VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Lineární algebra – SLA

Poznámky z přednášek

31. ledna 2022 David Sedlák (xsedla1d@stud.fit.vutbr.cz)

Pullrequesty a připomínky můžete směřovat do repozitáře: `www.github.com/Dajvid/SLA-notes`

Obsah

1 První přednáška

Matematika se historicky rodila jako celá řada disciplín, například jak tady máme jednu z nich, lineární algebra, nebo matematická analýza, teorie čísel a řada dalších...

Byly to takové historicky izolované disciplíny, v podobné situaci je dnes fyzika, ta má dnes také různé disciplíny a nedaří se je fyzikům spojit, i když se o to už dlouho pokoušejí a hledají tzv. teorii všeho. V matematice nějaká taková teorie všeho již byla nalezena a máme tu výhodu, že se podařilo najít ten „spojovací materiál", kterým je logika a teorie množin.

Díky tomu se matematiku podařilo dostat na společný jazyk, takže ať už studujete teorii pravděpodobnosti, nebo matematickou analýzu, tak se začne s nějakou definicí, co je jakási množina a tak dále...

1.1 Logika

V logice je základním pojmem výrok, neboli tvrzení, o kterém můžeme říct, zda je pravdivé, nebo nepravdivé. Tedy přiřazujeme mu pravdivostní hodnotu, nulu, nebo jedničku. Výroky následně rozlišujeme na jednoduché (atomární), které nejdou dále rozložit a na výroky složité, které jsou pospojovány logickými spojkami. Nejznámější logické spojky jsou tyto: $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$. Zdaleka se však nejedná o jejich vyčerpávajícíc výčet. Uvědomme si, že existuje 2^4 různých logických spojek (binárních).

Další nad čím je vhodné se z těchto základů pozastavit je pojem výroku. Ne všechno v běžné řeči je výrok. Je nutné si uvědomit, co výrok je a co není. A i když něco výrokem je, tak to ještě nezmanená, že jsme schopni určit pravdivostní hodnotu tohoto výroku. Například tvrzení: *Na Saturnově měsíci je voda*, určitě se jedná o výrok, ale jeho pravdivostní hodnotu neznáme. Výrokem ale určitě nejsou různá zvolání, výkřiky, otázky...

Je každá dobře utvořená oznamovací věta výrokem? Není, například věta *Colorless green ideas sleep furiously.* je z mluvnického hlediska utvořena správně a jedná se o oznamovací větu, ale významově je to takový nesmysl, že nelze určit, zda se jedná o výrok, protože tomu nelze přiřadit pravdivostní hodnota a to ani hypotetická.

Pomocí těchto výroků a spojek se snažíme dokazovat věty. V matematice máme 4 základní kameny:

- Primitivní pojmy: pojmy, které se nedefinují a nevysvětlují, například bod.

- Definice: zavádějí pojmy, pomocí pojmů již známých, například definice prvočísla.
- Axiomy: tvrzení, která se nedokazují a která se považují za platná.
- Věty: tvrzení, které se musí dokázat a odvozují se z tvrzení již známých.

1.2 Teorie množin

Množina je primitivní pojem. I přesto, že se jedná o primitivní pojem, budeme si ho nějakým způsobem specifikovat, aby si každý z nás pod tímto primitivním pojmem představil to stejné.

Primitivní pojem (Množina)

Množina je nějaký soubor prvků, které se neopakují. Nad množinami jsou opět definovány nějaké operace, jako sjednocení, průnik, doplněk... Množiny a operace nad nimi můžeme vizualizovat například pomocí vennových diagramů.

Mohutnost

Primitivní pojem (Mohutnost množiny)

Mohutnost množiny jednoduše udává počet jejich prvků. Mohutnost množiny A se značí jako $|A|$, nebo jako card(A). Mohutnost prázdné množiny je 0, $|\emptyset| = 0$.

Příklad (Mohutnost množiny)

Nechť $A = \{1, 2, 3\}$. Potom $|A| = card(A) = 3$.

Definice 1 (Mohutnost množiny přirozených čísel)

Mohutnost množiny přirozených čísel definujeme jako „alef nula“:

$$|\mathbb{N}| = \aleph_0$$

Relace

Před zavedením relace je nutné nejprve definovat pojem kartézského součinu množin.

Definice 2 (Kartézský součin množin)

Kartézský součin dvou množin se skládá z uspořádaných dvojic.

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

Příklad (Kartézský součin množin)

Mejme dvě množiny A a B:

$$A = \{u, v\}, B = \{1, 2, 3\}$$

Jejich kartézský součin $A \times B$ je potom:

$$A \times B = \{(u,1),(u,2),(u,3),(v,1),(v,2),(v,3)\}$$

Definice 3 (Relace)

Relace je libovolná podmnožina kartézského součinu.

$$R \subseteq A \times B, \text{ například: } R = \{(u,1),(u,2),(v,1)\}$$

Relaci lze vyjádřit i graficky jako orientovaný graf.

Některé binární relace jsou zobrazení, neboli funkce[1].

Definice 4 (Zobrazení)

Řekneme, že relace $R \subseteq A \times B$ je zobrazení, jestliže:

$$(a,b_1) \in R \wedge (a,b_2) \in R \Rightarrow b_1 = b_2$$

Zobrazení $f \subseteq A \times B$ můžeme značit jako:

$$f : A \to B$$

Definice 5 (Inverzní relace)

Uvažujme množiny A, B a binární relaci $R \subseteq B \times A$, potom pro inverzní relaci k relaci R platí:

$$R^{-1} \subseteq B \times A, (b,a) \in R^{-1} \Leftrightarrow (a,b) \in \mathbb{R}$$

Inverzní relaci k relaci R budeme značit jako R^{-1}

Neformálně řečeno je inverzní relace k relaci R stejná, jako relace R, jen v grafické reprezentaci otočíme šipky na druhou stranu.

Definice 6 (Definiční obor)

$$D(f) = Dom(f) = \{a \in A; \exists b \in B, f(a) = b\}$$

Budeme značit $D(f)$, nebo $Dom(f)$[2].

Definice 7 (Obor hodnot)

$$H(f) = Im(f) = \{b \in B; \exists a \in A, f(a) = b\}$$

[1] funkce jim říkáme tehdy, když je cílová množina číselná.

[2] Z anglického Domain.

Budeme značit $H(f)$, nebo $Im(F)$[3].

Definice 8 (Injekce, prosté zobrazení)

Řekneme, že zobrazení $f : A \to B$ je injekce (prosté zobrazení) jestliže:

$$f(a_1) = b \land f(a_2) = b \Rightarrow a_1 = a_2$$

Jestliže zobrazení f je injekce, potom inverzní relace je opět zobrazení (a opět injekce).

Definice 9 (Surjekce)

Uvažujme zobrazení $f : A \to B$

Potom řekneme, že zobrazení f je surjekce (zobrazení na), jestliže oborem hodnot je celá cílová množina, tedy právě tehdy, když:

$$H(f) = B$$

Definice 10 (Bijekce)

Uvažujme zobrazení $f : A \to B$

Jestliže je zobrazení f surjekce a současně injekce, řekneme, že se jedná o bijekci.[4]

Pokud existuje bijekce mezi konečnými množinami A a B, potom:

$$|A| = |B|$$

Binární relace na množinách

Relací na množině se rozumí binární relace, kde jsou oba prvky kartézského součinu tatáž množina, tedy $R \subseteq A \times A$. Specialní případy:

- Reflexivní relace: $(a, a) \in R, \forall a \in A$.
- Symetrická relace: $(a, b) \in R \Rightarrow (b, a) \in R$.
- Antisymetrická relace: $(a, b) \in R \land (b, a) \in R \Rightarrow a = b$.
- Tranzitivní relace: $(a, b) \in R \land (b, c) \in R \Rightarrow (a, c) \in R$.
- Ireflexivní relace: $(a, a) \notin R, \forall a \in A$.

Definice 11 (Relace ekvivalence)

Relace, která je současně reflexivní, symetrická a tranzitivní se nazývá relace ekvivalence.

[3] Z anglického Image.

[4] Za bijekci se navíc velmi často považuje zobrazení, které je bijekce a zároveň v platí $D(f) = A$.

Relace ekvivalence vždy rozdělí původní množinu na disjunktní podmnožiny, kterým říkáme třídy ekvivalence.

Definice 12 (Relace uspořádání)

Relace, která je reflexivní, antisymetrická a tranzitivní se nazývá relace uspořádání a vytváří POSET (Partialy Ordered SET).

Operace

Operace je obecně zobrazení, konkrétní podoba tohoto zobrazení záleží na aritě operace.

Binární operace je zobrazení z kartézského součinu dvou množin do nějaké další množiny, velmi často jsou všechny tyto 3 množiny totožné.

$$f : A \times B \to C$$

Konstrukce přirozených čísel

Z axiomů teorie množin víme, že prázdná množina existuje. Definujeme unární operaci následníka:

$$A' = A \cup \{A\}$$

Opakovanou aplikací operace následníka na původně prázdnou množinu jsme schopni vytvořit všechna přirozená čísla.

$$\emptyset' = \emptyset \cup \{\emptyset\} = \{\emptyset\}$$

$$\{\emptyset\}' = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$$

Definice operace plus (+) na takto definovaných přirozených číslech:

$$A + \emptyset = A$$

$$A + B' = (A + B)'$$

Definice operace krát ($\cdot$) na takto definovaných přirozených číslech:

$$A \cdot \emptyset = \emptyset$$

$$A \cdot B' = A \cdot B + A$$

Konstrukce celých čísel

Oproti přirozeným číslům musíme přidat nulu a záporné hodnoty. Můžeme k tomu využít relaci ekvivalence.

Uvažujme dvojice přirozených čísel:

$$(a, b) \in \mathbb{N} \times \mathbb{N}$$

Potom řekneme, že:

$$(a, b) \sim (c, d) : a + d = b + c$$

Věta 1
Výše definovaná relace $\sim$ je relace ekvivalence.

Důkaz. Je třeba ověřit splnění vlastností, které z definice požadujeme od relace ekvivalence:

- $(a, b) \sim (a, b) : a + b = b + a$ Reflexivita
- $(a, b) \sim (c, d) \Rightarrow (c, d) \sim (a, b) : a + d = b + c \Rightarrow c + b = d + a$ Symetrie
- $(a, b) \sim (c, d) \wedge (c, d) \sim (e, f) \Rightarrow (a, b) \sim (e, f) : a + d = b + c \wedge c + f = d + e \Rightarrow a + f = b + e$ Tranzitivita

□

Množinu $\mathbb{N} \times \mathbb{N}$ tedy relace $\sim$ rozdělí na třídy rozkladu, kde každá třída bude tvořena uspořádanými dvojicemi, se stejným rozdílem. Tyto třídy ekvivalence mohou reprezentovat všechna celá čísla.

Konstrukce racionalních čísel

Racionální čísla narozdíl od celých a přirozených mají lepší vlastnosti, umožňují dělení. Racionální čísla jsou první obor, který se nazývá těleso, nebo také pole, pole/těleso racionálních čísel.

Uvažujme uspořádané dvojice celých čísel $(a, b) \in \mathbf{Z} \times \mathbf{Z} \setminus \{0\}$. Na takovýchto dvojicích zavedeme následující relaci: $(a, b) \sim (c, d) : a \cdot d = b \cdot c$. Kde $\cdot$ představuje násobení nad množinou celých čísel.

Opět tvrdíme, že relace $\sim$ je relace ekvivalence a zase množinu $\mathbf{Z} \times \mathbf{Z} \setminus \{0\}$ rozdělí na třídy ekvivalence, kde jednotlivé třídy mohou reprezentovat všechna racionální čísla.

2 Druhá přednáška

2.1 Algebraické struktury

Algebraická struktura je množina, na které máme jednu, nebo více operací a tyto operace mají nějaké vlastnosti. Obecně $(G, *)$ je algebraická struktura na množině G s operací *. Algebraických struktur je mnoho, nas bude zajímat převážně Grupa a Pole. Pokud bychom z následující definice grupy vypustili všechny 3 podmínky, jednalo by se o tzv. Grupoid (také označován jako Magma). Při splnění první podmínky tedy Magma a 1. podmínka, dostáváme tzv. Pologrupu. Následně Pologrupou a splněním podmínky číslo 2 dostáváme Monoid.

2.1.1 Grupa

Definice 13 (Grupa)
Grupa $(G, *)$ je algebraická struktura s jednou operací $* : G \times G \to G$, kde operace $*$ splňuje následujicíc vlastnosti:

1. $a * (b * c) = (a * b) * c \ \forall a, b, c \in G$ — *Asociativita*
2. $\exists e \in G : e * a = a * e = a \ \forall a \in G$ — *Neutrální prvek*
3. $\forall a \in G, \exists a^{-1} \in G : a * a^{-1} = a^{-1} * a = e$ — *Inverzní prvky*

Definice 14 (Komutativní „Abelova" grupa)
Pokud k požadovaným vlastnostem operace $*$ tvořící grupu přidáme ještě čtvrtou vlastnost:

4. $a * b = b * a \ \forall a, b \in G$ — *Komutativita*

Dostaneme tzv. Abelovskou grupu.

Jako příklady grupy můžeme uvést $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$ $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ všechny tyto příklady jsou dokonce abelovskou grupou. Zajímavé je zamyslet se nad příkladem neabelovské grupy, kterým může být například grupa permutací (permutace s operací skládání s třemi a více prvky). Dalším příkladem neabelovské grupy je množina čtvercových regulárních matic s operací násobení.

Věta 2
Neutrální prvek je jediný.

Důkaz. Předpokládejme, že e_1 a e_2 jsou neutrální prvky. Budeme li chtít na tyto dva neutrální prvky aplikovat operaci $*$ podle definice neutrálního prvku vezmeme e_1 jako neutrální a dostáváme:

$$e_1 * e_2 = e_2$$

Zároveň ale můžeme podle definice neutrálního prvku vzít e_2 jako neutrální a v tom případě dostáváme:

$$e_1 * e_2 = e_1$$

Z toho vyplývá, že e_1 a e_2 jsou tentýž prvek a nemůže tedy nikdy exisovat více než jeden neutrální prvek. $\square$

2.1.2 Pole

Definice 15 (Pole)

Pole $(F, +, \cdot)$ je algebraická struktura se dvěma operacemi, kde množina F má alespoň dva prvky, operace $+$ splňuje následující vlastnosti[5]*:*

1. $a + (b + c) = (a + b) + c \ \forall a, b, c \in F$ — *Asociativita*
2. $\exists 0_f \in F : 0_f + a = a + 0_f = a \ \forall a \in F$ — *Neutrální prvek*
3. $\forall a \in F, \exists -a \in F : a + (-a) = -a + a = 0_f$ — *Inverzní prvky*
4. $a + b = b + a \ \forall a, b \in F$ — *Komutativita*

a zároveň operace $\cdot$ splňuje:

1. $a \cdot (b \cdot c) = (a \cdot b) \cdot c \ \forall a, b, c \in F$ — *Asociativita*
2. $\exists 1_f \in F : 1_f \cdot a = a \cdot 1_f = a \ \forall a \in F$ — *Neutrální prvek*
3. $\forall a \in F \setminus \{0_f\}, \exists a^{-1} \in F : a \cdot a^{-1} = a^{-1} \cdot a = 1_f$ — *Inverzní prvky*
4. $a \cdot (b + c) = a \cdot b + a \cdot c \wedge (b + c) \cdot a = b \cdot a + c \cdot a \ \forall a, b, c \in F$ — *Distributivita*

Definice 16 (Komutativní pole)

Pokud se jedná o pole a navíc je operace $\cdot$ komutativní, jedná se o komutativní pole:

5. $a \cdot b = b \cdot a \ \forall a, b \in F$ — *Komutativita*

Zatím jediným příkladem pole, který z přednášek známe je $(\mathbb{Q}, +, \cdot)$.[6]

Definice 17 (Uspořádané pole)

Řekneme, že pole F je uspořádané, jestliže v něm existuje $P \subseteq F$ tak, že je li $x, y \in P$ platí $x + y \in P \wedge x \cdot y \in P$ a dále $\forall x \in F$ platí, že splňuje právě jednu z následujicích podmínek:

1. $x \in P$

[5] Všiměte si, že jsou velmi podobné požadovaným vlastnostem na operaci $*$ z definice Abelovy grupy.
[6] Dalším příkladem by mohlo být pole racionálních funkcí $\mathbb{Z}(X)$, které bylo později velmi okrajově zmíněno na přednášce.

2. $-x \in P$
3. $x = 0_F$

Jinak řečeno, uspořádané pole bude takové, ve kterém je možné nějakým způsobem vybrat „kladnou“ podmnožinu. Příklady uspořádaných polí: $\mathbb{Q}, \mathbb{R}, \mathbb{Z}(x)$

Mejme uspořádané pole dle definice 17, potom zavedeme relaci $<$ následovně:

$$a < b, \text{jestliže}\, b - a \in P$$

Taková relace je ostré uspořádání[7].

Definice 18 (Husté pole)
Řekneme, že pole F je husté, jestliže $\forall a, b \in F, a < b$ existuje $c \in F$ takové, že $a < c < b$.

Příklady hustého pole: $\mathbb{Q}, \mathbb{R}$.

Definice 19 (Archimédovské pole)
Řekneme, že uspořádané pole F je archimédovské, jestliže:

$$\forall x, y \in P\, \exists n \in \mathbb{N}, n \cdot x > y$$

Příklady archimédovských polí: $\mathbb{Q}, \mathbb{R}$

2.1.3 Konečná pole

Definice 20
Konečné pole je pole $(F, +, \cdot)$, kde množina F má konečný počet prvků.

Věta 3 (Existence konečného pole)
Konečné pole $(F, +, \cdot)$ existuje právě tehdy, když $|F| = p^k$, kde p je prvočíslo a $k \in \mathbb{N}$. Toto konečné pole je zároveň jediné.

Z věty 3 vyplývá, že existují konečná pole se dvěma prvky, třemi prvky, se čtyřmi prvky, s pěti prvky, ale ne se šesti, protože 6 není ani prvočíslo, ani mocnina prvočísla.

Konečná pole budeme značit zdvojeným fontem a počtem prvků v dolním indexu např. $\mathbb{F}_{11}$

Konečná pole si rozdělíme na dva případy a to na prvočíselná pole a na neprvočíselná pole.

Abychom porozuměli konečným polím a mohli s nimi pracovat, potřebujeme vědět, jak na nich fungují operace $+$ a $\cdot$.

[7] To znamená, že je tato relace ireflexivní a tranzitivní

Prvočíselná pole

Definice 21 (Prvočíselné pole)
Prvočíselné pole je konečné pole $(F, +, \cdot)$, kde $|F| = p$, p je prvočíslo. Tedy všechny případy, kdy pro k z věty 3 platí, že $k = 1$.

Například v prvočíselném poli $\mathbb{F}_2$ máme 2 prvky a tyto prvky můžeme označit jak chceme, pro praktické počítání je však nejlepší označit tyto prvky čísly, v tomto případě od 0 do 1, kde 0 bude hrát roli hodnoty nula a 1 roli hodnoty jedna, tak jak potřebujeme.

Příklad (Prvočíselné pole $\mathbb{F}_2$)

$$\mathbb{F}_2 = \{0, 1\}$$

+	0	1			$\cdot$	0	1
0	0	1			0	0	0
1	1	0			1	0	1

Tabulka 1: Operace + a $\cdot$ nad $\mathbb{F}_2$

Můžeme si všimnout, že u obou operací v tomto případě vlastně počítáme modulo 2, tedy modulo počet prvků pole, tato vlastnost platí obecně u prvočíselných polí.

Příklad (Prvočíselné pole $\mathbb{F}_5$)

$$\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$$

+	0	1	2	3	4			$\cdot$	0	1	2	3	4
0	0	1	2	3	4			0	0	0	0	0	0
1	1	2	3	4	0			1	0	1	2	3	4
2	2	3	4	0	1			2	0	2	4	1	3
3	3	4	0	1	2			3	0	3	1	4	2
4	4	0	1	2	3			4	0	4	3	2	1

Tabulka 2: Operace + a $\cdot$ nad $\mathbb{F}_5$

Z definice pole15 vyplývá, že $(\mathbb{F}_5, +)$ musí tvořit Abelovskou grupu. V Abelovské grupě platí, že při rozepsání operace do tabulky je v každém sloupci a v každém řádku každý prvek obsažen právě jednou[8]*. Což si můžeme všimnout že zde platí.*

[8]V počátcích definic teorie grup se tato vlastnost používala pro definici grupy.

U operace $\cdot$ si můžeme všimnout, že bez prvního sloupce a bez prvního řádku (zeleně označená část) operace $\cdot$ tvoří grupu. Tato vlastnost u pole a jeho operace $\cdot$ platí vždy.

Neprvočíselná pole

Definice 22 (Neprvočíselné pole)
Neprvočíselné pole je konečné pole $(F, +, \cdot)$, kde $|F| = p^k$, p je prvočíslo a zároveň $k > 1, k \in \mathbb{N}$. Tedy všechny případy, kdy pro k z věty 3 platí, že $k > 1$.

V případě neprvočíselných polí nebude fungování operací tak zřejmé jako tomu bylo u prvočíselných polí. Použitím stejného triku jako u prvočíselných polí, tedy použití běžných operací + a $\cdot$ modulo počet prvků, totiž nejsme schopni vytvořit pole. Problém je v takovém případě operace $\cdot$, kdy pouze s přidáním modula nebude splňovat požadované vlastnosti z definice pole15.

Opět platí, že prvky pole můžeme označit jak chceme, ale je dobré, udělat to tak, aby se nám s nimi vhodně pracovalo. V případě neprvočíselných polí je pro jejich odvození vhodné označit si prvky jako polynomy v proměnné t, kde koeficienty jsou z $\mathbb{F}_p$ až do stupně $k - 1$, kde $n = p^k$ pro $\mathbb{F}_n$.
Příklad (Definice pro $\mathbb{F}_4$)

$$4 = 2^2,\ p = 2,\ k = 2$$

Polynomy v tomto případě tedy budou:

Polynomy	0	1	t	$t + 1$
Pomyslná hodnota	0	1	2	3

Tabulka 3: Vyjádření polynomů pro $\mathbb{F}_4$

Pro vytvoření aditivní operace stačí sčítat polynomy v každém stupni modulo p.
Příklad (Tvorba aditivní operace pro $\mathbb{F}_4$)
Budeme sčítat polynomy v každém stupni modulo p

$$2 + 3 = t + (t + 1) = \begin{array}{cc} t & +0 \\ t & +1 \\ \hline 0 & +1 \end{array} = 1$$

$$1+1=1+1=\frac{\begin{array}{cc}0t & +1\\ 0t & +1\end{array}}{\begin{array}{cc}0t & +0\end{array}}=0$$

$$1+2=1+t=\frac{\begin{array}{cc}0t & +1\\ t & +0\end{array}}{\begin{array}{cc}t & +1\end{array}}=3$$

Stejným postupem pro ostatní hodnoty (některé jdou rovnou doplnit díky vlastnostem operace +) dostaneme kompletní tabulku definující aditivní operaci +.

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Tabulka 4: Aditivní operace pro $\mathbb{F}_4$

Příklad (Příklad polynomů pro $\mathbb{F}_{125}$)

$$125=5^3,\ p=5,\ k=3$$

Polynomy budou následující:

$$0,\ 1,\ 2,\ 3,\ 4,\ t,\ t+1,\ t+2,\ t+3,\ t+4, 2t+1,\ \ldots\ 4t^2+4t+3,\ 4t^2+4t+4$$

Ukázka součtu dvou polynomů:

$$(4t+2)+(t^2+2t+3)=\frac{\begin{array}{ccc}0t^2 & +4t & +2\\ t^2 & +2t & +3\end{array}}{\begin{array}{ccc}t^2 & +1t & +0\end{array}}=t^2+t$$

Při vytváření multiplikativní operace se nám stane, že po vynásobení dvou polynomů vznikne polynom stupně, který je větší, než $k-1$ a tedy není mezi polynomy daného pole. Budeme proto potřebovat tzv. redukční polynom.

Definice 23 (Redukční polynom)

Redukční polynom P_{red} : polynom stupně k, který je nerozložitelný na součin polynomů stupně nižších (řekneme, že je ireducibilní).

Příklad (Hledání redukčního polynomu pro $\mathbb{F}_4$)

Všechny polynomy stupně $k = 2$:

- t^2 *lze rozložit na* $t \cdot t$
- $t^2 + 1$ *lze rozložit na* $(t + 1) \cdot (t + 1)$
- $t^2 + t$ *lze rozložit na* $t \cdot (t + 1)$
- $t^2 + t + 1$ *nelze rozložit*

$$(t+1)\cdot(t+1) = \begin{array}{ccc} & t & +1 \\ & t & +1 \\ \hline & t & +1 \\ t^2 & +t & \\ \hline t^2 & +0t & +1 \end{array} = t^2 + 1$$

Tvorba multiplikativní operace: po vynásobení dvou prvků z $\mathbb{F}_{p^k}$ vyjádřených pomocí polynomů odečítáme (je-li třeba) $t^h \cdot P_{red}$ tak dlouho, až je výsledek stupně nejvýše $k - 1$.

Příklad (Aplikace multiplikativní operace v $\mathbb{F}_4$ a využití P_{red})

$$t \cdot (t + 1) = t^2 + t$$

Polynom t^2+t má ale příliš vysoký stupeň (vyšší, než $k-1$). Začneme proto s odečítáním redukčního polynomu[9]*, který je v tomto případě $t^2 + t + 1$.*

$$(t^2 + t) - (t^2 + t + 1) = \begin{array}{ccc} t^2 & +t & +0 \\ -(t^2 & +t & +1) \\ \hline 0t^2 & +0t & +1 \end{array} = 1$$

Příklad (Tvorba tabulky multiplikativní operace v $\mathbb{F}_4$)

Hodnoty pro 0 *a* 1 *jsou jasné. V předchozím příkladu jsme spočítali, že* $3 \cdot 2 = 1$, *díky čemuž zároveň víme že,* $2 \cdot 3 = 1$. *Ostatní hodnoty jsme již schopni doplnit díky požadovaným vlastnostem operace* $\cdot$. *Ale pojďme ověřit* $2 \cdot 2$.

[9]Můžeme odečítat i jeho t^h násobky, ale v tomto případě stačí redukční polynom sám o sobě.

$$2 \cdot 2 = t \cdot t = t^2$$

Stupeň polynomu je větší, než $k-1$. Odečteme T_{red}.

$$t^2 - (t^2 + t + 1) = \frac{\begin{array}{ccc} t^2 & +0t & +0 \\ -(t^2 & +t & +1) \end{array}}{\begin{array}{ccc} 0t^2 & +t & +1 \end{array}} = t + 1 = 3$$

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Tabulka 5: Multiplikativní operace pro $\mathbb{F}_4$

2.2 Konstrukce množiny reálných čísel

Využijeme definici reálných čísel pomocí Dedekindových řezů.

Definice 24 (Dedekindův řez)

Dedekindův řez D je podmnožina racionálních čísel $D \subseteq \mathbb{Q}$, která splňuje:

1. $x \in D \Rightarrow \exists y > x, y \in D$ *Neexistence největšího prvku*
2. $x \in D, y < x \Rightarrow y \in D$

Příklady Dedekindových řezů:

- $\mathbb{Q}$ tento řez označme ∞
- $\emptyset$ tento řez označme $-\infty$
- $\mathbb{Q}^-$
- $\{x \in \mathbb{Q}; x < 7\}$
- $\{x \in \mathbb{Q}; x \cdot x < 2 \vee x < 0\}$

Budeme li uvažovat všechny Dedekindovy řezy, dostaneme množinu rozšířených reálných čísel, kterou budeme označovat $\overline{\mathbb{R}}$.

Potom

$$\mathbb{R} = \overline{\mathbb{R}} \setminus \{-\infty, \infty\}$$

Kde $\mathbb{R}$ označuje množinu reálných čísel.

Definice 25 (Součet Dedekindových řezů)

$$D + E = \{x + y; x \in D, y \in E\}$$

Definice 26 (Nezáporný Dedekindův řez)

Řekneme, že dedekindův řez D je nezáporný právě tehdy, když:

$$D \supseteq \mathbb{Q}^-$$

Definice 27 (Součin Dedekindových řezů)

Předpokládáme, že řezy D a E jsou nezáporné.

$$D \cdot E = \{x \cdot y; \forall x, y \geq 0, x \in D, y \in E\} \cup \{z; z < 0, z \in \mathbb{Q}\}$$

Pokud je jeden z řezů záporný a druhý nezáporný, potom musíme definovat opačný řez, k zápornému řezu vyrobit řez opačný, použijeme násobení nezáporných řezů a z výsledku opět vyrobíme řez opačný.

Pokud budou oba řezy záporné, z obou řezů vezmu opačné řezy, použiji násobení nezáporných řezů a dostanu korektní výsledek. [10]

Komplexní čísla

Uvažujme $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$. V $\mathbb{R}^2$ není definována multiplukativní operace $(a, b) \cdot (c, d)$. Pokud v $\mathbb{R}^2$ multiplikativní operaci definujeme takovým způsobem, aby splňovala vlastnosti na multiplikativní operaci z definice pole15, dostáváme:

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

Což je totéž jako

$$(a + bi) \cdot (c + di) = ac + (b + d)i^2 + a \cdot di + bi \cdot c = ac - bd + (ad + bc)i, \; i^2 = -1$$

Přidáním této operace dostaneme množinu komplexních čísel $\mathbb{C}$, která opět tvoří strukturu pole.

Byly snahy tento postup zobecnit. Pro $\mathbb{R}^3$ avšak vhodná multiplikativní operace, která by vyhovovala požadavkům z definice pole15 neexistuje.

[10]Násobení dedekindových řezů bylo na přednášce definováno pouze takto částečně.

Pro $\mathbb{R}^4$ už multiplikativní operaci splňující požadované vlastnosti vytvořit lze, tím dostáváme tzv. kvaterniony, značíme je $\mathbb{H}$. Opět máme „pomůcky" a pravidla pro jejich násobení. Kvaterniony zapisujeme ve tvaru:

$$a + bi + cj + dk$$

A pravidla pro jejich násobení jsou:

1. $i^2 = j^2 = k^2 = -1$
2. $ij = -ji = k$

U kvaternionů však máme jednu změnu, nejedná se o komutativní pole (je to zřejmé z druhého pravidla) a jsou tedy prvním příkladem nekomutativního pole se kterým jsme se v přednáškách zatím setkali.

2.3 Mohutnosti nekonečných množin

Kardinalita nejvšednější nekonečné množiny, přirozených čísel, je definována jako „alef 0"

$$|\mathbb{N}| = \aleph_0$$

Jakákoliv jiná nekonečná množina bude mít stejnou kardinalitu, pokud existuje bijekce mezi touto nekonečnou množinou a množinou přirozených čísel.

$\mathbb{N}$	1	2	3	4	5	6	7	8	9	10	...
$\mathbb{N}_0$	0	1	2	3	4	5	6	7	8	9	...
$2\mathbb{N}+1$	1	3	5	7	9	11	13	15	17	19	...
$\mathbb{Z}$	0	1	-1	2	-2	3	-3	4	-4	5	...
$\mathbb{Q}$	$\frac{0}{1}$	$\frac{-1}{1}$	$\frac{-2}{1}$	$\frac{-1}{2}$	$\frac{1}{2}$	$\frac{2}{1}$	$\frac{-3}{1}$	$\frac{-1}{3}$	$\frac{1}{3}$	$\frac{3}{1}$	...

Tabulka 6: Ukázka některých bijekcí s přirozenými čísly

Z bijekcí naznačených v tabulce 6 vyplývá:

$$|\mathbb{N}| = |\mathbb{N}_0| = |2\mathbb{N}+1| = |\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$$

Mohutnost množiny reálných čísel

Mohutnost množiny reaálných čísel je větší, než mohutnost množiny celých čísel.

$$|\mathbb{R}| > |\mathbb{N}|$$

Důkaz. Neexistence bijekce mezi $\mathbb{R}$ a $\mathbb{N}$

$$\begin{array}{rccccc} a_1 = & 0, & \boxed{a_{11}} & a_{12} & a_{13} & \dots \\ a_2 = & 0, & a_{21} & \boxed{a_{22}} & a_{23} & \dots \\ a_3 = & 0, & a_{31} & a_{32} & \boxed{a_{33}} & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Tabulka 7: Seřazení hodnot reálného intervalu $\langle 0, 1)$

Předpokládejme, že bijekce mezi $\mathbb{R}$ a $\mathbb{N}$ existuje. Vezměme reálný interval $\langle 0, 1)$ a předpokládejme, že jeho prvky lze seřadit[11].

Za předpokladu, že jsme schopni hodnoty tohoto intervalu seřadit, jsme schopni je všechny reprezentovat nekonečnou tabulkou 7.

Teď vytvoříme číslo $b = 0, b_1 b_2 b_3 \dots$, kde každou číslici b_i určíme následovně:

$$b_i = \begin{cases} 1 & \text{pokud } a_{ii} \neq 1 \\ 2 & \text{pokud } a_{ii} = 1 \end{cases}$$

Tím jsme ale zkonstruovali reálné číslo b, které se liší[12] od každého čísla v tabulce 7.

Z našich předpokladů však vycházelo, že v tabulce musí být obsažena všechna čísla z daného intervalu. Dostáváme tedy spor a z toho vychází, že naše předpoklady nebyly správné a neexistuje bijekce mezi $\mathbb{N}$ a reálným intervalem $\langle 0, 1)$. Tím pádem nemůže existovat bijekce ani mezi $\mathbb{R}$ a $\mathbb{N}$.

Z důkazu nám zároveň vychází, že $|\mathbb{R}| > |\mathbb{N}|$. □

Kardinalitu reálných čísel budeme značit c

$$|\mathbb{R}| = c > \aleph_0$$

Definice 28 (Kardinalita potenčních množin přirozených čísel)

Značíme pomocí $\aleph_i$

$$|P(\mathbb{N})| = \aleph_1$$

$$|P(P(\mathbb{N}))| = \aleph_2$$

$$|P(P(P(\mathbb{N})))| = \aleph_3$$

$$\vdots$$

Kde

$$\aleph_0 < \aleph_1 < \aleph_2 < \aleph_3 \dots$$

[11] Tento předpoklad vychází z předpokladu, že existuje bijekce s $\mathbb{N}$.

[12] A to alespoň v jedné číslici na diagonále (zobrazeno modře).

Důkaz. Neexistence bijekce mezi $\mathbb{N}$ a $P(\mathbb{N})$

Předpokládejme, že $f : \mathbb{N} \to P(\mathbb{N})$ je bijekce.

Nyní uvažujme množinu

$$D = \{n \in \mathbb{N}; n \notin f(n)\}$$

D je nějaká podmnožina všech přirozených čísel a, kde bijekce f zobrazí a na podmnožinu, která číslo a neobsahuje.

Vzhledem k tomu, že $D \subseteq \mathbb{N}$, musí platit $D \in P(\mathbb{N})$, pak

$$\exists m \in \mathbb{N} : f(m) = D$$

Potom ale

$$m \in D \Leftrightarrow m \notin D$$

Čímž se dostáváme ke sporu a bijekce f jejíž existenci jsme předpokládali neexistuje. □

Není jednoznačné, zda $\aleph_1 = c$ [13].

Mohutnost množiny komplexních čísel

$$|\mathbb{C}| = |\mathbb{R}^2| = |\mathbb{R}| = c$$

Což ovšem znamená, že musíme být schopni najít bijekci mezi $\mathbb{R}$ a $\mathbb{R}^2$.

Toho dosáhneme následovně, každé reálné číslo zobrazíme na uspořádanou dvojici takto:

$$0,3451239956\ldots \to (0,35295\ldots; 0,41396\ldots)$$

Tímto způsobem jsme schopni obecně najít bijekci mezi $\mathbb{R}$ a $\mathbb{R}^n$.

[13] Jedná se o nezávislý axiom.

3 Třetí přednáška

3.1 Vektorový prostor

Definice 29 (Vektorový prostor)

Vektorový prostor je především Abelovská grupa

$$(\mathcal{V}, +)$$

Kromě operace + budeme mít další operaci vztaženou k nějakému poli $(F, +, \cdot)$ *a to operaci*

$$\cdot : F \times \mathcal{V} \to \mathcal{V}$$

této operaci budeme říkat násobení skalárem a bude mít následující vlastnosti:

1. $a \cdot (\vec{u} + \vec{v}) = a \cdot \vec{u} + a \cdot \vec{v}, \forall a \in F \ \forall \vec{u}, \vec{v} \in \mathcal{V}$
2. $(a + b) \cdot \vec{u} = a \cdot \vec{u} + b \cdot \vec{u}, \forall a, b \in F \ \forall \vec{u} \in V$
3. $(a \cdot b) \cdot \vec{u} = a \cdot (b \cdot \vec{u}), \forall a, b \in F \ \forall \vec{u} \in V$
4. $1 \cdot \vec{u} = \vec{u}, \forall \vec{u} \in \mathcal{V}$

Tedy pokud máme nějaké pole F, nějakou abelovskou grupu $\mathcal{V}$ a definovanou operaci násobení skalárem $\cdot$ s uvedenými vlastnostmi. Potom řekneme, že $\mathcal{V}$ je vektorovým prostorem nad polem F.

Prvkům $\mathcal{V}$ pak budeme říkat vektory. Prvkům F často říkáme skaláry, nebo čísla.

Příklad (Příklad vektorového prostoru)

$$F = \mathbb{R}, \mathcal{V} = \mathbb{R}^3$$

$$\vec{u} + \vec{v} = (u_1 + v_1, u_2 + v_2, u_3 + v_3) \forall \vec{u}, \vec{v} \in \mathcal{V}$$

Je $(\mathcal{V}, +)$ abelovská grupa?

0. *Operace + je zjevně uzavřená na množině $\mathbb{R}^3$.*
1. *Asociativita vychází z asociativity sčítání v $\mathbb{R}$.*
2. *Neutrálním prvkem je: $\vec{o} = (0, 0, 0)$.*
3. *Inverzní prvek k prvku u dostaneme jako: $-\vec{u} = (-u_1, -u_2, -u_3)$.*
4. *Komutativita je v tomto případě také jasná.*

$(\mathcal{V}, +)$ je tedy abelovská grupa[14].

operaci násobení skalárem $\cdot$ zavedeme takto:

$$a \cdot (u_1, u_2, u_3) = (a \cdot u_1, a \cdot u_2, a \cdot u_3)$$

Je zřejmé, že tato operace splňuje všechny požadované vlastnosti z definice vektorového prostoru 29. Pojďme ověřit například třetí vlastnost:

Důkaz. Platnost třetí vlasnosti:

$$LS : (a \cdot b) \cdot (u_1, u_2, u_3) = (a \cdot b \cdot u_1, a \cdot b \cdot u_2, a \cdot b \cdot u_3)$$

$$PS : a \cdot (b \cdot (u_1, u_2, u_3)) = a \cdot (b \cdot u_1, b \cdot u_2, b \cdot u_3) = (a \cdot b \cdot u_1, a \cdot b \cdot u_2, a \cdot b \cdot u_3)$$

$$LS = PS$$

□

Ověření platnosti požadovaných vlastností bylo v případě 3.1 triviální. Podobně jednoduchý postup by šel použít i pro případy, kdy obecně $\mathcal{V} = \mathbb{R}^n, \forall n \in \mathbb{N}$. Existují však příklady, ke kterým se dostaneme později, kdy ověření platnosti není tak jednoduché.

Definice 30 (Triviální vektorový prostor)

Uvažujme libovolné pole F a abelovskou grupu

$$(\mathcal{V}, +), \mathcal{V} = \{\vec{o}\}$$

Což je zároveň minimální případ grupy, protože ta z definice vždy musí obsahovat minimálně jeden prvek, kterým je neutrální prvek.

A operaci násobení skalárem zavedeme takto:

$$a \cdot \vec{o} = \vec{o}, a \in F, \vec{o} \in \mathcal{V}$$

Opět budou splněny všechny požadované vlastnosti, jedná se tedy o vektorový prostor a tento vektorový prostor budeme označovat jako triviální vektorový prostor.

Dalším jednoduchý příklad vektorového prostorů: libovolné pole F, $\mathcal{V} = F^n, n \in \mathbb{N}$

Příklad (Je $\mathbb{R}$ vektorový prostor nad $\mathbb{Q}$?)

[14] Otázka k zamyšlení je, zda by bylo možné operaci + zavést nějak jinak a stále dodržet všechny požadované vlastnosti.

$$F = \mathbb{Q}, \mathcal{V} = \mathbb{R}$$

Víme, že $\mathbb{R}$ s běžnou operací + tvoří Abelovskou grupu. Násobení skalárem zavedeme jako běžné násobení. To že platí vlastnosti z definice vektorového prostoru29 plyne z vlastností bežné operace násobení $\cdot$ na množině $\mathbb{R}$.

Takže ano, v tomto případě se jedná o vektorový prostor.

Další příklady vektorových prostorů:

- $F = \mathbb{R}, \mathcal{V} = C^0\langle a, b\rangle$ [15]
- $F = \mathbb{R}, \mathcal{V} = C^1\langle a, b\rangle$
- $F = \mathbb{R}, \mathcal{V} =$ množina matic o velikosti $n \times n$
- $F = \mathbb{Q}, \mathcal{V} = \mathbb{R}$
- $F = \mathbb{R}, \mathcal{V} = \mathbb{C}$
- A dokonce i $F = \mathbb{C}, \mathcal{V} = \mathbb{R}$, v tomto případě však bude vytvoření vhodných operací netriviální.

Definice 31 (Vektorový podprostor)
Nechť $\mathcal{V}$ je vektorový prostor

$$\mathcal{W} \subseteq \mathcal{V}$$

A zároveň platí tyto vlastnosti:

1. $\vec{u}, \vec{v} \in \mathcal{W} \Rightarrow \vec{u} + \vec{v} \in \mathcal{W}$
2. $\vec{u} \in \mathcal{W}, a \in F \Rightarrow a \cdot \vec{u} \in \mathcal{W}$

Pokud je $\mathcal{W}$ podmnožina $\mathcal{V}$ a zároveň splňuje dvě výše uvedené vlastnosti, potom řekneme, že $\mathcal{W}$ je vektorovým podprostorem vektorového prostu $\mathcal{V}$.

Sjednocení dvou vektorových podprostorů obecně není vektorový podprostor. Naopak průnik podprostorů je vždy podprostor.

Příklad (Ověření vektorového podprostoru)
Mějme

$$F = \mathbb{R}, \mathcal{V} = \mathbb{R}^3$$

$$\mathcal{W}_1 = \{(a, 2 \cdot a, 1), a \in \mathbb{R}\}$$

Je $\mathcal{W}_1$ vektorový podprostor $\mathcal{V}$?

[15] $C^n\langle a, b\rangle$ značí množinu funkcí na reálném intervalu $\langle a, b\rangle$, které jsou spojité až do n-té derivace, $n \in \mathbb{N}$.

0. Je zřejmé, že $\mathcal{W}_1 \subseteq \mathbb{R}^3$

1. $(a, 2 \cdot a, 1) + (b, 2 \cdot b, 1) = (a + b, 2 \cdot a + 2 \cdot b, 2) \notin \mathcal{W}_1$

První podmínka tedy není splněna a $\mathcal{W}_1$ v tomto případě není vektorovým podprostorem vektorového prostoru $\mathcal{V}$.

Nyní uvažme $\mathcal{W}_2$ definované následovně:

$$\mathcal{W}_2 = \{(a, 2 \cdot a, 0), a \in \mathbb{R}\}$$

0. Opět je zřejmé, že $\mathcal{W}_2 \subseteq \mathbb{R}^3$

1. $(a, 2 \cdot a, 0) + (b, 2 \cdot b, 0) = (a + b, 2 \cdot (a + b), 0) = (c, 2 \cdot c, 0) \in \mathcal{W}$

2. $a \cdot (b, 2b, 0) = (a \cdot b, 2 \cdot a \cdot b, 0) = (c, 2c, 0) \in \mathcal{W}$

Všechny požadované vlastnosti platí a $\mathcal{W}$ je tedy vektorový podprostor vektorového prostoru $\mathcal{V}$.

3.2 Matice

Intuitivně můžeme matici definovat jako čísla, která jsou uspořádaná do obdélníkového schématu.
Definice 32 (Matice)
Uvažujme zobrazení a definované takto:

$$a = \{1 \dots m\} \times \{1 \dots n\} \to F$$

Toto zobrazení vlastně přiřazuje dvojici indexů (sloupcový a řádkový) hodnotu, která se v matici nachází na daném indexu. Indexy budeme značit dolním indexem jako a_{mn}

Psát matice jako zobrazení by bylo silně nepraktické, proto nadále budeme využívat právě ono uspořádání čísel do obdélníkového schématu a označovat je velkými písmeny.

Prvky $a_{11}, a_{22}, \dots, a_{kk}, k = min(m, n)$ budeme označovat jako hlavní diagonálu.

Dále budeme často používat indexování pomocí i, j, kde

$$i = 1, \dots, m$$

$$j = 1, \dots, n$$

Příklad (Matice)

Mějme matici A definovanou takto:

$$A = \begin{pmatrix} 3 & 2 & 1 & -5 \\ 2 & \sqrt{2} & 3 & -\frac{1}{3} \end{pmatrix}$$

Potom $a(2,2) = a_{22} = \sqrt{2}$, $a(2,4) = a_{24} = -\sqrt{13}$

3.3 Speciální případy matic

Mezi maticemi rozlišujeme celou řadu speciálních případů. Některé z nich jsou pouze pro případ matic čtvercových, ale některé se dají definovat i obecně pro obdélníkové matice.

Definice 33 (Horní trojúhelníková matice)

Jestliže jsou v matici A všechny prvky pod hlavní diagonálou 0, řekneme že matice A je horní trojúhelníková.

Řečeno formálně, v matici musí platit:

$$i < j \Rightarrow a_{ij} = 0$$

Podobně je definovaná dolní trojúhelníková matice, pouze se $i < j$ *změni na* $i > j$.

Definice 34 (Diagonální matice)

Jestliže jsou v matici A všechny prvky mimo hlavní diagonálou 0, řekneme že matice A je diagonální.

Řečeno formálně, v matici musí platit:

$$i \neq j \Rightarrow a_{ij} = 0$$

Definice 35 (Nulová matice)

Jestliže jsou v matici A všechny prvky 0, řekneme že matice A je nulová.

Řečeno formálně, v matici musí platit:

$$\forall i, j : a_{ij} = 0$$

Definice 36 (Jednotková matice)

Jestliže je matice A diagonální a zároveň jsou všechny hodnoty na hlavní diagonále 1, řekneme, že matice A je jednotková.

Řečeno formálně, v matici musí platit:

$$a_{ij} = \delta_{ij}{}^{16} = \begin{cases} 1 & pro\ i = j \\ 0 & pro\ i \neq j \end{cases}$$

Jednotkovou matici budeme značit E.

[16] Kroneckerovo delta

3.4 Základní operace na maticích

Množinu všech matic o m řádcích a n sloupcích nad polem F budeme označovat následovně

$$Mat_{m,n}(F)$$

Definice 37 (Součet matic)

$$+ : Mat_{m,n}(F) \times Mat_{m,n}(F) \to Mat_{m,n}(F)$$

$$c_{ij} = a_{ij} + b_{ij} \; \forall i, j$$

Tato operace je uzavřená, asociativní, má definovaný neutrální i inverzní prvek a navíc je komutativní.

A tvoří tedy Abelovskou grupu $(Mat_{m,n}(F), +)$

Definice 38 (Násobení matice skalárem)

$$\cdot : F \times Mat_{m,n}(F) \to Mat_{m,n}(F)$$

$$b_{ij} = k \cdot a_{ij}$$

Tato operace splňuje požadavky pro operaci násobení skalárem z definice vektorového prostoru 3.1.

A $Mat_{m,n}(F)$ *v kombinaci s operací + z definice součtu matic37 a s touto operací · tvoří vektorový prostor:*

$$(Mat_{m,n}(F), +, \cdot)$$

Definice 39 (Transpozice matice)

$$Mat_{m,n}(F) \to Mat_{m,n}(F)$$

$$B = A^T$$

$$b_{ji} = a_{ij}$$

$$(A^T)^T = A$$

$$(A + B)^T = A^T + B^T$$

Definice 40 (Násobení matic)

$$\cdot : Mat_{m,n}(F) \times Mat_{m,p}(F) \to Mat_{m,p}(F)$$

$$c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}$$

Tato operace nemusí být vždy definována (musí správně sedět dimenze). Je to operace asociativní. Ale není komutativní.

Omezíme li se na čtvercové regulární matice řádu n, dostaneme v kombinaci s touto operací strukturu grupy.

4 Čtvrtá přednáška

4.1 Vektorové prostory

Definice 41 (Lineární obal)

Mějme množinu $M \subseteq \mathcal{V}$

Budeme uvažovat průnik všech vektorových podprostorů vektorového prostoru $\mathcal{V}$*, které obsahují M. Množinu která z těchto průniků vznikne označíme jako lineární obal množiny M.*

Lineární obal množiny M budeme označovat jako $\langle M \rangle$

Definice 42 (Lineární kombinace)

Mějme nějaké vektory:

$$\vec{u_1}, \ldots, \vec{u_n}$$

Potom můžeme uvažovat jiný vektor $\vec{v}$ *ve tvaru:*

$$\vec{v} = c_1 \cdot \vec{u_1} + \ldots + c_n \cdot \vec{u_n}$$

Takovému vektoru v potom říkáme lineární kombinace věktorů $u_1, \ldots, u_n$

Zároveň platí, že vektor $\vec{v}$ *je lineárně zásivlý na vektorech* $\vec{u_1}, \ldots, \vec{u_n}$

Věta 4 (Rovnost množiny všech lin. kombinací a lineárního obalu)

Mějme množinu $M \subseteq \mathcal{V}$

Pro zjednodušení označme množinu všech lineárních kombinací vektorů z množiny M jako lcM[17]

Potom tvrdíme:

$$\langle M \rangle = lcM$$

Důkaz. Chceme ukázat, že platí:

$$\langle M \rangle \subseteq lcM \wedge \langle M \rangle \supseteq lcM$$

Pomocné tvrzení: lcM je vektorový podprostor:

1. Sečtením dvou lineárních kombinací z lcM dostaneme opět lineární kombinaci z lcM.

2. Vynásobením lineární kombinace z lcM skalárem dostáváme lineární kombinaci z lcM.

lcM je tedy vektorový podprostor. A pro každý vektor $\vec{v} \in M$ určitě existuje lineární kombinace $\vec{c}$ taková, že $\vec{v} = \vec{c} \cdot lcM$ tedy určitě obsahuje M.

[17] Pouze dočasně, toto označení nebudeme běžně používat.

Důkaz pro $\langle M\rangle \subseteq lcM$: plyne z toho, že lcM je vektorový podprostor obsahujicí M a z toho, že $\langle M\rangle$ je průnik všech takových vektorových podprostorů. A průnik je určitě podmnožinou.

Důkaz pro $\langle M\rangle \supseteq lcM$:

$$\vec{v} \in lcM \Rightarrow \vec{v} = c_1 \cdot \vec{u_1} + \ldots + c_n \cdot \vec{u_n}, \vec{u} \in M$$

Potom:

$$\vec{u_i} \in \mathcal{W}\ \forall \text{ vektorové podprostory } \mathcal{W} \subseteq \mathcal{V}$$

$$c_1 \cdot \vec{u_1} + \ldots + c_n \cdot \vec{u_n}\ \forall \text{ vektorové podprostory } \mathcal{W} \subseteq \mathcal{V}$$

to znamená, že $\vec{v} \in \bigcap_i \mathcal{W}_i$ □

Označení lcM nebudeme nadále používat, protože jak jsme ukázali, jedná se vlastně o ekvivalentní definici lienárního obalu.

Definice 43 (Lineární nezávislost vektorů)

Uvažujme množinu vektorů:

$$(\vec{u_1}, \ldots, \vec{u_n})$$

Řekneme, že vektory $\vec{u_1}, \ldots, \vec{u_n}$ jsou lineárně nezávislé, jestliže:

$$c_1 \cdot \vec{u_1} + \ldots + c_n \cdot \vec{u_n} = \vec{o} \Rightarrow \forall c_i = 0$$

Definice 44 (Báze vektorového podprostoru)

Báze $\mathcal{B}$ vektorového podprostoru $\mathcal{W}$ je uspořádaná n-tice lineárně nezávislých vektorů, které generují $\mathcal{W}$. Kde generují znamená, že $\langle\mathcal{B}\rangle = \mathcal{W}$.

Příklad (Příklad báze vektorového podprostoru)

$$\mathcal{W} = \mathcal{V} = \mathbb{R}^3$$

$$\mathcal{B} = \big((1,0,0),(0,1,0),(0,0,1)\big)$$

Je $\mathcal{B}$ báze vektorového podprostoru $\mathcal{W}$?

1. $(a,b,c) = a\cdot(1,0,0) + b\cdot(0,1,0) + c\cdot(0,0,1)$ *$\mathcal{B}$ generuje celé $\mathcal{W}$*
2. $c_1\cdot(1,0,0) + c_2\cdot(0,1,0) + c_3\cdot(0,0,1) = (0,0,0) \Rightarrow c_1 = 0, c_2 = 0, c_3 = 0$ *$\mathcal{B}$ je lineárně nezávislé*

A $\mathcal{B}$ je tedy báze vektorového podprostoru $\mathcal{W}$.

Definice 45 (Dimenze vektorového prostoru)

Počet prvků báze $\mathcal{B}$ budeme označovat jako dimenzi vektorového prostoru $\langle\mathcal{B}\rangle$

Příklad (Báze vektorového prostoru matic)

Uvažujme:

$$\mathcal{V} = Mat_{2,3}(\mathbb{R})$$

Potom bázi můžeme určit jako:

$$\mathcal{B} = \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right)$$

A vidíme, že dimenze tohoto vektorového prostoru je 6.

Což dává smysl mimo jiné díky tomu, že v případě $Mat_{2,3}$ v podstatě pracujeme s $\mathbb{R}^6$ pouze s tím, že jsme prvky uspořádali do obdélníku. Tato změna uspořádání nemá z hlediska aditivní grupy a vektorového prostoru jako takového žádný zvláštní význam a změna se projeví až ve chvíli, kdy začneme matice násobit.

4.1.1 Speciální zobrazení mezi vektorovými prostory

Definice 46 (Homomorfismus vektorovych prostorů)

Uvažujme dva vektorové prostory $\mathcal{V}, \mathcal{W}$ a zobrazení φ:

$$\varphi = \mathcal{V} \to \mathcal{W}$$

kde φ bude mít následujicí vlastnosti:

1. $\varphi(\vec{v_1} + \vec{v_2}) = \varphi(\vec{v_1}) + \varphi(\vec{v_2})\ \forall \vec{v_1}, \vec{v_2} \in \mathcal{V}$ *Zachování součtu*

2. $\varphi(k \cdot v) = k \cdot \varphi(\vec{v})\ \forall \vec{v} \in \mathcal{V}\ \forall k \in F$ *Zachování násobení skalárem*

Neformálně řeceno φ je zobrazení, které zachovává operace.

Potom zobrazení φ nazýváme homomorfismus[18] *(vektorových prostorů).*

Příklad (Homomorfismus vektorových prostorů)

$$\mathcal{V} = \mathbb{R}^2, \mathcal{W} = \mathbb{R}^4$$

$$\varphi(\vec{v}) = \vec{w}$$

$$\vec{w} = (v_1, 0, v_1, v_1 + v_2)$$

$$\varphi\big((1,2)\big) = (1,0,1,3)$$

Je takto definované φ homomorfismus? Musí platit podmínky z definice homomorfismu 46.

[18] Někdy se také používá pojem lineární zobrazení.

První podmínka:

$$LS = \varphi(\vec{u} + \vec{v}) = \varphi(u_1 + v_1, 0, u_1 + v_1 + u_2 + v_2), \vec{u}, \vec{v} \in \mathbb{R}^2$$

$$PS = \varphi(\vec{u}) + \varphi(\vec{v}) = (u_1, 0, u_1 + u_2) + (v_1, 0, v_1 + v_2) = (u_1 + v_1, 0, u_1 + u_2 + v_1 + v_2), \vec{u}, \vec{v} \in \mathbb{R}^2$$

$$LS = PS$$

První podmínka tedy platí a stejným postupem by bylo možné ukázat i platnost druhé podmínky, jedná se tedy o homomorfismus.

Definice 47 (Jádro a obraz homomorfismu)

Uvažujme vektorový prostor $\mathcal{V}$ a homomorfismus φ, potom je kernel ker *homomorfismu φ definován takto:*

$$ker\,\varphi = \{\vec{v} \in \mathcal{V}; \varphi(\vec{v}) = \vec{o}\}$$

A obraz im homomorfismu φ je definován takto:

$$im\,\varphi = \{\vec{w} \in \mathcal{W}; \exists \vec{v} \in \mathcal{V} \text{ tak, že } \varphi(\vec{v}) = \vec{w}\}$$

Věta 5 (*ker* φ a *im* φ jsou vektorové podprostory $\mathcal{V}$ a $\mathcal{W}$ v tomto pořadí)

1. *ker φ je vektorový podprostor $\mathcal{V}$, kde $\mathcal{V}$ je z definice 46.*
2. *im φ je vektorový podprostor $\mathcal{W}$, kde $\mathcal{W}$ je z definice 46.*

Důkaz.

1. $\vec{u}, \vec{v} \in ker\,\varphi : \varphi(\vec{u}) = \vec{o},\ \varphi(\vec{v}) = \vec{o}$
   $\varphi(\vec{u} + \vec{v}) = \varphi(\vec{u}) + \varphi(\vec{u})$[19] $= \vec{o} + \vec{o} = \vec{o}$
2. $\vec{u} \in ker\,\varphi$
   $\varphi(k \cdot \vec{u}) = k \cdot \varphi(u)$[20] $= k \cdot \vec{o} = \vec{o}$

Ukázali jsme, že *ker* φ splňuje všechny podmínky k tomu, aby byl vektorový podprostor $\mathcal{V}$.

Podobným způsobem bychom ukázali i druhou část věty o *im* φ a došli také ke kladnému závěru. □

Definice 48 (Monomorfismus)

Jestliže je homomorfismus injektivní, nazýváme ho monomorfismus.

Definice 49 (Epimorfismus)

Jestliže je homomorfismus surjektivní, nazýváme ho epimorfismus.

[19] Vychází z vlastností homomorfismu.
[20] Z definice homomorfismu

Definice 50 (Izomorfismus)

Jestliže je homomorfismus bijektivní, nazýváme ho izomorfismus.

Definice 51 (Endomorfismus)

Jestliže má homomorfismus φ výchozí i cílovou množinu totožnou, tedy:

$$\varphi : V \to V$$

nazveme ho endomorfismus.

Intuitivně můžeme říct, že se jedná o homomorfismus do sebe sama.

Definice 52 (Automorfismus)

Homomorfismu, který je endomorfismem a současně izomofismem nazveme automorfismus.

Věta 6

$$\varphi : \mathcal{V} \to \mathcal{W} \text{ je epimorfismus } \Leftrightarrow im\, \varphi = \mathcal{W}$$

Věta 7

$$\varphi : \mathcal{V} \to \mathcal{W} \text{ je monomorfismem } \Leftrightarrow ker\, \varphi = \{\vec{o}\}$$

Důkaz. Dokažme, že $\varphi : \mathcal{V} \to \mathcal{W}$ není monomorfismem $\Leftrightarrow ker\, \varphi \neq \{\vec{o}\}$

Důkaz pro $\varphi : \mathcal{V} \to \mathcal{W}$ není monomorfismem $\Rightarrow ker\, \varphi \neq \{\vec{o}\}$:

Předpokládejme, že φ nená monomorfismus, to znamená, že φ není inejktivní.

To, že φ není injektivní znamená, že existují nějaké vektory $\vec{u}, \vec{v} \in \mathcal{V}$, pro které:

$$\vec{u} \neq \vec{v}, \varphi(\vec{u}) = \varphi(\vec{v})$$

potom

$$\varphi(\vec{u} - \vec{v}) =^{21} \varphi(\vec{u}) - \varphi(\vec{u}) = \vec{o}$$

Ovšem $\vec{u}$ je různé od $\vec{v}$ a tedy:

$$\vec{u} - \vec{v} \in ker\, \varphi$$

A $\vec{u} - \vec{v}$ je nulový vektor, takže jádro je netriviální.

Důkaz pro $\varphi : \mathcal{V} \to \mathcal{W}$ není monomorfismem $\Leftarrow ker\, \varphi \neq \{\vec{o}\}$:

Předpokládejme, že $im\, \varphi$ je netriviální a ukážeme, že pak zobrazení nemůže být homomorfismem.

[21] Tato rovnost vychází z definice homomorfismu.

Z předpokladu netriviálního jádra:

$$\exists \vec{v} \neq \vec{o}, \vec{v} \in \mathcal{V} \text{ tak, že } \varphi(\vec{v}) = \vec{o}$$

$$\vec{u} \in \mathcal{V} \ \varphi(\vec{u}) = \vec{w} \in \mathcal{W}$$

$$\varphi(\vec{u} + \vec{v}) = \varphi(\vec{u}) + \varphi(\vec{v}) = \vec{w} + \vec{o} = \vec{w}$$

□

4.2 Matice

Definice 53 (Stopa)

Stopa je definována pro čtvercové matice. Jedná se o zobrazení, které čtvercové matici přiřadí jedno číslo. Stopu budeme značit tr[22]

$$tr : Mat_n(F) \to F$$
$$tr(A) = \sum_{i=1}^{n} a_{ii}$$

Vlastnosti:

- $tr(A^T) = tr(A)$
- $tr(A + B) = tr(A) + tr(B)$
- $tr(k \cdot A) = k \cdot tr(A)$
- $tr(A \cdot B) = tr(B \cdot A)$[23]

Důkaz. ($tr(A \cdot B) = tr(B \cdot A)$)

$$C = AB, D = BA$$
$$tr(AB) = \sum_{i=1}^{n} \sum_{k=1}^{n} a_{ik} \cdot b_{ki}$$
$$tr(BA) = \sum_{i=1}^{n} \sum_{k=1}^{n} b_{ik} \cdot a_{ki} = \sum_{i=1}^{n} \sum_{k=1}^{n} a_{ki} \cdot b_{ik} = \sum_{k=1}^{n} \sum_{i=1}^{n} a_{ik} \cdot b_{ki} = \sum_{i=1}^{n} \sum_{k=1}^{n} a_{ik} \cdot b_{ki}$$

□

[22] Z anglického trace.
[23] Zajímavé však je, že $tr(ABC) \neq tr(ACB)$

Definice 54 (Determinant)

Determinant budeme definovat pro čtvercové matice. Opět se jedná o zobrazení, které čtvercové matici přiřadí jedno číslo. Determinant matice A budeme značit det A, nebo také |A|.

$$det : Mat_n(F) \to F$$

$$det\,A = \sum_{\sigma \in S_n} sgn(\sigma) \cdot a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdot \ldots \cdot a_{n\sigma(n)}$$

Pří výpočtu podle vzorce je vhodné postupovat tak, že u řádkových indexů, začneme od jedničky a postupně zvyšujeme řádkový index a u sloupcových indexů uvažujeme všechny možné permutace n prvkové množiny těchto sloupcových indexů, tím nám vznikne nějaká permutace, která je buďto sudá, nebo lichá a danému součinu přiřadíme znaménko permutace.

Příklad (Výpočet determinantu pro matice řádu 1)

$$n = 1 : S_1 = \{1\}$$

$$det\,A = a_{11}$$

Příklad (Výpočet determinantu pro matice řádu 2)

$$n = 2 : S_2 = \{(1, 2), (2, 1)\}$$

$$det\,A = a_{11} \cdot a_{22} - a_{12} \cdot a_{21}$$

Příklad (Výpočet determinantu pro matice řádu 3)

$$n = 3 : S_3 = \{(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1)\}$$

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

Definice 55 (Schodovitá matice)

Je horní trojúhelníková matice, ve které můžeme nulovou část oddělit "schody", které mají výšku stupně 1.

5 Pátá přednáška

5.1 Metody pro výpočet determinantu

Vzorec pro obecný výpočet determinantu 54 vyžaduje všechny permutace řádkových indexů, pro matici řádu n je takových permutací $n!$ a jejich počet tak roste velmi rychle s řádem matice. Je proto komplikované tímto způsobem spočítat determinanty větších matic.

Dost často se v praxi vyskytují matice, které jsou nějakým způsobem speciální a to hlavně tím, že buď'to obsahují řádek, případně sloupec s hodně nulami, nebo nějakou jednoduchou úpravou můžeme takový řádek s hodně nulami do matice dostat. V takovém případě je možné použít následující metody a výpočet determinantu zefektivnit.

Pokud však takový řádek/sloupec s hodně nulami v matici neexistuje, nebo je jich tam velice málo, aplikováním těchto metod si příliš nepomůžeme a stále se bude jednat o problém s časovou náročností $n!$.

5.1.1 Laplaceova metoda

Laplaceova metoda rozvoje podle vybraného řádku, nebo podle vybraného sloupce. Vybereme řádek/sloupec podle kterého chceme rozvoj udělat, index tohoto řádku/sloupce označme jako i a následně pomocí tohoto řádku výpočet determninantu matice řádu n rozložit na součet n determninantů matice řádu $n-1$ vynásobené hodnotami z řádku/sloupce, podle kterého jsme rozvoj vytvářeli.

$$|A| = (-1)^{i+1} \cdot a_{i1} \cdot M_{i1} + (-1)^{i+2} \cdot a_{i2} \cdot M_{i2} + \ldots + (-1)^{i+n} \cdot a_{in} \cdot M_{in}$$
$$|A| = \sum_{j=1}^{n} (-1)^{i+j} \cdot a_{ij} \cdot M_{ij}$$

Kde M_{ij} představuje minor vzniklý vynecháním i-tého řádku a j-tého sloupce.

Mějme matici řádu 3:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Vyberme pro aplikaci Laplaceova rozvoje první řádek a zamysleme se, v jakých všech součinech bude figurovat jeho první člen a_{11}:

$$M_{a_{11}} = a_{11} \cdot a_{22} \cdot a_{33} - a_{11} \cdot a_{23} \cdot a_{32}$$

Když z $M_{a_{11}}$ vytkneme a_{11}, dostáváme:

$$M_{a_{11}} = a_{11} \cdot (a_{22} \cdot a_{33} - a_{23} \cdot a_{32}) = a_{11} \cdot \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix}$$

Totéž pro a_{12}:

$$M_{a_{12}} = a_{12} \cdot a_{23} \cdot a_{31} - a_{12} \cdot a_{21} \cdot a_{33}$$

$$M_{a_{12}} = a_{12} \cdot (a_{23} \cdot a_{31} - a_{21} \cdot a_{33}) = -a_{12} \cdot \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix}$$

Proto:

$$det(A) = a_{11} \cdot \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \cdot \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \cdot \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$$

Znaménka u jednotlivých prvků plynou ze znamének permutací ve výpočtu determinantu, můžeme však použít pomůcku, která říká, že pokud součet indexů prvku pro který počítáme minor bude sudý, bude mít znaménko + a pokud bude součet lichý, bude mít znaménko −.

Postup, který byl naznačen na matici řádu 3 funguje obecně pro libovolné matice řádu n.

Příklad (Výpočet determinantu pomocí Laplaceova rozvoje)

$$d = \begin{vmatrix} 2 & 1 & 5 & -1 & 0 \\ 3 & 2 & 4 & 0 & 0 \\ 1 & 0 & -2 & 1 & 1 \\ 3 & 2 & 0 & 5 & 0 \\ 2 & 0 & -2 & 4 & 9 \end{vmatrix}$$

$$d = 1 \cdot \begin{vmatrix} 2 & 1 & 5 & -1 \\ 3 & 2 & 4 & 0 \\ 3 & 2 & 0 & 5 \\ 2 & 0 & -2 & 4 \end{vmatrix} + 9 \cdot \begin{vmatrix} 2 & 1 & 5 & -1 \\ 3 & 2 & 4 & 0 \\ 1 & 0 & -2 & 1 \\ 3 & 2 & 0 & 5 \end{vmatrix}$$

$$d = -3 \cdot \begin{vmatrix} 1 & 5 & -1 \\ 2 & 0 & 5 \\ 0 & -2 & 4 \end{vmatrix} + 2 \cdot \begin{vmatrix} 2 & 5 & -1 \\ 3 & 0 & 5 \\ 2 & -2 & 4 \end{vmatrix} - 4 \cdot \begin{vmatrix} 2 & 1 & -1 \\ 3 & 2 & 5 \\ 2 & 0 & 4 \end{vmatrix} + 9 \cdot \left(-3 \cdot \begin{vmatrix} 1 & 5 & -1 \\ 0 & -2 & 1 \\ 2 & 0 & 5 \end{vmatrix} + 2 \cdot \begin{vmatrix} 2 & 5 & -1 \\ 1 & -2 & 1 \\ 3 & 0 & 5 \end{vmatrix} - 4 \cdot \begin{vmatrix} 2 & 1 & -1 \\ 1 & 0 & 1 \\ 3 & 2 & 5 \end{vmatrix} \right)$$

S použitím této metody je možné také vybrat více řádků/sloupců současně, což v některých případech může být výhodné.

Mějme matici A řádu n a indexy

$$i, j = 1, \dots n$$

Potom vybereme řádky

$$i_1 \dots i_q, 1 \leq q \leq n$$

Potom:

$$det(A) = (-1)^{i_1+\dots i_q+1+\dots+q} A_{i_1,\dots,i_q;1,\dots,q} M_{i_1,\dots,i_q;1,\dots,q} + \dots + (-1)^{i_1,\dots,i_q;n-q+1,\dots,n} \cdot A_{i_1,\dots,i_q;n-q+1,\dots,n} M_{i_1,\dots,i_q;n-q+1,\dots,n}$$

Příklad (Laplaceova metoda s výběrem více řádků/sloupců)

$$d = \begin{vmatrix} 2 & 1 & 0 & 1 & 5 \\ 0 & 0 & 2 & 0 & 7 \\ 3 & 1 & 5 & 2 & -2 \\ 1 & 0 & 0 & 0 & 0 \\ 2 & 5 & 2 & 3 & -8 \end{vmatrix}$$

$$d = (-1)^{2+4+1+2} \cdot \begin{vmatrix} 0 & 0 \\ 1 & 0 \end{vmatrix} \cdot \begin{vmatrix} 0 & 1 & 5 \\ 5 & 2 & -2 \\ 2 & 3 & -8 \end{vmatrix} \dots$$

Takových členů bude obecně $\binom{n}{q}$, kde q označuje počet vybraných řádků/sloupců v tomto případě tedy $\binom{5}{2}$. Díky vhodně vybraným řádkům pro vytvoření rozvoje však velká část těchto členů bude ve výsledku nulová a ty můžeme tedy stejně jako v předchozím příkladu rovnou vynechat a psát pouze ty nenulové a stejně tak můžeme rovnou vyjádřit hodnotu subdeterminantu, pokud je zřejmá.

$$d = -2 \cdot \begin{vmatrix} 1 & 1 & 5 \\ 1 & 2 & -2 \\ 5 & 3 & -8 \end{vmatrix} - 7 \cdot \begin{vmatrix} 1 & 0 & 1 \\ 1 & 5 & 2 \\ 5 & 2 & 3 \end{vmatrix}$$

5.2 Inverzní matice

Definice 56 (Algebraický doplňek)

Algebraický doplněk prvku a_{ij} je $(-1)^{i+j} \cdot M_{ij}$.

Definice 57 (Adjungovaná matice)

Adjungovaná matice A^* vznikne z matice A tak, že každý prvek nahradíme jeho algebraickým doplňkem.

Definice 58 (Inverzní matice)

Inverzní matice, je matice k dané matici A, která splňuje:

$$A \cdot A^{-1} = E = A^{-1} \cdot A$$

Inverzní matici můžeme spočítat jako:

$$A^{-1} = \frac{1}{|A|} \cdot (A^*)^T$$

Z Cauchyho věty o součinu 9 vyplývá, že determinant A musí být nenulový[24].

Příklad (Výpočet inverzní matice)

Spočítejte inverzní matici A^{-1} k matici A:

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 2 & -1 & 3 \\ 3 & 0 & 4 \end{pmatrix}$$

Prvním krokem je zjistit, zda je A vůbec regulární matice, tedy spočítat determinant A.

$$|A| = 1 \cdot (-1) \cdot 4 + 3 \cdot 2 \cdot 3 - (4 \cdot 2 \cdot 2) = -2$$

Následně potřebujeme vyjádřit adjungovanou matici A^*

$$A^* = \begin{pmatrix} \begin{vmatrix} -1 & 3 \\ 0 & 4 \end{vmatrix} & -\begin{vmatrix} 2 & 3 \\ 3 & 4 \end{vmatrix} & \begin{vmatrix} 2 & -1 \\ 3 & 0 \end{vmatrix} \\ -\begin{vmatrix} 2 & 0 \\ 0 & 4 \end{vmatrix} & \begin{vmatrix} 1 & 0 \\ 3 & 4 \end{vmatrix} & -\begin{vmatrix} 1 & 2 \\ 3 & 0 \end{vmatrix} \\ \begin{vmatrix} 2 & 0 \\ -1 & 3 \end{vmatrix} & -\begin{vmatrix} 1 & 0 \\ 2 & 3 \end{vmatrix} & \begin{vmatrix} 1 & 2 \\ 2 & -1 \end{vmatrix} \end{pmatrix} = \begin{pmatrix} -4 & 1 & 3 \\ -8 & 4 & 6 \\ 6 & -3 & -5 \end{pmatrix}$$

$$A^{-1} = \frac{1}{|A|} \cdot A^{*T} = \frac{1}{-2} \cdot \begin{pmatrix} -4 & -8 & 6 \\ 1 & 4 & -3 \\ 3 & 6 & -5 \end{pmatrix} = \begin{pmatrix} 2 & 4 & -3 \\ \frac{-1}{2} & -2 & \frac{3}{2} \\ \frac{-3}{2} & -3 & \frac{5}{2} \end{pmatrix}$$

Pro ověření:

$$A \cdot A^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

[24]Matice s nenulovým determinantem nazýváme regulární, a naopak matice s nulovým determinantem nazýváme singulární.

Pro každou regulární matici jsme schopni tímto způsobem najít matici inverzní. Vezmeme li množinu regulárních matic řádu n a operaci násobení matic, zjistíme, že toto násobení je asociativní, ke každé matici existuje matice inverzní a vzhledem k násobení máme i neutrální prvek, kterým je jednotková matice. Regulární matice nad polem F řádu n s operací násobení matic tvoří grupu! Tuto grupu značíme jako:

$$GL(n, F)$$

Příklad (Počet prvků grupy GL nad konečným polem)

Kolik prvků má $GL(n, \mathbb{F}_{2^k})$?

Příklad (Nad polem F_7 řešte maticovou rovnici)

$$X \cdot A = B$$

Pro neznámou matici X a

$$A = \begin{pmatrix} 2 & 3 \\ 5 & 1 \end{pmatrix}, \; B = \begin{pmatrix} 3 & 0 \\ 5 & 6 \end{pmatrix}$$

Je nutné pamatovat na to, že násobení matic není komutativní a správně vynásobit obě strany korektně inverzní maticí.

$$\begin{aligned} X \cdot A &= B \\ X \cdot A \cdot A^{-1} &= B \cdot A^{-1} \\ X &= B \cdot A^{-1} \end{aligned}$$

Vyjádříme inverzní matici A^{-1}:

$$A^{-1} = \frac{1}{|A|} \cdot A^{*T} = \frac{1}{1} \cdot \begin{pmatrix} 1 & 2 \\ 4 & 2 \end{pmatrix}^T = \begin{pmatrix} 1 & 4 \\ 2 & 2 \end{pmatrix}$$

A dosadíme do dříve získaného vztahu:

$$\begin{aligned} X &= \begin{pmatrix} 3 & 0 \\ 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 & 4 \\ 2 & 2 \end{pmatrix} \\ X &= \begin{pmatrix} 3 & 5 \\ 3 & 4 \end{pmatrix} \end{aligned}$$

5.3 Hodnost matice

Z definice 43 víme co je lineární nezávislost vektorů. V každé matici můžeme řádky (případně sloupce) uvažovat jako vektory. Může nás zajímat, kolik je v matici lineárně nezávislých řádků (případně sloupců).

Počet lineárně nezávislých řádků se nazývá hodnost matice. Hodnost matice je tedy počet jejich lineárně nezávislých řádků, což je totéž jako počet lineárně nezávislých sloupců. Hodnost matice A značíme:

$$h(A)$$

Nejmenší hodnost matice může být 0, hodnost 0 má pouze nulová matice, protože nulový vektor není nezávislý ani sám o sobě. A maximální možná hodnost pro matici o rozměrech $m \times n$ je $min(m,n)$.

$$0 \leq h(A) \leq min(m,n)$$

5.3.1 Výpočet hodnosti matice

Pro jednotlivé řádky by bylo možné využít vztahu z definice 43, pomocí něj sestavit soustavu lineárních rovnic a vypočítat její řešení. To však může být zbytečně zdlouhavé, budeme tedy používat tzv. ekvivalentní (elementární) úpravy matice, které nemění hodnost matice.

Ekvivalentními úpravami matice jsou:

1. Přičtení k-násobku řádku k jinému řádku.
2. Vynásobení řádku nějakým nenulovým číslem l.
3. Výměna řádků[25].

Pomocí těchto ekvivalentních úprav upravíme matici na schodovitou. A hodnost schodovité matice je velice snadné spočítat, protože u schodovité matice je její hodnost počet nenulových řádků (vektorů).

Maximální hodnost matice označujeme jako plnou hodnost.

Příklad (Výpočet hodnosti matice)

[25] Výměna řádků jde relizovat pomocí prvních dvou úprav, její uvádění zde tedy není nutné.

Vypočtěte hodnost matice Q.

$$Q = \begin{pmatrix} 1 & 2 & 0 & 5 \\ 2 & -1 & 2 & -3 \\ 2 & 1 & -3 & 6 \\ 6 & -1 & 1 & 0 \end{pmatrix}$$

Pomocí elementárních úprav převedeme matici Q do schodovitého tvaru.

$$Q \sim \begin{pmatrix} 1 & 2 & 0 & 5 \\ 0 & -5 & 2 & -13 \\ 0 & -3 & -3 & -4 \\ 0 & -13 & 1 & -30 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 & 5 \\ 0 & -5 & 2 & -13 \\ 0 & 15 & 15 & 20 \\ 0 & 65 & -5 & 150 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 & 5 \\ 0 & -5 & 2 & -13 \\ 0 & 0 & 21 & -19 \\ 0 & 0 & 21 & -19 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 & 5 \\ 0 & -5 & 2 & -13 \\ 0 & 0 & 21 & -19 \\ 0 & 0 & 0 & 0 \end{pmatrix} = R$$

Z upravené matice vidíme, že:

$$h(R) = 3 = h(Q)$$

5.4 Výpočet determinantu pomocí ekvivalentních úprav

S využitím ekvivalentních úprav 5.3.1 můžeme matici převést na schodovitý tvar a jednoduše spočítat determinant schodovité matice jako součin prvků na hlavní diagonále.

Při aplikaci úprav však musíme dávat pozor na to, jakým způsobem která úprava mění determinant upravené matice:

1. Přičtení k-násobku řádku k jinému řádku. Determinant se nemění.
2. Vynásobení řádku nějakým nenulovým číslem l. Determinant bude l krát větší.
3. Výměna řádků. Změní se znaménko determinantu.

Vliv těchto úprav na determinant je lehké ukázat na matici řádu 2. Platí však obecně pro jakoukoliv matici řádu n.

Z těchto pravidel lze také vyvodit, že každá čtvercová matice řádu n s plnou hodností je regulární a s jakoukoliv menší než plnou hodností je singulární.

Příklad (Výpočet determinantu pomocí ekvivalentních úprav)

Pomocí ekvivalentních úprav spočtěte determinant matice M.

$$M = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 6 & 2 \\ 0 & 0 & 5 & 6 \\ 0 & 1 & 10 & 1 \end{pmatrix} \overset{r_2 \cdot \frac{1}{2}}{\sim} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 1 \\ 0 & 0 & 5 & 6 \\ 0 & 1 & 10 & 1 \end{pmatrix} \overset{r_2 - r_1}{\sim} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & -3 \\ 0 & 0 & 5 & 6 \\ 0 & 1 & 10 & 1 \end{pmatrix} \overset{r_2 \leftrightarrow r_4}{\sim} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 10 & 1 \\ 0 & 0 & 5 & 6 \\ 0 & 0 & 0 & -3 \end{pmatrix} = N$$

$$det(N) = -15$$
$$det(N) = \frac{1}{2} \cdot -1 \cdot det(M)$$
$$det(M) = -2 \cdot det(N) = 30$$

Definice 59 (Symetrická matice)
Matice A je symetrická, pokud platí:

$$A^T = A$$

Pro jednotlivé prvky matice musí tedy platit:

$$a_{ij} = a_{ji}$$

Symetrickou matici značíme s dolním indexem sym, např. A_{sym}

Definice 60 (Antisymetrická matice)
Matice A je antisymetrická, pokud platí:

$$A^T = -A$$

Pro jednotlivé prvky matice musí tedy platit:

$$a_{ij} = -a_{ji}$$

Antisymetrickou matici značíme s dolním indexem alt, např. A_{alt}

Věta 8 (Rozklad čtvercové matice na symetrickou a antisymetrickou matici)
Každou čtvercovou matici lze rozložit na součet matice symetrické a antisymetrické.

$$A = A_{sym} + A_{alt}$$

Důkaz. Matice A_{sym} a A_{alt} můžeme vždy zkonstruovat následovně:

$$A_{sym} = \frac{1}{2} \cdot (A + A^T)$$

Takto zvolená matice A_{sym} je určitě symetrická, protože:

$$(A_{sym})^T = \frac{1}{2}(A^T + (A^T)^T) = A_{sym}$$

Podobně pro A_{alt}:

$$A_{alt} = \frac{1}{2} \cdot (A - A^T)$$

Takto zvolená matice A_{alt} je určitě antisymetrická, protože:

$$(A_{alt})^T = \frac{1}{2} \cdot (A^T - (A^T)^T) = -A_{alt}$$

Zároveň vidíme, že výsledkem součtu těchto dvou matic je opravdu původní matice:

$$A_{sym} + A_{alt} = \frac{1}{2} \cdot (A + A^T) + \frac{1}{2} \cdot (A - A^T) = A$$

□

5.5 Soustavy linearních rovnic

Soustavy lineárních rovnic můžeme řešit elementárně (vyjadřovat neznámé a dosazovat do ostatních rovnic, případně sečíst dvě rovnice a tím nějakou neznámou eliminovat). Tento způsob však má nevýhodu, že není algoritmický.

Proto budeme používat postupy pomocí matic, které jsou jednoduše algoritmizovatelné.

Soustava lineárních rovnic obecně:

$$\begin{aligned} a_{11} \cdot x_1 + \dots a_{1n} \cdot x_n &= b_1 \\ &\vdots \\ a_{m1} \cdot x_1 + \dots a_{mn} \cdot x_n &= b_m \end{aligned}$$

Proměnným a_{ij} říkáme koeficienty, které tvoří obdélníkovou matici o m řádcích a n sloupcích. Proměnné $x_1, \dots, x_n$ nazýváme neznámé, ty budeme počítat. A proměnné $b_1, \dots, b_m$ nazýváme absolutní členy. Tuto obecnou soustavu lineárních rovnic můžeme zapsat maticově:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

Někdy také zapisujeme jako:

$$A \cdot \vec{x} = \vec{b}$$

V případě, že je vektor absolutních členů $\vec{b}$ nulový vektor, tedy:

$$\vec{b} = \vec{o}$$

Nazýváme takovou soustavu homogenní. Homogenní soustava lineárních rovnic je vždy řešitelná. Obecně řešení homogenní soustavy lineárních rovnic tvoří vektorový podprostor.

A v případě nehomogenních soustav se nejedná o vektorový podprostor, ale o affinní podprostor.

5.5.1 Gaussova eliminační metoda

Matici soustavy[26] A a vektor absolutních členů $\vec{b}$ zapíšeme do jedné rozšířené matice následovně:

$$\left(A \;\middle|\; \vec{b}\right) = \left(\begin{array}{ccc|c} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & b_m \end{array}\right)$$

Tuto rozšířenou matici poté pomocí elementárních úprav upravujeme do vhodného (schodovitého) tvaru, ze kterého dokážeme lehce zjistit řešení celé soustavy. Ze schodovité matice pak jednoduše dostaneme řešení celé soustavy "zpětným chodem"od posledního řádku, kdy postupně zjišťujeme hodnoty neznámých.

Soustava rovnice je řešitelná právě tehdy, když:

$$h(A) = h\left(\left(A \;\middle|\; \vec{b}\right)\right)$$

V opačném případě matice řešitelná není.

V případě, že se hodnosti rovnají, a soustava je tedy řešitelná, mohou nastat dva případy:

1. $h(A) = n$, kde n je počet neznámých — Rovnice má právě jedno řešení.
2. $h(A) = k < n$ — Rovnice má nekonečně mnoho řešení[27].

Mohou tedy nastat pouze 3 případy:

[26] Tuto matici tvoří jednotlivé koeficienty.

[27] A tato řešení jsou závislá na $n - k$ libovolných parametrech. V případě, že navíc pracujeme nad konečným polem, není jich tedy nekonečně mnoho

1. Soustava není řešitelná.
2. Soustava je řešitelná a má právě jedno řešení.
3. Soustava je řešitelná a má nekončně mnoho řešení.

Příklad (Příklad neřešitelné soustavy)

Řešte následující soustavu rovnic:

$$
\begin{aligned}
x + y + z &= 2 \\
2x - y + 2z &= 1 \\
7x + 4y + 7z &= -3
\end{aligned}
$$

Tuto soustava přepíšeme do matice a upravíme do schodovitého tvaru:

$$
\left(\begin{array}{ccc|c} 1 & 1 & 1 & 2 \\ 2 & -1 & 2 & 1 \\ 7 & 4 & 7 & -3 \end{array}\right) \overset{r_2-2\cdot r_1, r_3-7\cdot r_1}{\sim} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 2 \\ 0 & -3 & 0 & -3 \\ 0 & -3 & 0 & -17 \end{array}\right) \overset{r_3-r_2}{\sim} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 2 \\ 0 & -3 & 0 & -3 \\ 0 & 0 & 0 & -14 \end{array}\right)
$$

Hodnost základní matice je v tomto případě zjevně 2 a hodnost celé rozšířené matice je zjevně 3. Hodnosti se nerovnají a soustava tedy nemá řešení.

6 Šestá přednáška

6.1 Matice

Věta 9 (Cauchyho věta o součinu)
Determinant součinu je součin determinantů.

$$|A \cdot B| = |A| \cdot |B|$$

Důkaz. Idea důkazu: Uvažujme matici H v tomto tvaru:

$$H = \begin{pmatrix} A & O \\ \begin{pmatrix} -1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & -1 \end{pmatrix} & B \end{pmatrix}$$

Jestliže matice A a B jsou řádu n, potom matice H je řádu $2 \cdot n$. Nyní zkonstruujeme matici K:

$$K = \begin{pmatrix} A & C \\ \begin{pmatrix} -1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & -1 \end{pmatrix} & O \end{pmatrix}$$

S tím, že:

$$C = A \cdot B$$

Zřejmě:

$$|H| = |A| \cdot |B|$$

$$|K| = |C|$$

A K lze obdržet vhodnými elementárními úpravami z H. □

6.2 Soustavy lineárních rovnic

Příklady na řešitelnost soustavy. Příklad na soustavu, která nemá řešení je na konci předchozí přednášky.

Příklad (Řešení soustavy linearních rovnic s právě jedním řešením)
Řešte následujicí soustavu linearních rovnic:

$$2x + y - z = 43$$

$$3x + 3y + 5z = 84$$

$$4x - y - 2z = 86$$

Soustavu přepíšeme do rozšířené matice a elementárními úpravami převedeme do schodovitého tvaru:

$$\left(\begin{array}{ccc|c} 2 & 1 & -1 & 43 \\ 3 & 3 & 5 & 84 \\ 4 & -1 & -2 & 86 \end{array}\right) \overset{r_2\cdot(-2);r_3\cdot(-1)}{\sim} \left(\begin{array}{ccc|c} 2 & 1 & -1 & 43 \\ -6 & -6 & -10 & -168 \\ -4 & 1 & 2 & 86 \end{array}\right) \overset{r_2+3\cdot r_1;r_3+2\cdot r_1}{\sim} \left(\begin{array}{ccc|c} 2 & 1 & -1 & 43 \\ 0 & -3 & -13 & -39 \\ 0 & 3 & 0 & 0 \end{array}\right) \overset{r_2+r_3;r_3\cdot\frac{1}{3};r_3\leftrightarrow r_2;}{\sim}$$

$$\overset{r_2+r_3;r_3\cdot\frac{-1}{3};r_3\leftrightarrow r_2;}{\sim} \left(\begin{array}{ccc|c} 2 & 1 & -1 & 43 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -13 & -39 \end{array}\right) \overset{r_3\cdot\frac{-1}{13}}{\sim} \left(\begin{array}{ccc|c} 2 & 1 & -1 & 43 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 3 \end{array}\right)$$

Hodnost základní matice je 3, hodnost rozšířené matice je také 3, soustava má tedy právě jedno řešení. Nyní provedeme „zpětný chod“ a ze schodovitého tvaru matice vyjádříme odspodu hodnoty jednotlivých proměnných.

$$z = 3$$

$$y = 0$$

$$2x + y - z = 43$$

$$2x + 0 - 3 = 43$$

$$2x = 46$$

$$x = 23$$

Příklad (Řešení soustavy linearních rovnic s nekonečným počtem řešení)

Řešte následujicí soustavu linearních rovnic v $\mathbb{R}$:

$$2a - b + c - 4d = -2$$

$$4a + 2b - c + 5d = 1$$

$$10a - b + 2c - 7d = -5$$

$$30a + 9b - 3c + 18d = 0$$

Soustavu přepíšeme do rozšířené matice a elementárními úpravami převedeme do schodovitého tvaru:

$$\left(\begin{array}{cccc|c} 2 & -1 & 1 & -4 & -2 \\ 4 & 2 & -1 & 5 & 1 \\ 10 & -1 & 2 & -7 & -5 \\ 30 & 9 & -3 & 18 & 0 \end{array}\right) \underset{\sim}{r_2\cdot(-1);r_3\cdot -1;r_4\cdot\frac{-1}{3}} \left(\begin{array}{cccc|c} 2 & -1 & 1 & -4 & -2 \\ -4 & -2 & 1 & -5 & -1 \\ -10 & 1 & -2 & 7 & 5 \\ -10 & -3 & 1 & -6 & 0 \end{array}\right) \underset{\sim}{r_2+2\cdot r_1;r_3+5\cdot r_1;r_4+5\cdot r_1}$$

$$\underset{\sim}{r_2+2\cdot r_1;r_3+5\cdot r_1;r_4+5\cdot r_1} \left(\begin{array}{cccc|c} 2 & -1 & 1 & -4 & -2 \\ 0 & -4 & 3 & -13 & -5 \\ 0 & -4 & 3 & -13 & -5 \\ 0 & -8 & 6 & -26 & -10 \end{array}\right) \underset{\sim}{r_3-r_2;r_4-2\cdot r_2} \left(\begin{array}{cccc|c} 2 & -1 & 1 & -4 & -2 \\ 0 & -4 & 3 & -13 & -5 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Vidíme, že hodnost základní matice soustavy je 2 a hodnost rozšířené matice soustavy je také 2 hodnosti se rovnají a soustava je tedy řešitelná. Máme ovšem 4 neznáme a hodnosti jsou rovny dvěma, řešení lze tedy vyjádřit pomocí $4 - 2 = 2$ *parametrů.*

Za neznámé c, d *dosadíme parametry* p, q *a pomocí těchto parametrů opět zpětným chodem vyjádříme ostatní neznámé.*

$$d = q$$
$$c = p$$
$$p, q \in \mathbb{R}$$

$$\begin{aligned} -4b + 3c - 13d &= -5 \\ -4b + 3p - 13q &= -5 \\ -4b &= -3p + 13q - 5 \\ b &= \frac{3p - 13q + 5}{4} \end{aligned}$$

$$\begin{aligned} 2a - b + c - 4d &= -2 \\ 2a - \frac{3p - 13q + 5}{4} + p - 4q &= -2 \\ 2a &= \frac{3p - 13q + 5}{4} + \frac{-4p + 16q - 8}{4} \\ 2a &= \frac{-p + 3q - 3}{4} \\ a &= \frac{-p + 3q - 3}{8} \end{aligned}$$

Jako parametry ovšem nebylo nutné zvolit zrovna neznámé c, d. Jako parametr jsme mohli vzít například a, nebo b, nebo také výraz $a + 2b$. Můžeme si je zkrátka zvolit dle potřeby a parametrické vyjádření tedy není jednoznačné. Ne vždy je navíc možné parametry volit takto vhodně „odzadu", jak jsme to udělali v tomto příkladu.

Příklad (Případ, kdy nejde neznámé parametrizovat odzadu)

Mějme rozšířenou matici soustavy upravenou na schodovitý tvar:

$$\left(\begin{array}{cccc|c} 1 & 1 & 1 & 2 & 3 \\ 0 & 0 & 0 & 2 & 5 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

V tomto případě si pro parametrizaci nemůžeme jednoduše zvolit poslední neznámou, protože ta má přesně danou hodnotu 5, k parametrizaci tak musíme využít jiný vhodný postup.

Příklad (Vytvoření soustavy rovnic dle požadavků)

Vytvořte soustavu tří různých linearnách rovnic o dvou neznámých, která má nekonečně mnoho řešení.

$$\begin{aligned} x &= 0 \\ 2y &= 0 \\ 3y &= 0 \end{aligned}$$

6.3 Výpočet inverzní matice pomocí Gaussovy metody

Gaussovu metodu můžeme použít i k výpočtu inverzní matice. Pro výpočet inverzní matice k matici A stačí vytvořit rozšířenou matici:

$$\left(A \mid E\right)$$

Kde matice E představuje jednotkovou matici. A pomocí elementárních úrav tuto rozšířeno matici upravit do tvaru, kdy jednotkovou matici dostaneme na levé straně, inverzní matice pak bude na pravé straně:

$$\left(E \mid A^{-1}\right)$$

Tato úprava je realizovatelná v případě, že je matice A regulární a existuje k ní tedy inverzní matice.

Příklad (Výpočet inverzní matice Gaussovou metodou)

Gaussovou metodou spočítejte inverzní matici A^{-1} k matici A.

$$A = \begin{pmatrix} 2 & 3 & 0 \\ 1 & 0 & -1 \\ 1 & 1 & 5 \end{pmatrix}$$

Matici přepíšeme do rozšířené matice s jednotkovou maticí na pravé straně a levou stranu pomocí elementárních úprav převedeme na matici jednotkovou.

$$\left(\begin{array}{ccc|ccc} 2 & 3 & 0 & 1 & 0 & 0 \\ 1 & 0 & -1 & 0 & 1 & 0 \\ 1 & 1 & 5 & 0 & 0 & 1 \end{array}\right) \overset{r_1 \leftrightarrow r_2; r_3 \cdot (-1)}{\sim} \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & 0 & 1 & 0 \\ 2 & 3 & 0 & 1 & 0 & 0 \\ -1 & -1 & -5 & 0 & 0 & -1 \end{array}\right) \overset{r_2 - 2 \cdot r_1; r_3 + r_1}{\sim}$$

$$\overset{r_2 - 2 \cdot r_1; r_3 + r_1}{\sim} \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & 0 & 1 & 0 \\ 0 & 3 & 2 & 1 & -2 & 0 \\ 0 & -1 & -6 & 0 & 1 & -1 \end{array}\right) \overset{r_2 + 3 \cdot r_3; r_2 \leftrightarrow r_3}{\sim} \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & 0 & 1 & 0 \\ 0 & -1 & -6 & 0 & 1 & -1 \\ 0 & 0 & -16 & 1 & 1 & -3 \end{array}\right) \overset{r_3 \cdot \frac{1}{16}}{\sim}$$

$$\overset{r_3 \cdot \frac{-1}{16}}{\sim} \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & 0 & 1 & 0 \\ 0 & -1 & -6 & 0 & 1 & -1 \\ 0 & 0 & 1 & \frac{-1}{16} & \frac{-1}{16} & \frac{3}{16} \end{array}\right) \overset{r_2 + 6 \cdot r_3; r_1 - r_3}{\sim} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & \frac{-1}{16} & \frac{15}{16} & \frac{3}{16} \\ 0 & -1 & 0 & \frac{-6}{16} & \frac{10}{16} & \frac{2}{16} \\ 0 & 0 & 1 & \frac{-1}{16} & \frac{-1}{16} & \frac{3}{16} \end{array}\right) \overset{r_2 \cdot (-1)}{\sim}$$

$$\overset{r_2 \cdot (-1)}{\sim} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & \frac{-1}{16} & \frac{15}{16} & \frac{3}{16} \\ 0 & 1 & 0 & \frac{6}{16} & \frac{-10}{16} & \frac{-2}{16} \\ 0 & 0 & 1 & \frac{-1}{16} & \frac{-1}{16} & \frac{3}{16} \end{array}\right)$$

6.4 Cramerovo pravidlo

Cramerovo pravidlo je k řešení soustav lineárních rovnic, kde základní matice soustavy je čtvercová regulární matice.

Cramerovo pravidlo říká, že i-tou neznámnou x_i z matice soustavy A můžeme vyjádřit jako:

$$x_i = \frac{|A_i|}{|A|}$$

Kde A_i je matice vytvořená z matice A tak, že i-tý sloupec nahradíme sloupcem absolutních členů soustavy.

Tuto metodu je výhodné použít když nepotřebujeme všechny neznámé, nebo když máme „nepěkné“ koeficienty.

Příklad (Výpočet neznámé pomocí cramerova pravidla)

Pomocí Cramerova pravidla vyjádřete neznámou y z následující soustavy rovnic:

$$\sqrt{2}x + y + z = 2\sqrt{2}$$

$$3x - \sqrt{2}z = 1$$

$$4y + 3 \cdot \sqrt{2}z = 1 + \sqrt{2}$$

Spočítáme potřebné determinanty

$$|A| = \begin{vmatrix} \sqrt{2} & 1 & 1 \\ 3 & 0 & -\sqrt{2} \\ 0 & 4 & 3 \cdot \sqrt{2} \end{vmatrix} = 12 - (-4 \cdot \sqrt{2} \cdot \sqrt{2} + 9 \cdot \sqrt{2}) = 20 - 9 \cdot \sqrt{2}$$

$$|A_2| = \begin{vmatrix} \sqrt{2} & 2 \cdot \sqrt{2} & 1 \\ 3 & 1 & -\sqrt{2} \\ 0 & 1 + \sqrt{2} & 3 \cdot \sqrt{2} \end{vmatrix} = 9 + 3 \cdot \sqrt{2} - [-2 - 2\sqrt{2} + 36] = -25 + 5\sqrt{2}$$

A pomocí nich vyjádříme neznámou y:

$$y = \frac{|A_2|}{|A|} = \frac{-25 + 5 \cdot \sqrt{2}}{20 - 9 \cdot \sqrt{2}} \cdot \frac{20 + 9 \cdot \sqrt{2}}{20 + 9 \cdot \sqrt{2}} = \frac{-500 - 225\sqrt{2} + 100\sqrt{2} + 90}{238} = \frac{-410 - 125\sqrt{2}}{238}$$

Definice 61 (Podobnost matic)

Řekneme, že matice B je podobná matici A, jestliže existuje regulární matice S tak, že:

$$B = S \cdot A \cdot S^{-1}$$

Věta 10 (Relace podobnosti matic)

Relace „být podobná" je ekvivalence.

Důkaz. Pro důkaz ekvivalence musíme dokázat, že se jedná o reflexivní, symetrickou a tranzitivní relaci:

Reflexivita:

$$A = S \cdot A \cdot S^{-1} \; pro \; S = E, \forall A$$

Symetrie: Předpokládejme, že B je podobná A:

$$B = S \cdot A \cdot S^{-1}$$

Potom musíme ukázat, že existuje regulární matice T taková, že:

$$A = T \cdot B \cdot T^{-1}$$

Pro splnění tohoto požadavku však stačí vzít $T = S^{-1}$

Tranzitivita: Předpokládejme, že B je podobná A a že C je podobná B.

$$B = SAS^{-1}$$
$$C = TBT^{-1}$$

A nyní chceme ukázat, že C je podobná A.

$$C = UAU^{-1}$$
$$C = TSAS^{-1}T^{-1}$$

Pro splnění tohoto požadavku stačí zvolit $U = TS$ □

6.5 Charakteristický polynom, vlastní čísla a vlastní vektory matice

Definice 62 (Charakteristický polynom)

Charakteristický polynom čtvercové matice A je polynom:

$$|A - \lambda E|$$

Definice 63 (Charakteristická rovnice)

Charakteristická rovnice čtvercové matice A je rovnice, kde charakteristický polynom položíme roven 0:

$$|A - \lambda E| = 0$$

Definice 64 (Vlastní hodnoty)

Vlastní hodnoty čtvercové matice A jsou kořeny charakteristického polynomu této matice.

Příklad

Vyjádřete charakteristický polynom a vlastní hodnoty matice A.

$$A = \begin{pmatrix} 5 & 1 \\ -1 & 0 \end{pmatrix}$$

$$|A - \lambda E| = 0$$

$$det\left(\begin{pmatrix} 5 & 1 \\ -1 & 0 \end{pmatrix} - \lambda \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 0$$

$$det\left(\begin{pmatrix} 5 & 1 \\ -1 & 0 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\right) = 0$$

$$\begin{vmatrix} 5 - \lambda & 1 \\ -1 & -\lambda \end{vmatrix} = 0$$

$$-5 \cdot \lambda + \lambda^2 + 1 = 0$$

$$\lambda^2 - 5 \cdot \lambda + 1 = 0$$

$$\lambda_{1,2} = \frac{5 \pm \sqrt{21}}{2}$$

Definice 65 (Vlastní vektor matice A)

Vezmeme li jednu konkrétní vlastní hodnotu λ_1 matice A. Potom nenulový vektor $\vec{u}$, který splňuje:

$$(A - \lambda_1 \cdot E) \cdot \vec{u} = \vec{o}$$

Nazýváme vlastní vektor matice A odpovídajicí vlastní hodnotě λ_1. Tento vlastní vektor tvoří vektorový podprostor.

Příklad (Vlastní hodnoty a vlastní vektory)

Najděte všechny vlastní hodnoty a vlastní vektory matice A.

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

Vyjádříme vlastní čísla:

$$\begin{vmatrix} 1 - \lambda & 0 \\ 0 & 2 - \lambda \end{vmatrix} = (1 - \lambda)(2 - \lambda)$$

$$\lambda_1 = 1$$

$$\lambda_2 = 2$$

K vlastním číslům vyjádříme vlastní vektory: Pro λ_1

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$u_1 = p$$

$$u_2 = 0$$

Pro λ_2 stejným postupem:

$$u_1 = 0$$

$$u_2 = p$$

A vlastní vektory matice A jsou tedy $\begin{pmatrix} p \\ 0 \end{pmatrix}$ *a* $\begin{pmatrix} 0 \\ p \end{pmatrix}$*, kde* $p \in \mathbb{R} \setminus 0$

Věta 11 (Nezávislost vlastních vektorů)

Vlastní vektory příslušné různým vlastním hodnotám jsou lineárně nezávislé.

Věta 12 (Vlastní hodnoty symetrické matice)

Vlastní hodnoty symetrické matice A jsou reálné ($\in \mathbb{R}$).

Věta 13 (Charakteristický polynom podobných matic)

Charakteristický polynom podobných matic je stejný a tedy mají i stejné vlastní hodnoty.

6.6 Matice homomorfismů

Definice 66 (Matice homomorfismů)

Mějme vektorový prostor $\mathcal{V}$ nad nějakým polem F, dimenze $\mathcal{V}$ bude m a báze $\mathcal{B} = (\vec{e_1}, \ldots, \vec{e_m})$. A vektorový prostor $\mathcal{W}$ s dimenzí n a bází $\overline{B} = (\vec{f_1}, \ldots, \vec{f_n})$.

Dále budeme mít zobrazení $\varphi : \mathcal{V} \to \mathcal{W}$, které bude homomorfismus (lineární zobrazení) Označme:

$$\vec{w_1} = \varphi(\vec{e_1})$$

$$\vdots$$

$$\vec{w_m} = \varphi(\vec{e_m})$$

Pak vektory $\vec{w_1}, \ldots, \vec{w_m}$ jsou lineárnímí kombinacemi bázových vektorů v prostoru $\mathcal{W}$.

$$\vec{w_1} = a_{11} \cdot \vec{f_1} + \ldots a_{1n} \cdot \vec{f_n}$$
$$\vdots$$
$$\vec{w_m} = a_{n1} \cdot \vec{f_1} + \ldots a_{mn} \cdot \vec{f_n}$$

Potom matici koeficientů a:

$$\begin{vmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{mn} \end{vmatrix}$$

Nazveme matice homomorfismu $\varphi : \mathcal{V} \to \mathcal{W}$ v bázích $\mathcal{B}$ a $\overline{\mathcal{B}}$.

Příklad (Matice homomorfismu)

Nechť:

$$\mathcal{V} = \mathbb{R}^3,\ \mathcal{B} = \Big((1,1,1),(1,0,1),(1,0,0)\Big)$$
$$\mathcal{W} = \mathbb{R}^2,\ \overline{\mathcal{B}} = \Big((2,3),(3,2)\Big)$$
$$\varphi\Big((\vec{v_1}, \vec{v_2}, \vec{v_3})\Big) = (0, \vec{v_2} + 2 \cdot \vec{v_3})$$

Potom:

$$\vec{w_1} = (0,3) = a_{11} \cdot (2,3) + a_{12} \cdot (3,2)$$
$$\vec{w_2} = (0,2) = a_{21} \cdot (2,3) + a_{22} \cdot (3,2)$$
$$\vec{w_3} = (0,0) = a_{31} \cdot (2,3) + a_{32} \cdot (3,2)$$

Vyřešíme tyto 3 soustavy lineárních rovnic a tím dostaneme následující matici homomorfismů:

$$\begin{pmatrix} 0 & 0 \\ \frac{6}{5} & \frac{-4}{5} \\ 0 & 0 \end{pmatrix}$$

7 Sedmá přednáška

7.1 Matice homomorfismů a přechodů

Příklad (Výpočet matice homomorfismu)

Vyjádřete matici homomorfismu φ v bázích $\mathcal{B}$ a $\overline{\mathcal{B}}$, kde:

$$\mathcal{V} = \mathbb{R}^3,\ \mathcal{B} = \Big(e_1 = (0,0,1), e_2 = (0,1,2), e_3 = (1,2,3)\Big)$$
$$\mathcal{W} = \mathbb{R}^4,\ \overline{\mathcal{B}} = \Big(f_1 = (0,0,0,1), f_2 = (0,0,-1,0), f_3 = (0,1,0,0), f_4 = (-1,0,0,0)\Big)$$
$$\varphi : \mathcal{V} \to \mathcal{W},\ \varphi\Big((v_1,v_2,v_3)\Big) = (v_1+v_2, v_2+v_3, v_1, v_2)$$

Měli bychom nejprve ověřit, že $\mathcal{B}$ a $\overline{\mathcal{B}}$ jsou opravdu báze vektorových prostorů $\mathcal{V}$ a $\mathcal{W}$. A to tak, že přepsáním báze do matice dostaneme matici se správnou hodností (v tomto případě 3 a 4). Což zde zjevně platí.

$$h\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} = 3$$
$$h\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} = 4$$

Dále je třeba ověřit, zda φ je skutečně homomorfismus. Musíme zkontrolovat platnost vlastností z definice homomorfismu 46: Platnost první vlastnosti $\varphi(\vec{u}+\vec{v}) = \varphi(\vec{u}) + \varphi(\vec{v})$ můžeme ověřit takto:

$$\varphi(\vec{u}+\vec{v}) = \varphi\Big((u_1+v_1, u_2+v_2, u_3+v_3)\Big) = (u_1+v_1+u_2+v_2, u_2+v_2+u_3+v_3, u_1+v_1, u_2+v_2)$$
$$\varphi(\vec{u}) + \varphi(\vec{v}) = (u_1+u_2, u_2+u_3, u_1, u_2) + (v_1+v_2, v_2+v_3, v_1, v_2)$$
$$L = P$$

Platnost druhé vlastnosti bychom ověřili podobným způsobem.

Nyní přes φ zobrazíme vektory báze prostoru $\mathcal{V}$ a vyjádříme tento obraz jako lineární kombinaci vektorů báze *prostoru $\mathcal{W}$:*

$$\vec{w_1} = \varphi(e_1) = (0,1,0,0) = a_{11} \cdot (0,0,0,1) + a_{12} \cdot (0,0,-1,0) + a_{13} \cdot (0,1,0,0) + a_{14} \cdot (-1,0,0,0)$$
$$\vec{w_2} = \varphi(e_2) = (1,3,0,1) = a_{21} \cdot (0,0,0,1) + a_{22} \cdot (0,0,-1,0) + a_{23} \cdot (0,1,0,0) + a_{24} \cdot (-1,0,0,0)$$
$$\vec{w_3} = \varphi(e_3) = (3,5,1,2) = a_{31} \cdot (0,0,0,1) + a_{32} \cdot (0,0,-1,0) + a_{33} \cdot (0,1,0,0) + a_{34} \cdot (-1,0,0,0)$$

Vyřešením těchto 3 soustav 4 lineárních rovnic dostaneme hodnoty koeficientů a, které tvoří matici homomorfismu: První řádek jde na první pohled vyřešit snadno jako:

$$a_{11} = a_{12} = a_{14} = 0$$
$$a_{13} = 1$$

Řádky 2 a 3 už nejsou tak zřejmé. Rozepíšeme tedy soustavu rovnic pro druhý řádek:

$$0 \cdot a_{21} + 0 \cdot a_{22} + 0 \cdot a_{23} - 1 \cdot a_{24} = 1 \Rightarrow a_{24} = -1$$
$$0 \cdot a_{21} + 0 \cdot a_{22} + 1 \cdot a_{23} + 0 \cdot a_{24} = 3 \Rightarrow a_{23} = 3$$
$$0 \cdot a_{21} - 1 \cdot a_{22} + 0 \cdot a_{23} + 0 \cdot a_{24} = 0 \Rightarrow a_{22} = 0$$
$$1 \cdot a_{21} + 0 \cdot a_{22} + 0 \cdot a_{23} + 0 \cdot a_{24} = 1 \Rightarrow a_{21} = 1$$

Díky jednoduchému zadání báze $\overline{\mathcal{B}}$ jsme byli schopni rovnou odvodit řešení této soustavy.

Nyní rozepíšeme a vyřešíme soustavu pro 3 řádek:

$$0 \cdot a_{31} + 0 \cdot a_{32} + 0 \cdot a_{33} - 1 \cdot a_{34} = 3 \Rightarrow a_{34} = -3$$
$$0 \cdot a_{31} + 0 \cdot a_{32} + 1 \cdot a_{33} + 0 \cdot a_{34} = 5 \Rightarrow a_{33} = 5$$
$$0 \cdot a_{31} - 1 \cdot a_{32} + 0 \cdot a_{33} + 0 \cdot a_{34} = 1 \Rightarrow a_{32} = -1$$
$$1 \cdot a_{31} + 0 \cdot a_{32} + 0 \cdot a_{33} + 0 \cdot a_{34} = 2 \Rightarrow a_{31} = 2$$

Ze zjištěných koeficientů nyní můžeme vyjádřit požadovanou matici homomorfismu φ v bázích $\mathcal{B}$ a $\overline{\mathcal{B}}$:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 3 & -1 \\ 2 & -1 & 5 & -3 \end{pmatrix}$$

Matici homomorfismu můžeme použít k rychlému převádění vektorů mezi bázemi.

Příklad (Převod vektorů mezi bázemi)

Mějme vektorové prostory, báze, φ a matici homomorfismu z příkladu 7.1.

A mějme vektor $\vec{w_{\mathcal{B}}}$ vyjádřený v bázi $\mathcal{B}$:

$$\vec{w_{\mathcal{B}}} = (2, 4, 3)$$

Vyjádřete tento vektor v bázi $\overline{\mathcal{B}}$ jako $\vec{w_{\overline{\mathcal{B}}}}$.

To, že je vektor $\vec{w_{\mathcal{B}}}$ vyjádřený v bázi $\mathcal{B}$ znamená, že se jedná o lineární kombinaci vektorů $\vec{e_1}, \vec{e_2}, \vec{e_3}$ s koeficienty $2, 4, 3$. *Tento vektor můžeme převést do implicitní báze*[28] *následovně:*

$$\vec{u} = (2 \cdot 0 + 4 \cdot 0 + 3 \cdot 1,\ 2 \cdot 0 + 4 \cdot 1 + 3 \cdot 2,\ 2 \cdot 1 + 4 \cdot 2 + 3 \cdot 3) = (3, 10, 19)$$

Nyní tento vektor $\vec{u}$ vyjádřený v kanonické bázi zobrazíme pomocí φ:

$$\vec{v} = \varphi(\vec{u}) = \varphi\big((3, 10, 19)\big) = (13, 29, 3, 10)$$

A nyní $\vec{v}$ vyjádříme v bázi $\overline{\mathcal{B}}$:

$$\vec{v_{\overline{\mathcal{B}}}} = (10, -3, 29, -13)$$

V tomto případě jsme převod provedli bez využití matice homomorfismu. Provedli jsme převod na kanonickou bázi, zobrazení a nakonec převod do cílové báze.

Stejný výsledek ovšem můžeme dostat pomocí matice homomorfismu, který v sobě má tohle všechno v podstatě zahrnuto, stačí vektor $\vec{w_{\mathcal{B}}}$ vynásobit maticí homomorfismu:

$$\vec{v_{\overline{\mathcal{B}}}} = \begin{pmatrix} 2 & 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 3 & -1 \\ 2 & -1 & 5 & -3 \end{pmatrix} = \begin{pmatrix} 10 & -3 & 29 & -13 \end{pmatrix}$$

Definice 67 (Matice přechodu)

[28] Implicitní báze je obvyklá báze, ve které, i když třeba nechceme, musíme implicitně pracovat, abychom se mohli numericky vyjadřovat. Implicitní báze je obvykle $\big((1, 0, 0), (0, 1, 0), (0, 0, 1)\big)$, takové bázi říkáme kanonická a může být podobně vyjádřena i pro jiné dimenze, než právě 3.

Mějme speciální případ matice homomorfismu, kde[29]*:*

$$\mathcal{V} = \mathcal{W},\ dim\,\mathcal{V} = n$$
$$\mathcal{B} = (\vec{e_1}, \ldots, \vec{e_n})$$
$$\overline{\mathcal{B}} = (\vec{f_1}, \ldots, \vec{f_n})$$
$$\varphi = id$$

A matici homomorfismu v tomto speciálním případě říkáme matice přechodu od báze $\mathcal{B}$ k bází $\overline{\mathcal{B}}$ a značíme ji $M(\overline{\mathcal{B}}, \mathcal{B})$.

Pro obecnou matici homomorfismu bychom museli přepsat obrazy do následující soustavy rovnic a tu vyřešit:

$$\begin{aligned}\vec{e_1} &= a_{11} \cdot f_1 + \ldots + a_{1n} \cdot \vec{f_n} \\ &\vdots \\ \vec{e_n} &= a_{n1} \cdot f_1 + \ldots + a_{nn} \cdot \vec{f_n}\end{aligned}$$

Matici přechodu však můžeme vyjádřit jednodušeji, než obecnou matici homomorfismu, a to vyřešením následující maticové rovnice, která je ekvivalentní výše zmíněné soustavě rovnic, kde $M_{\mathcal{B}}$ a $M_{\overline{\mathcal{B}}}$ představují matice bází $\mathcal{B}$ a $\overline{\mathcal{B}}$:

$$M_{\mathcal{B}} = A \cdot M_{\overline{\mathcal{B}}}$$
$$M_{\mathcal{B}} \cdot M_{\overline{\mathcal{B}}}^{-1} = A$$

Kde matice A je matice přechodu.

Příklad (Výpočet matice přechodu)

Spočítejte matici přechodu pro:

$$\mathcal{V} = \mathbb{R}^3$$
$$\mathcal{B} = \big((3,1,2),(3,2,0),(1,0,0)\big)$$
$$\overline{\mathcal{B}} = \big((3,3,1),(4,1,0),(2,2,-5)\big)$$

Opět bychom měli nejprve ukázat, že se jedná o korektní báze. V tomto případě jsou obě báze korektní a jejich matice mají hodnost 3, tak jak potřebujeme.

[29]Přičemž *id* označuje funkci identity.

Když víme že se jedná o báze, můžeme spočítat matici přechodu:

$$M(\overline{\mathcal{B}}, \mathcal{B}) = M_{\mathcal{B}} \cdot M_{\overline{\mathcal{B}}}^{-1}$$

Zapíšeme báze do matice:

$$M_{\mathcal{B}} = \begin{pmatrix} 3 & 1 & 2 \\ 3 & 2 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$$M_{\overline{\mathcal{B}}} = \begin{pmatrix} 3 & 3 & 1 \\ 4 & 1 & 0 \\ 2 & 2 & -5 \end{pmatrix}$$

A vyjádříme matici přechodu dle odvozeného vztahu:

$$M(\overline{\mathcal{B}}, \mathcal{B}) = M(\mathcal{B}) \cdot M(\overline{\mathcal{B}})^{-1} = \begin{pmatrix} 3 & 1 & 2 \\ 3 & 2 & 0 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 & 3 & 1 \\ 4 & 1 & 0 \\ 2 & 2 & -5 \end{pmatrix}^{-1}$$

Dopočítáním bychom dostali matici přechodu.

Následně pokud budeme mít nějaký vektor $\vec{u_{\mathcal{B}}}$ vyjádřený v bázi $\mathcal{B}$ a vynásobíme ho touto maticí přechodu dostaneme tentýž vektor v bázi $\overline{\mathcal{B}}$:

$$\vec{u_{\mathcal{B}}} \cdot M(\overline{\mathcal{B}}, \mathcal{B}) = \vec{u_{\overline{\mathcal{B}}}}$$

Tato matice se často používá ke transformaci vektorů mezi různými bázemi.

Věta 14 (Podobnost matic endomorfismu v různých bázích)
Matice endomorfismu v různých bázích jsou podobné.

Důkaz. Uvažujme vektorový prostor $\mathcal{V}$ dimenze m, který má dvě báze $\mathcal{B}$ a $\overline{\mathcal{B}}$, a vektorový prostor $\mathcal{W}$ dimenze n, který má dvě báze $\mathcal{C}$ a $\overline{\mathcal{C}}$ následovně:

$$\mathcal{V},\ dim\,\mathcal{V} = m,\ \mathcal{B} = (\vec{e_1}, \dots, \vec{e_m}),\ \overline{\mathcal{B}} = (\vec{f_1}, \dots, \vec{f_m})$$
$$\mathcal{W},\ dim\,\mathcal{W} = n,\ \mathcal{C} = (\vec{g_1}, \dots, \vec{g_m}),\ \overline{\mathcal{C}} = (\vec{h_1}, \dots, \vec{h_m})$$

Nechť A je matice homomorfismu $\varphi : \mathcal{V} \to \mathcal{W}$ v bázích $\mathcal{B}, \mathcal{C}$ a $\overline{A}$ je matice homomorfismu φ v bázích $\overline{\mathcal{B}}, \overline{\mathcal{C}}$.

Z výše uvedeného můžeme odvodit následující vztahy:

$$\vec{w_{\mathcal{B}}} \cdot A = \vec{v_C}$$
$$\vec{w_{\overline{\mathcal{B}}}} \cdot \overline{A} = \vec{v_{\overline{C}}}$$
$$\vec{u_{\overline{\mathcal{B}}}} \cdot M(\overline{\mathcal{B}}, \mathcal{B}) = \vec{u_{\mathcal{B}}}$$
$$\vec{v_{\overline{C}}} \cdot M(\overline{C}, C) = \vec{v_C}$$

A pomocí těchto vztahů odvodíme:

$$\vec{u_{\overline{B}}} \cdot M(\overline{\mathcal{B}}, \mathcal{B}) \cdot \overline{A} = \vec{v_C} \cdot M(\overline{C}, C)$$
$$\vec{u_{\overline{B}}} \cdot M(\overline{\mathcal{B}}, \mathcal{B}) \cdot \overline{A} = \vec{u_{\mathcal{B}}} \cdot A \cdot M(\overline{C}, C)$$
$$M(\overline{\mathcal{B}}, \mathcal{B}) \cdot \overline{A} = A \cdot M(\overline{C}, C)$$
$$\overline{A} = M^{-1}(\overline{\mathcal{B}}, \mathcal{B}) \cdot A \cdot M(\overline{C}, C)$$

Pro $\mathcal{V} = \mathcal{W}$, tedy když φ je endomorfismus dostaneme:

$$\overline{A} = M^{-1}(\overline{\mathcal{B}}, \mathcal{B}) \cdot A \cdot M(\overline{\mathcal{B}}, \mathcal{B})$$

A tedy matice A a $\overline{A}$ jsou v takovém případě podobné. □

Matice přechodu $M(\overline{\mathcal{B}}, \mathcal{B})$ je vždy regulární, tedy:

$$det M(\overline{\mathcal{B}}, \mathcal{B}) \neq 0$$

Můžeme tedy zavést následující relaci

$$\mathcal{B} \sim \overline{\mathcal{B}} \text{ pokud } det M(\overline{\mathcal{B}}, \mathcal{B}) > 0$$

Takto definovaná relace ∼ je relací ekvivalence, která rozdělí množinu bází na dvě třídy ekvivalence a to na souhlasně orientované báze a opačně orientované báze. To, zda jsou báze souhlasně, nebo opačně orientované pak může prakticky ovlivnit například znaménko determinantu (který vyjadřuje obsah). Orientovaný vektorový prostor je pak vektorový prostor, ve kterém je určena jedna z těchto dvou tříd bází.

7.2 Afinní prostory

V případě Afinních a později i Euklidovských prostoru se budeme omezovat na reálné pole z jistých důvodů, které později uvidíme. I když by se to dalo nějakým způsobem rozšířit, zůstaneme omezeni na reálné pole s upozorněním na situace, kde by se to dalo rozšířit.

Definice 68

Uvažujme neprázdnou množinu $\mathcal{A} \neq \emptyset$, reálný vektorový prostor $\mathcal{V}$, $\dim \mathcal{V} = n$ a zobrazení $\varphi : \mathcal{A} \times \mathcal{A} \to \mathcal{V}$, kde φ splňuje:

1. $\varphi(X, Z) = \varphi(X, Y) + \varphi(Y, Z)\ \forall X, Y, Z \in \mathcal{A}$. *Respektuje sčítání vektorů*
2. $\exists O \in \mathcal{A}$ *tak, že* $\varphi_O : \mathcal{A} \to \mathcal{V}$ *definované* $\varphi_O(X) = \varphi(O, X)$ *je bijekce.*

Potom trojici $(\mathcal{A}, \mathcal{V}, \varphi)$ nazveme afinní prostor. Přičemž:

- *$\mathcal{A}$ označujeme jako nosič afinního prostoru a prvky $\mathcal{A}$ se nazývají body.*
- *$\mathcal{V}$ označujeme jako zaměření afinního prostoru a jeho prvky nazýváme (volné) vektory*

Příklad (Ověření afinního prostoru)

Mějme:

$$\mathcal{A} = \mathbb{R}^n \text{ (pouze kartézská mocnina)}$$
$$\mathcal{V} = \mathbb{R}^n \text{ (vektorový prostor, včetně potřebných operací)}$$
$$\varphi(X, Y) = (y_1 - x_1, \dots, y_n - x_n)$$

Musíme ověřit, zda je splněno všechno co je požadováno v definici afinního prostoru.

Kontrola splnění podmínek pro φ

1. $\varphi(X, Y) + \varphi(Y, Z) = (z_1 - x_1, \dots, z_n - x_n) = \varphi(X, Z)$
2. *Stačí zvoli* $O = [0, \dots, 0] : \varphi_0(X) = \varphi(O, X) = (x_1, \dots, x_n)$ *a tedy:* $\varphi_O : [x_1, \dots, x_n] \to (x_1, \dots, x_n)$

V bodu 2 vidíme, že se jedná o bijekci, obě podmínky jsou tedy splněny. Bod O v tomto případě dokonce můžeme zvolit zcela libovolně a pořád se bude jednat o bijekci. Což vlastně znamená, že je v této geometrii jedno kde zvolíme počátek.

Příklad (Ověření složitějšího afinního prostoru)

Mějme:

$$\mathcal{A} = \{[x_1, x_2] \in \mathbb{R}^2,\ \frac{x_1^2}{\alpha^2} - \frac{x_2^2}{\beta^2} = 1;\ \alpha > 0, \beta > 0\}$$
$$\mathcal{V} = \mathbb{R}$$
$$\varphi(X, Y) = x_2 - y_2$$

Jedná se o afinní prostor?

Je nutné ověřit platnost podmínek z definice affinního prostoru.

$\mathcal{A}$ je zjevně neprázdná množina, např. $[\alpha, 0] \in \mathcal{A}$. Navíc se jedná o rovnici hyperboly. Kontrola splnění podmínek pro φ

1. *První podmínka zjevně platí.*
2. *Druhou podmínku nelze v tomto případě splnit.*

Druhá podmínka nelze splnit protože vezmeme li libovolný bod $O = [o_1, o_2]$, potom můžeme vzít dva různé body $X = [a, x_2]$, $\overline{X} = [b, x_2]$ ležící na různých větvích hyperboly ve stejné výšce a dostaneme dva vzory, které se zobrazí na jeden obraz následovně:

$$\varphi_O(X) = x_n - o_2$$
$$\varphi_O(\overline{X}) = x_n - o_2$$

A nemůže se tedy jednat o bijekci, druhá podmínka tedy není splněna a nejedná se o afinní prostor.

Definice 69 (Repér afinního prostoru)
Uvažujme nosič afinního prostoru $\mathcal{A}$ se zvoleným počátkem O a zaměření afinního prostoru $\mathcal{V}$ na bázi $\mathcal{B} = (\vec{u_1}, \ldots, \vec{u_n})$. Potom můžeme uvažovat následující $(n+1)$-tici:

$$\langle O; \vec{u_1}, \ldots, \vec{u_n} \rangle$$

Kterou nazveme repér afinního prostoru.

Repér tedy vyjadřuje počátek a bázové vektory afinního prostoru.

Změna repéru obecně obsahuje dva kroky:

1. *Změnu báze vektorového prostoru (např. pomocí matice přechodu).*
2. *Posunutí počátku (přidání nějakého vektoru).*

Definice 70 (Polohový vektor (radius vektor))
Polohový vektor bodu x budeme značit $\vec{r}_x$

Příklad (Změna repéru)
Uvažjumě bod X vyjádřený v reperu $\mathcal{R}$ s počátkem O a bází $\mathcal{B}$:

$$X = [1, 1, 1]_{\mathcal{R}}$$
$$\mathcal{R} : O = [1, 2, 3],\ \vec{u_1} = (1, 1, 1),\ \vec{u_2} = (1, 1, 0),\ \vec{u_3} = (1, 0, 0)$$

Vyjádřete bod X v repéru $\overline{\mathcal{R}}$ s počátkem O_1 a bází $\overline{\mathcal{B}}$:

$$\overline{\mathcal{R}}: O = [3,2,1],\ \vec{u_1} = (1,2,3),\ \vec{u_2} = (0,2,3),\ \vec{u_3} = (0,3,2)$$

Báze $\mathcal{B}$ repéru $\mathcal{R}$ je zřejmě báze (má správnou hodnost). U báze $\overline{\mathcal{B}}$ repéru $\overline{\mathcal{R}}$ to není tak zřejmé na první pohled, ale také se jedná o korektní bázi, hodnost můžeme snadno ověřit úpravou na trojuhelníkový tvar.

Bod x můžeme poté v repéru $\overline{\mathcal{R}}$ vyjádřit následovně:

$$\vec{r}_{x_{\overline{\mathcal{R}}}} = \vec{r}_{x_{\mathcal{R}}} \cdot M(\overline{\mathcal{B}}, \mathcal{B}) + \vec{r}_{O_{\overline{\mathcal{R}}}}$$

Definice 71 (Dimenze afinního prostoru)
Uvažujme afinní prostor $(\mathcal{A}, \mathcal{V}, \varphi)$ dimenze afinního prostoru je dimenze jeho zaměření.

$$dim(\mathcal{A}, \mathcal{V}, \varphi) = dim \mathcal{V}$$

Definice 72 (Vnitřní součin)
Uvažujme reálný vektorový prostor $\mathcal{V}$, potom je vnitřní součin π defiován následovně:

$$\pi : \mathcal{V} \times \mathcal{V} \to \mathbb{R}$$

A musí splňovat následujicí podmínky:

1. $\pi(\vec{u} + \vec{v}, \vec{w}) = \pi(\vec{u}, \vec{v}) + \pi(\vec{v}, \vec{w})\ \forall \vec{u}, \vec{v}, \vec{w} \in \mathcal{V}$ *Aditivita v první složce*
2. $\pi(c \cdot \vec{u}, \vec{v}) = c \cdot \pi(\vec{u}, \vec{v})\ \forall c \in \mathbb{R}, \forall \vec{u}, \vec{v} \in \mathcal{V}$ *Homogenita v první složce*
3. $\pi(\vec{u}, \vec{v}) = \pi(\vec{v}, \vec{u})\ \forall \vec{u}, \vec{v} \in \mathcal{V}$ *Symetrie*
4. $\pi(\vec{u}, \vec{u}) \geq 0$ *a pokud* $\pi(\vec{u}, \vec{u}) = 0 \Rightarrow \vec{u} = \vec{o}$

První dvě podmínky dohromady se nazívají linearita, linearita je tedy aditivita + homogenita. Nutnost platnosti symetrie nám také implikuje nutnost platnosti aditivity a homogenity i v druhé složce.

Pokud jsou všechny tyto podmínky splněny, řekneme že π je vnitřní součin[30] na $\mathcal{V}$.

Nejčastěji je vnitřní součin definován následovně:

$$\pi(\vec{u}, \vec{v}) = \sum_{i=1}^{n} u_i \cdot v_i = u_1 \cdot v_1 + \ldots + u_n \cdot v_n$$

[30] Často se také říká skalární součin, případně dot product a místo $\pi(\vec{u}, \vec{v})$ pak používáme značení $\vec{u}\vec{v}$

Ale můžeme ho zavést i jinak, například nad $\mathbb{R}^2$ takto:

$$\pi_{new}(\vec{u}, \vec{v}) = 3 \cdot u_1 \cdot v_1 - u_1 \cdot v_2 - u_2 \cdot v_2 + 2 \cdot u_2 \cdot v_2$$

Důležité je splnění vlastností požadovaných z definice (které jsou v tomto případě splněny).

Nejobvyklejší vnitřní součin tedy není jediný a můžeme ho zavést i nějak jinak. V případě že ho zavedeme jinak, tak to má ovšem nějaké konsekvence, protože o vnitřní součin se opírá velikost vektorů, úhly mezi vektory a vlastně celá geometrie. Běžný vnitřní součin vede na základní „plochou" geometrii, které bude probírána dále.

Definice 73 (Euklidovský prostor)

Afinní prostor, na kterém je definovaný vnitřní součin nazveme Euklidovský prostor.

Definice 74 (Norma vektoru indukovaná vnitřním součinem)

$$||\vec{u}|| = \sqrt{\pi(\vec{u}, \vec{u})}$$

Definice 75 (Metrika indukovaná vnitřním součinem)

$$d(X, Y) = ||\varphi(X, Y)||$$

8 Osmá přednáška

8.1 Aplikace vnitřního součinu

Věta 15 (Schwarzova nerovnost)

$$\vec{u} \cdot \vec{v} \leq ||\vec{u}|| \cdot ||\vec{v}||$$

Důkaz. Předpokládejme, že $\vec{u} = \vec{v}$, potom:

$$LS : |\vec{u} \cdot \vec{u}|$$
$$PS : \sqrt{\vec{u} \cdot \vec{u}} \cdot \sqrt{\vec{u} \cdot \vec{u}} = \sqrt{(\vec{u} \cdot \vec{u})^2}$$
$$LS = PS$$

Nyní předpokládejme, že $\vec{u} \neq \vec{v}$, potom:

$$(t\vec{u} + \vec{v})^2 \leq 0 \ \forall t \in \mathbb{R} \text{ tzn. i pro } t = \frac{-\vec{u} \cdot \vec{v}}{\vec{u}^2}$$

Dosadíme t a upravíme:

$$(\frac{-\vec{u} \cdot \vec{v}}{\vec{u}^2}\vec{u} + \vec{v})^2 \geq 0$$
$$(\frac{-\vec{u} \cdot \vec{v}}{\vec{u}^2}\vec{u} + \vec{v})(\frac{-\vec{u} \cdot \vec{v}}{\vec{u}^2}\vec{u} + \vec{v}) \geq 0$$
$$\frac{\vec{u}^2\vec{v}^2}{\vec{u}^4}\vec{u}^2 - 2\frac{\vec{u}\vec{v}}{\vec{u}^2} + \vec{v}^2 \geq 0$$
$$\vec{u}^2\vec{v}^2 - 2\vec{u} \cdot \vec{v}\vec{u} \cdot \vec{v} + \vec{u}^2\vec{v}^2 \geq 0$$
$$\vec{u}^2\vec{v}^2 \geq (\vec{u}\vec{v})^2$$
$$||\vec{u}|| \cdot ||\vec{v}|| \geq |\vec{u} \cdot \vec{v}|$$

□

Když nyní vezmeme následující výraz:

$$\frac{|\vec{u} \cdot \vec{v}|}{||\vec{u}|| \cdot ||\vec{v}||}$$

Budeme předpokládat, že $\vec{u}$ a $\vec{v}$ jsou nenulové vektory, potom díky Schwarzově nerovnosti můžeme vyvodit následující ohraničení:

$$0 \leq \frac{|\vec{u} \cdot \vec{v}|}{||\vec{u}|| \cdot ||\vec{v}||} \leq 1$$

A když odstraníme absolutní hodnotu v čitateli:

$$-1 \leq \frac{\vec{u} \cdot \vec{v}}{||\vec{u}|| \cdot ||\vec{v}||} \leq 1$$

Když si uvědomíme, jak vypadá funkce *cosinus* na intervalu $\langle 0, \pi \rangle$, která je na tomto intervalu monotonní. Tak dostaneme jednoznačně dané $\varphi \in \langle 0, \pi \rangle$ takto:

$$cos\varphi = \frac{\vec{u} \cdot \vec{u}}{||\vec{u}|| \cdot ||\vec{v}||}$$

Toto φ pak nazveme odchylka vektorů $\vec{u}$ a $\vec{v}$.

8.2 Gram-Schmidtův ortogonalizační proces

Definice 76 (Ortogonální báze)
Uvažujme bázi $\mathcal{B}$ v případě, že jsou všechny vektory této báze navzájem ortogonální, tedy jejich odchylka je $\varphi = \frac{\pi}{2}$, potom takovou bázi nazveme ortogonální.

Definice 77 (Ortonormální báze)
Je li báze $\mathcal{B}$ ortogonální a k tomu jsou všechny její vektory jednotkové, nazveme tuto bází ortonormální.

Nyní budeme řešit úlohu, jak nějakou libovolnou bázi ortogonalizovat, případně i ortonormalizovat. Tento proces se jmenuje Gramschmituv proces.

Předpokládejme, že máme nějaký vektorový prostor $\mathcal{V}$ a jeho bázové vektory $\vec{v_1}, \ldots, \vec{v_n}$ Nyní hledáme ortogonální bázi $\vec{u_1}, \ldots, \vec{u_n}$. První vektor můžeme vzít stejný jako z původní báze:

$$\vec{u_1} = \vec{v_1}$$

Další vektor potřebujeme vhodně „naklonit“, aby byl ortogonální k $\vec{u_1}$ a můžeme ho vyjádřit takto:

$$\vec{u_2} = \vec{v_2} - c \cdot \vec{u_1}$$

$$\vec{u_1} \cdot \vec{u_2} = 0$$

Dosadíme u_2 z první rovnice do druhé a vyjádříme c:

$$\vec{u_1} \cdot (\vec{v_2} - c \cdot \vec{u_1}) = 0$$
$$\vec{u_1} \cdot \vec{v_2} - \vec{u_1} \cdot c \cdot \vec{u_1} = 0$$
$$c = \frac{-\vec{u_1} \cdot \vec{v_2}}{\vec{u_1} \cdot \vec{u_1}}$$

A druhý $\vec{v_2}$ nové báze tedy určíme jako

$$\vec{u_2} = \vec{v_2} - \frac{-\vec{u_1} \cdot \vec{v_2}}{\vec{u_1} \cdot \vec{u_1}} \cdot \vec{u_1}$$

Stejným způsobem bychom pokračovali dále a $\vec{u_3}$ stejným způsobem vyjádřili jako

$$\vec{u_3} = \vec{v_3} - \frac{\vec{u_1} \cdot \vec{v_3}}{\vec{u_1} \cdot \vec{u_1}} \cdot \vec{u_1} - \frac{\vec{u_2} \cdot \vec{v_3}}{\vec{u_2} \cdot \vec{u_2}} \cdot \vec{u_2}$$

Tímto způsobem můžeme tedy nalézt ortogonální bázi, pokud potřebujeme bázi ortonormální, tak stačí najít ortogonální bázi a znormalizovat všechny její vektory takto:

$$\vec{w_i} = \frac{\vec{u_i}}{||\vec{u_i}||}$$

Příklad (Využití Gram-Schmidtova procesu k ortogonalizaci a ortonormalizaci báze)
Uvažujme vektorový prostor $\mathcal{V} = \mathbb{R}^5$ a množinu vektorů $\mathcal{W}$:

$$\mathcal{W} = \{(\vec{v_1}, \vec{v_2}, \vec{v_3}, \vec{v_4}, \vec{v_5}); \vec{v_1} + \vec{v_3} = \vec{v_2},\ \vec{v_3} + \vec{v_5} = 2 \cdot \vec{v_4}\}$$

1. *Ukažte, že $\mathcal{W}$ je vektorový podprostor vektorového prostoru $\mathcal{V}$ a najděte nějakou jeho bázi.*

2. *Bázi pomocí G-S procesu ortogonalizujte a následně ortonormalizujte.*

$\mathcal{W}$ můžeme o něco jasněji vyjádřit takto:

$$\mathcal{W} = \{(a, a + b, b, c, 2 \cdot c - b);\ a, b, c \in \mathbb{R}\}$$

K ověření že se jedná o vektorový podprosto by bylo nutné ověřit podmínky z definice vektorového podprostoru. Ty tady zjevně platí. A bázi $\mathcal{W}$ můžeme zvolit následovně:

$$\mathcal{B} = \{\vec{v_1} = (1, 1, 0, 0, 0),\ \vec{v_2} = (0, 0, 0, 1, 2),\ \vec{v_3} = (0, 1, 1, 0, -1)\}$$

Určitě se jedná o bázi, protože $\vec{v_1}$ vlastně vyjadřuje složku a, $\vec{v_3}$ vyjadřuje složku b, a $\vec{v_2}$ vyjadřuje složku c.

Můžeme si všimnout, že vektory $\vec{v_1}$ a $\vec{v_2}$ už jsou ortogonální:

$$\vec{v_1} \cdot \vec{v_2} = 0$$

Proto ho můžeme také rovnou využít a zjednodušit si práci.

$$\vec{u_1} = \vec{v_1} = (1, 1, 0, 0, 0)$$
$$\vec{u_2} = \vec{v_2} = (0, 0, 0, 1, 2)$$

A pomocí těchto $\vec{u_1}$ a $\vec{u_2}$ vyjádříme k nim ortogonální $\vec{u_3}$:

$$\vec{u_3} = \vec{v_3} - \frac{\vec{u_1} \cdot \vec{v_3}}{\vec{u_1} \cdot \vec{u_1}} \cdot \vec{u_1} - \frac{\vec{u_2} \cdot \vec{v_3}}{\vec{u_2} \cdot \vec{u_2}} \cdot \vec{u_2}$$
$$\vec{u_3} = (0, 1, 1, 0, -1) - \frac{1}{2} \cdot (1, 1, 0, 0, 0) - \frac{-2}{5} \cdot (0, 0, 0, 1, 2)$$
$$\vec{u_3} = (0, 1, 1, 0, -1) - (\frac{1}{2}, \frac{1}{2}, 0, 0, 0) - (0, 0, 0, \frac{-2}{5}, \frac{-4}{5})$$
$$\vec{u_3} = (\frac{-1}{2}, \frac{1}{2}, 1, \frac{2}{5}, \frac{-1}{5})$$

Ortogonální bázi $\mathcal{B}_{ortg}$ vektorového podprostoru $\mathcal{W}$ můžeme tedy vyjádřit jako:

$$\mathcal{B}_{ortg} = \{\vec{u_1} = (1, 1, 0, 0, 0),\ \vec{u_2} = (0, 0, 0, 1, 2),\ \vec{v_3} = (\frac{-1}{2}, \frac{1}{2}, 1, \frac{2}{5}, \frac{-1}{5})\}$$

A následně můžeme bázi $\mathcal{B}_{ortg}$ normalizovat a dostat ortonormální bázi $\mathcal{B}_{ortn} = \{\vec{w_1}, \vec{w_2}, \vec{w_3}\}$:

$$\vec{w_1} = \vec{u_1} \cdot \frac{1}{||\vec{u_1}||} = (1, 1, 0, 0, 0) \cdot \frac{1}{\sqrt{2}} = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0, 0, 0)$$
$$\vec{w_2} = \vec{u_2} \cdot \frac{1}{||\vec{u_2}||} = (0, 0, 0, 1, 2) \cdot \frac{1}{\sqrt{5}} = (0, 0, 0, \frac{1}{\sqrt{5}}, \frac{2}{\sqrt{5}})$$
$$\vec{w_3} = \vec{u_3} \cdot \frac{1}{||\vec{u_3}||} = (\frac{-1}{2}, \frac{1}{2}, 1, \frac{2}{5}, \frac{-1}{5}) \cdot \frac{1}{\sqrt{\frac{17}{10}}} = (\frac{-1}{2 \cdot \sqrt{\frac{17}{10}}}, \frac{1}{2 \cdot \sqrt{\frac{17}{10}}}, \frac{1}{\sqrt{\frac{17}{10}}}, \frac{2}{5 \cdot \sqrt{\frac{17}{10}}}, \frac{-1}{5 \cdot \sqrt{\frac{17}{10}}})$$

Příklad (Využití Gram-Schmidtova procesu k ortogonalizaci báze)

Uvažujme vektorový prostor $\mathcal{V} = \mathbb{R}^6$ a podprostor $\mathcal{W}$ definovaný následovně:

$$\mathcal{W} = \{(\vec{v_1}, \vec{v_2}, \vec{v_3}, \vec{v_4}, \vec{v_5}, \vec{v_6});\ \vec{v_1} + \vec{v_2} + \vec{v_3} = \vec{v_4} + \vec{v_5},\ \vec{v_1} + \vec{v_3} + \vec{v_4} = 2 \cdot \vec{v_2} + \vec{v_5},\ 3 \cdot \vec{v_1} - \vec{v_4} = 3 \cdot \vec{v_2} - \vec{v_5}\}$$

1. *Ukažte, že $\mathcal{W}$ je vektorový podprostor vektorového prostoru $\mathcal{V}$ a najděte nějakou jeho bázi.*

2. *Bázi pomocí G-S procesu ortogonalizujte.*

Upravami lineárních rovnic vyjádříme vztahy ve vhodnějším tvaru:

$$\vec{v_4} = \frac{3}{2}\vec{v_2}$$
$$\vec{v_3} = -4\vec{v_1} + 5\vec{v_2}$$
$$\vec{v_5} = -3\vec{v_1} + \frac{9}{2}\vec{v_2}$$

A z nich můžeme vytvořit vhodnější předpis vektorového podprostoru $\mathcal{W}$:

$$\mathcal{W} = \{(b, a, -4b + 5a, \frac{3a}{2}, -3b + \frac{9a}{2}, c)\}$$

Z toho můžeme odvodit bází $\mathcal{B}$:

$$\mathcal{B} = \{\vec{v_2} = (1, 0, -4, 0, -3, 0), \vec{v_3} = (0, 2, 10, 3, 9, 0), \vec{v_1} = (0, 0, 0, 0, 0, 1)\}$$

Vydíme že poslední vektor je kolmý s prvním i druhým. Prvná dva mezi sebou však kolmé nejsou.

$$\vec{u_1} = \vec{v_1}$$
$$\vec{u_2} = \vec{v_2}$$
$$\vec{u_3} = \vec{v_3} - \frac{\vec{v_3} \cdot \vec{u_1}}{\vec{u_1} \cdot \vec{u_1}} \cdot \vec{u_1} - \frac{\vec{v_3} \cdot \vec{u_2}}{\vec{u_2} \cdot \vec{u_2}}\vec{u_2} = (0, 2, 10, 3, 9, 0) + \frac{67}{26} \cdot (1, 0, -4, 0, -3, 0)$$

Jako další příklad aplikace vnitřního součinu můžeme uvést definici roviny pomocí proměnného polohového vektoru $\vec{r} = (x, y, z)$ a pevného normálového vektoru $\vec{n} = (a, b, c)$ takto:

$$\vec{r} \cdot \vec{n} = d$$

8.3 Další druhy součinu

Definice 78 (Vnější součin)

Vnější součin n vektorů $\vec{u_1} \dots \vec{u_n}$ budeme značit jako $[\vec{u_1}, \dots, \vec{u_n}]$ a definujeme ho takto:

$$[\vec{u_1}, \dots, \vec{u_n}] = \begin{vmatrix} u_{11} & \dots & u_{1n} \\ \vdots & \ddots & \vdots \\ u_{n1} & \dots & u_{nn} \end{vmatrix}$$

Operace vnějšího součinu má aplikaci ve výpočtu n-rozměrného objemu. V případě že nejsou vektory souhlasně orientované s vektory báze, výjde záporný.

Jedná se o zobrazení $\mathcal{V} \times \ldots \times \mathcal{V} \to F$

Definice 79 (Vektorový součin)

Vektorový součin je $(n-1)$-arní operace $\mathcal{V} \times \ldots \times \mathcal{V} \to \mathcal{V}$ definovaná takto:

$$\vec{u_1} \times \ldots \times \vec{u_n} = \begin{vmatrix} v_{11} & \ldots & v_{1n} \\ \vdots & \ddots & \vdots \\ v_{(n-1)1} & \ldots & v_{(n-1)n} \\ \vec{e_1} & \ldots & \vec{e_n} \end{vmatrix}$$

kde vektory $\vec{e_1}, \ldots, \vec{e_n}$ jsou vektory kanonické báze F^n.

8.4 Geometrie

Definice 80 (Afinní podprostor)

Víme, že obecně v afinním prostoru můžeme k nějakému bodu A přičíst vektor. Stejně tak ovšem můžeme k bodu A přičíst nějaký vektorový podprostor $\mathcal{W}$, čímž dostaneme množinu, které budeme říkat afinní podprostor.

$$A + \mathcal{W}$$

V případě, že je vektorový podprostor $\mathcal{W}$ dimenze 0, dostaneme takto afinní podprostor, který představuje bod.

Pokud je vektorový prostor $\mathcal{W}$ dimenze 1, dostaneme afinní podprostor, který představuje přímku.

A tak dále...

Budeme pracovat v prostoru E_2, respektive E_3, což je afinní prostor s vektorovým prostorem $\mathbb{R}^2$ respektive $\mathbb{R}^3$ a nosičem $\mathbb{R}^2$ respektive $\mathbb{R}^3$ a vnitřním součinem $\pi(\vec{u}, \vec{v}) = \sum_{i=1}^{n} u_i \cdot v_i$

V prostoru E_2 lze uvažovat tyto afinní podprostory:

- bod
- přímka

V prostoru E_3 lze uvažovat tyto afinní podprostory:

- bod
- přímka
- rovina

Definice 81 (Přímka v E_3)

Přímka v E_3 je množina bodů, kterou můžeme parametricky vyjádřit jako:

$$X = A + t \cdot \vec{u}$$

Nebo v rozepsaném tvaru:

$$x = a_1 + t \cdot u_1$$
$$y = a_2 + t \cdot u_2$$
$$z = a_3 + t \cdot u_3$$

Vyloučením parametru t dostaneme dvě obecné rovnice přímky.

Příklad (Vyjádření přímky v obecném tvaru z bodu a vektoru)

$$A = [0, 1, 0]$$
$$\vec{u} = (1, 1, 2)$$

$$x = 0 + t$$
$$y = 1 + t$$
$$z = 0 + 2t$$

Vyloučíme parametr t:

$$x - y + 1 = 0$$
$$2x - z = 0$$

Definice 82 (Rovina v E_3)

Rovina v E_2 je množina bodů, kterou můžeme parametricky vyjádřit jako:

$$A + t \cdot \vec{u} + s \cdot \vec{v}$$

Nebo v rozepsaném tvaru:

$$x = a_1 + t \cdot u_1 + s \cdot v_1$$
$$y = a_2 + t \cdot u_2 + s \cdot v_2$$
$$z = a_3 + t \cdot u_3 + s \cdot v_3$$

Vyloučením parametrů t a s dostaneme jednu obecnou rovnici roviny.

Příklad (Vyjádření roviny ze tří bodů)

$$A = [3, 5, 3]$$
$$B = [-2, 1, -1]$$
$$C = [7, 6, 4]$$

Z bodů vytvoříme dva vektory:

$$\vec{AB} = [-5, -4, -4] = \vec{u}$$
$$\vec{AC} = [4, 1, 1] = \vec{v}$$

Vidíme že jsou nezávislé a můžeme z nich vytvořit parametrické rovnice roviny.

$$x = 3 - 5 \cdot t + 4 \cdot s$$
$$y = 5 - 4 \cdot t + s$$
$$z = 3 - 4 \cdot t + s$$

Vyloučíme parametr odečtením druhé a třetí rovnice:

$$y - z = 2$$

8.4.1 Vzájemné polohy dvou přímek

V prostoru E_3 važujme přímku p definovanou bodem A a vektorem $\vec{u}$. A přímku q definovanou bodem B a vektorem $\vec{v}$:

$$p: \quad A, \vec{u}$$
$$q: \quad B, \vec{v}$$

Sestrojíme matice K a L:

$$K = \begin{pmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{pmatrix}$$
$$L = \begin{pmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \\ b_1 - a_1 & b_2 - a_2 & b_3 - a_3 \end{pmatrix}$$

Potom můžeme vzájemnou polohu klasifikovat pomocí hodností matic K a L tak jak je popsáno tabulce 8

	h(K)	$h(L)$
totožné	1	1
rovnoběžné	1	2
různoběžné	2	2
mimoběžné	2	3

Tabulka 8: Klasifikace vzájemné polohy dvou přímek v E_3

9 Devátá přednáška

9.1 Geometrie

Příklad (Příčka mimoběžek)

Mějme přímky p a q a bod K:

$$
\begin{aligned}
p: &\quad A = [2,1,1],\ B = [3,2,6] \\
q: &\quad C = [2,-5,-1],\ D = [0,-4,3] \\
K &= [-3,0,3]
\end{aligned}
$$

Bodem K veďte příčku r k mimoběžkám p, q.

Pro ověření že p a q jsou mimoběžky vytvoříme matici P a určíme její hodnost.

$$
P = \begin{pmatrix} \vec{AB} \\ \vec{CD} \\ \vec{AC} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 5 \\ -2 & 1 & 4 \\ 0 & -6 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 5 \\ 0 & 3 & 14 \\ 0 & -6 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 5 \\ 0 & 3 & 14 \\ 0 & 0 & 26 \end{pmatrix} = R
$$

$$h(R) = 3 = h(P)$$

Matice má plnou hodnost 3 *a určitě se tedy jedná o mimoběžky.*

Máme tedy dvě přímky, které jsou mimoběžné a bod K, nyní hledáme přímku, která prochází bodem K a zároveň má nějaké body P, Q, které tvoří průsečíky s přímkami p, q.

Pomocí vektoru $\vec{AB}$ a bodu A vyjádříme bod P pomocí parametru t:

$$P = [2+t, 1+t, 1+5t]$$

Podobně pomocí vektoru $\vec{CB}$ a bodu C vyjádříme bod Q pomocí parametru s:

$$Q = [2-2s, -5+s, -1+4s]$$

Nyní vyjádříme vektory $\vec{KP}$ a $\vec{KQ}$ o kterých víme, že mají být lineárně závislé.

$$
\begin{aligned}
\vec{KP} &= [5+t, 1+t, -2+5t] \\
\vec{KQ} &= [5-2s, -5+s, -4+4s]
\end{aligned}
$$

A z toho, že vektory $\vec{KP}$ a $\vec{KL}$ mají být lineárně závislé můžeme odvodit:

$$\vec{KP} = l \cdot \vec{KQ}$$

$$(5 + t, 1 + t, -2 + 5t) = l \cdot (5 - 2s, -5 + s, -4 + 4s)$$

Uvážíme li proměnné t, l, ls, potom dostaneme soustavu 3 lineárních rovnic o třech neznámých.

$$\left(\begin{array}{ccc|c} 1 & -5 & 2 & -5 \\ 1 & 5 & -1 & -1 \\ 5 & 4 & -4 & 2 \end{array}\right)$$

Z této soustavy nám k vyřešení úlohy stačí vyjádřit neznámou k, nebo s, k čemuž se nám hodí cramerovo pravidlo:

$$t = \frac{\begin{vmatrix} -5 & -5 & 2 \\ -1 & 5 & -1 \\ 2 & 4 & -4 \end{vmatrix}}{\begin{vmatrix} 1 & -5 & 2 \\ 1 & 5 & -1 \\ 5 & 4 & -4 \end{vmatrix}} = \frac{100 - 8 + 10 - (20 + 20 - 20)}{-20 + 8 + 25 - (50 - 4 + 20)} = \frac{78}{-53}$$

A můžeme vyjádřit vektoř $\vec{KT}$:

$$KP = (\frac{265 - 82}{53}, \frac{53 - 82}{53}, \frac{-106 - 410}{53}) = (\frac{183}{53}, \frac{-29}{53}, \frac{-516}{53})$$

Nás zajímá pouze směr tohoto vektoru, můžeme si pomocí něj tedy určit směrový vektor, který bude vhodně vynásobený:

$$\vec{u} = (183, -29, -516)$$

9.1.1 Úlohy o vzdálenostech

Vzdálenost dvou bodů můžeme vyjádřit jako

$$d(A, B) = ||\varphi(A, B)|| = \sqrt{\pi(\varphi(A, B)), \varphi(A, B)} = \sqrt{(b_1 - a_1)^2 + \ldots + (b_n - a_n)^2}$$

9.1.2 Vzdálenost bodu a přímky

Máme nějaký bod A a přímku p a chceme zjistit jejich vzájemnou vzdálenost $d(A, p)$. Pro tento problém existuje obecný vzorec. Nám jde ale spíše o to, jak takový vzorec odvodit, než ho jen použít.

Možnost řešení: vezmeme rovinu ρ která bude kolmá k p a zároveň bude procházet bodem A, najdeme průsečík K roviny ρ a přímky p (který bude jediný) a spočítáme vzdálenost bodů K a A.

9.1.3 Vzdálenost bodu a roviny

V případě vzdálenosti bodu a roviny můžeme použít obdobný přístup. Máme nějaký bod A a rovinu ρ, chceme spočítat $d(A, \rho)$.

K rovině najdeme kolmou přímku p, která prochází bodem A. Najdeme průsečík K přímky p a roviny ρ, a spočítáme vzdálenost bodů K a A.

9.1.4 Vzdálenost dvou rovnoběžných přímek

Máme dvě rovnoběžky p a q a chceme vypočítat jejich vzájemnou vzdálenost $d(p, q)$.

Na jedné z rovnoběžek si můžeme zvolit libovolný bod a postupovat stejně jako při výpočtu vzdálenosti bodu a přímky.

9.1.5 Vzdálenost prímky od roviny

Máme přímku p a rovnoběžnou rovinu ρ a chceme spočítat jejich vzájemnou vzdálenost $d(p, \rho)$.

Na přímce p můžeme zvolíme libovolný bod a postupovat stejně jako při výpočtu vzdálenosti bodu a roviny.

9.1.6 Vzdálenost dvou rovnoběžných rovin

Máme dvě rovnoběžné roviny ρ a σ a chceme spočítat $d(\rho, \sigma)$.

Na jedné z rovin si můžeme zvolit libovolný bod a postupovat stejně jako při výpočtu vzdálenosti roviny a bodu.

9.1.7 Vzdálenost dvou mimoběžných přímek

Máme dvě mimoběžné přímky p a q a chceme spočítat jejich vzájemnou vzdálenost $d(p, q)$.

Vezmeme dvě navzájem rovnoběžné roviny a v nichž leží přímky p a q. Normálový vektor rovin můžeme najít jako cross product směrových vektorů přímek p a q. A následně můžeme postupovat jako v případě vzdálenosti dvou rovin.

9.2 Úlohy o úhlech

Nejprve si připomeňme co je to odchylka vektorů. Odchylka vektorů $\vec{u}$ a $\vec{v}$ se definuje jako $\varphi \in \langle 0, \pi \rangle$, které splňuje:

$$cos\,\varphi = \frac{\vec{u} \cdot \vec{v}}{||\vec{u}|| \cdot ||\vec{v}||}$$

9.2.1 Vzájemný úhel dvou přímek

Úhel dvou různoběžných přímek budeme brát jako menší z úhlů, které mezi sebou svírají, a můžeme ho určit jako:

$$cos\,\varphi = \frac{|\vec{u} \cdot \vec{v}|}{||\vec{u}|| \cdot ||\vec{v}||}$$

kde || v čitateli vyjadřuje absolutní hodnotu.

V případě že přímky budou mimoběžné, tak jejich úhel vypočítáme úplně stejně a vždycky to bude pravý úhel.

9.2.2 Vzájemný uhel přímky a roviny

Máme rovinu ρ a přímu p, které tuto rovinu protíná. A chceme spočítat jejich vzájemný úhel.

Zkonstruujeme pomocnou rovinu σ, která je kolmá na rovinu φ ve které leží přímka p. K vytvoření této roviny stačí vzít bod na přímce p, směrový vektor přímky p a normálový vektor roviny ρ. Roviny ρ a σ se poté protnou v přímce q A nyní stačí spočítat vzájemný úhel přímek p a q.

9.2.3 Vzájemný úhel dvou rovin

Úhle dvou roviny můžeme vypočítat jako odchylku normálových vektorů, které vezmeme tak, aby jejich odchylka byla $\leq \frac{\pi}{2}$

9.2.4 Souhrnný příklad

Příklad (Souhrnný příklad)

Rovina ρ prochází body $A = [2, 1, 2]$, $B = [4, 0, 1]$ a $C = [-3, 3, 4]$. Rovina σ je rovnoběžná s ρ a má od ní vzdálenost $4\sqrt{2}$. Na rovině σ leží bod $S = [5, 0, ?]$

Spočtěte vzdálenost B a S.

Nejprve si vyjádříme obecnou rovnici roviny ρ:

$$x = 2 + 2t - 5s$$
$$y = 1 - 1t + 2s$$
$$z = 2 - 1t + 2s$$

$$y - z + 1 = 0$$

Normálový vektor $\vec{n}$ k rovině σ je tedy $\vec{n} = (0, 1, -1)$ a rovinu ρ pomocí něj můžeme vyjádřit jako:

$$y - z + d = 0$$

Musíme však ještě vyjádřit neznámou d.

Normálový vektor $\vec{n}$ upravíme tak, aby jeho délka byla rovna vzdálenosti obou rovin.

$$||\vec{n}|| = \sqrt{0^2 + 1^2 + (-1)^2} = \sqrt{2}$$
$$\vec{n_1} = 4 \cdot \vec{n} = (0, 4, -4)$$
$$\vec{n_2} = -4 \cdot \vec{n} = (0, -4, 4)$$

Nyní přičteme $\vec{n_1}$ k nějakému bodu $E = [0, 0, 1]$, který leží na ρ a dostaneme bod, který leží na σ:

$$S_1 = R + \vec{n_1} = [0, 4, -3]$$
$$S_2 = R + \vec{n_2} = [0, -4, 5]$$

A dosazením do rovnice pro rovinu σ můžeme získat hodnotu neznámé d, pro který máme dvě možná řešení.

$$\sigma_1 : \; y - z - 7 = 0$$
$$\sigma_2 : \; y - z + 9 = 0$$

Nyní můžeme podle obecné rovnice pro rovinu σ vyjádřit bod S.

$$S_1 = [5, 0, -7]$$
$$S_2 = [5, 0, 9]$$

A teď už jen spočítáme vzdálenosti bodů jak je požadování v zadání.

$$d(B, S_1) = \sqrt{1 + 0 + 64} = \sqrt{65}$$
$$d(B, S_2) = \sqrt{1 + 0 + 64} = \sqrt{65}$$

9.3 Formy

Uvažujme dva vektorové prostory $\mathcal{V}$ a $\mathcal{W}$, obecně nad nějakým polem F. A uvažujme množinu všech homomorfismů z $\mathcal{V}$ do $\mathcal{W}$, kterou budeme značit jako:

$$Hom(\mathcal{V}, \mathcal{W})$$

Tyto homomorfismy můžeme sčítat, mějme nějaké dva konkrétní homomorfismy $\alpha, \beta \in Hom(\mathcal{V}, \mathcal{W})$, potom můžeme zavést operaci sčítání jako:

$$(\alpha + \beta)(\vec{v}) = \alpha(\vec{v}) + \beta(\vec{v})$$

Kde znak + na levé straně představuje novou operaci sčítání homomorfismů, kterou právě definujeme a + na pravé straně představuje sčítání ve vektorovém prostoru $\mathcal{W}$.

Takto definované sčítání homomorfismů splňuje axiomy Abelovské grupy (asociativita, neutrální prvek, inverzní prvek, komutativita). Asociativita a komutativita zjevně platí a vyplývá z asociativity a komutativity ve vektorovém prostoru $\mathcal{W}$.

O něco zajímavější je neutrální prvek, musíme najít takový homomorfismus, který bude tvořit neutrální prvek. A bude jím nulový homomorfismus o (homomorfismus, který libovolný vektor zobrazí na nulový vektor).

Inverzním prvkem je potom opačný homomorfismus.

Podobně můžeme definovat operaci pro násobení homomorfismu skalárem:

$$(k \cdot \alpha)(\vec{v}) = k \cdot \alpha(\vec{v})$$

A takto definované násobení skalárem zjevně splňuje podmínky pro násobení skalárem z definice vektorového prostoru.

$Hom(\mathcal{V}, \mathcal{W})$ v kombinaci s výše definovanými operacemi + a $\cdot$ tedy tvoří vektorový prostor nad nějakým tělesem F.

Příklad (Homomorfismus)

$$\mathcal{V} = \mathbb{R}^2$$
$$\mathcal{W} = \mathbb{R}^3$$
$$\alpha(\vec{v}) = \alpha((v_1, v_2)) = (\alpha_{11} \cdot v_1 + \alpha_{12} \cdot v_2,\ \alpha_{21} \cdot v_1 + \alpha_{22} \cdot v_2,\ \alpha_{31} \cdot v_1 + \alpha_{32} \cdot v_2)$$

V tomto případě tedy bude celkem 6 souřadnic homomorfismu a jedná se tedy o vektorový prostor s dimenzí 6. Obecně pak platí, že dimenze homomorfismu je rovna součinu dimenzí obou vektorových prostorů.

$$dim\,\alpha = dim\,\mathcal{V} \cdot dim\mathcal{W} = 2 \cdot 3 = 6$$

Uvažujme specialní případ, kdy $\mathcal{W} = F$. Máme tedy $Hom(\mathcal{V}, F)$, což je opět vektorový prostor, a protože toto je dosti specialní, že cílový prostor je přímo to pole, tak má i specialní označení $\mathcal{V}^*$ a říkáme mu dualní prostor

$$\mathcal{V}^* = Hom(\mathcal{V}, F)$$

Jeho prvky jsou samozřejmě vektory, ale budeme je nazývat lineární formy.

Dále budeme pro běžné vektory používat značení s šipkou jako doposud, například:

$$\vec{u}, \vec{v}, \ldots \in \mathcal{V}$$

Ale pro vektory, které jsou linearními formami budeme používat řecká písmena:

$$\alpha, \beta, \ldots \in \mathcal{V}^*$$

Formu můžeme aplikovat na nějaký vektor:

$$\alpha(\vec{u})$$

Výsledkem této operace pak bude nějaké číslo, respektive prvek nějakého pole F, nad kterým pracujeme.

Dimenze dualního prostoru je stejná jako dimence původního protostu, protože dimenzi lze opět vyjádřit jako součin dimenzí jednotlivých prostorů a dimenze F je 1. Dimenzi $\mathcal{V}$ tedy pouze vynásobíme jedničkou a dostaneme opět stejnou dimenzi.

$$dim\,\mathcal{V}^* = dim\,\mathcal{V} \cdot dim\,F = dim\,\mathcal{V} \cdot 1 = dim\,\mathcal{V}$$

Nyní si můžeme klást zajímavou otázku: Když budeme mít nějaký vektorový prostor $\mathcal{V}$ s nějakou bází, tak jakou bázi má k němu dualní prostor $\mathcal{V}^*$?

Uvažujme vektorový prostor $\mathcal{V}$ s bází $\mathcal{B}$

$$\mathcal{V}\ \mathcal{B} = \{\vec{v_1}, \ldots, \vec{v_n}\}$$

Zřejmě $dim\mathcal{V} = |\mathcal{B}| = n$ Potom bázi duálního prostoru $\mathcal{V}^*$ označme $\alpha_1, \ldots, \alpha_n$ a můžeme ji vzít takto:

$$\alpha_i(\vec{v_j}) = \delta_{ij}$$

Kde δ představuje Kroneckerovo delta, tedy 1 pokud $i = j$ a 0 v případě že $i \neq j$. Což zjevně není jednoznačné a můžeme mít více možností.

Pak můžeme libovolnou linearní formu $\varphi \in \mathcal{V}^*$ vyjádřit jako linearní kombinaci prvků báze:

$$c_1 \cdot \alpha_1 + \ldots + c_n \cdot \alpha_n$$

Stačí vzít c_i jako $\varphi(\vec{v_i})$.

$$\varphi(\vec{v_1}) = c_1\alpha_1(\vec{v_1}) + \ldots + c_n\alpha_n(\vec{v_n}) = \varphi(\vec{v_1})\delta_{11} + \varphi(\vec{v_2})\delta_{12} + \ldots + \varphi(\vec{v_m})\delta_{1n} = \varphi(\vec{v_1}) + 0 + \ldots + 0 = \varphi(\vec{v_1})$$
$$\varphi(\vec{v_2}) = \varphi(\vec{v_2})$$
$$\varphi(\vec{v_3}) = \varphi(\vec{v_3})$$
$$\vdots$$

Kroneckerovo delta nám tedy zajistí, že formu φ skutečně vyjádříme jako linearní kombinaci bázových forem.

Příklad

Vektorový prostor $\mathcal{V} \subseteq \mathbb{R}^5$ je dán vztahy:

$$v_1 = v_2$$

$$v_1 + v_2 + v_3 = v_4 + v_5$$

Určete bázi a dimenzi $\mathcal{V}$ a najděte bázi $\mathcal{V}^*$.

$$\mathcal{V} = \{(a, a, b, c, 2a + b - c) \forall a, b, c \in \mathbb{R}\}$$

Dimenze vektorového prostoru je $\mathcal{V}$ tedy 3. A jeho bázi můžeme vyjádřit jako:

$$\mathcal{B} = \Big((1,1,0,0,2),(0,0,1,0,1),(0,0,0,1,-1)\Big)$$

Získali jsme tedy bázi prostoru $\mathcal{V}$ a nyní z ní chceme sestrojit bázi duálního prostoru $\mathcal{V}^*$.

Báze dualního prostoru se v tomto případě bude skládat ze tří forem α_1, α_2, α_3.

Nejprve vyjádříme α_1.

$$\alpha_1(\vec{v_1}) = 1$$

$$\alpha_1(\vec{v_2}) = 0$$

$$\alpha_1(\vec{v_3}) = 0$$

Z toho můžeme odvodit následujicí rovnice:

$$\begin{aligned}
\alpha_{11} \cdot 1 + \alpha_{12} \cdot 1 + \alpha_{13} \cdot 0 + \alpha_{14} \cdot 0 + \alpha_{15} \cdot 2 = 1 \\
\alpha_{11} \cdot 0 + \alpha_{12} \cdot 0 + \alpha_{13} \cdot 1 + \alpha_{14} \cdot 0 + \alpha_{15} \cdot 1 = 0 \\
\alpha_{11} \cdot 0 + \alpha_{12} \cdot 0 + \alpha_{13} \cdot 0 + \alpha_{14} \cdot 1 + \alpha_{15} \cdot (-1) = 0
\end{aligned}$$

Nyní stačí najít libovolné řešení této soustavy a tím vyjádřit α_1. Parametricky můžeme řešení popsat jako:

$$(1 - q - 2p,\ q,\ -p,\ p,\ p)$$

Můžeme p a q zvolit jako 0, potom dostaneme jedno z možných řešení:

$$(1,0,0,0,0,0)$$

Potom můžeme říct, že první forma funguje takto:

$$\alpha_1(\vec{u}) = u_1$$

Velmi podobně můžeme postupovat u ostatních dvou forem. Pro α_2:

$$\begin{aligned}
\alpha_{21} \cdot 1 + \alpha_{22} \cdot 1 + \alpha_{25} \cdot 2 = 0 \\
\alpha_{23} \cdot 1 + \alpha_{25} \cdot 1 = 1 \\
\alpha_{24} \cdot 1 + \alpha_{25} \cdot (-1) = 0
\end{aligned}$$

A zase stačí najít alespoň jedno řešení této soustavy, například:

$$(0,0,1,0,0,0)$$

Druhá bázová forma tedy může být:

$$\alpha_2(\vec{u}) = u_3$$

Pro α_3:

$$\begin{aligned} \alpha_{31} \cdot 1 + \alpha_{32} \cdot 1 + \alpha_{35} \cdot 2 &= 0 \\ \alpha_{33} \cdot 1 + \alpha_{35} \cdot 1 &= 0 \\ \alpha_{34} \cdot 1 + \alpha_{35} \cdot (-1) &= 1 \end{aligned}$$

Opět stačí najít alespoň jedno řešení této soustavy, například:

$$(0,0,0,1,0,0)$$

Třetí bázová forma tedy může být:

$$\alpha_3(\vec{u}) = u_4$$

To k čemu předchozí teorie směřovala je, že když vezmeme nějakou libovolnou formu, která působí na $\mathcal{V}$, tak tuto libovolnou formu lze vyjádřit jako lineární kombinaci těchto bázových forem.

Vezměmě formu

$$\varphi(\vec{u})) = u_1 + 2u_2 + 3u_3 + 4u_4 + 5u_5$$

A ukážeme, že φ lze na $\mathcal{V}^*$ vyjádřit jako linearní kombinaci α_1, α_2 a α_3.

$$\begin{aligned} \varphi &= c_1 \cdot \alpha_1 + c_2 \cdot \alpha_2 + c_3 \cdot \alpha_3 \\ kde: c_1 &= \varphi(\vec{v_1}) = 13 \\ c_2 &= \varphi(\vec{v_2}) = 8 \\ c_3 &= \varphi(\vec{v_3}) = -1 \end{aligned}$$

$$\varphi = 13 \cdot \alpha_1 + 8 \cdot \alpha_2 - \alpha_3$$

Nyní uvažujme $\vec{v} = (4, 4, 2, 3, 7) \in \mathcal{V}$ pomocí původního předpisu můžeme $\varphi(\vec{v})$ vyjádřit takto:

$$\varphi(\vec{v})4 + 2 \cdot 4 + 3 \cdot 2 + 4 \cdot 3 + 5 \cdot 7 = 4 + 8 + 6 + 12 + 35 = 65$$

A s použitím nového předpisu takto:

$$\varphi(\vec{v}) = 13 \cdot 4 + 8 \cdot 2 - 3 = 65$$

Pomocí duální báze jsme se dostali ke stejnému výsledku. Takto můžeme vyjádřit opravdu libovolnou formu na příslušném vektorovém prostoru.

S linearními formami se můžeme setkat například v analýze. Diferenciál v bodě můžeme uvažovat jako základní příklad lineárních forem. I když se tento „jazyk“ forem v analýze příliš nezažil, ale dx je vlastně lineární forma, která přiřazuje vektoru jeho první souřadnici a dy je vlastně lineární forma, která přiřazuje vektoru jeho druhou souřadnici, obecně d_{x_i} je lineární forma přiřazujicí vektoru jeho i-tou souřadnici. Při integrování tak vlastně integrujeme linearní formy a ne funkce jako takové.

10 Dvanáctá přednáška

10.1 Rychlý průlet bilinearních forem

Definice 83 (Bilineární forma)

Bilineární forma je zobrazení typu $\mathcal{V} \times \mathcal{V} \to \mathbb{R}$, které splňuje následující vlastnosti:

- $\beta(\vec{u} + \vec{v}, \vec{w}) = \beta(\vec{u}, \vec{w}) + \beta(\vec{v}, \vec{w})$ *Aditivita v první složce*
- $\beta(c \cdot \vec{u}, \vec{v}) = c \cdot \beta(\vec{u}, \vec{v})$ *Homogenita v první složce*
- $\beta(\vec{u}, \vec{v} + \vec{w}) = \beta(\vec{u}, \vec{v}) + \beta(\vec{u}, \vec{w})$ *Aditivita v druhé složce*
- $\beta(\vec{u}, c \cdot \vec{v}) = c \cdot \beta(\vec{u}, \vec{v})$ *Homogenita v druhé složce*

Definice 84 (Symetrická bilineární forma)

Bilineární forma se nazývá symetrická, jestliže:

$$\beta(\vec{u}, \vec{v}) = \beta(\vec{v}, \vec{u}) \ \forall \vec{u}, \vec{v}$$

Definice 85 (Antisymetrická bilineární forma)

Bilineární forma se nazývá antisymetrická, jestliže:

$$\beta(\vec{u}, \vec{v}) = -\beta(\vec{v}, \vec{u}) \ \forall \vec{u}, \vec{v}$$

Definice 86 (Pozitivně definitní bilineární forma)

Bilineární forma se nazývá pozitivně definitní, jestliže:

$$\beta(\vec{u}, \vec{u}) > 0 \ \forall \vec{u} \neq \vec{o}$$

Příkladem bilineární formy s touto vlastností může být třeba:

$$\beta(\vec{u}, \vec{v}) = u_1 v_1 + 2u_2 v_2$$

Definice 87 (Pozitivně semidefinitní bilineární forma)

Bilineární forma se nazývá pozitivně definitní, jestliže:

$$\beta(\vec{u}, \vec{u}) \geq 0 \ \forall \vec{u} \neq \vec{o}$$

Příkladem bilineární formy s touto vlastností může být třeba:

$$\beta(\vec{u}, \vec{v}) = u_1 v_1$$

Definice 88 (Negativně definitní bilineární forma)

Bilineární forma se nazývá negativně definitní, jestliže:

$$\beta(\vec{u}, \vec{u}) < 0 \ \forall \vec{u} \neq \vec{o}$$

Příkladem bilineární formy s touto vlastností může být třeba:

$$\beta(\vec{u}, \vec{v}) = -u_1 v_1 - 2u_2 v_2$$

Definice 89 (Negativně semidefinitní bilineární forma)

Bilineární forma se nazývá negativně definitní, jestliže:

$$\beta(\vec{u}, \vec{u}) \leq 0 \ \forall \vec{u} \neq \vec{o}$$

Příkladem bilineární formy s touto vlastností může být třeba:

$$\beta(\vec{u}, \vec{v}) = -u_1 v_1$$

Definice 90 (Indefinitní bilineární forma)

Bilineární forma se nazývá indefinitní, jestliže neplatí žádná z výše uvedených definitností.

Příkladem bilineární formy s touto vlastností může být třeba:

$$\beta(\vec{u}, \vec{v}) = u_1 v_1 - u_2 v_2$$

Vnítřní součin $\pi(\vec{u}, \vec{v})$ je příkladem symetrické pozitivně definitní bilineární formy.

Obecně bilineární forma vypadá takto:

$$\beta(\vec{u}, \vec{v}) = \sum_{i,j=1}^{n} \beta_{ij} \cdot u_i \cdot v_j$$

A k tomu můžeme asociaovat matici takto:

$$\begin{pmatrix} \beta_{11} & \dots & \beta 1n \\ \vdots & \ddots & \vdots \\ \beta_{n1} & \dots & \beta nn \end{pmatrix}$$

Jedná se o matici $n \times n$ na základě této matice jsme schopni identifikovat zda je bilineární forma pozitivně definitní, případně její další vlastnosti.

Definice 91 (Minor)

Minor je subdeterminant nějakého matice řádu $k, 1 \leq k \leq n$ která vznikne vybráním libovolných k řádků a libovolných k sloupců z původní matice.

Například vybrané řádky (2, 3, 4) a sloupce (3, 5, 8).

Definice 92 (Hlavní minor)

Hlavní minor je minor, ve kterém jsou vybrané řádky a sloupce stejné.

Pro hlavní minor mohou být tedy vybrány například řádky (2, 3, 4) a sloupce (2, 3, 4).

Definice 93 (Vedoucí hlavní minor)

Vedoucí hlavní minor je takový hlaví minor, ve kterém vybrané řádky a sloupce postupují v přirozeném pořadí.

Například tedy minor pro který jsou vybrány řádky (1, 2, 3) a sloupce (1, 2, 3).

Věta 16 (Sylvestrovo kritérium)

Bilineární forma β je pozitivně definitní $\Leftrightarrow$ všechny vedoucí hlavní minory jsou kladné, tedy:

$$M_1 > 0 \wedge M_2 > 0 \wedge \ \wedge M_n > 0$$

Bilineární forma β je negativně definitní $\Leftrightarrow$ všechny vedoucí hlavní minory střídají znaménka takto:

$$(-1)^1 \cdot M_1 > 0 \wedge (-1)^2 \cdot M_2 > 0 \wedge \ldots \wedge (-1)^n \cdot M_n$$

Pokud jsou všechny hlavní minory nezáporné, potom je bilineární forma pozitivně semidefinitní.

Pokud všechny hlavní minory střídají znaménka, potom je bilineární forma negativně semidefinitní.

Příklad

Uvažujme vektorový prostor $\mathcal{V} = \mathbb{R}^3$ a formu β.

$$\beta(\vec{u}, \vec{v}) = 2u_1v_1 + 3u_2v_2 + 4u_1v_3 + 4u_3v_1$$

Určete zda je β pozitivně definitní bilineární forma β.

Formě β můžeme přiřadati následující matici:

$$\begin{pmatrix} 2 & 0 & 4 \\ 0 & 3 & 0 \\ 4 & 0 & 0 \end{pmatrix}$$

Vidíme že matice je symetrická, protože bilineární forma β je také symetrická.

A nyní můžeme počítat vedoucí hlavní minory minory

$$M_1 = \begin{vmatrix} 2 \end{vmatrix} = 2$$
$$M_2 = \begin{vmatrix} 2 & 0 \\ 0 & 3 \end{vmatrix} = -6$$
$$M_3 = \begin{vmatrix} 2 & 0 & 4 \\ 0 & 3 & 0 \\ 4 & 0 & 0 \end{vmatrix} = -48$$

Vidíme že vedoucí hlavní minory M_1, M_2 a M_3 nejsou kladné, a dle sylvestrova kritérie β tedy není pozitivně definitní bilineární forma.

Příklad

Uvažujme vektorový prostor $\mathcal{V} = \mathbb{R}^2$ a zobrazení $\beta : \mathcal{V} \times \mathcal{V} \to \mathbb{R}$

$$\mathcal{B}(\vec{u}, \vec{v}) = 2\vec{u_1}\vec{v_1} + \vec{u_2}\vec{v_1} + \vec{u_2}\vec{v_2}$$

Jedná se o bilineární formu?

Musíme ověřit, že je lineární v první i druhé složce. To můžeme jednoduše udělat přímým ověřením a dojdeme k závěru, že je opravdu lineární v obou složkách.

Jedná se o symetrickou bilineární formu?

$$\beta(\vec{v}, \vec{u}) = 2\vec{v_1}\vec{u_1} + \vec{v_2}\vec{u_1} + \vec{v_2}\vec{u_2} \neq 2\vec{u_1}\vec{v_1} + \vec{u_2}\vec{v_1} + \vec{u_2}\vec{v_2}$$

Vidíme tedy že se nejedná o symetrickou bilineární formu.

Je tato forma pozitivně definitní?

$$\beta(\vec{u}, \vec{u}) = 2\vec{u_1}^2 + \vec{u_2}\vec{u_1} + \vec{u_2}^2$$

Existuje takový vektor $\vec{u}$, pro který tento výraz výjde záporně?

Ke každé bilineární formě můžeme asociovat matici, v tomto případě tuto:

$$\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$$

Reference

Přednášky SLA 1 - 8, přednášející: Kureš Miroslav, Doc. RNDr., Ph.D.