Lineární algebra 1

Martin Balko

5. přednáška

29. října 2020

Algebraická tělesa

Zdroj: https://galois.com

Tělesa

- **Těleso** je množina $\mathbb{T}$ spolu se dvěma komutativními binárními operacemi $+$ a $\cdot$ splňujícími:
  1. $(\mathbb{T}, +)$ je Abelova grupa (neutrální prvek 0, inverzním k a je $-a$),
  2. $(\mathbb{T} \setminus \{0\}, \cdot)$ je Abelova grupa (neutrální prvek 1, inverzním k a je a^{-1}),
  3. $\forall\, a, b, c \in \mathbb{T}\colon a \cdot (b + c) = a \cdot b + a \cdot c.$ (distributivita)
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ s klasickými operacemi sčítání a násobení tvoří tělesa,
- $\{0, 1\}$ se sčítáním a násobením modulo 2 je nejmenší možné těleso.

Tvrzení

Prvky tělesa splňují následující vlastnosti:

1. $0a = 0$,
2. $ab = 0$ implikuje $a = 0$ nebo $b = 0$,
3. $-a = (-1)a$.

Konečná tělesa

- Na množině $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ uvažme operace $+$ a $\cdot$ modulo n.
- Pak $\mathbb{Z}_2$ a $\mathbb{Z}_3$ tělesy jsou, ale $\mathbb{Z}_4$ ne (2 nemá inverzi 2^{-1}).

Lemma

Pro prvočíslo n a nenulové $a \in \mathbb{Z}_n$ při násobení modulo n platí

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

- Důkaz: Sporem, nechť $ka \equiv \ell a \pmod{n}$ pro nějaká různá $k, \ell \in \mathbb{Z}_n$.
- Pak $(k-\ell)a \equiv 0 \pmod{n}$. Protože n je prvočíslo, n dělí a nebo $k - \ell$.
- Protože $n > a, k - \ell$, tak $a = 0$ nebo $k - \ell = 0$,spor. $\square$

Věta

Množina $\mathbb{Z}_n$ tvoří těleso právě tehdy, když je n prvočíslo.

- Náčrt důkazu: Pokud $n = pq$ pro $1 < p, q < n$, pak je-li $\mathbb{Z}_n$ těleso, tak $pq \equiv 0 \pmod{n}$ implikuje $p \equiv 0$ či $q \equiv 0 \pmod{n}$, což neplatí.
- Pro n prvočíslo stačí ověřit axiomy tělesa. Existence inverze a^{-1} pro $a \neq 0$ plyne z lemmatu (mezi násobky a totiž musí být 1). $\square$

Příklad konečného tělesa

- Operace sčítání a násobení nad tělesem $\mathbb{Z}_5$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

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

- Inverzní prvky tělesa $\mathbb{Z}_5$

x	0	1	2	3	4
$-x$	0	4	3	2	1

x	0	1	2	3	4
x^{-1}	–	1	3	2	4

- Veškeré zatím probírané výsledky (například Gaussova eliminace) platí nad libovolným tělesem $\mathbb{T}$.

Velikosti konečných těles

- Existují konečná tělesa neprvočíselných velikostí?

Věta (O velikosti konečných těles)

Konečná tělesa existují právě o velikostech p^n, kde p je prvočíslo a $n \geq 1$.

- Ukážeme si jen, jak taková tělesa $GF(p^n)$ sestrojit.
- Prvky jsou polynomy stupně nanejvýš $n-1$ s koefiecienty z $\mathbb{Z}_p$, tedy

$$GF(p^n) = \{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \colon a_0, \ldots, a_{n-1} \in \mathbb{Z}_p\}.$$

- Sčítání je definováno jako sčítání pro reálné polynomy.
- Násobení je definováno jako násobení pro reálné polynomy modulo ireducibilní polynom stupně n.

- Příklad (těleso $GF(8)$):
  $GF(8) = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$, kde například
  $(x+1) + (x^2+x) = x^2+1$ a $x^2 \cdot x = x+1$ (modulo x^3+x+1).

Évariste Galois

- Tělesa $GF(p^n)$ se nazývají Galoisova tělesa („Galois field“).
- Každé konečné těleso velikosti p^n je isomorfní tělesu $GF(p^n)$.
- Évariste Galois byl francouzský matematik, jehož práce daly vzniknout teorii grup a moderní algebře.

Obrázek: Évariste Galois (1811–1832).

Zdroj: https://galois.com

Charakteristika tělesa

- Charakteristika tělesa $\mathbb{T}$ je nejmenší $n \in \mathbb{N}$ takové, že $\underbrace{1 + \cdots + 1}_{n} = 0.$

  Pokud takové n neexistuje, pak ji definujeme jako 0.
- Příklady:
  Tělesa $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{C}$ mají charakteristiku 0, těleso $\mathbb{Z}_p$ má charakteristiku p.

Tvrzení

Charakteristika každého tělesa je buď nula nebo prvočíslo.

- Důkaz:
- Protože $0 \neq 1$, tak charakteristika nemůže být 1.
- Sporem: pokud by charakteristika byla složené číslo $n = pq$, tak

$$0 = \underbrace{1 + \cdots + 1}_{n=pq} = (\underbrace{1 + \cdots + 1}_{p})(\underbrace{1 + \cdots + 1}_{q})$$

  a podle základních vlastností tělesa součet p nebo q jedniček dá nulu.
- To je spor s minimalitou n. $\square$

Malá Fermatova věta

- Pro každé prvočíslo p a nenulové $a \in \mathbb{Z}$ platí $a^{p-1} \equiv 1 \pmod{p}$.
- Používá se například v pravděpodobnostních testech prvočíselnosti.
- Formulace v jazyce konečných těles:

Malá Fermatova věta

Pro každé prvočíslo p a nenulové $a \in \mathbb{Z}_p$ platí

$$a^{p-1} = 1 \text{ v tělese } \mathbb{Z}_p.$$

- Důkaz:
- Z prvočíslenosti p již víme, že $\{0, 1, \dots, p-1\} = \{0a, 1a, \dots, (p1-)a\}$.
- Protože $0a = 0$, tak $\{1, \dots, p-1\} = \{1a, \dots, (p-1)a\}$.
- Tedy $1 \cdot 2 \cdot \dots \cdot (p-1) = (1a) \cdot (2a) \cdot \dots \cdot (p-1)a$.
- Vykrácením $1, 2, \dots, p-1$ dostáváme

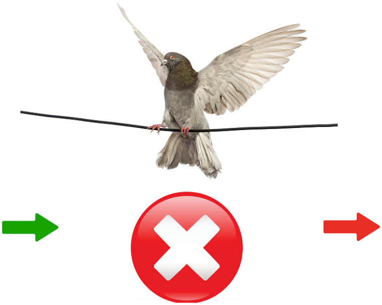
$$1 = a \cdot \dots \cdot a = a^{p-1}.$$

$\square$

Aplikace: samoopravné kódy

- Motivace: přenos dat.
- Chceme přenést data komunikačním kanálem.

„I will meet you after
I tape my other client“.



„I will meet you after
I rape my other client“.

- Při přenosu může dojít k chybám.
- Chceme být schopni chyby opravit a získat odeslanou zprávu.

Aplikace: samoopravné kódy

- Obecný postup kódování: odesílatel rozdělí zprávu na bloky k bitů, které určitou metodou přetransformuje na bloky o k' bitech. Příjemce pak každý blok transformuje na původní hodnoty.
- Příklad: Zdvojením bitů lze 1 chybu detekovat, ale ne opravit. Ztrojením bitů lze 1 chybu detekovat i opravit.
- Hammingův kód $(7, 4, 3)$: rozdělí zprávu na bloky b s $k = 4$ bity a ty transformuje na bloky b' s $k' = 7$ bity. Umí detekovat a opravit 1 chybu.
- Lze reprezentovat násobením generující maticí $H \in \mathbb{Z}_2^{7\times 4}$:

$$Hb = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = b'$$

- Příjemce obdrží zakódovaný blok b' zprávy, který musí dekódovat.

Aplikace: samoopravné kódy

- K detekci a opravě chyb používá příjemce detekční matici $D \in \mathbb{Z}_2^{3\times 7}$.
- Pokud $Db' = 0$, pak nenastala chyba při přenosu (nebo nastaly ≥ 2).
- Jinak nastala chyba v bitu na pozici, jejímž binárním zápisem je Db'.

- Příklad přenosu bez chyby:

$$Db' = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Aplikace: samoopravné kódy

- K detekci a opravě chyb používá příjemce detekční matici $D \in \mathbb{Z}_2^{3\times 7}$.
- Pokud $Db' = 0$, pak nenastala chyba při přenosu (nebo nastaly ≥ 2).
- Jinak nastala chyba v bitu na pozici, jejímž binárním zápisem je Db'.

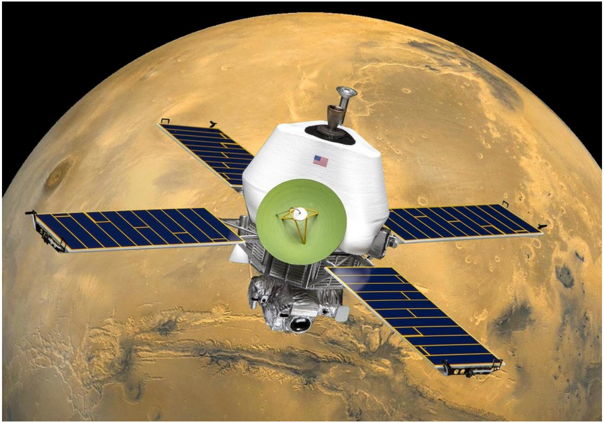
- Příklad přenosu s 1 chybou:

$$Db' = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ \color{red}{0} \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \Rightarrow \text{ chyba na pozici 6}$$

- Více o samoopravných kódech na přednášce Kombinatorika a grafy I.

Aplikace: samoopravné kódy

- Samoopravné kódy byly použity sondou Mariner 9 pro přenos prvních fotografií Marsu.

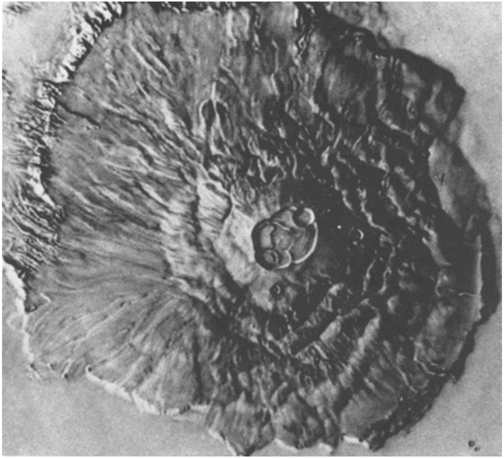


Obrázek: Sonda Mariner 9.

Zdroj: http://www.realspacemodels.com

Aplikace: samoopravné kódy

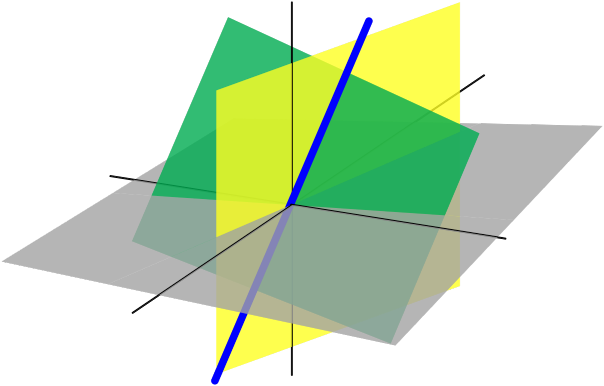
- Samoopravné kódy byly použity sondou Mariner 9 pro přenos prvních fotografií Marsu.



Obrázek: Fotografie hory Olympus Mons pořízená sondou Mariner 9.

Zdroj: https://www.khanacademy.org

Vektorové prostory



Zdroj: https://en.wikipedia.org

Vektorové prostory

- Zobecnění známého prostoru aritmetických vektorů $\mathbb{R}^n$.
- Buď $\mathbb{T}$ těleso s neutrálními prvky 0 a 1 pro sčítání a násobení. Vektorový prostor nad $\mathbb{T}$ je množina V s operacemi sčítání vektorů $+\colon V^2 \to V$ a násobení vektoru skalárem $\cdot\colon \mathbb{T} \times V \to V$ splňující pro každé $\alpha, \beta \in \mathbb{T}$ a $u, v \in V$:
  1. $(V, +)$ je Abelova grupa (neutrální prvek o, inverzním k u je $-u$),
  2. $\alpha(\beta v) = (\alpha\beta)v$, (asociativita)
  3. $1v = v$,
  4. $(\alpha + \beta)u = \alpha u + \beta u$, (distributivita)
  5. $\alpha(u + v) = \alpha u + \alpha v$. (distributivita)
- Prvky množiny V nazýváme vektory.
- Prvky množiny $\mathbb{T}$ nazýváme skaláry.

Příklady vektorových prostorů

1. Aritmetický prostor $\mathbb{R}^n$ nad $\mathbb{R}$, nebo obecněji $\mathbb{T}^n$ nad tělesem $\mathbb{T}$. Vektory sčítáme a násobíme skalárem po složkách.
2. Prostor matic $\mathbb{T}^{m\times n}$ nad tělesem $\mathbb{T}$.
3. Prostor $\mathcal{P}$ všech reálných polynomů proměnné x nad tělesem $\mathbb{R}$. Sčítání:
$$(a_nx^n + \cdots + a_0) + (b_nx^n + \cdots + b_0) = (a_n + b_n)x^n + \cdots + (b_0 + a_0).$$
Násobení skalárem: $\alpha(a_nx^n + \cdots + a_0) = \alpha a_nx^n + \cdots + \alpha a_0$.
4. Prostor $\mathcal{P}^n$ všech reálných polynomů proměnné x stupně $\leq n$ nad tělesem $\mathbb{R}$.
5. Prostor $\mathcal{F}$ všech reálných funkcí $f : \mathbb{R} \to \mathbb{R}$.
Sčítání: $(f + g)(x) = f(x) + g(x)$.
Násobení skalárem: $(\alpha f)(x) = \alpha f(x)$.
6. Prostor $\mathcal{C}$ všech spojitých reálných funkcí $f : \mathbb{R} \to \mathbb{R}$.
7. Prostor $\mathcal{C}_{a,b}$ všech spojitých reálných funkcí $f : [a, b] \to \mathbb{R}$.

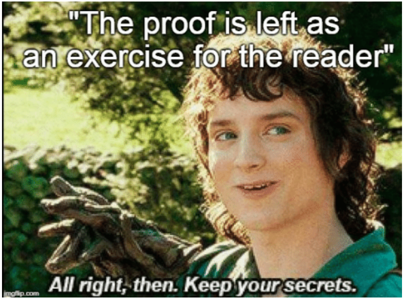
Základní vlastnosti vektorových prostorů

Tvrzení

V prostoru V nad tělesem $\mathbb{T}$ platí pro každý skalár $\alpha \in \mathbb{T}$ a vektor $v \in V$:

1. $0v = o$,
2. $\alpha o = o$,
3. $\alpha v = o$ implikuje $\alpha = 0$ nebo $v = o$,
4. $-v = (-1)v$.

- Důkaz je analogický důkazu základních vlastností tělesa.



Vektorové podprostory

- Je-li V vektorový prostor nad tělesem $\mathbb{T}$, pak $U \subseteq V$ je podprostorem V, pokud U tvoří vektorový prostor nad $\mathbb{T}$ se stejně definovanými operacemi. Značíme $U \Subset V$.
- Ekvivaletně U musí mít nulový vektor a být uzavřené na obě operace:

Tvrzení

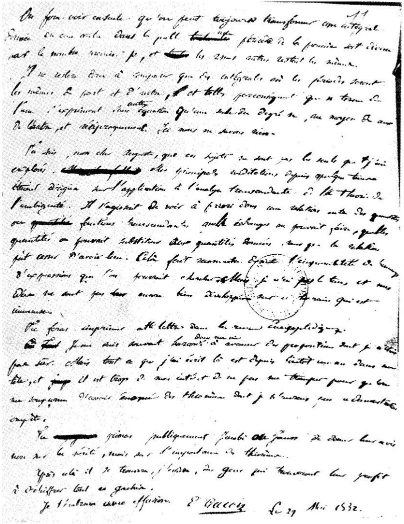
Podmnožina U vektorového prostoru V nad tělesem $\mathbb{T}$ je podprostorem V právě tehdy, když platí:

1. $o \in U$,
2. $\forall\, u, v \in U\colon u + v \in U$, (uzavřenost na sčítání)
3. $\forall\, \alpha \in \mathbb{T}\ \forall\, u \in U\colon \alpha u \in U$. (uzavřenost na násobení skalárem)

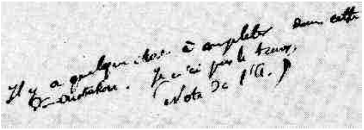
- Důkaz: (i) $\Rightarrow$: pokud $U \Subset V$, pak U tyto tři vlastnosti splňuje.
- (ii) $\Leftarrow$: Splňuje-li U tyto tři vlastnosti, pak zbylé vlastnosti vektorového prostoru platí také. Platí totiž pro V a tedy i pro $U \subseteq V$. Uzavřenost U na opačné vektory plyne z uzavřenosti na násobky a z $(-1)u = -u$. $\square$

Příklady vektorových podprostorů

1. Triviální podprostory vektorového prostoru V jsou V a $\{o\}$.
2. Každá přímka procházející počátkem je podporostorem $\mathbb{R}^2$.
3. $\mathcal{P}^n \Subset \mathcal{P} \Subset \mathcal{C} \Subset \mathcal{F}$.
4. Množina symetrických reálných matic řádu n je podprostorem $\mathbb{R}^{n \times n}$.
5. Množina $\mathbb{Q}^n$ nad $\mathbb{Q}$ je podprostorem $\mathbb{R}^n$ nad $\mathbb{Q}$, ale není podprostorem $\mathbb{R}^n$ nad $\mathbb{R}$ (pracuje nad jiným tělesem).



Je t'embrasse avec effusion. E Galois. Le 29 Mai 1832.



Il y a quelque chose à compléter dans cette démonstration. Je n'ai pas le temps. (Note de l'A.)

Obrázek: Dopis, který Galois sepsal noc před svou smrtí v duelu a ve kterém zachytil své matematické myšlenky. Poznámka vpravo říká „... Nemám čas.“.

Zdroje: https://conquermaths.com a https://mathshistory.st-andrews.ac.uk

Děkuji za pozornost.