Grupy, nehmotná tělesa a prostory plné vektorů

Lenka Zdeborová

Úkolem mojí přednášky je seznámit vás se základními pojmy algebry. Zde ve sborníku jsou uvedeny všechny potřebné definice, které budou na přednášce objasněny. Uvedeme si spoustu příkladů a dokážeme některé níže uvedené věty.

Množina

Definice. *Základní vlastností každé množiny M je, že o každém objektu a můžeme jednoznačně rozhodnout, zda náleží ($a \in M$) či nenáleží ($a \notin M$) do množiny M.*

Přesná definice množiny neexistuje, jen její vlastnosti můžeme popsat pomocí soustavy axiomů, to se ale tématu této přednášky příliš netýká.

Grupa

Definice. *Množinu G, na níž je definována binární operace $\oplus : G \times G \to G$, nazýváme grupou, platí-li vztahy:*

(1) $\forall a, b, c \in G \quad (a \oplus b) \oplus c = a \oplus (b \oplus c)$ *(asociativní zákon).*
(2) $(\exists \tilde{0} \in G)(\forall a \in G) \quad a \oplus \tilde{0} = \tilde{0} \oplus a = a$ *($\tilde{0}$ nazýváme neutrální resp. jednotkový prvek grupy).*
(3) $(\forall a \in G)(\exists b \in G) \quad a \oplus b = b \oplus a = \tilde{0}$ *(b nazýváme opačný resp. inverzní prvek k prvku a).*

Definice. *Abelova (komutativní) grupa je grupa, pro kterou navíc platí, že*

$$\forall a, b \in G \quad a \oplus b = b \oplus a \quad \text{(komutativní zákon).}$$

Definice. *Podgrupa grupy $(G, \oplus)$ je taková množina H, která je podmnožinou G a zároveň je to grupa s operací $\oplus$.*

Okruhy a tělesa

Definice. *Množinu M se dvěma binárními operacemi $\oplus$ a $\odot$, nazveme okruhem, je-li $(M,\oplus)$ Abelova grupa a navíc platí:*

(1) $\forall a,b,c \in M \quad (a\odot b)\odot c = a\odot(b\odot c)$.
(2) $(\exists \tilde{1} \in M)(\forall a \in M) \quad a\odot\tilde{1} = \tilde{1}\odot a = a$.
(3) $\forall a,b,c \in M \quad a\odot(b\oplus c) = (a\odot b)\oplus(a\odot c)$ *(levý distributivní zákon).*
(4) $\forall a,b,c \in M \quad (a\oplus b)\odot c = (a\odot c)\oplus(b\odot c)$ *(pravý distributivní zákon).*

Definice. *Okruh M nazveme tělesem, pokud*

$$(\forall a \in M)(\exists b \in M) \quad a\odot b = b\odot a = \tilde{1}.$$

V komutativním tělese navíc platí

$$\forall a,b \in M \quad a\odot b = b\odot a.$$

Vektorový (lineární) prostor

Nechť $(T,\oplus,\odot)$ je komutativní těleso (dále vždy uvažujme $\mathbb{R}$, není-li řečeno jinak). Množinu V nazveme lineárním nebo vektorovým prostorem nad T právě tehdy, když jsou na V definovány operace $\oplus : V\times V \to V$ a $\odot : T\times V \to V$ splňující následující axiomy:

(1) *$(V,\oplus)$ je Abelova grupa, její prvky značme $\mathbf{x}$, $\boldsymbol{y}$, $\boldsymbol{u}$, $\mathbf{v}, \dots$, nulový prvek $\boldsymbol{0}$.*
(2) $(\forall \alpha,\ \beta \in T)(\forall \boldsymbol{u} \in V) \quad \alpha\odot(\beta\odot\boldsymbol{u}) = (\alpha\odot\beta)\odot\boldsymbol{u}$.
(3) $\forall \boldsymbol{u} \in V \quad \tilde{1}\odot\boldsymbol{u} = \boldsymbol{u}$.
(4) $(\forall \boldsymbol{u},\ \mathbf{v} \in V)(\forall \alpha \in T) \quad \alpha\odot(\boldsymbol{u}\oplus\mathbf{v}) = (\alpha\odot\boldsymbol{u})\oplus(\alpha\odot\mathbf{v})$.
(5) $(\forall \boldsymbol{u} \in V)(\forall \alpha,\ \beta \in T) \quad (\alpha\oplus\beta)\odot\boldsymbol{u} = (\alpha\odot\boldsymbol{u})\oplus(\beta\odot\boldsymbol{u})$.

Definice. *Jsou-li W, V vektorové prostory nad stejným tělesem, se stejnými operacemi a navíc $W \subseteq V$, říkáme, že W je podprostorem V.*

Poznámka. V dalším textu budeme namísto $\oplus, \odot$ psát pro přehlednost $+, \cdot$ (přičemž „$\cdot$" můžeme vynechávat).

Definice. *Nechť $\boldsymbol{u}_1,\ \boldsymbol{u}_2, \dots,\ \boldsymbol{u}_n$ jsou prvky vektorového prostoru V. Lineární kombinací těchto vektorů nazveme každý vektor $\boldsymbol{u}$, který se dá vyjádřit ve* *tvaru*

$$\boldsymbol{u} = \sum_{i=1}^{n} \alpha_i \boldsymbol{u}_i,$$

kde $\alpha_1,\ \alpha_2, \ldots,\ \alpha_n$ *jsou reálná čísla. Je-li* $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$, *je* $\boldsymbol{u}$ *triviální lineární kombinací vektorů* $\boldsymbol{u}_1,\ \boldsymbol{u}_2, \ldots,\ \boldsymbol{u}_n$.

Definice. *Vektory nazveme lineárně závislé, je-li některý z nich netriviální lineární kombinací ostatních.*

Definice. *Lineárním obalem vektorů* $\boldsymbol{u}_1,\ \boldsymbol{u}_2, \ldots,\ \boldsymbol{u}_n \in V$ *nazveme množinu všech lineárních kombinací těchto vektorů. Lineárním obalem množiny* $M \subseteq V$ *nazveme množinu všech (konečných) lineárních kombinací vektorů z množiny* M*. Značíme ho* $L(M)$.

Definice. *Množina* $M \subseteq V$ *se nazývá báze vektorového prostoru* V*, je-li lineárně nezávislá a jejím lineárním obalem je celý prostor* V*. Dimenze prostoru je počet prvků baze.*

Věta. (Steinitzova) *Mějme vektorový prostor* V *a v něm*
1. *nějaké lineárně nezávislé vektory* $\mathbf{v}_1,\ \mathbf{v}_2, \ldots,\ \mathbf{v}_m$.
2. *další* $\mathbf{w}_1,\ \mathbf{w}_2, \ldots,\ \mathbf{w}_n$ *takové, že* $\forall i \quad \mathbf{v}_i \in L(\{\mathbf{w}_1,\ \mathbf{w}_2, \ldots,\ \mathbf{w}_n\})$.

Potom platí $m \leq n$.

Jiná formulace: V množině všech lineárních kombinací daných n *vektorů existuje nejvýše* n *lineárně nezávislých.*

Důsledek. Libovolnou množinu nezávislých vektorů $\mathbf{v}_1,\ \mathbf{v}_2, \ldots,\ \mathbf{v}_n$, pro kterou je $V = L(\{\mathbf{v}_1,\ \mathbf{v}_2, \ldots,\ \mathbf{v}_n\})$, jsme nazvali bazí. Ze Steinitzovy věty plyne, že libovolné dvě takto definované báze mají stejný počet prvků, neboli dimenze je definovaná jednoznačně.

Věta. *Nechť vektory* $\mathbf{v}_1,\ \mathbf{v}_2, \ldots,\ \mathbf{v}_n$ *tvoří bázi vektorového prostoru* V*. Je-li* $\mathbf{v}$ *libovolný prvek z* V*, pak existuje právě jedna n-tice* $\alpha_1,\ \alpha_2, \ldots,\ \alpha_n \in \mathbb{R}$ *taková, že platí*

$$\mathbf{v} = \sum_{i=1}^{n} \alpha_i \mathbf{v}_i.$$

Definice. *Čísla* $\alpha_1,\ \alpha_2, \ldots,\ \alpha_n$ *se nazývají souřadnice vektoru* $\mathbf{v}$ *v bázi* $\mathbf{v}_1,\ \mathbf{v}_2, \ldots,\ \mathbf{v}_n$.

Skalární součin

Definice. *Skalárním součinem na V nazveme zobrazení $\{\mathbf{x},\boldsymbol{y} \to (\mathbf{x},\boldsymbol{y})\} : V\times V \to \mathbb{C}$ splňující $(\forall \mathbf{x},\ \boldsymbol{y},\ \boldsymbol{z} \in V)(\forall \alpha \in \mathbb{C})$:*

(1) $(\boldsymbol{x}+\boldsymbol{y},\boldsymbol{z}) = (\boldsymbol{x},\boldsymbol{z}) + (\boldsymbol{y},\boldsymbol{z})$.
(2) $(\mathbf{x},\boldsymbol{y}+\boldsymbol{z}) = (\mathbf{x},\boldsymbol{z}) + (\mathbf{x},\boldsymbol{y})$.
(3) $(\alpha\mathbf{x},\boldsymbol{y}) = \alpha(\mathbf{x},\boldsymbol{y})$.
(4) $(\mathbf{x},\alpha\boldsymbol{y}) = \overline{\alpha}(\mathbf{x},\boldsymbol{y})$.
(5) $(\mathbf{x},\boldsymbol{y}) = \overline{(\boldsymbol{y},\mathbf{x})}$.
(6) $\boldsymbol{x} \neq \boldsymbol{0} \Rightarrow (\mathbf{x},\mathbf{x}) > 0$.

Poznámka. $\overline{\alpha}$ znamená α komplexně sdružené. My ovšem zde budeme pracovat pouze s reálnými čísly ($\{\mathbf{x},\boldsymbol{y} \to (\mathbf{x},\boldsymbol{y})\} : V\times V \to \mathbb{R}$). Podmínky (4), (5) tedy přejdou na:

(4*) $(\mathbf{x},\alpha\boldsymbol{y}) = \alpha(\mathbf{x},\boldsymbol{y})$.
(5*) $(\mathbf{x},\boldsymbol{y}) = (\boldsymbol{y},\mathbf{x})$.

Definice. *Funkci $\{\mathbf{x} \to \|\mathbf{x}\| \equiv \sqrt{(\mathbf{x},\mathbf{x})}\} : V \to \mathbb{R}_0^+$ nazveme normou na prostoru V, indukovanou skalárním součinem. Číslo $\|\mathbf{x}\|$ pak nazýváme normou vektoru $\mathbf{x}$.*

Věta. *Platí $\forall \mathbf{x},\boldsymbol{y} \in V$:*

(1) $(\mathbf{x},\boldsymbol{y}) = \frac{1}{2}(\|\mathbf{x}\|^2 + \|\boldsymbol{y}\|^2 + \|\mathbf{x}-\boldsymbol{y}\|^2)$.
(2) $(\mathbf{x},\boldsymbol{y}) = \frac{1}{4}(\|\mathbf{x}+\boldsymbol{y}\|^2 - \|\mathbf{x}-\boldsymbol{y}\|^2)$.

Věta. (Minkovského) *Platí trojúhelníková nerovnost:*

$$\forall \mathbf{x},\ \boldsymbol{y} \in V \quad \|\mathbf{x}+\boldsymbol{y}\| \leq \|\mathbf{x}\| + \|\boldsymbol{y}\|.$$

Věta. (Schwarz-Cauchy-Buňakovského) *Platí nerovnost:*

$$\forall \mathbf{x},\ \boldsymbol{y} \in V \quad (\mathbf{x},\boldsymbol{y}) \leq \|\mathbf{x}\|\ \|\boldsymbol{y}\|.$$

Definice. *Vektory $\mathbf{v}_1,\ \mathbf{v}_2,\dots,\ \mathbf{v}_n \in V$ nazveme vzájemně kolmé neboli ortogonální, platí-li $(\mathbf{v}_i,\mathbf{v}_j) = \delta_{ij}\|\mathbf{v}_i\|\|\mathbf{v}_j\|$, kde δ_{ij} je takzvané Kroneckerovo delta, pro něž je $\delta_{ij} = 1 \Leftrightarrow i = j$ a $\delta_{ij} = 0 \Leftrightarrow i \neq j$.*

Definice. *Množina $M \subseteq V$ je ortogonální, je-li*

$$\forall \mathbf{x},\ \boldsymbol{y} \in M \quad (\mathbf{x} \neq \boldsymbol{y} \Rightarrow (\mathbf{x},\boldsymbol{y}) = 0).$$

Je-li navíc $\forall \mathbf{x} \in M \quad \|\mathbf{x}\| = 1$, nazýváme M ortonormální.

Říkáme také, že množiny $M_1,\ M_2 \subseteq V$ jsou vzájemně ortogonální, je-li

$$(\forall \mathbf{x} \in M_1)(\forall \boldsymbol{y} \in M_2) \quad (\mathbf{x},\boldsymbol{y}) = 0.$$

Poznámka. V každém konečnědimenzionálním prostoru se skalárním součinem existuje ortonormální báze.