

UNIVERZA V LJUBLJANI  
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Jimmy Zakeršnik

**Linearna algebra nad polkolobarji**

Delo diplomskega seminarja

Mentor: prof. dr. Tomaž Košir

Ljubljana, 2021/22

## KAZALO

1. Uvod:	4
2. Osnovne Definicije:	4
3. Polmoduli:	5
4. Matrike:	6
5. Bideterminante:	6
6. Karakteristični bipolinom:	7
7. Posplošen Cayley-Hamiltonov izrek:	7
Slovar strokovnih izrazov	7
Literatura	7

## 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  $\forall a \in R; a \otimes 0 = 0 \otimes a = 0$ . Pojem polkolobarja obstaja že nekaj časa in mnogo klasičnih vprašanj, s stališča (linearne) algebre, ki se navezujejo nanje, 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 matrik nad polkolobarjem  $R$ , koncept bideterminante in bipolinoma matrike itd. . Na koncu bo predstavljen še posplošeni Cayley-Hamiltonov izreka in njegov dokaz. 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  $P_A^+(A) = P_A^-(A)$ .

## Linear 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 is absorbing for  $\otimes$ , i. e.  $\forall a \in R; a \otimes 0 = 0 \otimes a = 0$ . The term has existed for a long time now and as such many 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, the generalized Cayley-Hamilton theorem is presented and proven. The aforementioned states that for each square matrix  $A$  over a commutative semiring  $R$  and its 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

## 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, kriptografiji in teoriji mere. 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 obsegi. V tej nalogi 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, zveze med kardinalnostmi baz, kdaj so baze enolične 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. V vseh poglavjih se predvsem sklicujemo na [1].

## 2. OSNOVNE DEFINICIJE:

V tem poglavju bomo podali definicije ključnih osnovnih pojmov.

**Definicija 2.1.** Komutativen monoid  $(R, \oplus)$  je *delno urejen*, če je na kanonična relacija šibke urejenosti  $\leq$ , ki je združljiva z operacijo  $\otimes$ , torej zadošča pogoju  $a \leq \hat{a} \Rightarrow ((a \oplus \hat{a} \leq \hat{a} \oplus \hat{a}) \ \& \ (\hat{a} \oplus a \leq \hat{a} \oplus \hat{a}))$  za vse  $a, \hat{a} \in R$ , hkrati tudi antisimetrična (torej delna urejenost).

**Definicija 2.2.** 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. Z izrazoma *levi polkolobar* in *desni polkolobar* bomo po potrebi poudarili smer množenja. Če smeri ne poudarimo, privzememo, da je  $R$  levi polkolobar.

**Opomba 2.3.** Če je  $1 = 0$ , potem je avtomatsko  $R = \{0\}$ . Ker nas ta trivialen primer ne zanima, predpostavimo  $1 \neq 0$  od zdaj naprej.

**Zgled 2.4.** 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.  $\diamond$

**Zgled 2.5.** V tem zgledu bomo obravnavali poseben tip polkolobarja, ki se definira na (pod)množicah: Naj bo  $X$  neprazna množica in  $S \subseteq P(X)$  neprazen nabor podmnožic množice  $X$ . Nabor  $S$  je polkolobar (pod)množic za operaciji unije in preseka, če zanj velja:

- (1)  $\emptyset \in S$
- (2)  $E, F \in S \Rightarrow E \cap F \in S$
- (3) Če sta  $E, F \in S$ , potem obstaja končno mnogo disjunktnih množic  $C_1, C_2, \dots, C_n \in S$ , da je  $E \setminus F = \bigcup_{i=1}^n C_i \in S$ .

Opazimo, da iz 2 in 3 ter predpostavke  $S \neq \emptyset$  sledi 1. Prav tako iz 3 sledi, da je 1 resničen če in samo če  $S \neq \emptyset$ . Obravnavan tip polkolobarjev se uporablja v teoriji mere. Primer takega polkolobarja je nabor polzaprtih intervalov  $[a, b] \subset \mathbb{R}$  za unijo in presek.  $\diamond$

**Definicija 2.6.** Polkolobarju  $(R, \oplus, \otimes)$ , za katerega je komutativen monoid  $(R, \oplus)$  delno urejen, pravimo *diodid*. Zanj poleg osnovnih zahtev torej še velja:  
 $a \leq \acute{a} \Rightarrow a \oplus \hat{a} \leq \acute{a} \oplus \hat{a}$ ;  $\forall a, \acute{a}, \hat{a} \in R$ .

### 3. POLMODULI:

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

**Definicija 3.1.** Naj bo  $R$  levi polkolobar. Komutativnemu monoidu  $(M, +)$  z identiteto  $\theta$  pravimo *Levi R-polmodul*, če imamo na njem definirano preslikavo  $\cdot : R \times M \rightarrow M$ , ki zadošča naslednjim pogojem za vsaka  $\lambda, \mu \in R$  in vsaka  $a, b \in M$ :

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

Preslikavo  $\cdot$  imenujemo (levo) množenje s skalarjem. 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. Kadar je  $R$  komutativen polkolobar, sta levi in desni  $R$ -polmodul enaka.

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

- (1)  $a + b = (a_1 \oplus b_1, a_2 \oplus b_2, \dots, a_n \oplus b_n)^\top$
- (2)  $\lambda \cdot a = (\lambda \cdot a_1, \lambda \cdot a_2, \dots, \lambda \cdot a_n)^\top$

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

#### 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 -  $\mathbb{L} : M \mapsto \hat{M}$  more biti aditivna in homogena.

Nad polkolobarjem  $(R, \oplus, \otimes)$  lahko definiramo  $m \times n$  matrike, za poljubni  $m, n \in \mathbb{N}$ . Pri tem seštevanje definiramo enako kot za matrike nad obsegi (po komponentah), množenje pa na sledeč način za  $A \in M_{m \times n}(R), B \in M_{n \times l}(R)$ :

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

**Opomba 4.1.** Pri zgornji definiciji je vsota seveda glede na operacijo  $\oplus$ . Poleg tega, da malo skrajšamo zapis, uporabimo oznako  $\underline{n} = \{1, 2, 3, \dots, n\}$  za  $n \in \mathbb{N}$ . Pri množenju v vsoti moramo pravtako biti pozorni na to, da nimamo zagotovljene komutativnosti. Enota za seštevanje matrik je seveda kar ničelna matrika, torej matrika, kjer je vsak element aditivna enota iz polkolobarja. Za množenje je enota kar matrika, ki ima na diagonalni 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.

#### 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*. Preden se lotimo le te pa uvedemo še nekaj pomožnih konceptov.

**Definicija 5.1.** Naj bo  $X = \{1, 2, \dots, n\}$  neka končna množica. Pravimo, da je  $\sigma$  *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  $\{1, 2, \dots, n\}$ ,  $Per^+(n)$  množica vseh sodih permutacij na isti množici in analogno  $Per^-(n)$  množica vseh lih permutacij na tej množici. Na enak način označimo  $Part(n)$  kot množico vseh delnih permutacij množice  $\{1, 2, \dots, n\}$  in na enak način kot prej tudi  $Part^+(n)$  ter  $Part^-(n)$ .

Delno permutacijo  $\sigma$  lahko tudi razširimo na cel  $X$ :

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

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

**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:

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

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

## 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  $\lambda$ , definirana na naslednji način:

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

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

To pa nas privede do zadnje in najbolj zanimive točke:

## 7. POSPLOŠEN CAYLEY-HAMILTONOV IZREK:

**Izrek 7.1.** 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:

$$(3) \quad P_A^+(A) = P_A^-(A)$$

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

## SLOVAR STROKOVNIH IZRAZOV

$0 \in R$  is absorbing for  $\otimes$   $0 \in R$  izniči operacijo  $\otimes$ , torej  $\forall a \in R; a \otimes 0 = 0 \otimes a = 0$

**dioid** dioid

**semimodule** polmodul

**semiring** polkolobar

## LITERATURA

- [1] 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](https://www.researchgate.net/publication/266193429_Graphs_Dioids_and_Semirings_New_Models_and_Algorithms).
- [2] Y.J. Tan, *Bases in semimodules over commutative semirings*, Linear Algebra Appl. **443** (2014) 139 – 152.
- [3] Y.J. Tan, *Determinants of matrices over semirings*, Linear Multilinear Algebra **62** (2013) 498 – 517.
- [4] Y.J. Tan, *On invertible matrices over commutative semirings*, Linear Multilinear Algebra **61** (2013) 710 – 714.