (V, b) je v.p. se skalárním součinem a má konečnou dimenzi (v nekonečných dimenzích tato věta obecně neplatí), dále W je v.p.p. V. Pak platí:

1) $W \oplus W^\perp = V$

2) $(W^\perp)^\perp = W$

3) $V^\perp = \{0\}, \{0\}^\perp = V$

Důkaz.

1) i) Dokážeme direktnost součtu, tj. $W \cap W^\perp = \{0\}$. Předpokládejme, že $x \in W$ a zároveň $x \in W^\perp$. Protože x je z $W^\perp$, platí $\forall y \in W : b(x, y) = 0$, speciálně pro případ, že $y = x$. A z definice skalárního součinu $b(x, x) = 0 \Rightarrow x = 0$.

   ii) Z definic platí $W \oplus W^\perp \subseteq V$.

iii) Dokážeme, že $V \subseteq W \oplus W^\perp$.
Zvolíme bázi $\{w_1, \ldots, w_r\}$ podprostoru W a užijeme na ni Gramm-Schmidtovu ortogonalizaci, čímž dostaneme $\{f_1, \ldots, f_r\}$, ON bázi W. Nech tedy $x \in V$ a definujeme x' jako

$$x' := \sum_{i=1}^{r} b(x, f_i) f_i, \text{ zřejmě } x' \in W$$

Teď se přesvědčíme, že $x'' := x - x'$ patří do $W^\perp$. Musí tedy platit, že $\forall y \in W : b(x'', y) = 0$. Když $y \in W$, tak ho můžeme zapsat jako

$$y = \sum_{i=1}^{r} c^i f_i, \; c^i \in \mathbb{R}$$

Pak

$$b(x'', y) = b(x - \sum_{j=1}^{r} b(x, f_j) f_j, \sum_{i=1}^{r} c^i f_i)$$

Povytýkáme sumy a dostaneme:

$$b(x'', y) = \sum_{i=1}^{r} c_i b(x, f_i) - \sum_{j=1}^{r} \sum_{i=1}^{r} b(x, f_j) c^i b(f_j, f_i).$$

Jak už víme, $b(f_j, f_i)$ je δ_{ij}, čímž se vyruší jedna suma

$$b(x'', y) = \sum_{i=1}^{r} c^i b(x, f_i) - \sum_{i=1}^{r} c^i b(x, f_i) = 0,$$

takže opravdu každé $x \in V$ jde zapsat jako $x' + x''$ tak, že $x' \in W, x'' \in W^\perp$.

2) i) Dokážeme, že $W \subseteq (W^\perp)^\perp$. Když $w \in W$ a $w' \in W^\perp$, tak z definice $W^\perp$ plyne $b(w, w') = 0$, neboť $w' \in W^\perp$ musí být kolmé na všechny vektory z W. Jenomže to potom znamená, že když $w \in W$, tak je také kolmý na všechny vektory z $W^\perp$, což ale dáva $w \in (W^\perp)^\perp$.

ii) Dokážeme opačnou inkluzi, tj. $(W^\perp)^\perp \subseteq W$. Už víme, že $W \oplus W^\perp = V$ a rovněž $W^\perp \oplus (W^\perp)^\perp = V$. Obecně platí $\dim W \oplus W' = \dim W + \dim W'$ (důkaz bude za chvilku), takže $\dim W + \dim W^\perp = \dim V = \dim W^\perp + \dim(W^\perp)^\perp \Rightarrow \dim W = \dim(W^\perp)^\perp$. A jelikož mají W a $(W^\perp)^\perp$ stejnou dimenzi a navíc W je podmnožinou $(W^\perp)^\perp$, tak musí být nutně stejné, tj, $W = (W^\perp)^\perp$.

3) I) $\{0\}^\perp = V$, neboť
   i) $V \supseteq \{0\}^\perp$
   ii) $V \subseteq \{0\}^\perp$, neboť $\forall v \in V : b(v, 0) = 0$.

   II) $V^\perp = \{0\}$, protože víme, že $\{0\}^\perp = V \Rightarrow (\{0\}^\perp)^\perp = V^\perp = \{0\}$. □

Při posledním důkazu jsme použili už dokázanou druhou část věty, no možná jste postřehli, že v oném důkazu bylo užíto předpokladu koněčné dimenze, ale to, že $V^\perp = \{0\}$ platí i pro dimenze nekonečné, takže pro úplnosť uvádíme i jiný důkaz: $v \in V^\perp \Rightarrow v \in V \,\&\, \forall w \in V : b(v, w) = 0 \Rightarrow b(v, v) = 0 \Rightarrow v = 0$.

Poznámka 3.26.

1) V nekonečných dimenzích obecně Věta 3.28 neplatí, ale platí $(W^\perp)^\perp = \overline{W}$, přičemž $\overline{W} \supseteq W$ je **uzávěr** W.

Koho by to zajímalo, tak uzávěr množiny je nejmenší uzavřená množina topologického prostoru, která danou množinu obsahuje. Co to znamená si můžete dohledat třeba na Wikipedii, nás to čeká až za dlouho.

2) Teď přichází slibovaný důkaz, že $\dim W' \oplus W'' = \dim W' + \dim W''$. Zvolíme $\{c_i\}_{i=1}^k$ a $\{d_j\}_{j=1}^l$ jako báze W' a W'' a tvrdíme, že jejich zjednotení je bází $W' \oplus W''$.

   i) $\{c_i\}_{i=1}^k \cup \{d_j\}_{j=1}^l$ je l.n., neboť kdyby jejich l.k. byla nulová, tak

$$\sum_{i=1}^{k} \gamma^i c_i + \sum_{j=1}^{l} \delta^j d_j = 0 \Rightarrow \sum_{i=1}^{k} \gamma^i c_i = -\sum_{j=1}^{l} \delta^j d_j$$

   Jelikož ale $W \cap W' = \{0\}$, tak $\sum_{i=1}^k \gamma^i c_i = -\sum_{j=1}^l \delta^j d_j = 0 \Rightarrow \gamma^i = \delta^j = 0,\ \forall i, j$. Tedy $\{c_i\}_{i=1}^k, \{d_j\}_{j=1}^l$ jsou opravdu l.n.

   ii) Teď stačí dokázat, že $\{c_i\}_{i=1}^k \cup \{d_j\}_{j=1}^l$ generuje $W' \oplus W''$. Když $x \in W' \oplus W''$, tak určitě $x = x' + x''$; $x' \in W', x'' \in W''$.

$$\left.\begin{array}{r} \{c_i\}_{i=1}^k \text{ generuje } W' \Rightarrow x' = \sum_{i=1}^{k} \gamma^i c_i \\ \{d_j\}_{j=1}^l \text{ generuje } W'' \Rightarrow x'' = \sum_{j=1}^{l} \delta^j d_j \end{array}\right\} x = x' + x'' = \sum_{i=1}^{k} \gamma^i c_i + \sum_{j=1}^{l} \delta^j d_j,$$

   takže $\{c_i\}_{i=1}^k \cup \{d_j\}_{j=1}^l$ opravdu generuje $W' \oplus W''$.

Definice 3.23. Mějme matici $A \in M(m, n; \mathbb{R})$. Pak definujeme matici $A^T \in M(n, m; \mathbb{R})$, pro kterou platí, že $(A^T)^i{}_j = A_j{}^i$, $\forall i, j$ a budeme ji říkat transponovaná matice A.

Věta 3.29. Nechť $A \in M(m, n; \mathbb{R})$. Pak $\operatorname{rank}(A) = \operatorname{rank}(A^T)$.

Důkaz. Zavedeme zobrazení $f : \mathbb{R}^n \to \mathbb{R}^m; f(x) := Ax$, a $f^T : \mathbb{R}^m \to \mathbb{R}^n; f^T(x) := A^T x$, a budeme zkoumat $\operatorname{Ker} f$.

$$f(x) = \begin{pmatrix} a_1^1 & \dots & a_n^1 \\ \vdots & \ddots & \vdots \\ a_1^m & \dots & a_n^m \end{pmatrix} \begin{pmatrix} x^1 \\ \vdots \\ x^n \end{pmatrix} = \begin{pmatrix} a_1^1 x^1 + & \dots & +a_n^1 x^n \\ & \vdots & \\ a_1^m x^1 + & \dots & +a_n^m x^n \end{pmatrix} = \begin{pmatrix} (a^1, x) \\ \vdots \\ (a^m, x) \end{pmatrix}$$

Kde a^i je i-tý řádek A a $(\cdot, \cdot)$ obvyklý skalárny součin v $\mathbb{R}^n$. Takže $x \in \operatorname{Ker} f$ právě tehdy, když $(a^i, x) = 0, \forall i = 1, \dots, m$, neboli $x \in \{a^1, \dots, a^m\}^\perp$.

Nyní se podíváme na $\operatorname{Im} f^T$ a pokusíme se dokázat, že $\operatorname{Im} f^T = \mathcal{L}(\{a^1, \dots, a^m\})$.

$$f^T(x) = \begin{pmatrix} | & & | \\ a^1 & \dots & a^m \\ | & & | \end{pmatrix} \begin{pmatrix} x^1 \\ \vdots \\ x^m \end{pmatrix}$$

1) Nejspíš inkluze $\operatorname{Im} f^T \subseteq \mathcal{L}(\{a^1, \dots, a^m\})$. Nech tedy $y \in \operatorname{Im} f^T$. Potom určitě $\exists x \in \mathbb{R}^m$: $y = f^T(x)$. Zapíšme tenhle vektor do kanonické báze $\{e^i\}_{i=1}^m$, tedy $x = \sum_{i=1}^{m} \alpha_i e^i$. Pak $y = f^T(x) = f^T\Big(\sum_{i=1}^{m} \alpha_i e^i\Big) = \sum_{i=1}^{m} \alpha_i f^T(e^i)$. Vektor $f^T(e^i)$ je zřejmě a^i, takže jsme zapsali y jako l.k. a^i a inkluze je dokázána.

2) Opačná inkluze $\mathcal{L}(\{a^1, \dots, a^m\}) \subseteq \operatorname{Im} f^T$ se dokazuje naprosto stejně, ale z opačné strany, takže v rychlosti:

$$\sum_{i=1}^{m} \alpha_i a^i = \sum_{i=1}^{m} \alpha_i f^T(e^i) = f^T\Big(\sum_{i=1}^{m} \alpha_i e^i\Big) = f^T(x)$$

Takže celkem nám z výzkumu $\operatorname{Im} f^T$ a $\operatorname{Ker} f$ vyplývá, že $x \in \operatorname{Ker} f$ právě tehdy, když $x \in \{a^1, \ldots, a^m\}^\perp = (\mathcal{L}(\{a^1, \ldots, a^m\}))^\perp = (\operatorname{Im} f)^\perp$. Tudíž $\operatorname{Ker} f = (\operatorname{Im} f^T)^\perp$.

Podle Věty 2.17 v našem případě platí $\dim \operatorname{Ker} f + \dim \operatorname{Im} f = n$ a podle Věty 3.28 rovněž $\dim \operatorname{Im} f^T + \dim(\operatorname{Im} f^T)^\perp = n$. Z toho jednoduše zjistíme, že $\operatorname{rank}(A) = \dim \operatorname{Im} f = n - \dim \operatorname{Ker} f = n - (\operatorname{Im} f^T)^\perp = \dim \operatorname{Im} f^T = \operatorname{rank}(A^T)$, čímž slavnostně dospíváme k výsledku, že $\operatorname{rank}(A) = \operatorname{rank}(A^T)$. □

Poznámka 3.27. Při Gaussově eliminaci jsme (až do teď neopodstatněně) možná prováděli řádkové úpravy, i když jsme měli provádět sloupcové. Tato věta nám to konečně ospravedlnila, takže jsme všechno dělali správně a můžeme klidně spát.

4. Řešení soustav rovnic.

Věta 4.30. (Frobenius) Mějme matici $A \in M(m, n; \mathbb{R})$. Pak rovnice $Ax = b$, $b \in \mathbb{R}^m$ má alespoň jedno řešení právě tehdy, když $\operatorname{rank}(A) = \operatorname{rank}(A|b)$.

V týchto textech jsme zvlášť definovali rank matice a rank lineárního zobrazení - rankem matice myslíme dimenzi lineárního obalu jej sloupců, rankem zobrazení dimenzi jeho image-u. Když uvažujeme lineární zobrazení $\mathcal{A} : \mathbb{R}^n \to \mathbb{R}^m$ s predpisem $x \mapsto Ax$, kde A je matice, tak jako jsme si už nekolikrát uvedomili: $\operatorname{rank}(\mathcal{A}) = \operatorname{rank}(A)$ *(platí možná méně triviálně i pro obecné lineární zobrazení a jeho matici vůči nejakým bázím). Tedy rankem matice rozšírené myslíme* $\operatorname{rank}(A|b) = \mathcal{L}(\{a^1, \ldots, a^n, b\})$*, kde a^i sou sloupce matice A.*

Důkaz.

1) Budeme předpokládat, že $Ax = b$ má alespoň jedno řešení $\tilde{x} = (x^1, \ldots, x^n)$, což zapíšeme

$$A\tilde{x} = b \Rightarrow b = \begin{pmatrix} | \\ a^1 \\ | \end{pmatrix} x^1 + \cdots + \begin{pmatrix} | \\ a^n \\ | \end{pmatrix} x^n,$$

takže vidíme, že b je l.k. $\{a^1, \ldots, a^n\}$ a tudíž $b \in \mathcal{L}(\{a^1, \ldots, a^n\})$. Z toho je zřejmé, že $\dim \mathcal{L}(\{a^1, \ldots, a^n\}) = \dim \mathcal{L}(\{a^1, \ldots, a^n, b\}) \Rightarrow \operatorname{rank}(A) = \operatorname{rank}(A|b)$.

2) Dokážeme obrácenou implikaci, přičemž budeme postupovat obráceně, než v předchozím případě. Předpokládáme, že $\operatorname{rank}(A) = \operatorname{rank}(A|b) \Rightarrow \dim \mathcal{L}(\{a^1, \ldots, a^n\}) = \dim \mathcal{L}(\{a^1, \ldots, a^n, b\})$, z čehož plyne, že b je l.k. $\{a^1, \ldots, a^n\}$

$$b = \sum_{i=1}^{n} x_i a^i,$$

tedy $\tilde{x} = (x_1, \ldots, x_n)$ je zřejmě řešením $Ax = b$. □

Poznámka 4.28. Při řešení rovnice $Ax = b$ postupujeme takto:

1) Nalezneme **partikularní** řešení, tj. alespoň jedno řešení

$$Ax_p = b.$$

2) Pokusíme se vyřešit homogenní rovnici $Ax_h = 0$ a dostaneme obecné **homogenní** řešení. Nejlépe je najít bázi celého $\operatorname{Ker} A$, jelikož je to vektorový prostor a tým ho plně určíme.

3) A obecné řešení je součtem partikularního a homogenního, tedy

$$\{x | Ax = b\} = \{x_p + x_h | x_h \in \operatorname{Ker} A\}$$

protože jedním směrem je to zřejmé a když $Ax = b$, potom $A(x - x_p) = 0$, tedy

$$x - x_p \in \operatorname{Ker} A \Rightarrow \exists x_h \in \operatorname{Ker} A : x = x_p + x_h.$$

11. prednáška z lineárnej algebry

11. december 2007

5. Determinanty

Poznámka 5.29. S determinantami ste sa možno už na cvičení stretli - pomocou determinantov je možné počítať orientované objemy n-rozmerných rovnobežnostenov (určených n-vektormi)[4] v n-rozmernom priestore a tým napríklad (heuristicky) určiť lineárnu (ne)závislosť vektorov.

5.1. Permutácie

Predmetom dôležitosti súvisiacim s determinantami sú permutácie a grupa permutácií. Pomocou nich determinant definujeme a následne sa permutácie dostanú do mnohých viet (a dôkazov) o determinantoch. Preto naslednujúce slová si môžte zobrať k srdcu :-).

Definícia 5.24. Nech $n \in \mathbb{N}$. Každú bijekciu (zobrazenie prosté & na)

$$\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$$

nazveme **permutáciou**. Množinu všetkých týchto permutácií značíme $\mathfrak{S}_n$.

Poznámka 5.30. Na určenie permutácie ako zobrazenia môžme použiť výpis jej prvkov, tj. nasledujúca tabulka čísel, kde v hornom riadku píšeme prvky z definičného oboru a pod daným prvkom i sa v druhom riadku nachádza $\sigma(i)$

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Príklad 5.13. Uveďme jednoduché príklady, teda ukážme si, ako vyzerá množina všetkých permutácií množiny o $n = 1$, 2 a 3 prvkoch. Ak $n = 1$, tak v množine sa objaví iba identická permutácia

$$\sigma_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

V prípade $n = 2$ sú to

$$\sigma_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

V prípade $n = 3$ dostávame 6 prvkov

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Poznámka 5.31.

1) Pre počet prvkov množiny všetkých permutácií n-prvkovej množiny platí to, čo ak nie kôli ničomu inému, tak už len kôli názvu môžme čakať, a to $\#\mathfrak{S}_n = n!$

[4] Užitím determinantov sa dá počítať i objem k-rovnobežnostenu v n-rozmernom ($n > k$) priestore, a to tak, že si rovnobežnosten orotogonálne sprojektujeme do všetkých k-rozmerných rovín „natiahnutých“ nad k-prvkovou množinou kanonických vektorov, spočítame objemy týchto (je ich $\binom{n}{k}$) k-rovnobežnostenov teraz už v k-rozmernom priestore (rovine) pomocou determinantu a nakoniec užijeme „Pythagorovu“ vetu.

2) Ak $\sigma(i) = i$, tak v zápise pomocou $\sigma = \left(\cdots\right)$ môžme pre zjednodušenie vynechať stĺpec $\left(\begin{smallmatrix} i \\ i \end{smallmatrix}\right)$ a zápisom $\sigma = \left(\begin{smallmatrix} 1 & 3 \\ 3 & 1 \end{smallmatrix}\right)$ automaticky rozumieme $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right)$.

3) $\sigma \in \mathfrak{S}_n$ je možné skladať pomocou skladania zobrazení $\circ$, čiže máme prirodzene zavednú binárnu operáciu, ktorá priradí dvom prvkom $\sigma, \tau \in \mathfrak{S}_n$ znova prvok $\sigma \circ \tau \in \mathfrak{S}_n$ (keďže zložením dvoch permutácií, je znova permutácia - bijektívne zobrazenie). Označme ešte $e = \mathrm{id}$ (identické zobrazenie) a nakoniec inverzné zobrazenie k permutácii σ ako σ^{-1} (ktoré existuje pre všetky permutácie), pričom zrejme $\sigma^{-1} = \left(\begin{smallmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{smallmatrix}\right)$. Tieto označenia a poznámky niečo predznamenávajú a to niečo je formulované v nasledujúcej vete.

Veta 5.31. Sústava $\tilde{\mathfrak{S}}_n = (\mathfrak{S}_n, \circ, ^{-1}, e)$ tvorí grupu (pozrite si prípadne znova definíciu grupy).

Dôkaz.

a) Ako sme už povedali, operácia skladania je $\circ : \mathfrak{S}_n \times \mathfrak{S}_n \to \mathfrak{S}_n$ a ostáva nám overiť asosiacívnosť (výrazom typu $\sigma \circ \tau(i)$ implicitne myslíme $(\sigma \circ \tau)(i)$):

$$\sigma \circ (\tau \circ \rho)(i) = \sigma(\tau \circ \rho(i)) = \sigma(\tau(\rho(i)))$$
$$(\sigma \circ \tau) \circ \rho(i) = \sigma \circ \tau(\rho(i)) = \sigma(\tau(\rho(i)))$$

čo platí pre $i = 1, \ldots, n$, takže skutočne $\sigma \circ (\tau \circ \rho) = (\sigma \circ \tau) \circ \rho$.

b) Zrejme e je skutočne jednotkový prvok grupy v zmysle, že $\sigma \circ e = e \circ \sigma = \sigma$. Naozaj

$$\sigma \circ e(i) = \sigma(e(i)) = \sigma(i)$$
$$e \circ \sigma(i) = e(\sigma(i)) = \sigma(i)$$

c) Operácia inverze $^{-1} : \sigma \mapsto \sigma^{-1}$ skutočne nájde inverzný prvok k prvku $\sigma \in \mathfrak{S}_n$

$$\sigma^{-1} \circ \sigma(i) = \sigma^{-1}(\sigma(i)) = i$$
$$\sigma \circ \sigma^{-1}(\sigma(i)) = \sigma(\sigma^{-1}(\sigma(i))) = \sigma(i)$$

($\sigma(i)$ pre $i = 1, \ldots, n$ prebieha celú množinu). Teda $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{id} = e$. □

Týmto sme teda (snáď úplne presvedčivo) ukázali, že $\{\mathfrak{S}_n, \circ, e, ^{-1}\}$ je grupa, ktorú nazývame **permutačná grupa** (prípadne **symetrická grupa**[5]). V skutočnosti práve symetrická grupa je tou najprirodzenejšou grupou; napríklad každá grupa je izomorfná nejakej podgrupe nejakej symetrickej grupy $\mathcal{S}(X)$. Práve štúdium morfizmov grupy do nejakej podgrupy symetrickej grupy nám vie o grupe mnohé (alebo aspoň niečo) povedať - čo sa presvedčíme zachvíľu sami, akonáhle si definujeme znamienko permutácie.

Poznámka 5.32.

1) Zanedlho sa nám zíde fakt, a síce, že $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$ (kde koliečko pri zápise pre pohodlnosť vynechávame).

2) Predchádzajúci fakt platí i vo všeobecnej grupe. Už sme to používali pre matice, ktoré majú inverziu: $(AB)^{-1} = B^{-1}A^{-1}$. Toto lemma môžme dokázať tak, že overíme, že $\tau^{-1}\sigma^{-1}$ je lavá inverzia k $\sigma\tau$ (a to využitím iba vlastností grupy). Teda skutočne

$$(\tau^{-1}\sigma^{-1})(\sigma\tau) = \tau^{-1}(\sigma^{-1}\sigma)\tau = \tau^{-1}e\tau = e$$

Keďže lavá inverzia je v grupe len jedna a $(\sigma\tau)^{-1}$ je lavá (mimochodom i pravá) inverzia (ako sme ukázali), tak skutočne dostávame $\tau^{-1}\sigma^{-1} = (\sigma\tau)^{-1}$.

[5] V prípade pojmu symetrickej grupy sa už nemusíme obmedzovať na konkrétny tvar a konečnosť množiny z a do ktorej sú jednotlivé prvký grupy zobrazením. Takže ak X je ľubovolná neprázdna množina a $S(X)$ množina všetkých bijekcií na X, symetrickou grupou nazývame grupu $\mathcal{S}(X) = (S(X), \circ, \mathrm{id}_X, ^{-1})$.

*Definícia 5.25. [6] Permutáciu $\sigma \in \mathfrak{S}_n$ nazveme **cyklus**, ak

$$\sigma = \begin{pmatrix} i_1 & i_2 & \cdots & i_m & j_1 & \cdots & j_k \\ i_2 & i_3 & \cdots & i_1 & j_1 & \cdots & j_k \end{pmatrix}$$

pre vhodné $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\}$ a $\{j_1, \ldots, j_k\} \subseteq \{1, \ldots, n\}$ pričom $\{i_1, \ldots, i_m\} \cap \{j_1, \ldots, j_k\} = \emptyset$ a $m + k = n$.

*Poznámka 5.33.

1) Môžme si zaviesť ešte jednoduchšie (ale stále jednoznačne určujúce) značenie permutácií pomocou cyklov (viď nasledujúcu vetu o tom, že každá permutácia sa dá vyjadriť ako zloženie disjunktných cyklov). Cykly môžme namiesto

$$\begin{pmatrix} i_1 & i_2 & \cdots & i_m & j_1 & \cdots & j_k \\ i_2 & i_3 & \cdots & i_1 & j_1 & \cdots & j_k \end{pmatrix} \quad \text{písať ako} \quad (i_1\, i_2 \cdots i_m)$$

Čiže napríklad

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} = (1\,3\,2) \circ (4\,5) = (1\,3\,2)(4\,5)$$

a to je vlastne to isté ako napríklad $(3\,2\,1)(4\,5)$.

2) Taktiež môžme predchádzajúce znázorniť graficky. Napríklad cyklus $(1\,3\,2)$ znározníme tak, že na obvod kružnice pravidelne rozmiestnime prvky (čísla) 1, 3 a 2 tak, aby boli v tomto poradí idúc v smere hodinových ručičiek a prípadne dokreslíme šípky od 1 k 2 atď. Permutáciu $(1\,3\,2)(4\,5)$ potom znázorníme ako zloženie dvoch „kružníc“.

*Príklad 5.14. Cykly vieme spájať a rozpájať; majme permutáciu zloženú z dvoch disjunktných cyklov a skúsme cykly spojiť a následne rozpojiť. Overte, že:

$$(1\,4) \circ (1\,2\,3)(4\,5) = (1\,2\,3\,4\,5), \quad (1\,4) \circ (1\,2\,3\,4\,5) = (1\,2\,3)(4\,5)$$

*Tvrdenie 5.32. Každú permutáciu $\sigma \in \mathfrak{S}_n$ je možné napísať ako zloženie disjunktných cyklov. Pod disjunktnými cyklami myslíme cykly také, že pre každé dva cykly $(i_1, \ldots, i_k)$ a $(j_1, \ldots, j_m)$ platí, že $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_m\} = \emptyset$.

Dôkaz.

a) Nájdime v obecnej permutácii $\sigma \in \mathfrak{S}_n$ nejaký cyklus. Zoberme si ľubovolný prvok $p \in \{1, \ldots, n\}$ a uvažujme nekonečnú postupnosť prvkov

$$\sigma^0(p),\ \sigma^1(p),\ \sigma^2(p),\ \sigma^3(p),\ \ldots \qquad \text{kde} \qquad \sigma^k = \underbrace{\sigma \circ \sigma \circ \cdots \circ \sigma}_{k}, \quad \sigma^0 = e$$

Keďže $\sigma^k(p) \in \{1, \ldots, n\}$, pre $\forall k \in \mathbb{N}_0$, určite sa po chvíli prvky budú musieť začať opakovať, tj. existuje (i, j) tak, že $\sigma^i(p) = \sigma^j(p)$ a samozrejme $i \neq j$ a volme dvojicu tak, že $i < j$. Zoberme si takú dvojicu (i, j), že j je najmenšie (a i je ľubovolné, ale menšie ako j). Tvrdíme, že nutne $i = 0$ (a teda $\sigma^j(p) = p$). Pre spor nech $i > 0$. Keďže $(\sigma^i)^{-1}(\sigma^i(p)) = p$, tak dostáveme

$$\sigma^{j-i}(p) = ((\sigma^i)^{-1} \circ \sigma^j)(p) = (\sigma^i)^{-1}(\sigma^j(p)) = (\sigma^i)^{-1}(\sigma^i(p)) = p$$

[6] Ak uvidíte niekde túto hviezdičku, tak nesledujúca časť na prednáške nebola a nie je preto nutné to všetko vedieť. Ale napriek tomu (snáď) nič v texte nie je zbytočné - práve ohviezdičkované časti vám môžu pomôcť text lepšie pochopiť či sa napríklad dozvedieť i niečo naviac. Taktiež text napísaný malou italikou je len pre záujemcov.

kde prvé rovnítko je vďaka rovnosti medzi funkciami a predposledné vďaka $\sigma^j(p) = \sigma^i(p)$. Takže máme, že $\sigma^{j-i}(p) = p = \sigma^0(p)$, takže dvojica $(0, j-i)$ je dvojica s menším $j-i < j$, čo je spor. Položme $r := j$. Takže postupnosť

$$p,\ \sigma(p),\ \sigma^2(p),\ \ldots\ ,\sigma^{r-1}(p)$$

je postupnosť, v ktorej sa žiadne dve čísla neopakujú a ak by sme pokračovali, tak dostávame

$$\sigma^r(p) = p,\ \sigma^{r+1}(p) = \sigma(\sigma^r(p)) = \sigma(p),\ \ldots\ ,\sigma^{2r-1}(p) = \sigma^{r-1}(p),\ \ldots$$

postupnosť stále sa opakujúcich r čísel.

b) Volme $q \in \{1,\ldots,n\}\backslash\{p,\sigma(p),\ldots,\sigma^{r-1}(p)\}$. Ak by to bola množina prázdna, tak sme skončili a permutáciu ako jeden cyklus vyjadrili. Nech teda q zvolíme. Úplne rovnakým postupom ako v bode a) nájdeme r' tak, že v postupnosti

$$q,\ \sigma(q),\ \sigma^2(q),\ \ldots\ ,\sigma^{r'-1}(q)$$

sa žiadne dva prvky neopakujú a $\sigma^{r'-1}(q) = q$.

c) Takto postupujeme, až kým nedostaneme prázdnu množinu (čo sa môže stať maximálne po n opakovaniach)

d) Ostáva ukázať, že sme našli naozaj disjunktné postupnosti a že môžme konečne písať

$$\sigma = (p,\ \sigma(p),\ \sigma^2(p),\ \ldots\ ,\sigma^{r-1}(p))(q,\ \sigma(q),\ \sigma^2(q),\ \ldots\ ,\sigma^{r'-1}(q))\ldots$$

Overme pre prvé dva cykly (rovnaká argumentácia sa použije pre hociktoré dva). Pre spor predpokladajme nedisjunktnosť, teda že existuje také l, m, že $\sigma^l(p) = \sigma^m(q)$ a $0 \le l \le r-1$ a $0 \le m \le r'-1$. Ak $l \ge m$, tak znova $\sigma^{l-m}(p) = q$ a teda máme, že $q \in \{p,\sigma(p),\ldots,\sigma^{r-1}(p)\}$, čo je spor s výberom q. Podobne ak $l < m$, tak tiež $\sigma^{l-m}(p) = q$, pričom ak formálne umocňujeme na záporné číslo, znamená to príslušný počet inverzií σ^{-1}. Určite existuje $n \in \mathbb{N}$ také, že $0 \le l - m + nr \le r-1$. Ak počítame $\sigma^{l-m+nr}(p) = \sigma^{l-m}(\sigma^{nr}(p)) = \sigma^{l-m}(p) = q$, tak znova máme $q \in \{p,\sigma(p),\ldots,\sigma^{r-1}(p)\}$, čo je spor. □

Definícia 5.26. $\sigma \in \mathfrak{S}_n$ nezveme **transpozíciou**, ak existujú $i, j \in \{1,\ldots n,\}$ a $i \ne j$ tak, že $\sigma(i) = j$ a $\sigma(j) = i$ a pre $\forall k \in \{1,\ldots,n\} : k \ne i\ \&\ k \ne j$ platí $\sigma(k) = k$. To znamená, že transpozícia „vymení“ dva prvky a ostatné nehá napokoji. Inak povedané, σ je transpozícia, ak je cyklom typu (i,j) (teda cyklom dĺžky 2).

Poznámka 5.34. Triviálnu permutáciu e považujme (v zmysle nasledujúcich tvrdení) za zloženie nula transpozícií. Tiež si uvedomme, že inverzná permutácia k transpozícii (i,j) je zas ona sama.

Tvrdenie 5.33. Každú permutáciu $\sigma \in \mathfrak{S}_n$ je možné zložiť z transpozícií.

Dôkaz. Dôkaz prevedieme indukciou. Pre $n = 1$ a $n = 2$ je tvrdenie triviálne (jednotková transpozícia v oboch prípadoch je zložením nula transpozícií). Predpokladajme teda, že tvrdenie pre prípad $\sigma \in \mathfrak{S}_{n-1}$ platí. Vezmime teda $\sigma \in \mathfrak{S}_n$. Buď

a) $\sigma(n) := j_n = n$. Potom definujeme permutáciu $\sigma' \in \mathfrak{S}_{n-1}$, pričom $\sigma'(i) = \sigma(i)$ pre $i = 1,\ldots,n-1$, a je ju možné zapísať ako zloženie l transpozícií τ'_k ako $\sigma' = \tau'_1\tau'_2\ldots\tau'_l$. Ak definujeme τ_k pre $k = 1,\ldots,l$ ako $\tau_k(i) = \tau'_k(i)$ pre $i = 1,\ldots,n-1$ a $\tau_k(n) = n$, tak celkom triviálne dostaneme, že $\sigma = \tau_1\ldots\tau_l$.

b) alebo $\sigma(n) := j_n \ne n$. Potom definujeme permutáciu $\hat{\sigma} = (j_n, n)\sigma$, pre ktorú už platí $\hat{\sigma}(n) = n$ a v zmysle predchádzajúceho bodu ju vieme zapísať ako zloženie transpozící, čiže i $\sigma = (j_n,n)^{-1}\hat{\sigma} = (j_n,n)\hat{\sigma}$ je zložením transpozící. □

**Prichádzame k sľubovanej časti o znamienku permutácie. Motivácia zavedenia môže byť nasledujúca: Bolo by príjemné nájsť grupový morfizmus ϕ (skôr epimorfizmus) z grupy $\tilde{\mathfrak{S}}_{nn}$ do dvojprvkovej grupy (tá existuje len jedna a vyzerá napríklad ako $(\{1,-1\},\cdot,1,^{-1})$ alebo ako $\tilde{\mathfrak{S}}_2$). Takto by sme mohli permutácie rozdeliť do dvoch skupín - tie ktoré sa zobraznia na 1 a tie ktoré na -1. Automaticky dostávame $\phi(\sigma\tau)=\phi(\sigma)\phi(\tau)$ a ďalšie príjemné veci ako podgrupu[7] permutácií, ktoré sa zobraznia na 1, rovnaký počet prvkov v oboch skupinách,... Každopádne pre determinanty a podobné záležitosti je práve zmanienko permutácie veľmi podstatné.*

Poďme teda v zmysle motivácie nájsť spomínaný morfizmus grúp.

Definícia 5.27. Majme množinu $\mathfrak{S}_n$ všetkých permutácií $\sigma:\{1,\dots,n\}\to\{1,\dots,n\}$ a množinu všetkých (reálnych) polynómov n-premenných[8], označme ju $\mathbb{R}[x_1,\dots,x_n]$. Reálny polynóm n-premenných môžme chápať ako funkciu na vektorovom priestore R^n. Takže napríklad zápis $f(rx+y)$, kde $x,y\in\mathbb{R}^n$ a $r\in R$ má dobre definovaný zmysel. Ďalej každej permutácii $\sigma\in\mathfrak{S}_n$ priradíme zobrazenie $\mathbb{R}[x_1,\dots,x_n]\to\mathbb{R}[x_1,\dots,x_n]$, ktoré značíme $\sigma\cdot$, teda $\sigma\mapsto\sigma\cdot$, a jeho pôsobenie na polynóm f zapisujeme ako $f\mapsto\sigma\cdot f$ a definujeme ho tak, že

$$\sigma\cdot f=f\circ\varphi(g)$$

kde $\varphi:\mathfrak{S}_n\to GL(n)$, teda $\varphi(g)$ je invertovatelné[9] lineárne zobrazenie na vektorovom priestore R^n. Toto zobrazenie volíme tak, aby platilo $\varphi(\tau\sigma)=\varphi(\sigma)\circ\varphi(\tau)$ (všimnite si prehodenia). Existuje mnoho zobrazení, ktoré toto splňujú, ale my si vyberieme práve zobrazenie také, že pre maticu $[\varphi(\sigma)]$ lineárneho zobrazenia voči kanocikej bázi platí $[\varphi(\sigma)]_{ij}=\delta_{\sigma(i)j}$, čo môžme zapísať i ako $[\varphi(\sigma)]=P^{i\sigma(i)}$, čo je matica, ktorá má všade nuly okrem miest $(i,\sigma(i))$, $i=1,\dots,n$, kde sú jedničky. Ako ilustratívny príklad uvedieme:

$$\sigma=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\in\mathfrak{S}_3\ \Rightarrow\ [\varphi(\sigma)]=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}$$

Môžte ľahko overiť, že skutočne platí $\varphi(\tau\sigma)=\varphi(\sigma)\circ\varphi(\tau)$ (využite faktu, že súčin matíc dvoch zobrazení je matica zloženého zobrazenia a potom násobte matice alebo si uvedomte rovnosť $\sum_{j=1}^n\delta_{\sigma(i)j}\delta_{\tau(j)k}=\delta_{\tau(\sigma(i))k}$). Týmto sme teda definovali, čomu sa rovná $\sigma\cdot f$.

Ak sa vám celá táto konštrukcia zdá byť komplikovaná, tak vedzte, že nejde o nič inée ako o to, že polynóm f sa po zapoôsobení permutáciuou σ zobrazí na polynóm $\sigma\cdot f$, pre ktorý platí

$$\sigma\cdot f(x_1,\dots,x_n)=f\circ\varphi(\sigma)(x_1,\dots,x_n)=f(\varphi(\sigma)(x_1,\dots,x_n))=f(x_{\sigma(1)},\dots,x_{\sigma(n)})$$

takže sme toto pôsobenie mohli definovať jednoducho ako

$$\sigma\cdot f(x_1,\dots,x_n)=f(x_{\sigma(1)},\dots,x_{\sigma(n)})$$

Uveďme ešte príklad: nech $\sigma\in\mathfrak{S}_3$ a $\sigma=(1\,2\,3)$. Uvažujme teda nejaký polynóm troch premenných, napríklad $f(x,y,z)=z^2+xy+y$. Potom pre $\sigma\cdot f$ platí

$$\sigma\cdot f(x,y,z)=f(y,z,x)=x^2+yz+z$$

Lemma 5.34. Dôležitá vlastnosť tejto konštrukcie je

$$(\tau\sigma)\cdot f=\tau\cdot(\sigma\cdot f)$$

Dôkaz. Dôkaz je vďaka tomu, ako sme si zaviedli pôsebenie $\sigma\cdot$ vcelku jednoduchý. Počítajme teda

$$(\tau\sigma)\cdot f=f\circ(\varphi(\tau\sigma))=f\circ(\varphi(\sigma)\circ\varphi(\tau))=(f\circ\varphi(\sigma))\circ\varphi(\tau)=\tau\cdot(f\circ\varphi(\sigma))=\tau\cdot(\sigma\cdot f)$$

[7] A to dokonca normálnu ako pri jadre ľubovolného morfizmu.

[8] Tj, nejakú podmnožinu množiny všetkých funkcií $f:\mathbb{R}^n\to\mathbb{R}$

[9] To, že uvažujeme zobrazenie do množiny $GL(n)$ a nie do obecnej množiny všetkých lineárnych zobrazení môžte interpretovať tak, že na druhú spomínanú množinu nemáme takú peknú značku. No sú na to i iné, viac menej zbytočné dôvody.

Dôkaz by sa dal robiť aj podobne úpravou várazu $(\tau\sigma)\cdot f(x_1,\ldots,x_n) = f(x_{\tau(\sigma(1))},\ldots,x_{\tau(\sigma(n))})$, čo by mohlo byť komplikovanejšie. □

**Skonštruovali sme teda akciu grupy $\tilde{\mathfrak{S}}_n$ na množine $X = \mathbb{R}[x_1,\ldots,x_n]$, tj. morfizmus z grupy $\tilde{\mathfrak{S}}_n$ do symetrickej grupy $\mathcal{S}(X)$. Prečo symetrickej grupy? Zrejme zobrazenie $e\cdot$ je identita a každé zobrazenie typu $\sigma\cdot$ musí byť prosté - existuje k nemu inverzné zobrazenie $\sigma^{-1}\cdot$ v zmysle, že $\sigma^{-1}\cdot\sigma\cdot = (\sigma^{-1}\sigma)\cdot = e\cdot = \mathrm{id}$ a tiež je na - inak by nemohlo platiť $\sigma\cdot\sigma^{-1}\cdot = \mathrm{id}$, takže skutočne zobrazujeme do $S(X)$ a zobrazenie $\sigma\mapsto\sigma\cdot$, ako sme sme ukázali, je naviac morfizmus.*

Ak by sme našli polynóm Δ taký, že množina $\{\sigma\cdot\Delta|\sigma\in\mathfrak{S}_n\}$ by bola prípadne dvojprvková (napríklad $\pm\Delta$) tak máme spomínany morfizmus do dvojprvkovej symetrickej grupy (nad dvojprvkovou množinou), tj. grupy dvoch zobrazení $\varphi_1(\Delta)=\Delta$, $\varphi_1(-\Delta)=-\Delta$ a $\varphi_2(\Delta)=-\Delta$, $\varphi_2(-\Delta)=\Delta$. Iné zobrazenia možné nie sú: $-\Delta$ sa nemôže zobraziť na iný polynóm ako $\pm\Delta$ a tiež všetky zobrazenia sú prosté.

Definícia 5.28. Označme symbolom Δ nenulový polynom o n premenných ($\Delta\in\mathbb{R}[x_1,\ldots,x_n]$), že platí

$$\forall\sigma\in\mathfrak{S}_n : \sigma\cdot\Delta = \pm\Delta \qquad \& \qquad \exists\hat{\sigma}\in\mathfrak{S}_n : \hat{\sigma}\cdot\Delta = -\Delta$$

Poznámka 5.35. Existenciu tohto polynómu dokážeme neskôr.

Definícia 5.29. Nech Δ je polynóm z predchádzajúcej definície. Definujeme znamienko permutácie $\sigma\in\mathfrak{S}_n$ ktoré značíme $\mathrm{sgn}(\sigma)$ tak, že

$$\begin{aligned}\mathrm{sgn}(\sigma) = +1 \quad &\Leftrightarrow \quad \sigma\cdot\Delta = \Delta\\ \mathrm{sgn}(\sigma) = -1 \quad &\Leftrightarrow \quad \sigma\cdot\Delta = -\Delta\end{aligned}$$

Lemma 5.35. Pre $\forall\tau,\sigma\in\mathfrak{S}_n$ platí $\mathrm{sgn}(\tau\sigma) = \mathrm{sgn}(\tau)\,\mathrm{sgn}(\sigma)$.

Dôkaz. Najskôr si uvedomme, že platí $\sigma\cdot -\Delta = -\sigma\cdot\Delta$, čo je zrejmé z konštrukcie zobrazenia $\sigma\cdot$ na polynómoch[10]. Môžme teda písať

$$\mathrm{sgn}(\tau\sigma)\Delta = (\tau\sigma)\cdot\Delta = \tau\cdot(\sigma\cdot\Delta) = \tau\cdot(\mathrm{sgn}(\sigma)\Delta) = \mathrm{sgn}(\tau)\,\mathrm{sgn}(\sigma)\Delta \qquad \square$$

*Tvrdenie 5.36. Existuje zobrazenie $\mathrm{sgn}:\mathfrak{S}_n\to\{1,-1\}$ tak, že $\forall\tau,\sigma\in\mathfrak{S}_n$ platí $\mathrm{sgn}(\tau\sigma) = \mathrm{sgn}(\tau)\,\mathrm{sgn}(\sigma)$ a $\exists\hat{\sigma}\in\mathfrak{S}_n : \mathrm{sgn}(\hat{\sigma}) = -1$.

Dôkaz. Týmto zobrazením je práve nami skonštruované zobrazenie z Definície 5.29, čiže $\mathrm{sgn}:\sigma\mapsto\mathrm{sgn}(\sigma)$. Všetky vlastnosti vyplývajú buď priamo z Definície 5.28 polynómu Δ alebo z Lemmatu 5.35. Pre dokončenie celej konštrukcie treba ešte nájsť nejaký polynóm spĺňujúci podmienky z definície Δ, k čomu sa onedlho dostaneme. □

***V zmysle týchto minipoznámok (kde sa na permutácie pozeráme skôr ako na prvky grupy) môžme teda zobrazenie $\mathrm{sgn}:\mathfrak{S}_n\to\{-1,1\}$ chápať ako epimorfizmus medzi príslušnými grupami a v skutočnosti sa teda nejedná o nič iné, ako o hladaný morfizmus do dvojprvkovej grupy, ktorý teda vieme nájsť, ak nájdeme polynóm Δ (polynóm s dvojprvkovou orbitou). No toto zobrazenie je nezávislé na polynóme, keďže pre takýto epimorfizmus je znamienko určené počtom transpozícií, ktorými vieme danú permutáciu vyjadriť (keďže, ako ukážeme, transpozície majú nutne znamienko záporné), čo je predmetom nasledujúceho tvrdenia.*

Tvrdenie 5.37. Nech sgn je zobrazenie s vlastnosťami z Tvrdenia 5.36, teda nie nutne skonštruované pomocou nášho polynómu Δ. Ak σ ide zapísať ako párny (sudý) počet transpozícií, tak $\mathrm{sgn}(\sigma) = 1$. Ak permutáciu ide zapísať ako nepárny (lichý) počet transpozícií, tak $\mathrm{sgn}(\sigma) = -1$.

[10] No musí to platiť nezávisle na konštrukcii zobrazenia, pokiaľ vieme, že sa jedná o morfizmus: ukážeme, že platí $\sigma\cdot\pm\Delta = \mathrm{sgn}(\sigma)\pm\Delta$ (teda ide nám o to, čomu sa rovná $\sigma\cdot -\Delta$, pričom zrejme to určite bude $\pm\Delta$ a chceme zistiť to znamienko), čomu je tak preto, že $(\sigma^{-1}\sigma)\cdot\pm\Delta = \pm\Delta$ a teda nutne $\sigma\cdot\Delta = \pm\Delta \Rightarrow \sigma\cdot -\Delta = \mp\Delta$.

Ekvivalentne môžme tvrdenie modifikovať: zobrazenie sgn priradí transpozícii vždy záporné znamienko.

Poznámka 5.36.

1) Implikácie v Tvrdení je možné obrátiť. To je ale záležitosťou logiky a nie lineárnej algebry[11]...

2) Ak sa nám podarí nájsť polynóm Δ a tým konečne dokončiť dôkaz Tvrdenia 5.36 a dokážeme Tvrdenie pred poznámkou, tak dostaneme, že parita (párnosť/nepárnosť) je pre každú permutáciu nemenná! Tj. buď sa dá daná permutácia zapísať len pomocou párneho počtu transozícií alebo len nepárneho, keďže znamienko permutácie je určené jednoznačne (funkcia má vždy len jednu funkčnú hodnotu). Z tvrdenia tiež priamo vyplýva jednoznačnosť funkcie sgn, tj. existuje práve jedno zobrazenie z Tvrdenia 5.36. Dokonca je možné ekvivalentne definovať znamienko permutácie ako $\operatorname{sgn} : \sigma \mapsto (-1)^{n_\sigma}$, kde n_σ je počet transpozícií, ktorými sa dá permutácia zapísať a túto definíciu môžme použiť i v prípade permutácií obecných množín (teda nie nutne číslených ako v našom prípade).

3) Pomocou transpozícií môžme znamienko permutácie i počítať. No možnože existuje ešte vhodnejší spôsob: znamienko permutácie σ spočítame ako $\operatorname{sgn}(\sigma) = (-1)^{k_\sigma}$ kde k_σ je počet cyklov v rozklade permutácie na disjunktné cykly, ktoré sú párnej dĺžky (transpozícia má dĺžku 2). Túto skutočnosť nahliadneme ľahko tak, že cyklus dĺžky n sa dá vyjadriť ako $n-1$ transpozícií. Napríklad
$$(1\,2\,3\,4\,5) = (1\,2)(2\,3)(3\,4)(4\,5)$$

Dôkaz tvrdenia.

I.) Prípad σ je možné zapísať ako párny počet transpozícií. Stačí nám skúmať všetky permutácie tvaru $\sigma = (j_1,\, k_1)(j_2,\, k_2)$ (pričom $j_1 \neq k_1 \,\&\, j_2 \neq k_2$). Každá permutácia sa potom dá zapísať pomocou takýchto dvojíc.

   a) Najskôr si vezmime prípad $j_1 = j_2 \,\&\, k_1 = k_2$. No potom $\sigma = (j_1,\, k_1)(j_1,\, k_1) = e$ a $\sigma(e) = 1$, lebo
   $$\sigma(e) = \sigma(ee) = \sigma(e)\sigma(e) \;\Rightarrow\; 1 = \sigma(e)^{-1}\sigma(e) = \sigma(e)^{-1}\sigma(e)\sigma(e) = \sigma(e)$$
   lebo inverzia k $\sigma(e)$ (čo je určite ± 1) určite existuje.

   b) V prípade, že $j_1 = j_2 \,\&\, k_1 \neq k_2$ (to samé ako $j_1 \neq j_2 \,\&\, k_1 = k_2$, keďže $(a,\, b) = (b,\, a)$) si uvedomíme rovnosť
   $$(j_1,\, k_1)(j_1,\, k_2) = (j_1,\, k_1)(k_1,\, k_2)(j_1,\, k_1)(k_1,\, k_2)$$
   napríklad tak, že overíme, či danému číslu napravo zodpovedá to isté, čo nalavo. Napríklad číslo k_2 sa najskôr zobrazuje (ideme zprava) na j_1 a po zložení permutácie s tou nalavo sa zobrazí na k_1. Podobne napravo sa najskôr číslo k_2 zobrazuje na k_1, potom na j_1, potom sa nezmení na nakoniec sa zobrazí na k_1. Takto overíme ostávajúce dva čísla.
   Teda máme
   $$\operatorname{sgn}(\sigma) = \operatorname{sgn}((j_1,\, k_1)(j_1,\, k_2)) = \operatorname{sgn}((j_1,\, k_1)(k_1,\, k_2))^2 = 1$$

[11] Obmenou prvej implikácie dostaneme, že ak $\operatorname{sgn}(\sigma) \neq -1$, tak nutne permutáciu nejde zapísať pomocou nepárneho počtu transpozícií. Ale tiež platí $\operatorname{sgn}(\sigma) \neq -1 \Leftrightarrow \operatorname{sgn}(\sigma) = 1$ a ak nejde permutáciu zapísať pomocou nepárneho počtu transpozícií tak ju ide zapísať pomocou párneho počtu tranzozícií, lebo vždy existuje číslo $n \in \mathbb{N}_0$ také, že permutáciu ide zapísať pomocou n transpozícií. Celkovo dostávame, že $\operatorname{sgn}(\sigma) = 1$ implikuje, že permutáciu ide zapísať pomocou (len) párneho počtu transpozícií.

c) Nakoniec prípad j_1, k_1, j_2, k_2 všetky rôzne. Znova môžte overiť, že

$$(j_1,\, k_1)(j_1,\, k_2) = ((j_1,\, k_1)(j_1,\, k_2))((k_2,\, j_1)(k_2,\, j_2))$$

Využijeme bod b) a môžme písať

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}((j_1,\, k_1)(j_1,\, k_2)(k_2,\, j_1)(k_2,\, j_2)) = 1 \cdot 1 = 1$$

II.) Prípad, že σ ide zapísať zložením nepárneho počtu transpozícií. Z definície zobrazenia sgn vieme, že musí existovať $\hat{\sigma} \in \mathfrak{S}_n$ tak, že $\operatorname{sgn}(\hat{\sigma}) = -1$. Podľa bodu I.) vieme, že $\hat{\sigma}$ nemôže byť zapísatelná zložením párneho počtu transpozícií a teda je zapísatelná pomocou nepárneho počtu transpozícií. Platí $\sigma = \hat{\sigma}\hat{\sigma}^{-1}\sigma$ a určite $\hat{\sigma}^{-1}\sigma$ je zapísatelné pomocou párneho počtu transpozícií ($\hat{\sigma}^{-1}$ dostaneme napríklad tak, že zmeníme poradie transpozícií permutáciu tvoriacich). Potom

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\hat{\sigma}\hat{\sigma}^{-1}\sigma) = \operatorname{sgn}(\hat{\sigma})\operatorname{sgn}(\hat{\sigma}^{-1}\sigma) = -1 \cdot 1 = -1 \qquad \square$$

TVRDENIE 5.38. Polynóm Δ n premenných definovaný ako[12]

$$\begin{aligned}\Delta(x_1, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_j - x_i) = (x_2 - x_1)(x_3 - x_1)\cdots(x_n - x_1)\\ (x_3 - x_2)\cdots(x_n - x_2)\\ \cdots\\ (x_n - x_{n-1})\end{aligned}$$

spĺňa Definíciu 5.28.

DÔKAZ. Nech $\sigma \in \mathfrak{S}_n$. Všimnime si, že v polynóme sa každá dvojica premenných vyskytuje spolu v zátvorke práve raz (je ich tam teda $\binom{n}{2}$) a teda ak za x_i dosadíme $x_{\sigma^{-1}(i)}$, tak jediné, čo sa môže stať je, že polynóm zmení znamienko (žiadna z dvojích tam ani nepribudne ani neubudne). Permutácia meniaca znamienko bude určite napríklad $\hat{\sigma} = (1\,2)$.

*POZNÁMKA 5.37. Tento polynóm môžme chápať iba ako pomocnú konštrukciou na dokázanie, že parita počtu transpozícií je nemenná. Znamienko podľa neho nepočítame (aj napriek tomu, že by to šlo - znamienko permutácie sa potom rovná $\operatorname{sgn}(\sigma) = (-1)^{i_\sigma}$ kde i_σ je počet tzv. inverzií, tj. počet dvojíc (i, j) takých, že $i < j \,\&\, \sigma(i) > \sigma(j)$) a celkovo pod definíciou znamienka si môžme skôr predstaviť spomínanú ekvivalentnú definíciu s počtom transpozícií.

***Skutočne platí už naznačené, a to, že počet permutácií s kladným a záporným znamienkom je rovnaký? Skúmajme všetky párne permutácie (ktoré tvoria v $\widetilde{\mathfrak{S}}_n$ podgrupu, označme ju teraz ako A_n). Zoberme si prvok $\tau \notin A_n$ a definujme $B_n := \{\tau\sigma | \sigma \in \mathfrak{S}_n\}$. Tvrdíme, že $\#B_n = \#A_n$ a že $B_n = \mathfrak{S}_n \backslash A_n$, teda, že B_n sú všetky nepárne permutácie. Skúste ukázať, že zobrazenie $\tau \mapsto \tau\sigma$ je prosté a že ľubovolnú nepárnu permutáciu vieme zapísať ako $\tau\sigma$, kde $\sigma \in A_n$ (využite fakt, že v grupe má každý prvok inverziu).*

5.2. Determinanty: definícia a základné vlastnosti

DEFINÍCIA 5.30. Polynóm v n^2 premenných x_{ij}, $i, j = 1, \ldots, n$ tvaru

$$\sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) x_{1\sigma(1)} x_{2\sigma(2)} \cdots x_{n\sigma(n)}$$

nazveme **determinat**[13]. Pre $A \in M(n, n, \mathbb{R})$ definujem $\det A$ (determinant matice) ako determinant, kde dosadím $x_{ij} := a^i{}_j$, kde $A = (a^i{}_j)^{i=1,\ldots,n}_{j=1,\ldots,n}$.

[12]Tento polynóm sa dostane ako Vandermondov determinat Vandermondovej matice $n \times n$, ktorý má práve n premenných. Permutácia premenných v polynóme zodpovedá permutácii riadkov v matici, čo, ako zanedlho zistíme, zodpovedá zmene determinantu práve o $\operatorname{sgn}(\sigma)$.

[13]Bližšie poradie premenných v argumente nie je potrebné špecifikovať - budeme hovoriť skôr o determinante matice a tam bude všetko jasné.

Poznámka 5.38.

1) Všimnite si, že determinat má zmyslel len pre štvorcové matice.

2) Neskôr si ešte ukážeme, ako táto abstraktná definícia súvisí so spomínanými objemami. Teraz len poznamenajme, že ten súvis sa skrýva práve v tom činiteli $\operatorname{sgn}(\sigma)$ a ide tam práve o to, že potrebujeme priradiť danej permutácii premenných znamienko podľa toho, koľkými transpozíciami sme k nej došli.

Príklad 5.15. Spočítajme determinant matice typu 2×2

$$\det A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \operatorname{sgn}(e) a_{11} a_{22} + \operatorname{sgn}((1\,2)) a_{12} a_{21} = a_{11} a_{22} - a_{12} a_{21}$$

U prvkov matice nie je v tomto momente, keď hovoríme o determinantoch, nutné rozlišovať medzi indexami hore/dole/napravo/nalavo - to sa nám zišlo vtedy, keď sme o maticiach hovorili v kontexte lineárnych zobrazení.

12. prednáška z lineárnej algebry

18. december 2007

MINULE. Minule sme si zadefinovali determinant matice, k čomu sme potrebovali pojem permutácie a znamienka permutácie. Permutáciu v definícii využívame na zápis istého výberu n činitelov n^2 premenných v každom sčítanci. každej permutácii priradíme znamienko podla toho, koľkými transpozíciami sme sa k nej mohli dostať, pričom tento počet je vždy buď párny (sudý) alebo nepárny (lichý).

VETA 5.39. Nech $A \in M(n,n,\mathbb{R})$. Potom platí $\det A = \det A^T$.

DÔKAZ. Budeme upravovať rozpísaný výraz $\det A^T$, pričom transpozícia znamená: $(A^T)_{ij} = (A)_{ji}$ pre $\forall i,j = 1,\dots,n$. Takže dostávame:

$$\begin{aligned}\det A^T &= \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1}a_{\sigma(1)2}\cdots a_{\sigma(n)n} = \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma) a_{1\sigma^{-1}(1)}a_{2\sigma^{-1}(2)}\cdots a_{n\sigma^{-1}(n)}\\ &= \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma^{-1}) a_{1\sigma^{-1}(1)}a_{2\sigma^{-1}(2)}\cdots a_{n\sigma^{-1}(n)} = \sum_{\sigma^{-1}} \operatorname{sgn}(\sigma^{-1}) a_{1\sigma^{-1}(1)}a_{2\sigma^{-1}(2)}\cdots a_{n\sigma^{-1}(n)}\\ &= \sum_{\sigma'\in\mathfrak{S}_n} \operatorname{sgn}(\sigma') a_{1\sigma'(1)}a_{2\sigma'(2)}\cdots a_{n\sigma'(n)} = \det A\end{aligned}$$

V prvej rovnosti sme využili definíciu transpozície; v druhej sme dômyselne poprehadzovali v (komutatívnom) súčine členy tak, že napríklad na prvé miesto sme dali vždy člen z prvého riadku, pričom v každom sčítanci sa v nejakom stĺpci (konkrétne v $\sigma^{-1}(1)$-vom) vždy zobrazíme na prvý riadok; v tretej sme využili fakt, že $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$; v štvrtej sme len zapísali, že sčítavame cez množinu všetkých $\sigma^{-1}\dots$; v piatej sme premenovali σ^{-1} na σ' a uvedomili si faktu, že daná σ^{-1} je v sume vždy iba raz a tiež, že σ^{-1} obieha celú množinu $\mathfrak{S}_n$.[14] □

VETA 5.40. (linearita determinantu) Determinant matice môžme pretransformovať ako funkciu riadkov resp. stĺpcov matice. Tvrdíme, že táto funkcia je lineárna v každom riadku, resp. stĺpci. Teda ak maticu A zapíšeme symbolicky ako $A = (a_1, a_2, \dots, a_n)$, kde a_i sú riadky, resp. stĺpce matice a funkciou $\det(a_1,\dots,a_n)$ myslíme príslušný $\det A$, tak môžme písať $\forall c \in \mathbb{R}$

$$\det(a_1,\dots,a_i' + ca_i'',\dots,a_n) = \det(a_1,\dots,a_i',\dots,a_n) + c\det(a_1,\dots,a_i'',\dots,a_n),\ \forall i = 1,\dots,n$$

DÔKAZ. Dôkaz je vcelku ľahký. Stačí užiť definíciu determinantu (dôkaz spravíme pre riadky, pre stĺpce sa potom naviac využije predchádzajúce tvrdenie dvakrát):

$$\begin{aligned}\det(a_1,\dots,a_i' + ca_i'',\dots,a_n) &= \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)}\dots(a'_{i\sigma(i)} + ca''_{i\sigma(i)})\dots a_{n\sigma(n)}\\ &= \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)}\dots a'_{i\sigma(i)}\dots a_{n\sigma(n)} + c\sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)}\dots a''_{i\sigma(i)}\dots a_{n\sigma(n)}\\ &= \det(a_1,\dots,a_i',\dots,a_n) + c\det(a_1,\dots,a_i'',\dots,a_n)\end{aligned}$$ □

POZNÁMKA 5.39. (dva dôsledky)

1) Napíšme predchádzajúce tvrdenie trošíčka obecnejšie a teraz pre zmenu v maticovom tvare pre stĺpce:

$$\det\begin{pmatrix} a_{11} & \cdots & \sum_{\nu=1}^m c_\nu a_{1i}^\nu & \cdots & a_{1n}\\ \vdots & & & & \vdots\\ a_{n1} & \cdots & \sum_{\nu=1}^m c_\nu a_{ni}^\nu & \cdots & a_{nn}\end{pmatrix} = \sum_{\nu=1}^m c_\nu \det\begin{pmatrix} a_{11} & \cdots & a_{1i}^\nu & \cdots & a_{1n}\\ \vdots & & & & \vdots\\ a_{n1} & \cdots & a_{ni}^\nu & \cdots & a_{nn}\end{pmatrix}$$

[14] Skutočne: $\forall\sigma' \in \mathfrak{S}_n \exists!\sigma'^{-1} \in \mathfrak{S}_n : e = \sigma'\sigma'^{-1} \Rightarrow \sigma' = (\sigma'^{-1})^{-1}$

2) Ak je stĺpec, resp. riadok nulový, tak je determinant nulový, teda

$$\det \begin{pmatrix} a_{11} & \cdots & 0 & \cdots & a_{1n} \\ \vdots & & & & \vdots \\ a_{n1} & \cdots & 0 & \cdots & a_{nn} \end{pmatrix} = 0$$

Veta 5.41. Čo sa stane s determinantom ak „zpermutuje“ stĺpce, resp. riadky? Nasledujúce: Nech $\tau \in \mathfrak{S}_n$, $A \in M(n,n,\mathbb{R})$ a použime zápis $A = (a_1, \ldots, a_n)$, kde a_i sú stĺpce, resp. riadky. Potom (A' označuje „zpermutovanú“ maticu)

$$\det A' = \det(a_{\tau(1)}, a_{\tau(2)}, \ldots, a_{\tau(n)}) = \operatorname{sgn}(\tau) \det(a_1, a_2, \ldots, a_n) = \operatorname{sgn}(\tau) \det A$$

Dôkaz. Dôkaz prevedieme pre stĺpce (pre riadky dostaneme znova triviálne užitím Vety 5.39). Znova determinant na lavej strane rovnosti rozpíšeme podľa definície a upravíme:

$$\begin{aligned} \det A' &= \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) a_{1\tau(\sigma(1))} \ldots a_{n\tau(\sigma(n))} = \operatorname{sgn}(\tau) \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\tau\sigma) a_{1\tau\sigma(1)} \ldots a_{n\tau\sigma(n)} \\ &= \operatorname{sgn}(\tau) \sum_{\tau\sigma} \operatorname{sgn}(\tau\sigma) a_{1\tau\sigma(1)} \ldots a_{n\tau\sigma(n)} = \operatorname{sgn}(\tau) \sum_{\sigma' \in \mathfrak{S}_n} \operatorname{sgn}(\sigma') a_{1\sigma'(1)} \ldots a_{n\sigma'(n)} \\ &= \operatorname{sgn}(\tau) \det A \end{aligned}$$

Znova je potrebné si uvedomiť, že $\tau\sigma$ ak σ prebieha celú množinu $\mathfrak{S}_n$ ju „prosto“ prebieha celú tiež. Teraz pre zmenu to poriadnejšie overme. Chceme teda ukázať, že pre dané $\sigma' \in \mathfrak{S}_n$ vieme nájsť práve jedno $\sigma \in \mathfrak{S}_n$ tak, že $\sigma' = \tau\sigma$ $(*)$. Môžme sa presvedčiť, že prvok $\sigma = \tau^{-1}\sigma'$ určite spĺňa $(*)$. No je jediný? Nech existujú teda dva prvky σ_1 a σ_2, že spĺňajú $(*)$. Potom teda $\tau\sigma_1 = \tau\sigma_2$ a keď pravú i lavú stranu zľava zložíme s τ^{-1}, tak dostaneme rovnosť $\tau^{-1}(\tau\sigma_1) = \tau^{-1}(\tau\sigma_2)$, ale skladanie zobrazení je asociatívne, takže nutne $\sigma_1 = \sigma_2$. □

Poznámka 5.40.

1) Pri výmene dvoch stĺpcov, resp. riadkov determinant zmení znamienko (jedná sa o transpozíciu; transpozície majú znamienko -1).

2) Determinant matice s dvomi rovnakými stĺpcami, resp. riadkami je nulový. Nech i-tý a j-tý stĺpec, resp. riadok je rovnaký. Potom podľa bodu 1) pri permutácii (i,j) dostaneme $\det A' = -\det A$, ale zroveň $\det A = \det A'$ a to je možné len vtedy, ak $\det A = \det A' = 0$

3) Pričítaním ľubovolej lineárnej kombinácie stĺpcov, resp. riadkov matice k danému sĺpcu, resp. riadku, pričom v danej l.k. daný riadok resp. stĺpec obshaknutý nie je, tak sa determinant nezmení. Fakt je dôsledkom bodu 2) ako aj Vety 5.40 o linearite determinantu. Teda:

$$\det \begin{pmatrix} a_{11} & \cdots & a_{1i} + \sum_{\nu \neq i}^{n} c_\nu a_{1\nu} & \cdots & a_{1n} \\ \vdots & & & & \vdots \\ a_{n1} & \cdots & a_{ni} + \sum_{\nu \neq i}^{n} c_\nu a_{n\nu} & \cdots & a_{nn} \end{pmatrix} = \det \begin{pmatrix} a_{11} & \cdots & a_{1i} & \cdots & a_{1n} \\ \vdots & & & & \vdots \\ a_{n1} & \cdots & a_{ni} & \cdots & a_{nn} \end{pmatrix}$$

4) [15] Odvodili sme teda (okrem iných) nasledujúce vlastnosti determinantov: linearita v každom riadku, zmena znamienka pri prehodení dvoch riadkov, či z toho vyplývajúca zmena determinantu o znamienko permutácie pri obecnej permutácii a tiež si môžme uvedomiť, že determinant jednotkovej matice je 1. No postupovať sme mohli aj opačne. Hľadať funkciu $\det : M(n,n,\mathbb{R}) \to \mathbb{R}$ takú, že je multilineárna v riadkoch, antisymetrická voči výmene dvoch riadkov a $\det \mathbb{1} = 1$. Táto funkcia koniec koncov má práve tie vlastnosti, ktoré by sme požadovali od objemu rovnobežnostenu, „natiahnutého“ nad vektormi tvoriacimi riadky matice

[15] „Nepovinná“ poznámka

typu $M(n,n,\mathbb{R})$. Spomínaná linearita je základnou vlastnosťou objemov (pre konkrétnosť uvažujme objem v dvoch rozmeroch - kreslite). Antisymetriu nahliadneme tak, že určite ak sa dva vektory tvoriace rovnobežnosten opakujú, jeho objem je nula, teda ak počítame objem (objem značíme ako $\det(\dots)$) rovnobežnostenu tvaru

$$\begin{aligned} 0 &= \det(a_1,\dots,a_{i-1},a_i+a_j,\dots,a_{j-1},a_j+a_i,\dots,a_n) \\ &= \det(a_1,\dots,a_i,\dots,a_j,\dots,a_n)+\det(a_1,\dots,a_j,\dots,a_i,\dots,a_n) \end{aligned}$$

tak dostávame

$$\det(a_1,\dots,a_i,\dots,a_j,\dots,a_n) = -\det(a_1,\dots,a_j,\dots,a_i,\dots,a_n)$$

pre $\forall i<j$. Nenehajte sa zmiasť zápornými objemami - tie sú priam žiadúce, keďže zrejme

$$0=\det(0,a_2,\dots,a_n)=\det(a_1,a_2,\dots,a_n)+\det(-a_1,a_2,\dots,a_n)$$

Dá sa z týchto vlastností funkcie det dôjsť spätne k Definícii determinantu 5.30? Odpoveď je dá a môžme sa o to i pokúsiť: Majme teda maticu A a funkciu det s predchádzajúcimi vlastnosťami. Môžme teda písať

$$\det A = \sum_{p_1,\dots,p_n} a_{1p_1}a_{2p_2}\dots a_{np_n}\det(e_{p_1},e_{p_2},\dots,e_{p_n})$$

kde sme využili multilinearitu a zápis e_i znamená kanonický vektor s jedničkou na i-tom mieste. Definujme zobrazenie $\pi_{p_1\dots p_n}:\{1,\dots,n\}\to\{1,\dots,n\}$ predpisom $\pi_{p_1\dots p_n}(i)=p_i$ a znamienko tohto zobrazenia $\operatorname{sgn}(\pi_{p_1\dots p_n})$ tak, že je to ±1 ak to je párna resp. nepárna permutácia a 0 v ostatných prípadoch (teda ak to nie je zobrazenie prosté $\Leftrightarrow$ nie je na). Potom zrejme môžme písať

$$\det A = \sum_{p_1,\dots,p_n} a_{1\pi(1)}a_{2\pi(2)}\dots a_{n\pi(n)}\operatorname{sgn}(\pi)$$

kde dolné indexy u $\pi_{p_1\dots p_n}(i)$ pre jednoduchosť nepíšeme. Ak v sume nepíšeme nulové členy, tak konečne dostaneme

$$\det A = \sum_{\pi\in\mathfrak{S}_n}\operatorname{sgn}(\pi)a_{1\pi(1)}a_{2\pi(2)}\dots a_{n\pi(n)}$$

čo je presne tvar determinantu v jeho definícii.

Definícia 5.31. Nech $i,j\in\{1,\dots,n\}$. Definujeme **algebraický doplnok** (i,j) k matici $A\in M(n,n,\mathbb{R})$ ako

$$\Delta_{ij}=(-1)^{i+j}\det\begin{pmatrix} a_{11} & \dots & a_{1j-1} & a_{1j+1} & \dots & a_{1n}\\ \vdots & & & & & \vdots\\ a_{i-11} & \dots & a_{i-1j-1} & a_{i-1j+1} & \dots & a_{i-1n}\\ a_{i+11} & \dots & a_{i+1j-1} & a_{i+1j+1} & \dots & a_{i+1n}\\ \vdots & & & & & \vdots\\ a_{n1} & \dots & a_{nj-1} & a_{nj+1} & \dots & a_{nn}\end{pmatrix}$$

Veta 5.42. Dôležitým nástrojom ako spočítať („riedke“) determinanty môže byť práve jeho rozvýjanie podľa vhodného riadka, resp. stĺpca (prípadne s pomocou užitia bodu 3. v prechádzajúcej poznámke). Rozvýjať determinant podla i-tého riadka resp. j-tého stĺpca znamná využiť nasledujúcu rovnosť

$$\det A = a_{i1}\Delta_{i1}+\dots+a_{in}\Delta_{in}$$

resp.

$$\det A = a_{1j}\Delta_{1j}+\dots+a_{nj}\Delta_{nj}$$

ktorá je predmetom tohto tvrdenia.

Dôkaz. Nabudúce. □

12. přednáška z lineární algebry

8. leden 2008

VĚTA 5.43. Buď $A \in M(n,n,\mathbb{R})$ regulární. Pak platí:

$$\det A = x_{1j}\Delta_{1j} + x_{2j}\Delta_{2j} + \ldots + x_{nj}\Delta_{nj} \qquad \text{rozvoj podle j-tého sloupce}$$

$$\det A = x_{i1}\Delta_{i1} + x_{i2}\Delta_{i2} + \ldots + x_{in}\Delta_{in} \qquad \text{rozvoj podle i-tého řádku}$$

DŮKAZ. Důkaz stačí provést jen pro rozvoj řádku, protože pokud se nám toto povede dokázat, budeme vědět, že věta platí i pro sloupce díky $\det A = \det A^T$.

Určitě můžeme napsat, že platí:

$$\det(x_{ij}) = c'_1 x_{i1} + c'_2 x_{i2} + \ldots + c'_n x_{in}$$

Kde c'_j je polynom, který vzniká tak, že se napíše celý determinant a členy které obsahují prvek x_{ij} se dají k sobě a tento prvek se vytkne (rozmyslete si, jak je možné, že v žádném členu nebude zároveň například x_{i1} a x_{i2}). V závorce nám pak zbyde polynom c'_1. V celém důkazu nám teď půjde o ověření faktu, že tento polynom je roven Δ_{ij}.

Dosaďme do determinantu: $x_{ij} = 1,\ x_{ik} = 0\ \forall k \neq j$. Dostaneme tak:

$$\det \begin{pmatrix} x_{11} & \ldots & x_{1,j-1} & x_{1j} & x_{1,j+1} & \ldots & x_{1n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ x_{n1} & \ldots & x_{n,j-1} & x_{nj} & x_{n,j+1} & \ldots & x_{nn} \end{pmatrix} = c'_j$$

Na to, proč platí tato rovnost přijdete celkem snadno. Ze všech sčítanců, které tvoří determinant této matice jsou totiž nenulové jen ty, které obsahují jedničku. A protože jsou násobené jedničkou je výsledkem právě jen tento polynom. Označme si výše uvedenou matici symbolem $\square$. Bude platit:

$$\det(\square) = \operatorname{sgn}(\tau_1) \det \begin{pmatrix} x_{1j} & x_{11} & \ldots & x_{1n} \\ x_{2j} & x_{21} & \ldots & x_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ x_{nj} & x_{n1} & \ldots & x_{nn} \end{pmatrix} = \operatorname{sgn} \begin{pmatrix} 1 & 2 & \ldots & j-1 & j \\ 2 & 3 & \ldots & j & 1 \end{pmatrix} \det(\square') =$$

Kde τ_1 je cyklická permutace. Jednoduše si ověříte, že její znaménko je $(-1)^{j-1}$. $\square'$ je tentokrát matice už s permutovanými sloupci. Všimněte si, že mezi sloupci napravo od sloupce x_{i1} chybí j-tý sloupec! Permutace ho dostala na první pozici! Podobně si zavedeme permutaci τ_2, která nám trochu zamíchá s řádky:

$$= (-1)^{j-1} \operatorname{sgn}(\tau_2) \det \begin{pmatrix} 1 & 0 & \ldots & 0 \\ x_{1j} & x_{11} & \ldots & x_{1n} \\ x_{2j} & x_{21} & \ldots & x_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ x_{nj} & x_{n1} & \ldots & x_{nn} \end{pmatrix} = (-1)^{j-1}(-1)^{i-1} \det \begin{pmatrix} x_{11} & \ldots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{n1} & \ldots & x_{nn} \end{pmatrix}$$

Opět je třeba si uvědomit, že v poslední matici chybí j-tý sloupec a i-tý řádek.

$$= (-1)^{j+i} \det \begin{pmatrix} x_{11} & \ldots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{n1} & \ldots & x_{nn} \end{pmatrix} = \Delta_{ij} \quad \text{z definice } \Delta_{ij}. \qquad \square$$

Věta 5.44. Nechť $A \in M(n,n,\mathbb{R})$ a $\det A \neq 0$. Pak existuje A^{-1} a platí:

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} \Delta_{11} & \Delta_{21} & \dots & \Delta_{n1} \\ \Delta_{12} & \Delta_{22} & \dots & \Delta_{n2} \\ \dots & \dots & \dots & \dots \\ \Delta_{1n} & \Delta_{2n} & \dots & \Delta_{nn} \end{pmatrix}$$

Pozor na prohozené řádky a sloupce!

Důkaz. Ověřme, že platí:

$$\sum_{i=1}^{n} a_{ij}\Delta_{ik} = \delta_{jk} \det A \tag{1}$$

$j = k$: $\sum_{i=1}^{n} a_{ij}\Delta_{ij} = \det A$ viz minulá věta (rozvoj podle sloupce)

$j \neq k$: $\sum_{i=1}^{n} a_{ij}\Delta_{ik} = 0$ neboť zde se jedná o rozvoj determinantu matice, která má v k-tém sloupci znovu j-tý sloupec a z vlastností determinantu vyplývá, že musí být nulový.

Označme maticu symbolom Δ, ktorá má prvky $(\Delta)_{jk} = \Delta_{jk}$. Počítajme, čomu sa rovná maticový súčin $A\Delta^T$:

$$(A\Delta^T)_{jk} = \sum_{i=1}^{n} (A)_{ji}(\Delta^T)_{ik} = \sum_{i=1}^{n} (A)_{ji}(\Delta)_{ki} = \sum_{i=1}^{n} a_{ji}\Delta_{ki} = \delta_{jk} \det A$$

Totéž se dá vyjádřit jako:

$$A\Delta^T = \det A \mathbb{1} \quad \Rightarrow \quad \frac{\Delta^T}{\det A} A = \mathbb{1}$$

Což znamená, že A má inverzi rovnou: $A^{-1} = \frac{\Delta^T}{\det A}$. □

Věta 5.45. Nechť $A, B \in M(n,n,\mathbb{R})$ jsou matice. Pak $\det(AB) = \det A \cdot \det B$

Důkaz. Z definice maticového násobení je levá strana rovna:

$$L = \det(A \cdot B) = \det \begin{pmatrix} \sum_{i_1=1}^{n} a_{1i_1} b_{i_1 1} & \dots & \sum_{i_n=1}^{n} a_{1i_n} b_{i_n n} \\ \vdots & & \vdots \\ \sum_{i_1=1}^{n} a_{ni_1} b_{i_1 1} & \dots & \sum_{i_n=1}^{n} a_{ni_n} b_{i_n n} \end{pmatrix} =$$

Kde $i_1 \dots i_n$ jsou různé sčítací indexy. To můžme napsat i jako

$$= \det\left(\begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix} b_{11} + \begin{pmatrix} a_{12} \\ \vdots \\ a_{n2} \end{pmatrix} b_{21} + \dots \begin{pmatrix} a_{1n} \\ \vdots \\ a_{nn} \end{pmatrix} b_{n1}, \begin{pmatrix} \sum_{i_2=1}^{n} a_{1i_2} b_{i_2 2} & \dots & \sum_{i_n=1}^{n} a_{1i_n} b_{i_n n} \\ \vdots & & \vdots \\ \sum_{i_2=1}^{n} a_{ni_2} b_{i_2 2} & \dots & \sum_{i_n=1}^{n} a_{ni_n} b_{i_n n} \end{pmatrix} \right) =$$

Nyní můžeme použít vlastnost multilinearity determinantu a psát:

$$= \sum_{i_1=1}^{n} b_{i_1 1} \det\left(\begin{pmatrix} a_{1i_1} \\ \vdots \\ a_{ni_1} \end{pmatrix} \begin{pmatrix} \sum_{i_2=1}^{n} a_{1i_2} b_{i_2 2} & \dots & \sum_{i_n=1}^{n} a_{1i_n} b_{i_n n} \\ \vdots & & \vdots \\ \sum_{i_2=1}^{n} a_{ni_2} b_{i_2 2} & \dots & \sum_{i_n=1}^{n} a_{ni_n} b_{i_n n} \end{pmatrix} \right)$$

$$= \sum_{i_1=1}^{n} b_{i_1 1} \sum_{i_2=1}^{n} b_{i_2 2} \cdots \sum_{i_n=1}^{n} b_{i_n n} \det \begin{pmatrix} a_{1i_1} & \dots & a_{1i_n} \\ \vdots & & \vdots \\ a_{ni_1} & \dots & a_{ni_n} \end{pmatrix}$$

co dostaneme tak, že použijeme stejný postup na všechny sloupce sum. Uvědomme si, že všechny sčítance v sumě, kde se čo i len dva indexy (i_j a i_k) rovnají, sou nulové. V opačném prípade je

zobrazení $j \mapsto i_j$ je permutace. Můžme tedy místo determinantu psát následující, kde si zavedeme znaménko nečeho, co není permutace jako nula. Tedy:

$$= \sum_{i_1 \dots i_n} b_{i_1 1} \dots b_{i_n n} \operatorname{sgn} \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \det \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} = \det B \cdot \det A \qquad \square$$

VĚTA 5.46. Nechť $A \in M(n, n, \mathbb{R})$. Existuje-li A^{-1} pak $\det A \neq 0$.

DŮKAZ. Když existuje inverzní matice, tak platí:

$$\det A \cdot \det A^{-1} = \det(AA^{-1}) = \det \mathbb{1} = 1$$

Z toho plyne, že $\det A \neq 0$ a navíc víme, že $\det A^{-1} = (\det A)^{-1}$. $\square$

POZNÁMKA 5.41.

a) Věty 5.44 a 5.46 společně říkají, že A má inverzní matici (tj. je regulární) právě tehdy když $\det A \neq 0$. Navíc Věta 5.44 nám dává postup na výpočet A^{-1} a Věta 5.46 nám umožňuje jednoduše spočítat determinant inverzní matice.

b) Platí následující ekvivalence

$$A^{-1}\text{existuje} \Leftrightarrow \det A \neq 0 \Leftrightarrow \operatorname{rank}(A) = n \Leftrightarrow \dim(\operatorname{Im}(A)) = n \Leftrightarrow \dim(\operatorname{Ker}(A)) = 0$$

Doporučujeme čtenáři, aby si uvedené ekvivalence, které shrnují naše dosavadní znalosti o determinantech, zkusil dokázat. Je možné, že se objeví v některé ze zkouškových písemek. První ekvivalence je už dokázaná (viz první bod této poznámky). Zkusme třeba výrok: A^{-1}existuje $\Leftrightarrow \operatorname{rank}(A) = n$:

To, že existuje inverzní matice znamená, že $AA^{-1} = \mathbb{1}$ takže $\forall y \in \mathbb{R}^n : \; AA^{-1}y = y$ neboli každé y má při zobrazení pomocí matice A svůj vzor $A^{-1}y$, což znamená, že A je surjektivní $\Rightarrow \; \dim(\operatorname{Im}(A)) = n = \operatorname{rank}(A)$

A naopak: $\operatorname{rank}(A) = n \Rightarrow \dim(\operatorname{Im}(A)) = n \;\&\; \dim(\operatorname{Ker}(A)) = 0 \Rightarrow A$ je surjektivní & injektivní. Inverzní matice potom existuje, keďže můžme skonštruovať inverzní zobrazení předpisem: $A^{-1}y = x \Leftrightarrow y = Ax$, přičemž A^{-1} je lineární zobrazení. Platí $A^{-1}A = AA^{-1} =$ ⊮, takže matice A^{-1} je skutočně inverzní k A.

Při důkazech se hojně využívá Vět 2.16, 2.17 a 2.18.

VĚTA 5.47. (Cramerovo pravidlo)
$A \in M(n, n, \mathbb{R})$, $\det A \neq 0$. Pak rovnice $Ax = b$, $\forall b \in \mathbb{R}^n$ má právě jedno řešení a sice:

$$x = \begin{pmatrix} x^1 \\ \vdots \\ x^n \end{pmatrix}, \text{ kde } x^i = \frac{det \begin{pmatrix} a_1^1 & \dots & b^1 & \dots & a_n^1 \\ \dots & \dots & \dots & \dots & \dots \\ a_1^n & \dots & b^n & \dots & a_n^n \end{pmatrix}}{\det A}$$

Determinant v čitateli má nahrazený í-tý sloupec pravou stranou rovnice.
DŮKAZ.

a) Ať pro spor existuje více řešení x_0, x_1 takových, že $x_0 \neq x_1$. Z čehož vyplývá:

$$Ax_0 = b \;\&\; Ax_1 = b \quad \Rightarrow \text{ A není injektivní } \Rightarrow \det A = 0$$

Podle poznámky, čímž máme spor s předpokladem.

b) Rovnice má určitě řešení (inak zas spor s předpokladmi). Buď tedy x_0 jediné řešení rovnice $Ax = b$. Vynásobme tuto rovnici zleva inverzní maticí (o které víme, že existuje) a dostaneme:

$$A^{-1}Ax_0 = A^{-1}b$$
$$x_0 = A^{-1}b$$

Inverzní matici ale umíme vyjádřit pomocí algebraických doplňků:

$$x_0 = A^{-1}b = \frac{1}{\det A}\begin{pmatrix}\Delta_{11} & \dots & \Delta_{n1}\\ \vdots & & \vdots\\ \Delta_{1n} & \dots & \Delta_{nn}\end{pmatrix}\cdot b = \frac{1}{\det A}\begin{pmatrix}\sum_{j=1}^{n}\Delta_{j1}b_j\\ \vdots\\ \sum_{j=1}^{n}\Delta_{jn}b_j\end{pmatrix} =$$

A tyto sumy už nápadně připomínají předpis z první věty této přednášky, tudíž jsou určitě determinanty následujících matic:

$$= \frac{1}{\det A}\begin{pmatrix}\det\begin{pmatrix}| & | & & |\\ b & a^2 & \dots & a^n\\ | & | & & |\end{pmatrix}\\ \vdots\\ \det\begin{pmatrix}| & & | & |\\ a^1 & \dots & a^{n-1} & b\\ | & & | & |\end{pmatrix}\end{pmatrix}$$

což jsme měli za úkol dokázat. □

6. Zbytky

Definice 6.32. Nechť $A \in M(n,n,\mathbb{R})$ pak stopou matice A (značíme $\mathrm{Tr}(A)$) nazvu číslo:

$$\mathrm{Tr}(A) = \sum_{i=1}^{n} a^i{}_i$$

Tvrzení 6.48. Ať $A, B \in M(n,n,\mathbb{R})$ Pak

$$\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$$

Důkaz.

$$\mathrm{Tr}(AB) = \sum_{i=1}^{n}(AB)^i{}_i = \sum_{i=1}^{n}\sum_{j=1}^{n} a^i{}_j b^j{}_i = \sum_{j=1}^{n}\sum_{i=1}^{n} b^j{}_i a^i{}_j = \sum_{j=1}^{n}(BA)^i{}_i = \mathrm{Tr}(BA) \qquad \square$$

Poznámka 6.42. (Důsledky tvrzení)

i) $\mathrm{Tr}(Q^{-1}AQ) = Tr(A)$, protože $\mathrm{Tr}(Q^{-1}AQ) = \mathrm{Tr}(AQ^{-1}Q) = \mathrm{Tr}(A\mathbb{1}) = \mathrm{Tr}(A)$

ii) Toto by nás mohlo přivést na myšlenku definovat stopu lineárního zobrazení. Máme-li f lineární zobrazení vůči bázi $\mathcal{B}$ a matici A tohoto zobrazení, řekneme, že $\mathrm{Tr}(f) = \mathrm{Tr}(A)$. Definice je korektní, protože z prvního bodu této poznámky vyplývá, že stopa zobrazení je invariatní vůči změně bází, a proto jednoznačná.

iii) Determinant se také zachovává:

$$\det(Q^{-1}AQ) = \det Q^{-1}\det A\det Q = (\det Q)^{-1}\det A\det Q = \det A$$

Definice 6.33. (Ortogonální projekce)
(V, b) buď vektorový prostor konečné dimenze se skalárním součinem. Dále $W \subseteq V$, $\dim W = n$. P_W nazvu ortogonální projekcí V na W pokud $\forall x \in V$:

$$P_W(x) = \sum_{i=1}^{m} b(x, e_i)e_i, \text{ kde } \{e_i\}_{i=1}^{n} \text{ je ON báze } W$$

Spočítat ortogonální projekci vektoru na podprostor znamená určit si libovolnou bázi tohoto podprostoru, ortonormalizovat ji pomocí Gramm-Schmidtova algoritmu a použít výše uvedený vzorec.

Věta 6.49. (Vlastnosti projekcí) (V, b) buď vektorový prostor konečné dimenze se skalárním součinem. $W \subseteq V$. $\dim W = n$. P_W je příslušná projekce. Pak:

1) $(x - P_W(x)) \in W^\perp$, $\forall x \in V$.
2) P_W nezávisí na výběru ON báze ve W.
3) $P_W(x) = x$, $\forall x \in W$.
4) $P_W(x) = 0$, $\forall x \in W^\perp$.
5) $P_W^2 = P_W$.
6) Projekce je lineární zobrazení.
7) Pre $\forall x, y \in V$ platí: $b(P_W(x), y) = b(x, P_W(y))$. Ak $\mathcal{B}$ je ortonormální báze, tak $[P_W]_{\mathcal{B}}^{\mathcal{B}} = ([P_W]_{\mathcal{B}}^{\mathcal{B}})^T$ - projekce má symetrickou matici vůči ortonormální bázi.

Důkaz.

1) Nechť $\{e_i\}_{i=1}^{n}$ je ON báze ve W. Nechť $w \in W$ a w^i jsou jeho souřadnice vůči naši bázi. Počítajme

$$b((x - P_W(x), w) = b(x, w) - b(P_W(x), w) = \sum_{i=1}^{n} b(x, e_i)w^i - \sum_{i=1}^{n}\sum_{j=1}^{n} b(x, e_j)b(e_j, e_i)w^i$$
$$= \sum_{i=1}^{n} b(x, e_i)w^i - \sum_{i=1}^{n} b(x, e_i)w^i = 0$$

2) Nechť $\{e_i\}_{i=1}^{n}$ a $\{f_i\}_{i=1}^{n}$ jsou dvě ON báze ve W. Nechť $P_W^e(x)$ a $P_W^f(x)$ jsou projekce vektoru x spočtěné pomocou první resp. druhé báze. Upravením dostáváme, že

$$(x - P_W^e(x)) - (x - P_W^f(x)) = P_W^f(x) - P_W^e(x)$$

kde levá strana náleží do $W^\perp$ a pravá do W, což znamená, že to je nulový vektor (protože zrejmě $W^\perp \cap W = \{0\}$).

3) Nechť vektor x ma souřadnice x^i vůči bázi $\{e_i\}_{i=1}^{n}$. Počítejme

$$P_W(x) = \sum_{i=1}^{n}\sum_{j=1}^{n} b(e_j, e_i)e_i x^j = \sum_{i=1}^{n} e_i x^i = x$$

4) Zřejmý důsledek definice - ak $x \in W^\perp$ tak $b(x, w)$, $\forall w \in W$, specielně pro vektory ON báze.

5) Stačí si uvědomit, že $P_W(x) \in W$ a spomenúť si na bod 3).

6) Vyplývá z toho, že skalární součin je (v první složke určitě) lineární. Tedy výraz typu $b(x_1 + cx_2, e_i)e_i$ se rovná $b(x_1, e_i)e_i + +cb(x_2, e_i)e_i$. Můžete tedy snadno důkaz dokončit.

7) Druhá část tvrzení je důsledkem první, tj. že $b(P_W(x), y) = b(x, P_W(y))$. Dokážme tedy nejspíš tenhle důsledek: Označme matici $[P]^{\mathcal{B}}_{\mathcal{B}}$ jako P a souřadnice vektorů x a y vůči bázi $\mathcal{B}$ jako x^i a y^i. Potom vzhledem k ortonormalitě báze $\mathcal{B}$ platí

$$b(x, P_W(y)) = \sum_{i,j} x^i (P)^i{}_j y^j$$

ale také

$$b(x, P_W(y)) = b(P_W(x), y) = \sum_{i,j} (P)^j{}_i x^i y^j = \sum_{i,j} x^i (P^T)^i{}_j y^j$$

Co to znamená? Jelikož vztah, ku kterému jsme došli, a sice

$$\sum_{i,j} x^i (P)^i{}_j y^j = \sum_{i,j} x^i (P^T)^i{}_j y^j$$

platí pro všechna vektory x, y, tedy pro všechna čísla $x^i, y^i \in \mathbb{R}$, tedy specielně i pro $x^i = y^j = 0$ pro všechny i, j kromě $i = k$ a $j = l$, přičemž $x^k = y^l = 1$. Touto specielní volbou dostáváme rovnost $(P)^k_l = (P^T)^k_l$. Kdybychom poračovali, dostaneme celkem $P = P^T$.

Nyní stačí ověřit rovnost $b(P_W(x), y) = b(x, P_W(y))$. Počítejme:

$$b(P_W(x), y) = b\big(\sum_{i=1}^{n} b(x, e_i)e_i, y\big) = \sum_{i=1}^{n} b(x, e_i)b(y, e_i) = b\big(x, \sum_{i=1}^{n} b(y, e_i)e_i\big) = b(x, P_W(y)) \qquad \square$$