Úvod do lineární algebry

Tomáš Matoušek

Tělesa, vektorové prostory

Definice. *Tělesem nazveme množinu M, na které jsou definována zobrazení $\oplus, \odot$: $M \times M \to M$ (binární operace) splňující následující axiomy:*

(1) $(\forall x, y \in M)\ x \oplus y = y \oplus x$. *(komutativita)*
(2) $(\forall x, y, z \in M)\ x \oplus (y \oplus z) = (x \oplus y) \oplus z$. *(asociativita)*
(3) $(\exists o \in M)(\forall x \in M)\ x \oplus o = o \oplus x = x$. *(neutrální prvek)*
(4) $(\forall x \in M)(\exists \bar{x} \in M)\ x \oplus \bar{x} = \bar{x} \oplus x = o$. *(opačný prvek)*
(5) $(\forall x, y \in M)\ x \odot y = y \odot x$. *(komutativita)*
(6) $(\forall x, y, z \in M)\ x \odot (y \odot z) = (x \odot y) \odot z$. *(asociativita)*
(7) $(\exists i \in M)(\forall x \in M)\ x \odot i = i \odot x = x$. *(neutrální prvek)*
(8) $(\forall x \in M, x \neq o)(\exists x^{-1} \in M)\ x \odot x^{-1} = x^{-1} \odot x = i$. *(inverzní prvek)*
(9) $(\forall x, y, z \in M)\ x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$. *(distributivita)*
(10) $i \neq o$.

Pro zjednodušení se místo $x \oplus \bar{y}$ píše $x \ominus y$, $x \odot y^{-1} = x \oslash y$, $\bar{x} = \ominus x$, $x \odot y = xy$. Z axiomů pak lze odvodit základní vlastnosti těles: všechny existenční kvantifikátory v axiomech se dají nahradit jednoznačnou existencí, dále např. $(\forall x \in M)\ ox = o$, $(\forall a, x, y \in M, a \neq o)\ ax = ay \Leftrightarrow x = y$, $(\forall a, x, y \in M)\ a \oplus x = a \oplus y \Leftrightarrow x = y$, $(\ominus i)x = \bar{x} = \ominus x$, ...

Některá tělesa jistě znáte. Např. $(\mathbb{R}, +, \cdot)$ nebo $(\mathbb{Q}, +, \cdot)$. Můžete si ověřit, že skutečně splňují všech 10 axiomů, přičemž operace $\odot$ odpovídá násobení a $\oplus$ sčítání, neutrální prvek vzhledem k násobení je $i = 1$ a vzhledem ke sčítání $o = 0$. Rozmyslete si naopak, proč $(\mathbb{N}, +, \cdot)$, $(\mathbb{N}_0, +, \cdot)$ ani $(\mathbb{Z}, +, \cdot)$ nejsou tělesa.

Pro naše účely budou vhodná tělesa $(\mathbb{Z}_p, +, \cdot)$, kde $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, p je prvočíslo. Operace sčítání a násobení budou odpovídat standardním operacím modulo p.

Definice. *Vektorovým prostorem nad tělesem $(\mathbb{T}, +, \cdot)$ nazveme množinu $\mathcal{V}$, na které jsou definovány binární operace sčítání $\oplus : \mathcal{V} \times \mathcal{V} \to \mathcal{V}$ a násobení skalárem (tj. prvkem tělesa $\mathbb{T}$) $\odot : \mathbb{T} \times \mathcal{V} \to \mathcal{V}$ splňující axiomy:*

(1) $(\forall \mathbf{x}, \mathbf{y} \in \mathcal{V})\ \mathbf{x} \oplus \mathbf{y} = \mathbf{y} \oplus \mathbf{x}$. *(komutativita)*
(2) $(\forall \mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathcal{V})\ \mathbf{x} \oplus (\mathbf{y} \oplus \mathbf{z}) = (\mathbf{x} \oplus \mathbf{y}) \oplus \mathbf{z}$. *(asociativita)*
(3) $(\exists \mathbf{o} \in \mathcal{V})(\forall \mathbf{x} \in \mathcal{V})\ \mathbf{x} \oplus \mathbf{o} = \mathbf{o} \oplus \mathbf{x} = \mathbf{x}$. *(neutrální prvek)*
(4) $(\forall \mathbf{x} \in \mathcal{V})(\exists \bar{\mathbf{x}} \in \mathcal{V})\ \mathbf{x} \oplus \bar{\mathbf{x}} = \bar{\mathbf{x}} \oplus \mathbf{x} = \mathbf{o}$. *(opačný prvek)*
(5) $(\forall a, b \in \mathbb{T}, \mathbf{x} \in \mathcal{V})\ (ab) \odot \mathbf{x} = a \odot (b \odot \mathbf{x})$.

(6) $(\forall \mathbf{x} \in \mathcal{V})\ i \odot \mathbf{x} = \mathbf{x}$.
(7) $(\forall a \in \mathbb{T},\ \mathbf{x}, \mathbf{y} \in \mathcal{V})\ a \odot (\mathbf{x} \oplus \mathbf{y}) = (a \odot \mathbf{x}) \oplus (a \odot \mathbf{y})$.
(8) $(\forall a, b \in \mathbb{T},\ \mathbf{x} \in \mathcal{V})\ (a + b) \odot \mathbf{x} = (a \odot \mathbf{x}) \oplus (b \odot \mathbf{x})$.

Prvky $\mathcal{V}$ nazýváme vektory. Zkrácení zápisu: $\mathbf{x} \oplus \bar{\mathbf{y}} = \mathbf{x} \ominus \mathbf{y}$, $\bar{\mathbf{x}} = \ominus\mathbf{x}$, $a \odot \mathbf{x} = a\mathbf{x}$.

Uvažujme nyní množinu $\mathcal{V}$ všech n-tic prvků tělesa $\mathbb{T}$. Každý prvek $\mathbf{x}$ můžeme napsat jako $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, kde $x_1, x_2, \ldots, x_n \in \mathbb{T}$. Definujme sčítání dvou n-tic $\mathbf{x}, \mathbf{y}$ jako sčítání po složkách, tj.

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

a násobení skalárem a takto:

$$a(x_1, \ldots, x_n) = (ax_1, \ldots, ax_n).$$

Nulovým vektorem bude n-tice (0,0, ... ,0). Pak lze ověřit, že množina $\mathcal{V}$ spolu s těmito operacemi je vektorovým prostorem nad $\mathbb{T}$.

Pro názornost dále uvažujme jen tělesa $\mathbb{R}$ a $\mathbb{Z}_p$.

Definice. *Buď $\mathcal{V}$ vektorový prostor nad $\mathbb{T}$, $\mathbf{x}_1, \mathbf{x}_2, \ldots \mathbf{x}_n \in \mathcal{V}$ soubor vektorů. Řekneme, že tento soubor je lineárně nezávislý, pokud pro libovolné $a_1, \ldots, a_n \in \mathbb{T}$*

$$\sum_{i=1}^{n} a_i \mathbf{x}_i = \mathbf{o} \Rightarrow a_1 = a_2 = \cdots = a_n = 0.$$

Matice

Definice. *Matice typu $m \times n$ s prvky z tělesa $\mathbb{T}$ je m-tice n-tic čísel z tělesa $\mathbb{T}$. Bude-li $m = n$ nazveme takovou matici maticí čtvercovou. Např. matici A typu 2×3 můžeme zapsat takto:*

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

kde $a_{ij} \in \mathbb{T}, i \in \{1, \ldots, m\}, j \in \{1, \ldots, n\}$. Když bude zřejmé o jaký typ matice se jedná, budeme používat jen zápisu $A = (a_{ij})$. Dále budeme i-tým řádkem matice (a_{ij}) myslet n-tici $(a_{i1}, a_{i2}, \ldots, a_{in})$ a j-tým sloupcem této matice m-tici $(a_{1j}, a_{2j}, \ldots, a_{mj})$.

Definice. *Buď $A = (a_{ij})$. Pak A je nulová, je-li $(\forall i, j)\ a_{ij} = 0$, značíme pak $A = O$. Je-li navíc A typu $n \times n$, je A*

(1) *jednotková, je-li $(\forall i, j)\ a_{ij} = \delta_{ij}$, kde $\delta_{ij} = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$, značíme $A = I_n$.*

(2) *diagonální, je-li* $(\forall i \neq j)\ a_{ij} = 0, A \neq O$.
(3) *dolní trojúhelníková, je-li* $(\forall i < j)\ a_{ij} = 0, A \neq O$.
(4) *horní trojúhelníková, je-li* $(\forall i > j)\ a_{ij} = 0, A \neq O$.

Abychom s maticemi mohli něco dělat, definujeme si několik operací. Buď $A = (a_{ij}), B = (b_{ij})$ matice typu $m \times n$. Pak $C = A + B$ je matice typu $m \times n$ taková, že

$$(\forall i, j)\ c_{ij} = a_{ij} + b_{ij}.$$

Buď $A = (a_{ij})$ matice typu $m \times n$, $c \in \mathbb{T}$. Pak $C = cA$ je matice typu $m \times n$ taková, že

$$(\forall i, j)\ c_{ij} = ca_{ij}.$$

Buď $A = (a_{ij})$ matice typu $m \times n$, $B = (b_{ij})$ matice typu $n \times l$. Pak $C = A \times B = AB$ je matice typu $m \times l$ taková, že

$$(\forall i, j)\ c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

Jelikož sčítání matic je vlastně jen sčítáním jejich odpovídajících prvků, snadno nahlédneme, že je komutativní, asociativní, existuje neutrální prvek vzhledem ke sčítání (tj. nulová matice) a ke každé matici najdeme i matici opačnou. Na přednášce si ukážeme, že násobení matic je asociativní, ale není komutativní (tj. násobení zprava je obecně něco jiného, než násobení zleva), existuje neutrální prvek vzhledem k násobení zprava i zleva a ne ke každé matici existuje zleva či zprava inverzní matice.

Tvrzení. Množina všech matic typu $m \times n$ s prvními dvěma výše uvedenými operacemi tvoří vektorový prostor nad $\mathbb{T}$.

Soustavy lineárních rovnic

Nyní uvidíme, že definováním matic si velmi zjednodušíme práci se soustavami lineárních rovnic. Budeme pracovat s obecnými soustavami, které mají m rovnic o n neznámých.

Definice. *Buď* $a_{ij}, b_j \in \mathbb{T}, i \in \{1, \ldots, n\}, j \in \{1, \ldots, n\}$ *a buď*

$$\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\
a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\
&\vdots \\
a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m
\end{aligned}$$

soustava lineárních rovnic pro neznámé $x_i, i \in \{1, \ldots, n\}$. Pak matici (a_{ij}) typu $m \times n$ nazveme maticí soustavy a matici $(a_{ij}|b_i)$ typu $m \times (n+1)$ (tj. matice soustavy, k níž je přidán sloupec pravých stran pro přehlednost graficky oddělený svislou čárou) nazveme rozšířenou maticí soustavy.

Gaussova-Jordanova eliminace

Definice. *Nechť $(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ je n-tice vektorů. Elementární úpravou nazveme provedení jedné z následujících úprav:*
(1) *prohození vektorů $\mathbf{x}_i, \mathbf{x}_j$ $(i \neq j)$.*
(2) *vynásobení vektoru $\mathbf{x}_i$ skalárem $k \in \mathbb{T}, k \neq 0$.*
(3) *nahrazení vektoru $\mathbf{x}_i$ vektorem $\mathbf{x}_i + k\mathbf{x}_j, i \neq j, k \in \mathbb{T}, k \neq 0$.*

Definice. (Gaussova-Jordanova eliminace) *Buď $A = (a_{ij})$ matice soustavy typu $m \times n$ a $B = (a_{ij}|b_i)$ rozšířená matice soustavy. Nechť J je množina všech nenulových sloupců a I množina všech nenulových řádků matice.*
(1) *Z množiny J vyjmeme nějaký sloupec, nechť je to j-tý sloupec matice A.*
(2) *Z tohoto sloupce vybereme nenulový prvek a_{ij} takový, že $i \in I$, a z množiny I odebereme řádek i. Pokud žádný takový prvek neexistuje, zopakujeme (1).*
(3) *Ke každému řádku k $(k \neq i)$ matice B přičteme $-a_{ij}^{-1}a_{kj}$ násobek řádku i.*
(4) *Opakujeme body (1) až (3) dokud je množina J neprázdná.*

Pozorování. Po provedení *GJE* (Gaussovy-Jordanovy eliminace) bude v matici A v každém sloupci nejvýše jeden nenulový prvek. Výsledná rozšířená matice soustavy, reprezentuje soustavu rovnic ekvivalentní s původní soustavou.

Věta. *Nechť n-tici vektorů $(\mathbf{y}_1, \ldots, \mathbf{y}_n)$ dostaneme z $(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ elementární úpravou. Pak $(\mathbf{y}_1, \ldots, \mathbf{y}_n)$ je lineárně nezávislá právě tehdy, když $(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ je lineárně nezávislá.*

Důsledek. Pomocí *GJE* můžeme zjistit, zda jsou vektory lineárně nezávislé.

Definice. *Sloupcová hodnost matice* je maximální počet lineárně nezávislých sloupců matice. *Řádková hodnost matice* je maximální počet lineárně nezávislých řádků matice.

Věta. *GJE zachovává řádkovou hodnost matice.*

Důsledek. Pomocí *GJE* můžeme zjistit řádkovou hodnost matice.

Věta. *Sloupcová a řádková hodnost každé matice se rovnají.*

Věta. (Frobeniova podmínka řešitelnosti soustavy) *Buď $A = (a_{ij})$ matice soustavy a $B = (a_{ij}|b_i)$ rozšířená matice téže soustavy. Soustava rovnic má řešení právě tehdy, když sloupcová hodnost matice A je rovna sloupcové hodnosti matice B.*