1 Úvod

Definice 1.1 (Matice)

Reálná matice typu $m \times n$ je obdélníkové schéma (tabulka) reálných čísel. Prvek na pozici $(i,\ j)$ matice A značíme a_{ij} nebo A_{ij}. A i-tý řádek matice A značíme A_{i*} a j-tý řádek matice A značíme A_{*j}.

Definice 1.2 (Vektor)

Reálný n-rozměrný aritmetický sloupcový vektor (standardní) je matice typu $n \times 1$ a řádkový $1 \times n$.

Definice 1.3 (Soustava lineárních rovnic)

Lineární = neznámé jsou v 1. mocnině.
Soustava = více rovnic.
Rovnice výraz z neznámých (bez absolutního členu) a koeficientů rovný konstantě.

Definice 1.4 (Řešení)

Řešením rozumíme každý vektor hodnot neznámých vyhovující všem rovnicím.

Definice 1.5 (Matice soustavy)

Matice soustavy je matice koeficientů u neznámých.
Rozšířená matice soustavy je matice soustavy „následována“ vektorem hodnot konstant jednotlivých rovnic.

Poznámka (Geometrický význam)
Průsečík n „přímek“ v n rozměrném prostoru

Definice 1.6 (Elementární řádkové úpravy)

- Vynásobení řádku nenulovým reálným číslem.
- Přičtení jednoho řádku k druhému.
- Výměna dvou řádků. (Není elementární, protože jde vytvořit pomocí prvních dvou.)

Tvrzení 1.1

Elementární řádkové operace zachovávají množinu řešení soustavy.

Důkaz
Elementární úpravou neztratíme žádné řešení, protože pokud je x řešením před úpravou, je i po úpravě. A naopak ho lze invertovat, takže žádné řešení ani nepřibude. □

Definice 1.7 (Odsupňovaný tvar matice REF)

Matice $A \in^{m \times n}$ je v řádkově odstupňovaném tvaru, pokud existuje r takové, že platí: řádky $1, \ldots, r$ (tzv. bazické) jsou nenulové (obsahují alespoň 1 nenulový prvek), řádky $r+1, \ldots, m$ jsou nulové, a navíc označíme-li jako $p_i = minj; a_{ij} \neq 0$ (tzv. pivot) pozici prvního nenulového prvku v i-tém řádku, tak platí: $p_1 < p_2 < \cdots < p_r$.

Například
Matice, které jsou, a matice, které nejsou.

Definice 1.8 (Hodnost matice)

Počet nenulových řádků po převodu do odstupňovaného tvaru (nebo libovolného s maximálním počtem nulových řádků) značený $\text{rank}(A)$.

Dále jsme dělali Gaussovu eliminaci (nemá řešení ($\text{rank}(A) \neq \text{rank}(A|b)$), má 1 řešení ($\text{rank}(A|b) = n$), má mnoho řešení (pak bazické proměnné vyjádřím pomocí nebazických)).

Definice 1.9 (Redukovaný odstupňovaný tvar matice RREF)

Matice v odstupňovaném tvaru je v redukovaném OT, jestliže $\forall 0 \leq i \leq r, i \in: a_{ip_i} = 1 \wedge \forall i > x \in a_{xp_i} = 0$.

Poznámka
Tento tvar je jednoznačný.

Definice 1.10 (Rovnost matic)

Dvě matice se rovnají, pokud mají stejné rozměry a stejné prvky na stejných souřadnicích.

Definice 1.11 (Součet matic)

Pro součet musí mít matice stejné rozměry a poté sčítáme po složkách.

Poznámka (Vlastnosti)
Komutativita (pokud jsou prvky matice komutativní).

Definice 1.12 (Násobení skalárem)

Násobíme po složkách.

Definice 1.13 (Součin matic)

Nechť $A \in^{m\times n}$ a $B \in^{n\times o}$ jsou matice. Potom matice $C \in^{m\times o}$ definovaná jako $c_{ij} = a_{i*} \cdot b_{*j}$ je jejich součinem.

Poznámka (Vlastnosti)
Komutativita neplatí.

Asociativita, distributivita zleva a distributivita z prava platí. Stejně tak „asociativita" násobení skalárem.

Definice 1.14 (Transpozice)

Buď $A \in^{m\times n}$. Potom $A^T \in^{n\times m}$ definována jako $(A^T)_{ij} = a_{ji}$ je transponovaná matice A.

Poznámka (Vlastnosti)
Je sama sobě inverzním zobrazením. Distributivita pro všechny operace (pozor u násobení je antisymetrická).

$$(A^T)^T = A$$
$$(A + B)^T = A^T + B^T$$
$$(\alpha A)^T = \alpha A^T$$
$$(AB)^T = B^T A^T$$

Definice 1.15 (Symetrická a antisymetrická matice)

Matice A je symetrická, pokud $A = A^T$, a antisymetrická $A = -A^T$.

Poznámka (Vlastnosti)
Symetrické matice jsou uzavřené na součet, ale na součin ne.

Definice 1.16 (Jednotkový vektor)

e_j definovaný jako $(e_j)_j = 1$ a $\forall i \neq j\, (e_j)_i = 0$ je j-tý jednotkový vektor.

Poznámka (Vlastnosti)

$$Ae_i = A_{*i}$$
$$e_i^T = A_{i*}$$

Definice 1.17 (Skalární součin vektorů)

$u \cdot v = u^T v$ je skalární součin vektorů u a v.

uv^T je ? součin vektorů u a v

Poznámka (Zápis SLR jako maticové násovení)
SLR lze zapsat jako $Ax = b$.

Poznámka (Matice a lineární zobrazení $x \to Ax$)
Je užitečné se na matici $A \in \mathbb{R}^{m \times n}$ jako na určité zobrazení z $\mathbb{R}^n$ do $\mathbb{R}^m$ definované předpisem $x \to Ax$.

Na řešení SLR se lze pak dívat jako na vzor b v zobrazení dané A.

Zároveň na maticový součin se lze dívat na skládání $(BA)x = B(Ax)$. (Základní motivace, aby se součin definoval tak, jak je.)

TODO?

Definice 1.18 (Regulární matice)

Buď $A \in \mathbb{R}^{n \times n}$. Pak následující tvrzení jsou ekvivalentní:

1. A je regulární,
2. $\mathrm{RREF}(A) = \mathcal{I}_n$,
3. $\mathrm{rank}(A) = n$
4. pro nějaké $b \in \mathbb{R}^n$ má soustava $Ax = b$ jediné řešení,
5. pro všechna $b \in \mathbb{R}^n$ má soustava $Ax = b$ jediné řešení.

Matice A nesplňující tvrzení je singulární.

Tvrzení 1.2 (Uzavřenost na součin)

Buďte $A, B \in \mathbb{R}^{n \times n}$ regulární matice. Pak AB je také regulární.

Důkaz
Buď x řešení soustavy $ABx = 0$. Chceme ukázat, že x musí být nulový vektor. Z předchozího tvrzení $\forall y Ay = 0$ má jediné řešení. Zároveň $\forall y Bx = y$ má jediné řešení. □

Tvrzení 1.3

Je-li alespoň jedna z matic $A, B \in \mathbb{R}^{n\times n}$, pak AB je také singulární.

Důkaz
Je-li matice B singulární, pak $Bx = 0$ pro nějaké $x \neq 0$. Z toho ale plyne $(AB)x = A(Bx) = A(0) = 0$, tedy i AB je singulární.

Nyní předpokládejme, že matice B je regulární, tedy matice A singulární a existuje $y \neq 0$ takové, že $Ay = 0$. Z regularity matice B existuje $x \neq 0$ takové, že $Bx = y$. Celkem dostáváme $(AB)x = A(Bx) = Ay = 0$, tedy AB je singulární. □

Definice 1.19 (Matice elementárních úprav)

Elementární úpravy jdou reprezentovat násobením tzv. elementární maticí zleva: $E_i(\alpha)$ jako násobení řádku i číslem α je jednotková matice s α místo i-té jedničky. E_{ij} jako prohození řádků i, j je jednotková matice s prohozeným i-tým a j-tým řádkem, …

Tyto matice jsou regulární.

Věta 1.4

Buď $A \in \mathbb{R}^{m\times n}$. Pak $\mathrm{RREF}(A) = QA$ pro nějakou regulární matici $Q \in \mathbb{R}^{m\times m}$.

Důkaz
$\mathrm{RREF}(A)$ získáme aplikací konečně mnoha elementárních řádkových úprav a součin regulárních matic je regulární matice. □

Tvrzení 1.5

Každá regulární matice $A \in \mathbb{R}^{n\times n}$ se dá vyjádřit jako součin konečně mnoha elementárních matic.

Důkaz
Elementární úpravy lze invertovat elementárními úpravami, tedy i inverze úprav regulární matice na $\mathcal{I}$ je regulární (a $\mathcal{I}$ je také regulární). □

Definice 1.20 (Inverzní matice)

Buď $A \in \mathbb{R}^{n\times n}$. Pak A^{-1} je inverzní maticí k A, pokud splňuje $AA^{-1} = A^{-1}A = \mathcal{I}_n$.

Například
$\mathcal{I}_n^{-1} = \mathcal{I}_n$, 0_n^{-1} neexistuje.

Věta 1.6 (O existenci inverzní matice)

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

Důkaz
Existence: A je regulární, tedy soustava $Ax = e_j$ má řešení x_j pro každé j. Ukážeme, že $A^{-1} = (x_1|x_2|\dots|x_n)$ je hledaná inverze. (Porovnáním po sloupcích: $(AA^{-1})_{*j} = Ax_j = e_j = \mathcal{I}_{*j}$. Komutativní výraz dokážeme $A(A^{-1}A - \mathcal{I}) = AA^{-1}A - A = \mathcal{I}A - A = 0$, $A^{-1}A - \mathcal{I}$ je vektor, který je jednoznačně určen tím, že A je regulární.)

Jednoznačnost. Nechť pro nějakou matici B platí $AB = BA = \mathcal{I}$. Pak

$$B = B\mathcal{I} = B(AA^{-1}) = (BA)A^{-1} = \mathcal{I}A^{-1} - A^{-1}.$$

Naopak. Nechť pro A existuje inverzní matice. Buď x řešení soustavy $Ax = 0$. Pak

$$x = \mathcal{I}x = (A^{-1}A)x = A^{-1}(Ax) = A^{-1}0 = 0,$$

tedy A je regulární. □

Tvrzení 1.7 (Vlastnosti inverzní matice)

Je-li A regulární, pak A^T je regulární.

Důkaz
Je-li A regulární, pak existuje inverze a platí $AA^{-1} = A^{-1}A = \mathcal{I}_n$. Po transponování všech stran dostaneme

$$(AA^{-1})^T = (A^{-1}A)^T = \mathcal{I}_n^T,$$

neboli

$$(A^{-1})^T A^T = A^T (A^{-1})^T = \mathcal{I}_n.$$

Matice A^T má inverzi a je tudíž regulární. (Navíc $(A^T)^{-1} = (A^{-1})^T$, občas se značí A^{-T}). □

Věta 1.8 (Jedna rovnost stačí)

Buďte $A, B \in \mathbb{R}^{n\times n}$. Je-li $BA = I_n$, pak obě matice A, B jsou regulární a navzájem k sobě inverzní, to jest $B = A^{-1}$ a $A = B^{-1}$.

Důkaz
Regularita vyplývá z dřívějšího tvrzení vzhledem k regularitě $\mathcal{I}_n$. Tudíž existují inverze A^{-1}, B^{-1}. Odvodíme

$$B = B\mathcal{I}_n = B(AA^{-1}) = (BA)A^{-1} = \mathcal{I}_n A^{-1} = A^{-1}.$$

Úplně stejně druhá rovnost. □

Poznámka (Výpočet inverzní matice)
Důkaz věty ukázal návod: j-tý sloupec A^{-1} je řešením soustavy $Ax = e_j$.

Věta 1.9 (Výpočet inverzní matice)

Buď $A \in \mathbb{R}^{n\times n}$. Je-li $\mathrm{RREF}(A|\mathcal{I}_n) = (I_n|B)$, *pak $B = A^{-1}$, jinak je A singulární.*

Důkaz
Je-li $\mathrm{RREF}(A|\mathcal{I}_n) = (\mathcal{I}_n|B)$, potom existuje regulární Q tak, že $(\mathcal{I}_n|B) = Q(A|\mathcal{I}_n)$. Po roztržení na dvě části $\mathcal{I}_n = QA$ tj. $Q = A^{-1}$ a $B = Q\mathcal{I}_n = Q = A^{-1}$.

Pokud není toho tvaru, pak z definice A není regulární. □

Tvrzení 1.10 (Vlastnosti inverzní matice)

Buďte $A, B \in \mathbb{R}^{n\times n}$ regulární. Pak:

1. $(A^{-1})^{-1} = A$
2. $(A^{-1})^T = (A^T)^{-1}$
3. $(\alpha A)^{-1} = \frac{1}{\alpha}A^{-1}$ … $(\alpha \neq 0)$
4. $(AB)^{-1} = B^{-1}A^{-1}$

Důkaz
1., 2. triviální, 3. vynásobím $A\alpha$, 4. přezávorkuji. □

Poznámka
Pro $(A + B)^{-1}$ žádný jednoduchý vzoreček není.

Poznámka (Inverzní matice a soustava rovnic)
Buď Q regulární. Pak soustava $Ax = b$ je ekvivalentní s (QA)x = (Qb).

Důkaz
Žádné řešení neztratíme, zpět se dostaneme přednásobením Q^{-1} zleva. □

Věta 1.11 (Soustava rovnic a inverzní matice)

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

Poznámka (Inverzní matice - geometrie)
Buď $A \in \mathbb{R}^{n\times n}$ regulární matice. Pro každé $y \in \mathbb{R}^n$ existuje právě jedno $x \in \mathbb{R}^n$ takové, že $Ax = y$, zobrazení je tedy bijekcí.

Poznámka
Skládání zobrazení nám může dát i vhled do toho, jak funguje inverze součinu matic.

2 Grupy

Abstraktní algebraické struktury k popisu symetrií.

Definice 2.1 (Grupa)

Grupa je dvojicí $(G, \circ)$, kde G je množina a $\circ : G^2 \to G$ je binární operace na množině splňující

$$\forall a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c, \text{(asociativita)}$$

$$\exists e \in G \forall a \in G : e \circ a = a \circ e = a, \text{neutrální prvek}$$

$$\forall a \in G \exists b \in G : a \circ b = b \circ a = e. \text{(inverzní prvek)}$$

Definice 2.2 (Abelova grupa)

Abelova grupa je grupa, která splňuje

$$\forall a, b \in G : a \circ b = b \circ a. \text{(komutativita)}$$

Poznámka
Je-li operací sčítání, pak neutrální prvek značíme 0 a opačný $-a$.

Je-li operací sčítání, pak neutrální prvek značíme 1 a opačný $\frac{1}{a}$.

Například
Abelovy grupy: $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+),(\mathbb{Q}\backslash\{0\},\cdot),(\mathbb{R}\backslash\{0\},\cdot),(\mathbb{C}\backslash\{0\},\cdot)$, grupa matic $(\mathbb{R}^{m\times n},+),($

Ne nutně abelovy grupy: množina všech zobrazení na množině s operací skládání, množina regulárních matic řádu n s násobením, …

Negrupy: $(\mathbb{N},+),(\mathbb{Z},-),(\mathbb{Z}\setminus\{0\},\cdot),(\mathbb{R}\setminus\{0\},:),\ldots$

Tvrzení 2.1 (Vlastnosti grup)

Prvky grupy $(G,\circ)$ splňují následující vlastnosti

1. $a\circ c=b\circ c$ *implikuje* $a=b$ *(krácení),*
2. *neutrální prvek je jednoznačně určen,*
3. $\forall a\in G$ *je jeho inverzní prvek určen jednoznačně,*
4. *rovnice* $a\circ x=b$ *má právě jedno řešení* $\forall a,b\in G$*,*
5. $(a^{-1})^{-1}=a$,
6. $(a\circ b)^{-1}=b^{-1}\circ a^{-1}$

Důkaz

1. $a\circ c=b\circ c \implies a\circ(c\circ c^{-1})=b\circ(c\circ c^{-1}) \implies a\circ e=b\circ e \implies a=b.$
2. Nechť e_1, e_2 jsou neutrální prvky $\implies e_1=e_1\circ e_2=e_2.$
3. Inverzní prvky a_1 a a_2 k a $\implies a_1\circ a=e=a_2\circ a \implies a_2=a_1.$
4. Vynásobením rovnice prvkem a^{-1} zleva dává $x=a^{-1}\circ b.$
5. $e=e \implies (a^{-1})^{-1}\circ a^{-1}=a\circ a^{-1}.$
6. $e=e \implies (a\circ b)^{-1}\circ(a\circ b)=b^{-1}\circ b=b^{-1}\circ e\circ b=(b^{-1}\circ a^{-1})\circ(a\circ b).$

□

Definice 2.3 (Podgrupa)

Podgrupa grupy $(G,\circ)$ je grupa $(H,\circ_H)$ taková, že platí $H\subseteq G$ a pro všechna $a,b\in H$ platí $a\circ b=a\circ_H b$.

Neboli v H platí uzavřenost TODO.

2.1 permutace

Definice 2.4 (Vzájemně jednoznačné)

Zobrazení je vzájemně jednoznačné (bijekce), pokud je prosté a na.

Definice 2.5 (Permutace)

Permutace je vzájemně jednoznačné zobrazení množiny na sebe samu.

Poznámka (Možné zápisy permutací)
Tabulkou (nahoře vzory, dole obrazy), grafem (šipka vede ze vzoru do obrazu), rozložením na cykly (v závorce jsou ve skupinkách čísla, které se postupně zobrazují na sebe, prvky které se zobrazují sami na sebe, tak se nemusí psát)

Definice 2.6 (Identita, transpozice, inverzní permutace)

Permutace zobrazující každý prvek na sebe se nazývá identita (id).

Transpozice je permutace, která prohazuje dva prvky. (Permutace s jediným „nejednotkovým“ cyklem, který má 2 prvky).

Pro permutace p, q je složená permutace $p \circ q$ daná předpisem $(p \circ q)(i) = p(q(i))$.

Inverzní permutace (p^{-1}) k permutaci p je daná předpisem $p \circ p^{-1} = id$. (Např transpozice sama k sobě.)

Definice 2.7 (Znaménko pemutace)

Pokud se permutace $p \in S_n$ skládá z k cyklů, pak znaménkem permutace je číslo $\operatorname{sgn}(p) = (-1)^{n-k}$.

Například
$\operatorname{sgn}(id) = 1, \operatorname{sgn}((i,j)) = -1, \operatorname{sgn}((1,3,4)(2,5)) = -1$

Věta 2.2 (O znaménku složení permutace s transpozicí)

Buď $p \in S_n$ permutace a $t = (i,j) \in S_n$ transpozice. Pak

$$\operatorname{sgn}(p) = -\operatorname{sgn}(t \circ p) = -\operatorname{sgn}(p \circ t)$$

Důkaz
Stačí dokázat jednu rovnost, druhá je analogicky. Rozlišíme dva případy, pokud jsou i, j ve stejném cyklu, pak se transpozicí rozpadne, pokud jsou v jiném, tak se naopak spojí, tedy se v obou případech změní počet cyklů o 1 a znaménko tedy na $-$ původní. □

Věta 2.3

Každou permutaci lze rozložit na složení transpozic.

Důkaz
Postupně na transpozice rozložíme všechny cykly. □

Důsledek
Platí $\operatorname{sgn}(p) = (-1)^r$, kde r je počet transpozic v rozkladu permutace p.

Pro $p, q \in S_n$ platí $\operatorname{sgn}(p \circ q) = \operatorname{sgn}(p) \cdot \operatorname{sgn}(q)$.

Pro $p \in S_n$ platí $\operatorname{sgn}(p) = \operatorname{sgn}(p^{-1})$.

Definice 2.8 (Symetrická grupa)

Množina permutací S_n tvoří s operací skládání $\circ$ takzvanou symetrickou grupu $(S_n, \circ)$.

Poznámka
Symetrické grupy popisují symetrie různých objektů.

Každá grupa je isomorfní nějaké podgrupě symetrické grupy (např. rubikova grupa (popisující r. kostku) je isomorfní S_{48}).

2.2 Algebraická tělesa

Zobecnění číselných oborů jako např. $\mathbb{R}$.

Definice 2.9 (Těleso)

Těleso je množina $\mathbb{T}$ spolu se dvěma komutativními binárními operacemi + a $\cdot$ splňujícími: $(\mathbb{T}, +)$ je Abelova grupa (neutrální prvek 0, inverzním k a je $-a$), $(\mathbb{T} \subseteq \{0\}, \cdot)$ je Abelova grupa (neutrální prvek 1, inverzním k a je a^{-1}), $\forall a, b, c \in \mathbb{T} : a \cdot (b + c) = a \cdot b + a \cdot c$ (distributivita).

Poznámka
Operace nemusí představovat klasické sčítání a násobení.

Budeme psát ab místo $a \cdot b$.

Každé těleso má alespoň dva prvky, protože $0 \neq 1$

Zavedeme značení pro inverzní operace, jak je známe.

Například
Tělesa jsou $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ (např nejmenší možný těleso $\mathbb{Z}_2$), kvaterniony (pokud definujeme těleso jako ne nutně komutativní).

$\mathbb{Z}$ ne.

Tvrzení 2.4 (Vlastnosti těles)

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

Důkaz
Jednoduchý, podobný vlastnostem grup. □

Poznámka (Konečná tělesa)
Na množině $\mathbb{Z}_n$ uvažme operace + a $\cdot$ modulo n. Pak $\mathbb{Z}_2$ a $\mathbb{Z}_3$ tělesy jsou, ale $\mathbb{Z}_4$ ne ($\nexists 2^{-1}$).

Lemma 2.5

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

$$\{0, 1, \ldots, n-1\} = \{00a, 1a, \ldots, (n-1)a\}.$$

Důkaz
Sporem, nechť $ka \equiv la(\mod n)$ pro nějaká různá $k, l \in \mathbb{Z}_n$. Pak $(k-l)a \equiv 0(\mod n)$. Protože n je prvočíslo, n dělí a nebo $k - l$. □

Věta 2.6

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

Důkaz
Pokud $n = pq$ pro $1 < p, q < n$, pak je-li $\mathbb{Z}_n$ těleso, pak $pq \equiv 0(\mod n)$ implikuje $p = 0$ a $q = 0$, .

Pro n je prvočíslo stačí ověřit axiomy tělesa. (Existence inverze a^{-1} plyne z lemmatu výše.) □

Věta 2.7 (O velikosti konečných těles)

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

Důkaz (Pouze jedním směrem, druhým si ho nebudeme ukazovat)

$$GF(p^n) = \left\{a_{n-1}x^{n-1} + \cdots + a_1x + a_0 : a_0, \ldots, a_{n-1} \in \mathbb{Z}_p\right\}.$$

Sčítání je definováno jako pro běžné polynomy (modulo p). Násobení je definováno jako násobení pro běžné polynomy (modulo p) modulo ireducibilní (= nerozložitelný) polynom stupně n. □

Poznámka
GF, protože Galois field (Galoisova těles). Každé konečné těleso je izomorfní s nějakým GF.

Definice 2.10 (Charakteristika tělesa)

Charakteristika tělesa $\mathbf{T}$ je nejmenší $n \in \mathbb{N}$ takové, že $1 + \cdots + 1 = 0$ (1 je tam $n$kráť). Pokud takové n neexistuje, pak ji definujeme jako 0.

Tvrzení 2.8

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 $0 = n(n \text{ jedniček}) = p(p \text{ jedniček}) \cdot q(q\text{jedniček})$, tedy $p = 0$ nebo $q = 0$ (vlastnosti tělesa), *lightning.* □

Věta 2.9 (Malá fermatova věta)

Pro každé prvočíslo p a nenulové $a \in \mathbb{Z}_p$ platí $a^{p-1} = 1$.

Důkaz
Z prvočíselnosti p již víme, že platí lemma výše.

Protože $0a = 0$, tak $\{1, \ldots, p-1\} = \{1a, \ldots, (p-1)a\}$.

Tedy $1 \cdot 2 \cdot \ldots \cdot (p-1) = (1a) \cdot (2a) \cdot \ldots \cdot ((p-1)a)$. Zkrátím a vyjde $1 = a^{p-1}$. □

Poznámka
Následně jsme si ukazovali použití v samoopravných kódech (nejdříve pouze zdvojení a ztrojení bitů, poté tzv. Hammingův kód(…), kde se násobí maticemi $\mathbb{Z}_2^{3\times 7}$).

3 Vektorové prostory

Definice 3.1 (Vektorový prostor)

Buď $\mathbf{T}$ těleso s neutrálními prvky 0 a 1 pro sčítání a násobení. Vektorový prostor nad $\mathbf{T}$ je množina V s operacemi sčítání vektorů $+ : V^2 \to V$ a násobení vektoru skalárem $\cdot : \mathbf{T} \times V \to V$ splňující pro každé $\alpha, \beta \in \mathbf{T}$ a $\mathbf{u}, \mathbf{v} \in V$: TODO!

Například
Aritmetický prostor $\mathbf{T}^n$ $\mathbf{T}$. Prostor matic $\mathbf{T}^{m \times n}$ nad $\mathbf{T}$. Prostor $\mathcal{P}$ všech reálných polynomů proměnné x nad tělesem $\mathbb{R}$. Prostor $\mathcal{P}^n$ všech reálných polynomů proměnné $x \leq n$ stupně nad tělesem $\mathbb{R}$. Prostor $\mathcal{F}$ všech reálných funkcí. Prostor $\mathcal{C}$ všech spojitých reálných funkcí, …

Tvrzení 3.1 (Základní vlastnosti vektorových prostorů)

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

$$0\mathbf{v} = \mathbf{o},$$

$$\alpha\mathbf{o} = \mathbf{o}$$

$$\alpha v = \mathbf{o} \implies v = \mathbf{o} \vee \alpha = 0$$

$$-\mathbf{v} = (-1)\mathbf{v}$$

Důkaz
Stejný jako u ostatních vlastností. □

Definice 3.2 (Vektorové podprostory)

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

$$\mathbf{o} \in U,$$

$$\forall \mathbf{u}, \mathbf{v} \in U : \mathbf{u} + \mathbf{v} \in U,$$

$$\forall \alpha \in \mathbf{T} \forall \mathbf{u} \in U : \alpha\mathbf{u} \in U.$$

Důkaz
Jednoduchý? □

Například
Triviální podprostory V jsou V a $\{\mathbf{o}\}$.

Každá přímka procházející počátkem je podprostorem $\mathbb{R}^2$.

$\mathcal{P}^n, \mathcal{P}, \mathcal{C}, \mathcal{F}$ jsou v tomto pořadí podprostory dalších.

Množina symetrických reálných matic řádu n je podprostorem $\mathbb{R}^{n \times n}$.

Množina $\mathbb{Q}^n$ nad $\mathbb{Q}$ je podprostorem $\mathbb{R}^n$ nad $\mathbb{Q}$, ale není podprostorem $\mathbb{R}^n$ nad $\mathbb{R}$.

Tvrzení 3.2

Nechť $\mathbf{V}$ *je vektorový prostor nad tělesem* $\mathbb{T}$. *Pak průnik libovolného systému* $\{\mathbf{V}_i\}_{i\in I}$ *vektorových podprostorů prostoru* $\mathbf{V}$ *je vektorový podprostor* $\mathbf{V}$.

Důkaz
Podle tvrzení výše stačí ověřit uzavřenost a obsažení nulového prvku. Obojí je zřejmé z toho, že prvek je v průniku právě tehdy, když je prvkem všeho, přes co děláme průnik. □

Definice 3.3 (LO)

Pro vektorový prostor $\mathbf{V}$ nad tělesem $\mathbb{T}$ a $W \subseteq \mathbf{V}$ je průnik všech podprostorů obsahujících W lineárním obalem množiny $\mathbf{W}$. Značíme (W).

Definice 3.4 (Generátory a množiny generátorů)

Nechť $\mathbf{U} = (W)$, pak říkáme, že W generuje prostor $\mathbf{U}$ a prvky množiny W jsou generátory prostoru $\mathbf{U}$.

Pokud $\mathbf{U}$ je generovaný nějakou konečnou množinou, pak je konečně generovaný.

Definice 3.5 (Lineární kombinace)

Viz definice v OM1!

Věta 3.3

Lineární obal je roven podprostoru generovaného stejnou množinou vektorů.

Důkaz
Inkluze jedním směrem se dokáže z uzavřenosti, druhým směrem to dokážeme tak, že LO je uzavřený na operace $\mathbf{V}$ a obsahuje všechny „generující vektorový“. □

Definice 3.6 (Lineárně závislé a lineárně nezávislé)

Nechť $\mathbf{V}$ je vektorový prostor nad $\mathbb{T}$ a nechť $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbf{V}$. Pak vektory $\mathbf{v}_1, \ldots, \mathbf{v}_n$ jsou lineárně nezávislé, pokud $\sum_{i=1}^{n} \alpha_i \mathbf{v}_i = \mathbf{o}$ nastane pouze pro $\alpha_1 = \ldots = \alpha_n = 0$. V opačném případě jsou lineárně závislé.

Definice 3.7

Nekonečná množina vektorů je nezávislá, pokud je každá její konečná podmnožina nezávislá.

Věta 3.4

Nechť $\mathbf{V}$ *je vektorový prostor nad* $\mathbb{T}$ *a nechť* $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbf{V}$*. Pak jsou tyto vektory lineárně závislé právě tehdy, když nějaký z nich patří do lineárního obalu zbytku. (Lze jeden z nich vyjádřit jako lineární kombinaci zbylých vektorů.)*

Důkaz
Úpravami rovnic z definicí. □

Definice 3.8

Nechť $\mathbf{V}$ je vektorový prostor nad $\mathbb{T}$. Pak bází je jakýkoliv lineárně nezávislý systém generátorů prostoru $\mathbf{V}$.

Věta 3.5

Nechť báze $\mathbf{V}$ *je konečná. Pak každý vektor z* $\mathbf{V}$ *lze jednoznačně vyjádřit jako lineární kombinaci báze.*

Důkaz
Snadný. □

Věta 3.6

Každý vektorový prostor má bázi.

Důkaz
Dokážeme jen pro konečně generované: systém generátorů buď je lineárně nezávislý (a tím pádem báze), nebo z něj postupně můžeme odebírat prvky pomocí jedné z předchozích vět, až zbudou jen lineárně nezávislé - báze. □