Linearna algebra nad polkolobarji

Jimmy Zakeršnik

mentor: prof. dr. Tomaž Košir

26. junij 2023

Napovednik

Motivacija

Polkolobarjev je veliko - pojavljajo se v skoraj vsakem področju matematike. Nekateri primeri so:

- $\mathbb{N}_0$ oz. $\mathbb{Z}^+$, $\mathbb{Q}^+$, $\mathbb{R}^+$ za standardne operacije $+$ in $*$,
- *max-plus algebra* $(\mathbb{R} \cup \{-\infty\}, max, +)$ in *min-plus algebra* $(\mathbb{R} \cup \{\infty\}, min, +)$,
- Boolove algebre,
- Potenčne množice za $\cup$ in $\cap$.

Monoidi in urejenost

Definicija

Komutativen monoid $(M, *)$ je *kanonično urejen*, če je kanonična šibka urejenost $x \leq y \iff \exists z \in M : y = x * z$ na M antisimetrična.

Monoidi in urejenost

Definicija

Komutativen monoid $(M, *)$ je *kanonično urejen*, če je kanonična šibka urejenost $x \leq y \iff \exists z \in M : y = x * z$ na M antisimetrična.

Izrek

Monoid ne more hkrati biti grupa in kanonično urejen.

Monoidi in urejenost

Definicija

Komutativen monoid $(M, *)$ je *kanonično urejen*, če je kanonična šibka urejenost $x \leq y \iff \exists z \in M : y = x * z$ na M antisimetrična.

Izrek

Monoid ne more hkrati biti grupa in kanonično urejen.

Izrek

Naj bo monoid $(M, *)$ okrajšljiv in naj zadošča pogoju pozitivnosti. Potem je kanonična šibka urejenost $\leq$ na M antisimetrična.

Polkolobarji in dioidi

Definicija

Za neprazno množico R, ki je opremljena z operacijama $\oplus$ in $\otimes$ pravimo, da je *polkolobar*, če zanjo velja naslednje:

1. $(R, \oplus)$ je komutativen monoid z nevtralnim elementom 0,
2. $(R, \otimes)$ je monoid z enoto 1,
3. (leva in desna) distributivnost $\otimes$ in $\oplus$,
4. $0 \otimes a = 0 = a \otimes 0; \forall a \in R$.

Če je operacija $\otimes$ komutativna, pravimo, da je polkolobar R komutativen.
Oznaka: $(R, \oplus, \otimes)$.

Polkolobarji in dioidi

Definicija

Naj bo $(R, \oplus, \otimes)$ polkolobar. Če je $(R, \oplus)$ kanonično urejen monoid, pravimo, da je $(R, \oplus, \otimes)$ *dioid*.

Polkolobarji in dioidi

Definicija

Naj bo $(R, \oplus, \otimes)$ polkolobar. Če je $(R, \oplus)$ kanonično urejen monoid, pravimo, da je $(R, \oplus, \otimes)$ *dioid*.

Trditev

Če je $(R, \oplus, \otimes)$ polkolobar na katerem kanonična šibka urejenost $\leq_\oplus$ ni antisimetrična in je $\mathcal{E}$ ekvivalenčna relacija s predpisom $x \mathcal{E} y \iff x \leq y \;\&\; y \leq x$, je $R/\mathcal{E}$ dioid za inducirani operaciji.

Polmoduli in moduloidi

Definicija

Naj bo R polkolobar. *Levi R-polmodul* je komutativen monoid $(M, +)$ z aditivno identiteto θ, na katerem imamo definirano množenje s skalarjem $\cdot : R \times M \to M$, ki zadošča naslednjim pogojem za vsaka $\lambda, \mu \in R$ in vsaka $x, y \in M$:

1. $(\lambda\mu) \cdot x = \lambda \cdot (\mu \cdot x)$,
2. $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$ in $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$,
3. $1 \cdot x = x$ in $\lambda \cdot \theta = \theta = 0 \cdot x$

Če je R dioid in $(M, +)$ kanonično urejen, mu pravimo R-moduloid.

Polmoduli in moduloidi

Definicija

Naj bo X neka neprazna družina elementov R-polmodula $(M, +)$. Najmanjši R-podpolmodul v M, ki vsebuje X, imenujemo R-polmodul generiran z X in ga označimo z $\langle X \rangle$. Če je $\langle X \rangle = M$, pravimo, da X *generira* M. Če je X končna družina, ki generira M, pravimo, da je M *končno generiran*.

Polmoduli in moduloidi

Definicija

Naj bo X neka neprazna družina elementov R-polmodula $(M, +)$. Najmanjši R-podpolmodul v M, ki vsebuje X, imenujemo R-polmodul generiran z X in ga označimo z $\langle X \rangle$. Če je $\langle X \rangle = M$, pravimo, da X *generira* M. Če je X končna družina, ki generira M, pravimo, da je M *končno generiran*.

Definicija

Rang R-polmodula $(M, +)$ je najmanjše naravno število $n \in \mathbb{N}$ za katerega obstaja družina $X \subseteq M$ kardinalnosti n, ki generira M.

Polmoduli in moduloidi

Definicija

Naj bo $(M, +)$ R-polmodul z enoto θ in $X = (x_j)_{j \in J}$ neka neprazna (končna ali neskončna) družina elementov iz M. Pravimo, da je X *linearno neodvisna*, če za vsak disjunktni par $I_1, I_2 \subseteq J$ velja $\langle X_{I_1} \rangle \cap \langle X_{I_2} \rangle = \{\theta\}$.

Polmoduli in moduloidi

Definicija

Naj bo $(M,+)$ R-polmodul z enoto θ in $X=(x_j)_{j\in J}$ neka neprazna (končna ali neskončna) družina elementov iz M. Pravimo, da je X *linearno neodvisna*, če za vsak disjunktni par $I_1, I_2 \subseteq J$ velja $\langle X_{I_1}\rangle \cap \langle X_{I_2}\rangle = \{\theta\}$.

Definicija

Naj bo $(M,+)$ R-polmodul z enoto θ in $X=(x_j)_{j\in J}$ neka neprazna (končna ali neskončna) družina elementov iz M. Pravimo, da je X *šibko linearno neodvisna*, če za njo velja pogoj: $\forall j \in J : x_j \notin \langle X \setminus \{x_j\}\rangle$.

Polmoduli in moduloidi

Definicija

Naj bo $(M, +)$ R-polmodul z enoto θ in $X = (x_j)_{j \in J}$ neka neprazna (končna ali neskončna) družina elementov iz M. Pravimo, da je X *baza* M, če je linearno neodvisna in generira M.

Polmoduli in moduloidi

Definicija

Naj bo $(M, +)$ R-polmodul z enoto θ in $X = (x_j)_{j \in J}$ neka neprazna (končna ali neskončna) družina elementov iz M. Pravimo, da je X *baza* M, če je linearno neodvisna in generira M.

Definicija

Naj bo $(M, +)$ R-polmodul z enoto θ in $X = (x_j)_{j \in J}$ neka neprazna (končna ali neskončna) družina elementov iz M. Pravimo, da je X *šibka baza* M, če je šibko linearno neodvisna in generira M.

Polmoduli in moduloidi

Definicija

Naj bo $(M, +)$ R-polmodul z enoto θ in $X = (x_j)_{j \in J}$ neka neprazna (končna ali neskončna) družina elementov iz M. Pravimo, da je X *prosta baza* R-polmodula M, če je prosta množica v M in generira cel M. Polmodulu, ki premore kako prosto bazo, pravimo *prosti polmodul*.

Proste baze so hkrati tudi šibke.

Polmoduli in moduloidi

Definicija

Naj bo $(M, +)$ R-polmodul z enoto θ in $X = (x_j)_{j \in J}$ neka neprazna (končna ali neskončna) družina elementov iz M. Pravimo, da je X *prosta baza* R-polmodula M, če je prosta množica v M in generira cel M. Polmodulu, ki premore kako prosto bazo, pravimo *prosti polmodul*.

Proste baze so hkrati tudi šibke.

Izrek

Če R-polmodul M premore kako neskončno šibko bazo, so vse šibke baze M neskončne.

Polmoduli in moduloidi

Definicija

Naj bo $(M, +)$ R-polmodul z enoto θ in $X = (x_j)_{j \in J}$ neka neprazna družina elementov iz M. Pravimo, da je vektor x *razcepen* na $\langle X \rangle$, če in samo če obstajata taka vektorja $y, z \in \langle X \rangle$, oba različna od x, da je $x = y + z$. Če x ni razcepen na $\langle X \rangle$, pravimo, da je *nerazcepen* na $\langle X \rangle$.

Polmoduli in moduloidi

Izrek

Naj bo $(R, \oplus, \otimes)$ dioid z enotama 0 in 1 za katerega velja $r \oplus p = 1 \Rightarrow r = 1 \vee p = 1$ in $r \otimes p = 1 \Rightarrow r = 1 \wedge p = 1$. Naj bo $(M, +)$ R-moduloid na katerem za $y \in M \setminus \{\theta\}, x \in M \setminus \{y\}$ in poljuben $\lambda \in R$ velja $y = \lambda \cdot y + x \Rightarrow \lambda = 1$. Potem velja, da če M premore kako bazo, je ta enolično določena.

Primer: $(\mathbb{N}_0, +, *)$

Matrike

Izrek

Naj bo R komutativen polkolobar ter naj bosta $A, B \in M_n(R)$. Če velja $A * B = I_n$, je tudi $B * A = I_n$.

Matrike

Izrek

Naj bo R komutativen polkolobar ter naj bosta $A, B \in M_n(R)$. Če velja $A * B = I_n$, je tudi $B * A = I_n$.

Trditev

Naj bo R komutativen polkolobar v katerem $1 \notin V(R)$ in za $\forall u, v \in R$ velja sklep $1 = u \oplus v \Rightarrow u \in U(R) \vee v \in U(R)$. Naj bo $A \in M_n(R)$. Če za $\forall i, j \in \{1, 2, \ldots n\}$ velja $a_{ii} \in U(R)$ in $a_{ij} \in V(R)$, je matrika A obrnljiva.

Matrike

Definicija

Naj bo M končno generiran R-polmodul in T ter S neki njegovi šibki bazi. Matriki A, ki slika elemente T v elemente S pravimo *prehodna matrika* iz T v S.

Matrike

Definicija

Naj bo M končno generiran R-polmodul in T ter S neki njegovi šibki bazi. Matriki A, ki slika elemente T v elemente S pravimo *prehodna matrika* iz T v S.

Definicija

Naj bo R komutativen polkolobar in $A \in M_{n\times m}(R)$. Najmanjšemu številu $k \in \mathbb{N}$, za katerega obstajata matriki $B \in M_{n\times k}(R)$ in $C \in M_{k\times m}(R)$, da je $A = B * C$, pravimo *faktorski rang* matrike A in ga označimo z $\rho_s(A)$.

Matrike

Izrek

Naj bo R komutativni polkolobar in M R-polmodul ranga r s šibkima bazama S in T. Potem za vsako prehodno matriko A iz T v S velja $r \leq \rho_s(A)$ in obstaja prehodna matrika $\widehat{A}$ iz T v S za katero je $r = \rho_s(\widehat{A})$.

Matrike

Izrek

Naj bo R komutativni polkolobar in M R-polmodul ranga r s šibkima bazama S in T. Potem za vsako prehodno matriko A iz T v S velja $r \leq \rho_s(A)$ in obstaja prehodna matrika $\widehat{A}$ iz T v S za katero je $r = \rho_s(\widehat{A})$.

Trditev

Naj bo R komutativen polkolobar in M končno generiran prost R-polmodul. Potem za vsako šibko bazo S in za poljubno prosto bazo T velja $|T| \leq |S|$.

Matrike

Izrek

Naj bo R komutativen polkolobar in M prost R-polmodul ranga r. Naj bo T neka prosta baza M. Potem so za šibko bazo S naslednje trditve ekvivalentne:

1. S je prosta baza M
2. $|S| = r$
3. prehodna matrika med T in S je enolično določena in obrnljiva

Matrike

Definicija

Naj bo R polkolobar in $M = R^n$ polmodul nad R. Naj bo $A \in M_n(R)$ matrika, ki pripada endomorfizmu $h\ : M \to M$. Pravimo, da je $\lambda \in R$ ***lastna vrednost*** matrike A, če obstaja tak $v \in M \setminus \{\theta\}$, da velja $A * v = \lambda \cdot v$. Takemu vektorju v, če obstaja, pravimo *lastni vektor* matrike A za λ.

Matrike

Definicija

Naj bo R polkolobar in $M = R^n$ polmodul nad R. Naj bo $A \in M_n(R)$ matrika, ki pripada endomorfizmu $h\ : M \to M$. Pravimo, da je $\lambda \in R$ *lastna vrednost* matrike A, če obstaja tak $v \in M \setminus \{\theta\}$, da velja $A * v = \lambda \cdot v$. Takemu vektorju v, če obstaja, pravimo *lastni vektor* matrike A za λ.

Izrek

Naj bo R komutativen dioid in $A \in M_n(R)$. Potem je λ lastna vrednost matrike A natanko tedaj, ko so stolpci matrike $\bar{A}(\lambda) = \begin{bmatrix} A & \lambda \cdot I_n \\ I_n & I_n \end{bmatrix}$ linearno odvisni.

Pideterminanta in karakteristični pipolinom

Definicija

Naj bo R nek polkolobar in $X \in M_n(R)$. Urejeni dvojici podani s predpisom

$$\begin{aligned} pdt(X) &= \Big(\bigoplus_{\substack{\pi \in P^+(n) \\ \sigma \in P(n)}} \sigma(\bar{\pi}(X)), \bigoplus_{\substack{\pi \in P^-(n) \\ \sigma \in P(n)}} \sigma(\bar{\pi}(X)) \Big) \\ &= (\llbracket det^+(X) \rrbracket, \llbracket det^-(X) \rrbracket) = (pdt^+(X), pdt^-(X)) \end{aligned}$$

pravimo *pideterminanta* matrike X.

Pideterminanta in karakteristični pipolinom

Definicija

Naj bo R nek polkolobar in $X \in M_n(R)$. *Karakteristični pipolinom* matrike X v spremenljivki λ je urejena dvojica polinomov, podana s predpisom

$$\begin{aligned} pp_X(\lambda) &= ([\![p_X^+(\lambda)]\!], [\![p_X^-(\lambda)]\!]) \\ &= (pp_X^+(\lambda), pp_X^-(\lambda)) \end{aligned}$$

Pri tem polinoma $p_X^+(\lambda)$ in $p_X^-(\lambda)$ dobimo tako, da se pretvarjamo, da delamo nad poljem in zapišemo pripadajoči karakteristični polinom $p_X(\lambda) = p_X^+(\lambda) \ominus p_X^-(\lambda)$.

Posplošeni Cayley-Hamiltonov izrek

Izrek

Naj bo R poljuben polkolobar in $X \in M_n(R)$ neka kvadratna matrika nad R. Potem je $pp_X^+(X) = pp_X^-(X)$.

Literatura

- M. Akian, S. Gaubert in A. Guterman, *Linear independence over tropical semirings and beyond*, v: Tropical and Idempotent Mathematics vol. **495** (ur. G. Litvinov in S. Sergeev), Amer. Math. Soc., Providence, 2008, str. 1–38.
- M. Gondran in M. Minoux, *Graphs, dioids and semirings: New models and algorithms*, Operations Research/Computer Science Interfaces **41**, Springer, Boston, 2008; dostopno tudi na `https://www.researchgate.net/publication/266193429_Graphs_Dioids_and_Semirings_New_Models_and_Algorithms`.

Literatura

- R. Grosu, *The Cayley-Hamilton theorem for noncommutative semirings*, v: Implementation and Application of Automata (ur. M. Domaratzki, K. Salomaa), Springer, Berlin, 2011, str. 143–153.
- C. Reutenauer in H. Straubing, *Inversion of matrices over a commutative semiring*, Journal of Algebra **88** (1984) 350–360.
- D. E. Rutherford, *XIX.–The Cayley-Hamilton theorem for semi-rings*, v: Proceedings of the Royal Society of Edinburgh Section A **66** (1964) 211–215.
- Y. J. Tan, *Bases in semimodules over commutative semirings*, v: Linear Algebra Appl. **443** (2014) 139–152.