Vysoké učení technické v Brně
Fakulta informačních technologií

Lineární algebra – SLA

Poznámky z přednášek

2. listopadu 2021 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.
- Vety: 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:

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

Zobrazení 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.

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

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)

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

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:

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

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: $(a, b) \in R \wedge (b, a) \in R \Rightarrow a = b$.
- Tranzitivní relace: $(a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$.
- 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.

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).

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

Opeace

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 následujicí 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. □

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 následujicí vlastnosti*[5]*:*

[5] Všiměte si, že jsou velmi podobné požadovaným vlastnostem na operaci $*$ z definice Abelovy grupy.

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. $a \cdot (b + c) = a \cdot b + a \cdot c \wedge (b + c) \cdot a = b \cdot a + c \cdot a \; \forall a, b, c \in F$

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. $x \in P$
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: $\mathbb{Q}, \mathbb{R}$

[6] Dalším příkladem by mohlo být pole racionálních funkcí $\mathbb{Z}(X)$, které bylo později velmi okrajově zmíněno na přednášce.
[7] To znamená, že je tato relace ireflexivní a tranzitivní

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 $\cdot$.

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			·	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 $\mathbb{F}_5$)

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

Z definice pole vyplývá, že operace + musí být Abelovská grupa. 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.*

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.*

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

+	0	1	2	3	4			·	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 · nad $\mathbb{F}_5$

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 · modulo počet prvků, totiž nejsme schopni vytvořit pole. Problém je v takovém případě operace ·, 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

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

$$1 + 1 = 1 + 1 = t = \begin{array}{rr} 0t & +1 \\ 0t & +1 \\ \hline 0t & +0 \end{array} = 0$$

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

Stejným postupem pro ostatní hodnoty (některé jdou rovnou doplnit díky vlasnostem 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:

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

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*

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

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 $t^2 + t + 1$.*

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

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 $2 \cdot 2$.

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

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

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

$\cdot$	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 (Dedekinduv 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 $-\infty$
- $\mathbb{Q}^-$
- $\{x \in \mathbb{Q};\ x < 7\}$

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

- $\{x \in \mathbb{Q};\ x \cdot x < 2 \vee x < 0\}$

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 $\mathbb{R}^3$ však vhodná multiplikativní operace, která by vyhovovala požadavkům z definice pole15 neexistuje.

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

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

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	…
$\mathbb{Z}$ d	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 $\mathbb{N}$

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 $b = 0, b_1 b_2 b_3 \ldots$, kde každou číslici b_i určíme následovně:

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

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

$a_1 =$	0,	a_{11}	a_{12}	a_{13}	…
$a_2 =$	0,	a_{21}	a_{22}	a_{23}	…
$a_3 =$	0,	a_{31}	a_{32}	a_{33}	…
⋮	⋮	⋮	⋮	⋮	⋱

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

Tím jsme ale zkonstruovali reálné číslo b, které se však 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

$$\aleph_0 < \aleph_1 < \aleph_2 < \aleph_3 \ldots$$

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 $\mathbb{R}^n$.

[12] A to alespoň v jedné číslici na diagonále (zobrazeno modře).
[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 následujicí 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 definovaný skalární součin $\cdot$ 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:

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

□

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

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

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

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 $\mathbb{Q}$?)

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

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. Průnik podprostorů je podprostor.

[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, $n \in \mathbb{N}$.

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 $\mathcal{V}$?

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 $i < j$ změní na $i > j$.
Definice 34 (Diagonální matice)
Jestliže jsou v matici A všechny prvky mimo hlavní diagonálou 0, řekneme že matice A je horní 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.

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)

$$+ : Mat_{m,n}(F) \times Mat_{m,n}(F) \rightarrow Mat_{m,n}(F)$$
$$c_{ij} = a_{ij} + b_{ij}\ \forall i, j$$

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)

$$\cdot : F \times Mat_{m,n}(F) \rightarrow Mat_{m,n}(F)$$
$$b_{ij} = k \cdot a_{ij}$$

[16] Kroneckerovo delta

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 $\cdot$ 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:

$$u_1, \ldots, u_n$$

Potom můžeme uvažovat jiný vektor v ve tvaru:

$$v = c_1 \cdot u_1 + \ldots + c_n \cdot u_n$$

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

Zároveň platí, že vektor v je lineárně zásivlý na vektorech $u_1, \ldots, u_n$
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 $\vec{v} = \vec{c}$. *lcM* tedy určitě obsahuje *M*.

Důkaz pro $\langle M \rangle \subseteq lcM$: plyne z toho, že *lcM* je vektorový podprostor obsahující *M* a z toho, že $< M >$ 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.

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

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 vektorového podprostoru $\mathcal{W}$ je uspořádaná n-tice B lineárně nezávislých vektorů, které generují $\mathcal{W}$. Kde generují znamená, že $\langle B \rangle = \mathcal{W}$.
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. $c_1 \cdot (1,0,0) + c_2 \cdot (0,1,0) + c_3 \cdot (0,0,1) = (0,0,0) \Rightarrow c_1 = 0, c_2 =, c_3 = 0$ — *$\mathcal{B}$ 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 $\langle B \rangle$
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 báze 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).

[18] Někdy se také používá pojem lineární zobrazení.

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.

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:

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

Věta 5 (*ker φ* a *im φ* jsou vektorové podprostory V a 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.
Definice 50 (Izomorfismus)
Jestliže je homomorfismus bijektivní, nazýváme ho izomorfismus.

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

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:

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

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.

Z předpokladu netriviálního jádra:

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

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

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

□

[21] Tato rovnost vychází z definice homomorfismu.

4.2 Matice

Definice 53 (Stopa)
Stopa je definována pro čtvercové matice. Jedná se o nějaké 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. $(tr(A \cdot B) = tr(B \cdot A))$

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

□

Definice 54 (Determinant)
Determinant budeme definovat pro čtvercové matice. Opět se jedná o nějaké zobrazení, které čtvercové matici přiřadí jedno číslo. Determinant matice A budeme značit det A, nebo také |A|.

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

Příklad (Výpočet determinantu pro matice řádu 1)

$$n = 1 : S_1 = \{1\}$$
$$det\, A = a_{11}$$

Příklad (Výpočet determinantu pro matice řádu 2)

$$n = 2 : S_2 = \{(1, 2), (2, 1)\}$$
$$det\, A = a_{11} \cdot a_{22} - a_{12} \cdot a_{21}$$

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

Příklad (Výpočet determinantu pro matice řádu 3)

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

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

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

Definice 55 (Schodovitá matice)

5 Pátá přednáška

TBD

Reference

Přednášky SLA 1 - 4, přednášející: Kureš Miroslav, Doc. RNDr., Ph.D.