ÚSTAV ROBOTIKY
A KYBERNETIKY

Kolekcia učebných textov

apríl 2024
github.com/PracovnyBod/KUT
RM

v0.9
KUTooX

O algebraických štruktúrach s dvomi binárnymi operáciami

1 Algebraické štruktúry s dvomi binárnymi operáciami

Neskúsenejší čitateľ pravdepodobne po prečítaní pojmu lineárna algebra už radšej ďalej nepokračoval. Skúsenejší čitateľ sa už možno aj stretol s pojmami ako pole, teleso alebo okruh, avšak neprišlo mu jednoznačné prečo sú dané veci tak pomenované a na čo vlastne slúžia. Všetko sú to predsa pojmy z abstraktnej matematiky, názvy teda niekedy treba brať s nadhľadom.

Gro abstraktnej matematiky spočíva v triedení - škatuľkovaní podľa určitých vlastností. Stanovíme si nejaké spoločné vlastnosti, ktoré sú spoločné pre skupinu objektov, tieto vlastnosti sa nazývajú axiómy. Pokiaľ teda niečo spĺňa všetky axiómy z nejakej skupiny, tak môžeme tvrdiť, že do tejto skupiny aj patrí - zaškatuľkujeme to. Z týchto axiómov sú potom odvoditeľné lemmy a vety, ktoré sú používané v iných odvetviach a vieme, že pre všetky naše zaškatuľkované veci platia a sú teda použiteľné.

Príklad lineárna kombinácia sa používa vo frekvenčnej analýze a pri riešení lineárnych diferenciálnych rovníc, čiže v podstate sa s ňou stretávame neustále v lineárnej teórii riadenia. Ďalším príkladom, môže byť stavová rovina, v ktorej stavy sú vektory, na to, aby sme vedeli povedať čo je to vektor a aké vlastnosti má potrebujeme definíciu vektorového priestoru.

V tejto časti si uvedieme štruktúry, ktoré majú dve binárne operácie: operáciu súčtu $\oplus$ a operáciiu násobenia $\odot$. Symboly pre operácie sú zámerne uvedené v krúžku, aby sme ich odlíšili od štandardne definovaného $+$ a $\cdot$, pretože dané operácie môžu byť definované podľa čitateľovej fantázie. Rovnako rozlišujeme špeciálnu nulu $\mathbb{0}$ a jednotku $\mathbb{1}$, ktoré tak isto nemusia zodpovedať svojím numerickým náprotivkom.

Definícia 1.1. Axiómy algebraických štruktúr s dvomi binárnymi operáciami $\oplus$ a $\odot$:

0. Definujeme dve binárne operácie súčet $\oplus$ a násobenie $\odot$, na objekte $\mathbb{P}$ s prvkami a, b:
$$\oplus: \ \mathbb{P} \times \mathbb{P} \ni \{a, b\} \ \rightarrow \ a \oplus b \in \mathbb{P}$$
$$\odot: \ \mathbb{P} \times \mathbb{P} \ni \{a, b\} \ \rightarrow \ a \odot b \in \mathbb{P}$$
Z tohto axiómu vidíme, že pokiaľ vykonáme operáciu $\oplus$ alebo $\odot$, tak výsledok je stále z objektu $\mathbb{P}$.

1. Operácia $\oplus$ je asociatívna:
$$(a \oplus b) \oplus c = a \oplus (b \oplus c)$$

2. Existuje prvok identity $\mathbb{0}$ ("nulový prvok") pre operáciu $\oplus$:
$$\exists \ \mathbb{0} \in \mathbb{P}: \ \mathbb{0} \oplus a = a \oplus \mathbb{0} = a$$

3. Pre každý prvok a z $\mathbb{P}$ pre operáciu $\oplus$ xistuje inverzný prvok $-a$:
$$\forall \ a \in \mathbb{P} \ \exists \ -a: \ a \oplus (-a) = \mathbb{0}$$

4. Operácia $\oplus$ je komutatívna:
$$a \oplus b = b \oplus a$$

5. Distributívnosť operácie $\odot$ zľava:
   $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$

6. Distributívnosť operácie $\odot$ sprava:
   $(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$

7. Operácia $\odot$ je asociatívna:
   $(a \odot b) \odot c = a \odot (b \odot c)$

8. Existuje prvok identity $\mathbb{1}$ pre operáciu $\oplus$:
   $\exists\, \mathbb{1} \in \mathbb{P}: \ \mathbb{1} \odot a = a \odot \mathbb{1} = a$

9. Pre každý prvok a z $\mathbb{P}$ pre operáciu $\odot$ existuje inverzný prvok a^{-1}:
   $\forall a \neq 0\ \exists\, a^{-1}: \ a \odot a^{-1} = a^{-1} \odot a = \mathbb{1}$

10. Operácia $\odot$ je komutatívna:
    $a \odot b = b \odot a$

Pokiaľ sú splnené axiómy (0)-(10) hovoríme o poli, pre (0)-(9) hovoríme o telese, pre (0)-(7) hovoríme o okruhu, pokiaľ pre okruh platí aj axióm (8), hovoríme o okruhu s jednotkou. Príkladom poľa sú napríklad reálne a komplexné čísla, nechávame na čitateľovom zamyslení si dané tvrdenie overiť kontrolovou jednotlivých axiómov, ďalším zamyslením môže byť či aj celé čísla sú poľom. Nad poľom definujeme ďalší dôležitý pojem z lineárnej algebry - vektorový priestor.

2 Vektorový priestor

Definícia 2.1 (Vektorový priestor)**.** Vektorový priestor V nad poľom K je neprázdna množina s dvomi definovanými operáciami $\oplus : V \times V \to V$ a $\odot : K \times V \to V$, ktorá spĺňa nasledujúcich 8 axiómov:

1. Asociatívnosť:
   $\mathbf{u} \oplus (\mathbf{v} \oplus \mathbf{w}) = (\mathbf{u} \oplus \mathbf{v}) \oplus \mathbf{w}, \quad \mathbf{u}, \mathbf{v}, \mathbf{w} \in V$

2. Komutatívnosť:
   $\mathbf{u} \oplus \mathbf{v} = \mathbf{v} \oplus \mathbf{u}, \quad \mathbf{u}, \mathbf{v} \in V$

3. Prvok identity vektorového súčtu:
   $\mathbf{u} \oplus \mathbf{0} = \mathbf{u}, \quad \mathbf{u}, \mathbf{0} \in V$

4. Inverzný prvok:
   $\mathbf{u} \oplus \mathbf{v} = \mathbf{0}, \quad \mathbf{u}, \mathbf{v}, \mathbf{0} \in V$

5. Kompatibilita skalárneho násobenia s násobením poľa
   $\alpha \odot (\beta \odot \mathbf{u}) = (\alpha\beta) \odot \mathbf{u}, \quad \alpha, \beta \in K, \quad \mathbf{u} \in V$

6. Prvok identity skalárneho násobenia:
   $\mathbb{1} \odot \mathbf{u} = \mathbf{u}, \quad \mathbb{1} \in K, \quad \mathbf{u} \in V$

7. Distributívnosť vzhľadom na vektorový súčet:
   $\alpha \odot (\mathbf{u} \oplus \mathbf{v}) = \alpha \odot \mathbf{u} \oplus \alpha \odot \mathbf{v}, \quad \alpha \in K, \quad \mathbf{u}, \mathbf{v} \in V$

8. Distributívnosť vzhľadom na súčet poľa:
   $(\alpha + \beta) \odot \mathbf{u} = \alpha \odot \mathbf{u} \oplus \beta \odot \mathbf{u}, \quad \alpha, \beta \in K, \quad \mathbf{u} \in V$

V definícii (2.1) sme zámerne označili operácie $+$ a $\cdot$ v krúžku, aby sme ich rozlíšili od štandardne definovaného súčtu a súčinu, je možné ale používať aj označenie bez krúžku. Prvky $\mathbf{0}$ a $\mathbb{1}$ sú špeciálne a pre každý vektorový priestor originálne, nemusia nutne zodpovedať číselnej 0 a 1.

Príklad 2.1. Vyšetrite či komplexné čísla $\mathbf{z} = \alpha + i\beta$ so štandardne definovanými operáciami $+, \cdot$ tvoria vektorový priestor V nad reálnymi číslami $\mathbb{R}$, $\mathbf{z} \in V$, $\alpha, \beta \in \mathbb{R}$.

1.

$$\begin{aligned}
\alpha_1 + i\beta_1 + (\alpha_2 + i\beta_2 + \alpha_3 + i\beta_3) &= \alpha_1 + i\beta_1 + (\alpha_2 + \alpha_3 + i(\beta_2 + \beta_3)) \\
&= \alpha_1 + \alpha_2 + \alpha_3 + i(\beta_1 + \beta_2 + \beta_3) \\
(\alpha_1 + i\beta_1 + \alpha_2 + i\beta_2) + \alpha_3 + i\beta_3 &= (\alpha_1 + \alpha_2 i(\beta_1 + \beta_2)) + \alpha_3 + i\beta_3 \\
&= \alpha_1 + \alpha_2 + \alpha_3 + i(\beta_1 + \beta_2 + \beta_3)
\end{aligned}$$

2.

$$\begin{aligned}
\alpha_1 + i\beta_1 + \alpha_2 + i\beta_2 &= \alpha_1 + \alpha_2 + i(\beta_1 + \beta_2) \\
\alpha_2 + i\beta_2 + \alpha_1 + i\beta_1 &= \alpha_2 + \alpha_1 + i(\beta_2 + \beta_1) \\
&= \alpha_1 + \alpha_2 + i(\beta_1 + \beta_2)
\end{aligned}$$

3.

$$\begin{aligned}
&\alpha + i\beta + o_r + io_i = \alpha + i\beta \\
&\alpha + o_r = \alpha \implies o_r = 0 \\
&\beta + o_i = \beta \implies o_i = 0 \\
&\mathbf{0} = 0 + i0
\end{aligned}$$

4.

$$\begin{aligned}
&\alpha_1 + i\beta_1 + \alpha_2 + i\beta_2 = 0 + i0 \\
&\alpha_1 + \alpha_2 = 0 \implies \alpha_1 = -\alpha_2 \\
&\beta_1 + \beta_2 = 0 \implies \beta_1 = -\beta_2 \\
&\mathbf{z} + (-\mathbf{z}) = \mathbf{0}
\end{aligned}$$

5. $\mu,\ \nu \in \mathbb{R}$

$$\begin{aligned}
&\mu(\nu(\alpha + i\beta)) = \mu(\nu\alpha + i\nu\beta)) = \mu\nu\alpha + i\mu\nu\beta \\
&(\mu\nu)(\alpha + i\beta) = \mu\nu\alpha + i\mu\nu\beta
\end{aligned}$$

6.

$$\begin{aligned}
&\mathbb{1}\alpha + i\mathbb{1}\beta = \alpha + i\beta \\
&\mathbb{1}\alpha = \alpha \implies \mathbb{1} = 1 \\
&\mathbb{1}\beta = \beta \implies \mathbb{1} = 1 \\
&\mathbb{1} = 1
\end{aligned}$$

7. $\mu,\ \nu \in \mathbb{R}$

$$\begin{aligned}
\mu(\alpha_1 + i\beta_1 + \alpha_2 + i\beta_2) &= \mu(\alpha_1 + \alpha_2 + i(\beta_1 + \beta_2)) \\
&= \mu(\alpha_1 + \alpha_2) + i\mu(\beta_1 + \beta_2) \\
&= \mu\alpha_1 + \mu\alpha_2 + i(\mu\beta_1 + \mu\beta_2) \\
\mu(\alpha_1 + i\beta_1) + \mu(\alpha_2 + i\beta_2) &= \mu\alpha_1 + i\mu\beta_1 + \mu\alpha_2 + i\mu\beta_2 \\
&= \mu\alpha_1 + \mu\alpha_2 + i(\mu\beta_1 + \mu\beta_2)
\end{aligned}$$

8. $\mu,\ \nu \in \mathbb{R}$

$$\begin{aligned}
(\mu + \nu)(\alpha + i\beta) &= (\mu + \nu)\alpha + i(\mu + \nu)\beta \\
&= \mu\alpha + \nu\alpha + i(\mu\beta + \nu\beta) \\
\mu(\alpha + i\beta) + \nu(\alpha + i\beta) &= \mu\alpha + i\mu\beta + \nu\alpha + i\nu\beta \\
&= \mu\alpha + \nu\alpha + i(\mu\beta + \nu\beta)
\end{aligned}$$

Vidíme, že všetky axiómy sú splnené a môžeme teda tvrdiť, že komplexné čísla tvoria vektorový priestor nad reálnymi číslami.