prof. dr. To-[redacted]
maž Ko-[redacted]
šir[redacted]
Trditev[redacted]
UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Jimmy Zakeršnik

Linearna algebra nad polkolobarji

Delo diplomskega seminarja

Ljubljana, 2021/22

Kazalo

Linearna algebra nad polkolobarji

Povzetek

Delo obravnava algebraično strukturo polkolobarja z dodatno pozornostjo na posebnem primeru znanim pod imenom dioid. Množica R je polkolobar za binarni notranji operaciji $\oplus$ in $\otimes$, če je $(R, \oplus)$ komutativen monoid z enoto 0, $(R, \otimes)$ monoid z enoto 1, med $\otimes$ in $\oplus$ velja leva ter desna distributivnost in velja, da 0 izniči $\otimes$, torej $\forall a \in R; a \otimes 0 = 0 \otimes a = 0$. Če je $(R, \oplus)$ poleg tega še delno urejen s kanonično relacijo *leq* polkolobarju $(R, \oplus, \otimes)$ pravimo dioid. Tako pojem dioida kot pojem polkolobarja obstajata že nekaj časa in mnogo klasičnih vprašanj s stališča (linearne) algebre ima že odgovore. V nalogi bodo predstavljeni bolj osnovni izmed teh. Obravnavana vprašanja bodo predvsem centrirana na posplošitvah konceptov iz klasične linearne algebre nad obsegi, npr. obstoj in lastnosti baz polmodula nad polkolobarjem R, obrnljivost matrike nad polkolobarjem R, koncept bideterminante in bipolinoma matrike nad polkolobarjem ter na koncu še dokaz posplošenega Cayley-Hamiltonovega izreka. Le ta nam pove, da za vsako kvadratno matriko A nad komutativnim polkolobarjem R in njen karakteristični bipolinom $(P_A^+(\lambda), P_A^-(\lambda))$ velja $P_A^+(A) = P_A^-(A)$.

Linearna algebra over semirings

Abstract

This paper discusses the algebraic structure of a semiring, with special attention given to the special case of a dioid. The set R is a semiring for the binary internal laws $\oplus$ and $\otimes$ if $(R, \oplus)$ is a commutative monoid with the neutral element 0, $(R, \otimes)$ is a monoid with the neutral element 1, $\otimes$ is left- and right-distributive with respect to $\oplus$ and if 0 ">absorbs<" $\otimes$, i. e. $\forall a \in R; a \otimes 0 = 0 \otimes a = 0$. If additionally $(R, \oplus)$ is also ordered with the cannonic relation *leq*, we instead use the name dioid for the appropriate semiring $(R, \oplus, \otimes)$. Both terms have existed for a long time now and as such most of the classical questions relating to the structures from the perspective of linear algebra have already been answered. The paper will present some of these results. In particular, the focus will lie on generalizations of already familiar concepts from classical linear algebra over commutative rings, such as the existence and properties of bases of an R-semimodule, the inversibility of a matrix over a semiring R, the concept of a bideterminant and bipolynomial of a square matrix over the semiring R etc. Finally, we show a proof of the generalized Cayley-Hamilton theorem which states that for each square matrix A over a commutative semiring R and her characteristic bipolynomial $(P_A^+(\lambda), P_A^-(\lambda))$ the following holds true: $P_A^+(A) = P_A^-(A)$.

Math. Subj. Class. (2020): 16Y60, 12K10

Ključne besede: Linearna algebra, algebra, polkolobar, polmodul, dioid, bideterminanta, karakteristični bipolinom, posplošeni Cayley-Hamiltonov izrek

Keywords: Linear algebra, algebra, semiring, semimodule, dioid, bideterminant, characteristic bipolynomial, generalized Cayley-Hamilton theorem

LINEARNA ALGEBRA OVER SEMIRINGS

Key words and phrases. Linear algebra, algebra, semiring, semimodule, dioid, bideterminant, characteristic bipolynomial, generalized Cayley-Hamilton theorem.

1. Uvod

Polkolobarji so algebraična struktura, s katero se srečamo, čim začnemo obravnavati številske množice. Med primere spadajo množica nenegativnih celih števil, množica nenegativnih racionalnih števil, množica nenegativnih realnih števil, razne strukture nad množicami, ki se izkažejo kot uporabne v topologiji, t. i. tropski polkolobarji, ki se uporabljajo za ocenjevanje učinkovitosti zaposlenih itd. Uporabo imajo tudi v teoretični računalniški znanosti in kriptografiji. Kljub njihovi uporabnosti in pogostem pojavljanju, tako polkolobarji kot strukture nad njimi v sklopu standardne matematične izobrazbe eksplicitno ne prejmejo kaj dosti pozornosti. Poleg popolnoma praktičnih motivacij za obravnavo teh struktur se izkaže, da nas obravnava polkolobarjev oz. linearne algebre nad njimi privede tudi do bistva definicij določenih lastnosti in konceptov v klasični linearni algebri nad vektorskimi prostori. V tem delu bom obravnaval nekaj razmeroma osnovnih lastnosti polkolobarjev (in v manjši meri tudi dioidov) ter linearne algebre nad njimi. V drugem razdelku bom na kratko definiral in obravnaval polkolobarje, njihove posebne primere in trditve, ki jih lahko dokažemo o njih. Nato bom v tretjem razdelku definiral polmodule − posplošitve modulov. Pri polmodulih bom obravnaval tipična vprašanja, ki se nanašajo na vektorske prostore v klasični linearni algebri, kot so vprašanje obstoja baze, obstoja dimenzije, itd. Sledila bo definicija linearnih preslikav in matrik nad polkolobarji ter obravnava lastnosti le teh v četrtem razdelku. Posebej bom pozornost posvetil konceptu bideterminante v petem razdelku in karakterističnega bipolinoma v šestem razdelku − oboje kot posplošitvi determinante in karakterističnega polinoma nad vektorskimi prostori. Na koncu bom v sedmem razdelku obravnaval posplošen Cayley-Hamiltonov izrek.

2. Osnovne Definicije:

Definicija 2.1. Neprazna množica M, opremljena z operacijo $*$, je *monoid*, če za operacijo $*$ na M velja:

(1) $a * (b * c) = (a * b) * c; \forall a, b, c \in M$
(2) $\exists e \in M; a * e = e * a = a; \forall a \in M$

Lastnost 1. se imenuje *asociativnost*, lastnost 2. pa *obstoj enote*.

Definicija 2.2. *Relacija delne urejenosti* $\leq$ na množici X je binarna relacija, ki je tranzitivna in antisimetrična. Zanjo torej velja:

(1) $a \leq b \ \& \ b \leq c \Rightarrow a \leq c; \ \forall a, b, c \in X,$
(2) $a \leq b \ \& \ b \leq a \Rightarrow a = b; \ \forall a, b \in X.$

Če je poleg tega še sovisna, torej če velja $\forall a, b \in X : a \leq b \vee b \leq a$, pravimo, da je relacija *linearna urejenost*.

Definicija 2.3. Monoid $(R, *)$ je *delno urejen*, če je na njem definirana relacija delne urejenosti $\leq$, ki zadošča pogoju:
$a \leq \acute{a} \Rightarrow ((a * \hat{a} \leq \acute{a} * \hat{a}) \ \& \ (\hat{a} * a \leq \hat{a} * \acute{a}))$ za vse $a, \acute{a}, \hat{a} \in R$.

Definicija 2.4. Za neprazno množico R, ki je opremljena z notranjima binarnima 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) $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ in $(b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a); \ \forall a, b, c \in R,$

(4) $\forall a \in R; 0 \otimes a = a \otimes 0 = 0$.

Oznaka: $(R, \oplus, \otimes)$.
Polkolobar $(R, \oplus, \otimes)$ je *komutativen*, če je multiplikativna operacija $\otimes$ na njem komutativna.

Opomba 2.5. Če je $1 = 0$, potem je avtomatsko $R = \{0\}$. Ker nas ta trivialen primer ne zanima, predpostavimo $1 \neq 0$ od zdaj naprej.

Zgled 2.6. Nenegativna cela števila $\mathbb{Z}^+$ s standardnim seštevanjem in množenjem tvorijo polkolobar. Enako velja za nenegativna racionalna števila $\mathbb{Q}^+$ in nenegativna realna števila $\mathbb{R}^+$ za standardno seštevanje in množenje.

Definicija 2.7. Polkolobarju $(R, +, \cdot)$, za katerega je komutativen monoid $(R, +)$ delno urejen, pravimo *dioid*. Zanj poleg osnovnih zahtev torej še velja:
$a \leq \acute{a} \Rightarrow a + \hat{a} \leq \acute{a} + \hat{a};\ \forall a, \acute{a}, \hat{a} \in R$.

3. Polmoduli:

Tako kot lahko nad kolobarji definiramo posplošitve vektorskih prostorov - module, lahko podobno strukturo formiramo tudi nad polkolobarji:

Definicija 3.1. Naj bo R polkolobar. *Levi R-polmodul* je komutativen monoid $(M, +)$ z aditivno identiteto θ, na katerem imamo definirano preslikavo:
$\cdot : R \times M \to M$, ki jo imenujemo množenje s skalarjem. Ta preslikava zadošča naslednjim pogojem za vsaka $\lambda, \mu \in R$ in vsaka $a, b \in M$:

(1) $(\lambda\mu) \cdot a = \lambda \cdot (\mu \cdot a)$,
(2) $\lambda \cdot (a + b) = \lambda \cdot a + \lambda \cdot b$,
(3) $(\lambda + \mu) \cdot a = \lambda \cdot a + \mu \cdot a$,
(4) $1 \cdot a = a$,
(5) $\lambda \cdot \theta = \theta = 0 \cdot a$

Analogno definiramo desni R-polmodul.

Opomba 3.2. Od zdaj naprej bomo pod imenom polmodul obravnavali leve polmodule. Analogi rezultatov, ki jih bomo dokazali, seveda veljajo v tudi za desne polmodule.

Zgled 3.3. Naj bo $R^n = \{(a_1, a_2, \ldots, a_n)^\top |\ a_i \in R \text{ za } i \in 1, 2, \ldots, n\}$, pri čemer je $(a_1, a_2, \ldots, a_n)^\top$ transpozicija $(a_1, a_2, \ldots, a_n)$ in $n \geq 1$. Definiramo:

$$a + b = ((a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)^\top) \tag{1}$$

in

$$\lambda \cdot a = (\lambda \cdot a_1, \lambda \cdot a_2, \ldots, \lambda \cdot a_n)^\top \tag{2}$$

za vse $a = (a_1, a_2, \ldots, a_n)^\top$ in $b = (b_1, b_2, \ldots, b_n)^\top$ iz R^n ter vse $\lambda \in R$. Potem je R^n levi R-polmodul.

4. Matrike:

Podobno kot za vektorske prostore in module, lahko tudi za polmodule pod določenimi pogoji definiramo baze in jim tudi določimo dimenzije preko kardinalnosti najmanjše baze. Na njih lahko tudi izvajamo linearne preslikave, ki so definirane na enak način, kot na vektorskih prostorih - $\mathbb{L} : M \mapsto \grave{M}$ more biti aditivna in homogena.
Nad polkolobarjem $(R, +, \cdot)$ lahko definiramo mxn matrike, za poljubna $m, n \in \mathbb{N}$. Pri tem seštevanje definiramo enako kot za matrike nad obsegi (po komponentah), množenje pa na sledeč način za $A \in M_{m\times n}(R), B \in M_{n\times l}(R)$:

$$A * B = C \in M_{m\times l}(R);\ c_{ij} = \sum_{k=1}^{n}(a_{ik}b_{kj}) \forall i \in \{1, 2, \ldots, m\}\ \&\ \forall j \in \{1, 2, \ldots, l\}$$

Pri množenju moramo seveda biti pozorni na to, da tukaj nimamo komutativnosti. Enota za seštevanje je tukaj seveda kar ničelna matrika, kjer je vsak element aditivna enota iz polkolobarja, za množenje pa je enota kar matrika, ki ima na diagonali multiplikativno enoto, izven diagonale pa aditivno.
Hitro se da preveriti, da če je R polkolobar, je tudi množica kvadratnih matrik $M_n(R)$ nad R polkolobar in če je R dioid, je tudi $M_n(R)$ dioid. Tudi tukaj se da najti pogoje za obrnljivost kvadratnih matrik nad polkolobarji.

5. Bideterminante:

Tako kot imajo matrike nad obsegi determinante, lahko definiramo podobno preslikavo tudi za matrike nad polkolobarji. Preslikava, ki nas bo v tem primeru zanimala kot posplošitev determinante, je t.i. *bideterminanta.*

Definicija 5.1. Naj bo $X = \{1, 2, \ldots, n\}$ neka končna množica. Pravimo, da je σ *delna permutacija* X, če je permutacija neke podmnožice $S \subseteq X$. Na enak način kot za navadne permutacije tudi za delne definiramo parnost.
Oznaka: $Per(n)$ je množica vseh permutacij množice $\{1, 2, \ldots, n\}$, $Per^+(n)$ množica vseh sodih permutacij na isti množici in analogno $Per^-(n)$ množica vseh lihih permutacij na tej množici. Na enak način označimo $Part(n)$ kot množico vseh delnih permutacij množice $\{1, 2, \ldots, n\}$ in na enak način kot prej tudi $Part^+(n)$ ter $Part^-(n)$.
Delno permutacijo σ lahko tudi razširimo na cel X:

$$\hat{\sigma} = \begin{cases} \hat{\sigma(i)} = \sigma(i); i \in dom(\sigma) \\ \hat{\sigma(i)} = i; \sigma(i) \in X \setminus dom(\sigma) \end{cases}$$

kjer je $dom(\sigma)$ domena delne permutacije σ.

Definicija 5.2. Naj bo A neka $n \times n$ matrika nad komutativnim polkolobarjem R. *Bideterminanta matrike* A je urejeni par $(det^+(A), det^-(A))$, kjer sta vrednosti $det^+(A)$ in $det^-(A)$ definirani na naslednji način:

$$det^+(A) = \sum_{\pi \in Per^+(n)} (\prod_{i=1}^{n} (a_{i,\pi(i)}))$$

$$det^-(A) = \sum_{\pi \in Per^-(n)} (\prod_{i=1}^{n} (a_{i,\pi(i)}))$$

6. Karakteristični bipolinom:

Definicija 6.1. Naj bo A neka $n \times n$ matrika nad komutativnim polkolobarjem R. *Karakteristični bipolinom matrike* A je dvojica $(P_A^+(\lambda), P_A^-(\lambda))$, kjer sta $P_A^+(\lambda)$ in $P_A^-(\lambda)$ polinoma stopnje n v spremenljivki λ, definirana na naslednji način:

$$P_A^+(\lambda) = \sum_{q=1}^{n} \left(\left(\sum_{\substack{\sigma \in Part^+(n) \\ |dom(\sigma)|=q}} \left(\prod_{i \in dom(\sigma)} (a_{i,\sigma(i)}) \right) \right) * \lambda^{n-q} \right) + \lambda^n$$

$$P_A^-(\lambda) = \sum_{q=1}^{n} \left(\left(\sum_{\substack{\sigma \in Part^-(n) \\ |dom(\sigma)|=q}} \left(\prod_{i \in dom(\sigma)} (a_{i,\sigma(i)}) \right) \right) * \lambda^{n-q} \right)$$

To pa nas privede do zadnje in najbolj zanimive točke:

7. Posplošen Cayley-Hamiltonov izrek:

Izrek 1. *Naj bo A neka $n \times n$ matrika nad komutativnim polkolobarjem z nevtralnim elementom 0 in enoto 1 in naj bo $(P_A^+(\lambda), P_A^-(\lambda))$ bipolinom, ki pripada matriki A. Tedaj velja:*

$$P_A^+(A) = P_A^-(A) \tag{3}$$

kjer sta $P_A^+(A)$ in $P_A^-(A)$ matriki, ki ju dobimo, če v $P_A^+(\lambda)$ in $P_A^-(\lambda)$ faktorje λ^{n-q} zamenjamo z A^{n-q}. Pri tem razumemo A^0 kot multiplikativno identiteto v polkolobarju $M_n(R)$.

Slovar strokovnih izrazov

semiring polkolobar
semimodule polmodul
dioid dioid
$0 \in R$ **is absorbing for** $\otimes$ $0 \in R$ izniči operacijo $\otimes$, torej $\forall a \in R; a \otimes 0 = 0 \otimes a = 0$

Literatura

[1] J. Golan, *Semirings and their applications*, Springer, Dordrecht, 1999; dostopno tudi na `https://link.springer.com/book/10.1007/978-94-015-9333-5`.

[2] 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`.

[3] Y.J. Tan, *Bases in semimodules over commutative semirings*, Linear Algebra Appl.˜443 (2014) 139−152.

[4] Y.J. Tan, *Determinants of matrices over semirings*, Linear Multilinear Algebra **62** (2013) 498−517.

[5] Y.J. Tan, *On invertible matrices over commutative semirings*, Linear Multilinear Algebra **61** (2013) 710˘714.
[6] *Semiring*, v: Wikipedia, The Free Encyclopedia, [ogled 15. 2. 2022], dostopno na `https://en.wikipedia.org/wiki/Semiring`.