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

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 ali desna distributivnost ter 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 obravnavana zgolj osnovna izmed teh. Obravnavana vprašanja so predvsem centrirana na lastnostih polkolobarjev in dioidov ter posplošitvah konceptov iz klasične linearne algebre nad polji, kot so obstoj in lastnosti baz R-polmodula nad polkolobarjem R ter lastnosti in obrnljivost matrik nad polkolobarjem R.

Linear algebra over semirings

Abstract

This paper discusses the algebraic structure of a semiring, with additional 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- or right-distributive with respect to $\oplus$ and if 0 is absorbing for $\otimes$, i. e. $\forall a \in R; a \otimes 0 = 0 \otimes a = 0$. If additionally $(R, \oplus)$ is also ordered with the canonical order relation $\leq$, we instead call $(R, \oplus, \otimes)$ a dioid. 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 be on the properties of semirings and dioid and on generalizations of concepts from classical linear algebra over fields, such as the existence and properties of bases of an R-semimodule and the properties and invertibility of a matrix over a semiring R.

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 nenegativni odseki celih, racionalnih ter realnih števil (opremljeni s standardnim seštevanjem in množenjem), razne strukture nad množicami, ki so uporabne v topologiji, t. i. tropski polkolobarji, ki se uporabljajo za ocenjevanje učinkovitosti v podjetjih 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 bodo obravnavane nekatere razmeroma osnovne lastnosti polkolobarjev (in v manjši meri tudi dioidov) ter linearne algebre nad njimi. V drugem razdelku bodo na kratko definirani in obravnavani polkolobarji, njihovi posebni primeri in razne trditve, v večji meri skupaj z dokazi. V tretjem razdelku bodo definirani polmoduli kot posplošitve modulov in obravnavavana bodo tipična vprašanja, ki se nanašajo na vektorske prostore v klasični linearni algebri, kot je na primer vprašanje obstoja in kardinalnosti baze. Sledila bo definicija linearnih preslikav in matrik nad polkolobarji ter obravnava lastnosti le teh v četrtem razdelku.

Za začetek obravnavajmo motivacijski primer, ki nam bo pokazal, da četudi operaciji $\oplus$ in $\otimes$ na neki algebrajski strukturi $(E, \oplus, \otimes)$ nista obrnljivi, še vedno lahko rešujemo določene tipe enačb. Osnovni primer so enačbe, s katerimi se spoznamo že v osnovni šoli. Vzemimo za primer množico naravnih števil skupaj z 0, torej $\mathbb{N}_0$, opremljeno s standardnim seštevanjem ter množenjem. Naj bosta $a, b \in \mathbb{N}_0$ parametra v enačbi $a + x = b$. Ta enačba ima na $(\mathbb{N}_0, +, \cdot)$ rešitev, čim je $a \leq b$. Naslednji zgled je povzet iz [4, str. 1 – 2].

Zgled 1.1. Množico nenegativnih realnih števil $\mathbb{R}_+$ opremimo s standardnima operacijiama seštevanja in množenja in to strukturo označimo z oznako $(\mathbb{R}_+, +, \cdot)$. Na tej strukturi ima enačba $x = a \cdot x + b$ rešitev za vsak b čim je $a < 1$:

$$x = \frac{1}{1-a} \cdot b = \sum_{i=0}^{\infty} a^i \cdot b = (1 + a + a^2 + \ldots) \cdot b$$

♢

Izkaže se, da lahko nad polkolobarji počnemo več kot le reševanje preprostih enačb. Da to vidimo je dovolj, da obravnavamo kvadratne matrike nad $\mathbb{R}_+$. Naj bo $A \in \mathbb{R}^{n \times n}$ realna kvadratna matrika za katero velja, da so vse vrednosti v njej nenegativne, torej $a_{ij} \geq 0, \forall i, j \in \{1, 2, \ldots, n\}$. Perron-Frobeniusov izrek nam potem zagotovi, da bo A imela nenegativno realno lastno vrednost λ, enako njenemu spektralnemu radiju $\rho(A)$, ter da bo pripadajoč lasten vektor w imel same nenegativne realne koeficiente, torej $w_i \geq 0; \forall i \in \{1, 2, \ldots, n\}$. Za matriko A, za katero veljalo pogoji iz prej omenjenega izreka, lahko rečemo, da v resnici spada v množico $\mathbb{R}_+^{n \times n}$. Ker je ta množica polkolobar, kot bomo premislili kasneje, lahko torej govorimo, ne samo o rešitvah enačb nad polkolobarji, ampak tudi o matrikah in lastnih vrednostih nad temi strukturami, čeprav niti $(\mathbb{R}_+, +, \cdot)$ niti $(\mathbb{R}_+ \setminus \{0\}, +, \cdot)$ nista polji. Ta tip

matrik (in prej omenjen izrek) se pojavlja na področju verjetnosti, predvsem v teoriji dinamičnih sistemov. Nepresenetljivo, struktura $(\mathbb{R}_+, +, \cdot)$ tudi igra pomembno vlogo v teoriji mere.

2. Monoidi, polkolobarji in dioidi:

V tem razdelku se bomo prvič srečali s pojmi, ki jih bomo obravnavali skozi celo nalogo. Snov za to bomo pretežno črpali iz [4, Poglavje 1], kadar bomo kaj povzeli iz drugega vira, pa bo to posebej navedeno.

2.1. **Monoidi:** Za začetek bomo osvežili znanje o monoidih in dokazali nekaj relevantnih rezultatov, preden se lotimo obravnave novih konceptov.

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) $\exists e \in M; a * e = e * a = a; \forall a \in M$

Prva lastnost se imenuje *asociativnost*, druga pa *obstoj enote*.

Dodatno navedimo še definicijo relacije urejenosti, saj bodo tudi te igrale pomembno vlogo v tej nalogi.

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

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

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*.

Tudi monoidi, kot množice, lahko premorejo kako relacijo urejenosti, ki je lahko v neki zvezi z operacijo na monoidu, ali pa ne. Iz tega razloga uvedemo nov pojem za tiste monoide, v katerih velja določena zveza.

Definicija 2.3. Monoid $(M, *)$ je *urejen*, če je na njem definirana relacija urejenosti $\leq$, ki zadošča pogoju:

$$a \leq \acute{a} \Rightarrow ((a * \hat{a} \leq \acute{a} * \hat{a}) \ \& \ (\hat{a} * a \leq \hat{a} * \acute{a})) \text{ za vse } a, \acute{a}, \hat{a} \in M.$$

Pravimo tudi, da je na $(M, *)$ relacija $\leq$ *usklajena* z operacijo $*$.

Od tod naprej bomo za operacijo v monoidu M namesto $*$ uporabili $\oplus$. Če je $(M, \oplus)$ komutativen monoid, mu lahko priredimo t. i. kanonično šibko urejenost na sledeč način:

$$a \leq b \Rightarrow \exists c \in M : b = a \oplus c$$

Ta relacija je zaradi obstoja nevtralnega elementa refleksivna, poleg tega je pa tudi tranzitivna, kar tukaj na hitro premislimo: Če za neke elemente $a, b, c \in M$ velja $a \leq b$ in $b \leq c$, potem obstajata $d, e \in M$; $b = a \oplus d$ in $c = b \oplus e$ torej je $c = a \oplus d \oplus e = a \oplus (d \oplus e)$ in od tod pa sledi $a \leq c$.

Ključna lastnost, ki loči kanonično relacijo šibke urejenosti od tega, da bi bila delna urejenost, je torej antisimetričnost. Antisimetrični kanonični relaciji šibke urejenosti pravimo kanonična relacija delne urejenosti oz. kanonična delna urejenost.

Dodatno premislimo, da kanonična šibka urejenost zadošča pogoju usklajenosti s komutativno notranjo operacijo $\oplus$, ki je zapisana v definiciji urejenega (komutativnega) monoida: Denimo, da za neka $a, b \in M$ velja $a \leq b$ potem $\exists c \in M : b = a \oplus c$ in za vsak element $d \in M$ velja $b \oplus d = a \oplus c \oplus d = a \oplus d \oplus c$ zaradi komutativnosti $\oplus$. Od tod sklepamo: $a \oplus d \leq b \oplus d$.

Definicija 2.4. Za komutativen monoid $(R, \oplus)$, ki je urejen s kanonično šibko urejenostjo $\leq$, pravimo, da je *kanonično* urejen, če je $\leq$ delna urejenost (torej, če je $\leq$ antisimetrična).

S pomočjo navedenih definicij bomo sedaj izrazili in dokazali prvi izrek te naloge.

Izrek 2.5. *Monoid ne more hkrati biti grupa in kanonično urejen.*

Dokaz. Naj bo $(G, \oplus)$ grupa in za vsak element $a \in G$ označimo njegov inverz kot $-a$. Denimo, da je ta grupa tudi kanonično urejena in naj bosta x ter y dva poljubna različna elementa iz G (torej $x \neq y$). Ker je $(G, \oplus)$ grupa obstaja tak $z \in G$, da je $x = y \oplus z$, torej je $y \leq x$. Konkretno: vzamemo $z = (-y) \oplus x$. Poleg tega obstaja tak $w \in G$, da je $y = x \oplus w$ (vzamemo kar $w = (-x) \oplus y$), torej je $x \leq y$. Potem po antisimetričnosti $\leq$ sledi $a = b$, kar nas privede v protislovje. □

Opomba 2.6. Izrek 2.5 motivira klasifikacijo monoidov. Razred vseh monoidov razdelimo na tri disjunktne razrede: grupe, kanonično urejene monoide in ostale monoide (to so tisti, ki niso niti grupe, niti kanonično urejeni).

Kanonično urejeni monoidi imajo še eno zanimivo lastnost, ki nam je znana iz računanja nad nenegativnimi celimi števili $\mathbb{N}_0$ – to, da se noben par neničelnih števil ne more sešteti v 0.

Trditev 2.7. *V kanonično urejenem monoidu $(M, \oplus)$ velja naslednje:*

$$x, y \in M \ \& \ x \oplus y = 0 \Rightarrow x = 0 \ \& \ y = 0$$

Dokaz. Denimo, da za neka $x, y \in M$ velja $x \oplus y = 0$. Od tod sledi $x \leq 0$ in $y \leq 0$. Velja pa tudi $x = 0 \oplus x$ in $y = 0 \oplus y$, od koder sklepamo, da velja $0 \leq x$ in $0 \leq y$. Po antisimetričnosti $\leq$ potem sledi $x = 0$ in $y = 0$. □

Opomba 2.8. Lastnosti iz trditve 2.7 pravimo *pozitivnost*, za strukturo, ki ima to lastnost, pa pravimo, da zadošča pogoju pozitivnosti. Tipičen primer, ki zadošča tej lastnosti, je $(\mathbb{N}_0, +)$.

Za konec tega odseka uporabimo lastnost pozitivnosti v naslednjem izreku.

Izrek 2.9. *Naj bo vsak element x komutativnega monoida $(M, \oplus)$ okrajšljiv, torej $\forall a, b \in M$:*

$$a \oplus x = b \oplus x \Rightarrow a = b$$

in

$$x \oplus a = x \oplus b \Rightarrow x = y$$

Dodatno, naj M zadošča pogoju pozitivnosti. Potem je kanonična šibka urejenost definirana na M antisimetrična in M je kanonično urejen.

Dokaz. Denimo, da za neka elementa $x, y \in M$ velja $x \leq y$ in $y \leq x$. Potem obstajata $z, w \in M$, da velja $y = x \oplus z$ in $x = y \oplus w$. Ko prvo enakost vstavimo v drugo, dobimo $x \oplus 0 = x = (x \oplus z) \oplus w = x \oplus (z \oplus w)$, od tod pa, zaradi okrajšljivosti elementa x, sklepamo $z \oplus w = 0$. Zaradi pozitivnosti sledi $z = 0$ in $w = 0$, od tod pa $x = y$. □

2.2. **Polkolobarji.** Sedaj, ko smo osvežili in dopolnili znanje o monoidih, se lahko lotimo polkolobarjev.

Definicija 2.10. 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.

V posebnem primeru, ko je $1 = 0$, za polkolobar R velja $R = \{0\}$. Ker nas ta trivialen primer ne zanima, od zdaj naprej predpostavimo $1 \neq 0$.

Opomba 2.11. Dodatno lahko definirano *levi polkolobar* na enak način kot polkolobar, le da zahtevamo samo levo distributivnost in analogno lahko definiramo tudi *desni polkolobar*. $(R, \oplus, \otimes)$ je potem polkolobar če je hkrati levi in desni polkolobar.

Opomba 2.12. V resnici bi lahko gledali še malo manj opremljene strukture, t. i. pred-polkolobarje (»pre-semirings« v angleščini). Definicija zanje je identična kot za polkolobar, le da ne zahtevamo obstoja enot (0 in 1) za operaciji in tudi ne lastnosti 4 iz definicije polkolobarja. V nekateri literaturi pod imenom polkolobarja obravnavajo pred-polkolobar, ki ima aditivno enoto (ne pa multiplikativne).

Zgled 2.13. Nenegativna cela števila $\mathbb{N}_0$ 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. ♢

Polkolobarji pa seveda niso omejeni samo na številske množice. V naslednjem zgledu navedemo primer polkolobarja nad množicami:

Zgled 2.14. Naj bo X neprazna množica in $P(X)$ potenčna množica množice X. Potem je $(P(X), \cup, \cap)$ polkolobar. To bomo tudi utemeljili.

$P(X)$ je očitno zaprta za $\cup$ in za $\cap$. Enota za $\cup$ je $\emptyset$, enota za $\cap$ pa kar X. Obe operaciji sta nad $P(X)$ asociativni ter komutativni, med njima pa velja tudi obojestranska distributivnost. Ne samo, da je $(P(X), \cup, \cap)$ polkolobar, je tudi komutativen polkolobar. ♢

Občasno nam bo prišlo prav, če bomo imeli oznake za množico aditivno obrnljivih elementov in za množico multiplikativno obrnljivih elementov v polkolobarju. Nasledno definicijo pozemamo iz [6, str. 3].

Definicija 2.15. Naj bo $(R, \oplus, \otimes)$ polkolobar. Z $V(R)$ označimo množico vseh aditivno obrnljivih elementov v R in z $U(R)$ označimo množico vseh multiplikativno obrnljivih elementov iz R.

Opazimo lahko, da multiplikativna enota ni nujno vsebovana v $V(R)$. Da to vidimo, je dovolj vzeti polkolobar iz zgleda 2.14, kjer ne obstaja taka množica Y, da bi veljalo $Y \cup X = \emptyset$.

V nadaljevanju nam bo prišla prav tudi naslednja lema iz [6, Lema 2 1].

Lema 2.16. *Naj bo $(R, \oplus, \otimes)$ komutativen polkolobar.*
Potem velja $\forall p, q \in V(R), \forall r \in R : (-p) \otimes r = -(p \otimes r)$ & $(-p) \otimes (-q) = p \otimes q$.

Dokaz. Očitno velja $-p \in V(R)$ in $-(-p) = p \ \forall p \in V(R)$. Poleg tega za vse $p, q \in V(R)$ in vse $r \in R$ velja $(-p) \otimes r \oplus p \otimes r = ((-p) \oplus p) \otimes r = 0 \otimes r = 0$, torej $(-p) \otimes r = -(p \otimes r)$. Potem je pa tudi $(-p) \otimes (-q) = -(p \otimes (-q)) = -(-(p \otimes q)) = p \otimes q$. □

Pri spoznavanju grup, kolobarjev in ostalih algebraičnih struktur se neizogibno pojavi obravnava njihovih produktov. Tako kot pri kartezičnih produktih prej omenjenih struktur, tudi za polkolobarje v naslednjem zgledu obravnavamo, ali je produkt polkolobarjev, opremljen z induciranima operacijama, spet polkolobar.

Zgled 2.17. Denimo, da imamo m polkolobarjev $(R_i, \oplus_i, \otimes_i)$; $i \in \{1, 2, \ldots, m\}$. Potem označimo $R = R_1 \times \ldots \times R_m$ in elementi iz R so oblike $x = \begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix}$. Za $\forall x, y \in R$ definiramo operaciji $\oplus$ in $\otimes$ na naslednji način:

$$x \oplus y = \begin{bmatrix} x_1 \oplus_1 y_1 \\ \vdots \\ x_m \oplus_m y_m \end{bmatrix} \text{ in } x \otimes y = \begin{bmatrix} x_1 \otimes_1 x_m \\ \vdots \\ x_m \otimes_m y_m \end{bmatrix}$$

Brez težav lahko preverimo, da operaciji $\oplus$ in $\otimes$ podedujeta lastnosti operacij $\oplus_i$ in $\otimes_i$, torej je tudi $(R, \oplus . \otimes)$ polkolobar. ♢

Preden preidemo na obravnavo podstruktur se spomnimo izreka 2.5, s pomočjo katerega lahko naravno razdelimo razred polkolobarjev na disjunktne podrazrede, glede na to, ali $\oplus$ opremi množico R s strukturo abelove grupe ali s strukturo kanonično urejenega monoida ali pa z nobeno od prej navedenih struktur. Prej omenjen izrek 2.5 nam namreč pove, da $(R, \oplus)$ ne more hkrati biti abelova grupa in kanonično urejen. V prvem primeru ima $(R, \oplus, \otimes)$ v resnici kar strukturo kolobarja, v drugem pa strukturo dioida, ki ga bomo definirali v naslednjem podpoglavju. Na ta način klasificiramo vse polkolobarje – njihov razred razdelimo na razred kolobarjev, razred dioidov in še razred ostalih polkolobarjev, torej tistih, za katere $(R, \oplus)$ ni niti abelova grupa, niti kanonično urejen monoid. Ti razredi so očitno paroma disjunktni.

Sedaj definirajmo in obravnavajmo še podstrukture polkolobarjev, torej podpolkolobarje.

Definicija 2.18. Naj bo $(R, \oplus, \otimes)$ (levi) polkolobar. Neprazna množica P je (levi) podpolkolobar v R, če je podmnožica v R in če je zaprta za operaciji $\oplus_{|P}$ in $\otimes_{|P}$, ki ju podeduje od R. Operaciji $\oplus_{|P}$ in $\otimes_{|P}$ sta torej zožitvi $\oplus$ in $\otimes$ na P.

Trditev 2.19. *Naj bo $(R, \oplus, \otimes)$ (levi) polkolobar in $P \subseteq R$ neprazna podmnožica v R. Tedaj je P (levi) podpolkolobar v R, čim je zaprt za zoženi operaciji in vsebuje obe enoti.*

Dokaz. Denimo, da velja pogoj iz trditve. Operacija $\oplus_{|P}$ potem ima enoto v P in od $\oplus$ podeduje asociativnost in komutativnost. Torej je $(P, \oplus_{|P})$ komutativen monoid. Podobno $\otimes_{|P}$ podeduje asociativnost in ima v P enoto, torej je $(P, \otimes_{|P})$ monoid. Tudi (leva) distributivnost se podeduje od operacij v R in enako velja za lastnost, da aditivna enota izniči $\otimes_{|P}$ in s tem vidimo, da je $(P, \oplus_{|P}, \otimes_{|P})$ res podpolkolobar. □

Zgornji dokaz je dovolj preprost, da bi se ga dalo brez težav opustiti. Kljub temu ga navedemo, da dodatno poudarimo, da relativna preprostost struktur, s katerimi imamo trenutno opravka, v resnici ne oteži naše obravnave osnovnih konceptov. Zgoraj navedena trditev in dokaz sta izjemno podobna analogni trditvi in pripadajoćemu dokazu za kolobarje.

Sedaj preidemo na preslikave med polkolobarji, specifično homomorfizme, ki so definirani na skoraj enak način kot homomorfizmi kolobarjev.

Definicija 2.20. Naj bosta $(R, \oplus, \otimes)$ in $(P, \boxplus, \boxtimes)$ (leva) polkolobarja. Naj bosta 0 in 1 enoti v R ter e in ε enoti v P. Preslikava $\phi : R \to P$ je homomorfizem polkolobarjev, če zadošča naslednjim pogojem:

- $\phi(0) = e$
- $\phi(1) = \varepsilon$
- $\phi(x \oplus y) = \phi(x) \boxplus \phi(y);\ \forall x, y \in R$
- $\phi(x \otimes y) = \phi(x) \boxtimes \phi(y);\ \forall x, y \in R$

Tudi tukaj lahko uvedemo klasične izraze kot so monomorfizem (za injektivne homomorfizme), epimorfizem (surjektivni homomorfizem), izomorfizem (bijektivni homomorfizem), endomorfizem (homomorfizem iz polkolobarja nazaj vase) in avtomorfizem (bijektivni endomorfizem).

Preden premaknemo pozornost na dioide, omenimo še, da lahko, tako kot za kolobarje, tudi za polkolobarje definiramo ideale, brez da bi samo definicijo bistveno spremenili.

Definicija 2.21. Neprazni podmnožici I polkolobarja $(R, \oplus, \otimes)$ pravimo *levi ideal*, če za njo velja

- $a \oplus b \in I\ ;\ \forall a, b \in I$
- $r \otimes a \in I\ ;\ \forall a \in I\ \wedge\ \forall r \in R$

Podobno definiramo desne ideale. Pravimo, da je I ideal R, če je hkrati levi in desni ideal R. Idealu (levemu, desnemu ali obojestranskemu) I polkolobarja R pravimo *maksimalen ideal*, če zanj velja naslednje:

- $I \neq R$
- $I \subseteq J \subseteq R \Rightarrow I = J$ ali $J = R$ za vse ideale J polkolobarja R.

Preprost primer ideala polkolobarja najdemo v množici sodih naravnih števil (označeno z $2\mathbb{N}$) v $(\mathbb{N}_0, +, \cdot)$. Vsota dveh sodih števil je spet sodo število, poleg tega pa je vsak produkt poljubnega števila iz $\mathbb{N}_0$ in sodega števila spet sodo število.

2.3. **Dioidi.** Kot smo že napovedali v prejšnjem podpoglavju, zahvaljujoč se izreku 2.5, lahko obravnavamo podkolobarje, ki so opremljeni s kanonično delno ureditvijo in se posledično ne obnašajo kot nam že znani kolobarji. Tem strukturam pravimo dioidi. Vseeno zapišimo formalno definicijo preden se lotimo obravnave.

Definicija 2.22. Polkolobarju $(R, \oplus, \otimes)$, na katerem je kanonična relacija šibke urejenosti (definirana preko $\oplus$) delna urejenost, pravimo *dioid*. Komutativnemu polkolobarju R, na katerem je kanonična relacija šibke urejenosti delna urejenost, pravimo *komutativen dioid*.

Upoštevajoč opombo 2.8 lahko klasificiramo dioide kot polkolobarje, ki zadoščajo pogoju pozitivnosti.

Opomba 2.23. Če namesto (obojestranskega) polkolobarja vzamemo levi ali desni polkolobar in v njem opremimo $(R, \oplus)$ s kanonično delno urejenostjo, dobljeni strukturi pravimo levi oz. desni dioid.

Preprosti primer dioida je množica nenegativnih celih števil $\mathbb{N}_0$, opremljena z navadnim seštevanjem in množenjem ter kanonično delno (celo linearno) urejenostjo. Dodatno navedemo še nenegativna racionalna števila $\mathbb{Q}_+$ in nenegativna realna števila $\mathbb{R}_+$.

Podobno, kot se množica celih števil $\mathbb{Z}$ s standardnim seštevanjem $+$ smatra za »prototip« abelovih grup, nam $(\mathbb{N}_0, +, \cdot)$ služij kot »prototip« dioidov. Seveda dioidi niso omejeni zgolj na nenegativne odseke številskih množic opremljene s $+$ in $\cdot$. Znane množice lahko opremimo tudi z manj standardnimi operacijami in tako pridobimo dioide, kot bo pokazal naslednji zgled.

Zgled 2.24. Z $\bar{\mathbb{R}}$ označimo množico $\mathbb{R} \cup \{-\infty, +\infty\}$. Potem sta $(\bar{\mathbb{R}}, \min, +)$ in $(\bar{\mathbb{R}}, \max, +)$ dioida. V primeru prvega dioida je nevtralni element $+\infty$, enota pa je 0, v primeru drugega pa sta enoti $-\infty$ in 0. V obeh primerih sta obe operaciji komutativni in asociativni, med njima tudi očitno velja distributivnost in nevtralni element prve operacije izniči $+$. Obravnavani strukturi sta torej komutativna polkolobarja.

Dodatno vidimo da je kanonična šibka urejenost, definirana preko min, tudi antisimetrična: $a \leq b \Rightarrow \exists c \in \bar{\mathbb{R}};\ b = \min\{a, c\}$ in $b \leq a \Rightarrow \exists d \in \bar{\mathbb{R}};\ a = \min\{b, d\}$, torej je $b = \min\{\min\{b, d\}, c\}$ oz. $b = \min\{b, d, c\} = \min\{b, \min\{d, c\}\}$. Sledi, da je $\min\{c, d\} = +\infty$, kar je možno edino ko $c = +\infty = d$, torej je $a = b$. Na enak način pokažemo antisimetričnost kanonične urejenosti definirane preko max.

Torej sta oba polkolobarja res tudi dioida. $(\bar{\mathbb{R}}, \min, +)$ in $(\bar{\mathbb{R}}, \max, +)$ imenujemo tropska polkolobarja oz. tropska dioida, odvisno od konteksta. ♢

Trditev 2.25. *Naj bo $(R, \oplus, \otimes)$ dioid. Potem je kanonična delna urejenost $\leq$ usklajena z operacijama $\oplus$ in $\otimes$.*

Dokaz. To, da je $\leq$ usklajena z operacijo $\oplus$ vemo že iz definicije dioida. Pokažimo torej enako še za $\otimes$. Vemo, da velja $a \leq b \iff \exists c \in R : b = a \oplus c$. Potem iz $a \leq b$ za $\forall x \in R$ sledi $(a \oplus c) \otimes x = b \otimes x$. Po distributivnosti potem sledi $(a \otimes x) \oplus (c \otimes x) = b \otimes x$. Potem je pa $a \otimes x \leq b \otimes x\ \forall x \in R$. Podobno pokažemo tudi $x \otimes a \leq x \otimes b$. Sledi, da je $\leq$ usklajena z $\otimes$. □

Tudi pri dioidih lahko obravnavamo strukturo njihovih produktov. Denimo, da imamo m dioidov $(R_i, \oplus_i, \otimes_i)$, jih zmnožimo v $R = R_1 \times \ldots \times R_m$ in na to množico vpeljemo operaciji $\oplus$ in $\otimes$ na naslednji način:

$$\forall x, y \in R : x \oplus y = \begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix} = \begin{bmatrix} x_1 \oplus_1 y_1 \\ \vdots \\ x_m \oplus_m y_m \end{bmatrix}$$

in

$$\forall x, y \in R : x \otimes y = \begin{bmatrix} x_1 \otimes_1 y_1 \\ \vdots \\ x_m \otimes_m y_m \end{bmatrix}$$

V zgledu 2.17 smo že premislili, da je $(R, \oplus, \otimes)$ polkolobar. Poleg tega hitro vidimo, da je $\oplus$ usklajena s kanonično delno ureditvijo na R, saj za vsaka $x = \begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix}$ in $y = \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix}$ iz R velja $x \leq y \iff x_1 \leq_1 y_1 \ \& \ \ldots \ \& \ x_m \leq_m y_m$.

Tudi vprašanje podstruktur pri dioidih se splača obravnavati. Tem podstrukturam bomo pravili *poddioidi*. Njihov obstoj nam namigujejo »prototipni« dioidi - nenegativni odseki številskih množic opremljeni s standardnim seštevanjem in množenjem: $\mathbb{N}_0 \subseteq \mathbb{Q}_+ \subseteq \mathbb{R}_+$.

Definicija 2.26. Neprazna množica P je poddioid dioida $(R, \oplus, \otimes)$, če je podmnožica v R, ki vsebuje obe enoti, in če je tudi sama dioid za operaciji, ki ju podeduje od $(R, \oplus, \otimes)$.

Hitro se da opaziti, da v preverjanju, ali je P poddioid, ni treba direktno obravnavati urejenosti. Izkaže se, da je dovolj, da za podmnožico P v dioidu R preverimo, če je polkolobar.

Trditev 2.27. *Naj bo $(R, \oplus, \otimes)$ (levi) dioid in naj bo $P \subseteq R$ neprazna podmnožica v R. Potem je P poddioid v $R \iff P$ je podpolkolobar v R.*

Dokaz. Če je P poddioid je očitno tudi podpolkolobar. Denimo torej da za P vemo zgolj, da je podpolkolobar v dioidu R in si poglejmo kanonično šibko urejenost $\leq$ na njem. Ker je kanonična šibka urejenost na R antisimetrična, ima to lastnost tudi na P, torej je $\leq$ na P v resnici kanonična delna urejenost. Sledi, da je P dioid, torej je poddioid v R. □

Pri obravnavi dioidov se omenimo še preslikave med njimi. Izkaže se, da v resnici ni treba uvesti nobenih novih pojmov, saj homomorfizmi polkolobarjev ohranjajo strukturo dioidov. Da to vidimo, si oglejmo poljubna dva dioida, $(R, \oplus, \otimes)$ in $(P, \boxplus, \boxtimes)$, ter preslikavo med njima, $\phi : R \to P$, ki zadošča pogojem za homomorfizem polkolobarjev. Slednja zahteva je minimalna, saj mora homomorfizem dioidov hkrati biti tudi homomorfizem polkolobarjev.

Predpostavimo sedaj, da za neka elementa $a, b \in R$ velja $a \leq_R b$. Potem obstaja tak $c \in R$, da je $\phi(b) = \phi(a \oplus c) = \phi(a) \boxplus \phi(c)$, torej je $\phi(a) \leq_P \phi(b)$. Lahko se sicer zgodi, da za neprimerljiva elementa x in y iz R velja, da sta $\phi(x)$ in $\phi(y)$ primerljiva, torej $\phi(x) \leq \phi(y)$ ali $\phi(x) \geq \phi(y)$. V prvem primeru obstaja nek element $z \in P$, da je $\phi(y) = \phi(x) \boxplus z$, a v tem primeru ne obstaja noben element $w \in R$, ki se preslika v z. Drugače povedano, $z \notin Im(\phi)$, kar pa nas ne moti. Simetričen premislek velja za primer $\phi(x) \geq \phi(y)$. Homomorfizmi polkolobarjev torej ohranjajo urejenost.

Da se dodatno prepričamo, lahko preverimo, da je $(Im(\phi), \boxplus, \boxtimes)$ dioid. To lahko naredimo tako, da pokažemo, da je kanonična šibka urejenost na $Im(\phi)$ antisimetrična, ali pa tako, da upoštevamo, da je $(Im(\phi), \boxplus, \boxtimes)$ podpolkolobar v dioidu $(P, \boxplus, \boxtimes)$ in potem po trditvi 2.27 sledi da je poddioid v P, torej tudi sam dioid.

To, da imamo v dioidih (kanonično) relacijo delne urejenosti, nas motivira, da dioide dodatno ločimo glede na lastnosti pripadajoče ureditve. Kot je navedeno v [4, str. 10], je delno urejena množica $(R, \leq)$ *polna* (»complete«), ko ima vsaka podmnožica $P \subseteq R$ t. i. *supremum*. Velja, da je $r \in R$ supremum $P \subseteq R$, ko je zgornja meja P

($\forall p \in P$ velja $p \leq r$) in $\forall q \in R$ velja sklep: q je zgornja meja $P \Rightarrow r \leq q$. Polnost urejenosti nas privede do naslednje definicije, povzete iz [4, definicija 6. 1. 8.].

Definicija 2.28. Dioid $(R, \oplus, \otimes)$ je *poln* oz. *kompleten*, če je za kanonično delno urejenost $\leq$ urejena množica $(R, \leq)$ polna in če poleg tega ustreza še t. i. posplošeni distributivnosti:

$$\forall P \subseteq R, \forall r \in R : \Big(\bigoplus_{p \in P} p\Big) \otimes r = \bigoplus_{p \in P} (p \otimes r)$$

in

$$r \otimes \Big(\bigoplus_{p \in P} p\Big) = \bigoplus_{p \in P} (r \otimes p)$$

Iz definicije sledi, da za vsaki podmnožici $P, Q \subseteq R$ velja:

$$\Big(\bigoplus_{p \in P} p\Big) \otimes \Big(\bigoplus_{q \in Q} q\Big) = \bigoplus_{(p,q) \in P \times Q} (p \otimes q)$$

.

V polnem dioidu označimo kot zadnji element kar vsoto vseh elementov dioida $T = \bigoplus_{r \in R} r$. Prvi element je ravno aditivna enota 0 (saj $0 \leq r \ \forall r \in R$). Poleg tega velja: $\forall r \in R : T \oplus r = T$ in $T \otimes 0 = 0$.

Zgled 2.29. Dioida $(\mathbb{R} \cup \{-\infty\}, \max, +)$ in $(\mathbb{R} \cup \{+\infty\}, \min, +)$ nista polna. Da postaneta polna, jima moramo dodati njuna zadnja elementa. Za prvi dioid je to $T = +\infty$., za drugi dioid pa je $T = -\infty$. Tropska dioida iz zgleda 2.24 sta torej polna dioida. ♢

Opomba 2.30. Omenimo še dualni pojem *infimuma* množice, kot je definiran v [4, str. 10]. Element $r \in R$ je infimum $P \subseteq R$ ko je spodnja meja P ($\forall p \in P$ velja $r \leq p$) in $\forall q \in R$ velja sklep (q je spodnja meja $P \Rightarrow q \leq r$). Če ima v $(R, \leq)$ vsaka podmnožica infimum, pravimo, da je $(R, \leq)$ dualno polna. Urejeni množici $(R, \leq)$, ki je hkrati polna in dualno polna, pravimo *polna mreža*.

Lastnosti dioidov glede na lastnosti kanonične delne urejenosti se da obravnavati v večjem obsegu, a to ni ključnega pomena za to nalogo. Zgoraj navedene definicije in zgledi, ki spadajo pod to temo, so navedeni primarno kot zanimivost in zavoljo malo širše obravnave. Preden se posvetimo primeru praktične aplikacije dioidov, navedimo še en zgled, ki ni vezan na znane številske množice. Zgleda 2.31 in 2.32 v nadaljevanju sta povzeta iz [4, poglavje 6. 2.].

Zgled 2.31. Naj bo $(R, +)$ kanonično urejen komutativen monoid z enoto 0. Na množici E endomorfizmov R potem uvedemo operaciji $\oplus$ in $\otimes$ na sledeč način:

$$\forall f, g \in E : (f \oplus g)(r) = f(r) + g(r) \text{ in } (f \otimes g)(r) = f(r) \circ g(r) \ \forall r \in R,$$

kjer je $\circ$ navadno komponiranje preslikav. Hitro vidimo, da je $(E, \oplus, \otimes)$ dioid. ♢

Naslednji zgled, nam demonstrira praktično aplikacijo zgleda 2.31.

Zgled 2.32. Vsebino zgleda 2.31 lahko uporabimo v teoriji grafov v iskanju časovno najkrajše poti. Denimo, da imamo graf $G = (V, E)$ in da vsaki povezavi (i, j) pripada preslikava h_{ij}, ki nam poda čas prihoda t_j v vozlišče j, če zapustimo vozlišče i ob času t_i. Torej $t_j = h_{ij}(t_i)$. Iščemo najkrajši čas, da prispemo iz vozlišča t_1 v izbrano vozlišče t_i.

Za ta problem vzamemo $R = \mathbb{R} \cup \{+\infty\}, \oplus = \min, 0 = +\infty$. Za množico E vzamemo množico nepadajočih funkcij $f : R \mapsto R$, za katere gre $f(t) \to +\infty$ ko se

t bliža $+\infty$. Te funkcije so endomorfizmi nad $(\mathbb{R} \cup \{+\infty\}, \min)$, saj $f(\min\{t, \acute{t}\}) = \min\{f(t), f(\acute{t})\}$ in $f(+\infty) = +\infty$. Na enak način kot v prejšnjem zgledu sestavimo dioid $(E, \oplus, \otimes)$. $\diamondsuit$

Problem najkrajše poti lahko torej obravnavamo s pomočjo dioida endomorfizmov iz prejšnjega zgleda 2.32. Rešitve tega problema skupaj z algoritmi so, med drugimi, obravnavali Cooke in Halsey (1966) ter Minoux (1976).

Na koncu izpostavimo še eno povezavo med polkolobarji in dioidi: Kot lahko vidimo v [4, poglavje 6. 9.], vsakemu polkolobarju pripada nek dioid. Pri določanju tega dioida bo seveda ključno to, da kanonični šibki urejenosti na izbranem polkolobarju dodamo antisimetričnost. Kako to naredimo, nam pove trditev [4, trditev 6. 9. 1.], ki je navedena spodaj.

Trditev 2.33. *Naj bo $(R, \oplus, \otimes)$ polkolobar v katerem kanonična relacija šibke urejenosti $\leq$ ni antisimetrična (torej ni delna ureditev). Naj bo $\mathcal{E}$ ekvivalenčna relacija definirana na R:*

$$\forall r, s \in R : r \mathcal{E} s \iff r \leq s \ \& \ s \leq r$$

Potem je množica $\widehat{R} = R/\mathcal{E}$, opremljena z operacijama, ki ju inducirata $\oplus$ in $\otimes$, dioid. Temu dioidu pravimo dioid, ki je kanonično asociiran s polkolobarjem $(R, \oplus, \otimes)$.

Dokaz. Relacija $\mathcal{E}$, definirana zgoraj v izreku, je očitno refleksivna, tranzitivna in simetrična, torej je ekvivalenčna relacija. Potem so elementi $\widehat{R}$ ravno ekvivalenčni razredi relacije $\mathcal{E}$ na R in ohranimo oznaki $\oplus$ in $\otimes$ za operacije, ki jih operaciji na R inducirata na $\widehat{R}$. Nevtralna elementa v $\widehat{R}$ sta ekvivalenčna razreda, ki pripadata nevtralnima elementoma iz R. Ker aditivna enota 0 v $(R, \oplus, \otimes)$ izniči $\otimes$, sledi da v $(\widehat{R}, \oplus, \otimes)$ razred kateremu pripada 0 izniči operacijo, ki jo inducira $\otimes$. Hitro vidimo, da je $(\widehat{R}, \oplus, \otimes)$ polkolobar. Poleg tega kanonična relacija šibke urejenosti $\leq$ inducira antisimetrično relacijo šibke urejenosti, torej delno urejenost. Torej je $(\widehat{R}, \oplus, \otimes)$ dioid. $\square$

Opomba 2.34. Dodatno lahko definiramo še eno strukturo, t. i. *polpolje*, kot polkolobar v katerem je vsak od 0 različen element obrnljiv glede na $\otimes$ ([4, poglavje 1, definicija 5. 2. 3.]). Izkaže se, da so mnogi dioidi polpolja. Takšna sta na primer $(\mathbb{R} \cup \{+\infty\}, \min, +)$ in $(\mathbb{R} \cup \{-\infty\}, \max, +)$. To omenimo zgolj kot zanimivost, saj nas v nadaljevanju polpolja ne bodo kaj preveč zanimala.

3. Polmoduli in moduloidi:

Tako kot lahko nad polji definiramo vektorske prostore in nad kolobarji module, lahko podobne strukture uvedemo tudi nad polkolobarji in dioidi. Kot bomo kmalu videli, se bodo strukture nad polkolobarji ravnale po intuiciji vektorskih prostorov in modulov. Za začetek bomo navedli definicije teh struktur, nato bomo obravnavali vprašanje homomorfizmov in kvocientnih struktur, na koncu poglavja pa se bomo posvetili vprašanju baz. V večji meri se bomo pri tem sklicevali na vir [4, poglavje 5. 2.], kjer bo vir drug pa bo to tudi navedeno.

3.1. Definicije in elementarni primeri:

V tem podpoglavju bomo definirali strukture nad polkolobarji in dioidi.

Definicija 3.1. Naj bo $(R, \oplus, \otimes)$ polkolobar z nevtralnima elementoma 0 in 1.
Levi R-polmodul je komutativen monoid $(M, +)$ z aditivno identiteto θ, na katerem

je definirana zunanja operacija $\cdot : R \times M \to M$, ki jo imenujemo množenje s skalarjem. Množenje s skalarjem zadošča naslednjim pogojem za vsaka $\lambda, \mu \in R$ in vsaka $m, n \in M$:

A1 $\lambda \cdot (m + n) = \lambda \cdot m + \lambda \cdot n$
A2 $(\lambda \oplus \mu) \cdot m = \lambda \cdot m + \mu \cdot m$
A3 $(\lambda \otimes \mu) \cdot m = \lambda \cdot (\mu \cdot m)$
A4 $1 \cdot m = m$
A5 $\lambda \cdot \theta = \theta = 0 \cdot m$

Analogno definiramo desni R-polmodul. Elementom polmodula pravimo vektorji. Polmodule (leve, desne in obojestranske) bomo na kratko označevali z $(M, +, \cdot)$.

Kadar je operacija $\otimes$ na polkolobarju $(R, \oplus, \otimes)$ komutativna, koncepta levega in desnega R-polmodula sovpadata. Drugače povedano, $(M, +, \cdot)$ nad $(R, \oplus, \otimes)$ je obojestranski R-polmodul, če je hkrati levi in desni R-polmodul. Analogi rezultatov, ki jih bomo dokazali za leve R-polmodule seveda veljajo tudi za desne in obojestranske R-polmodule. Od zdaj naprej bomo pod imenom R-polmodul obravnavali leve R-polmodule nad polkolobarjem R.

Zgled 3.2. Naj bo R levi polkolobar in poglejmo njegov n-kratni kartezični produkt $R^n = \{(a_1, a_2, \ldots, a_n)^\top |\ a_i \in R \text{ za } i \in \{1, 2, \ldots, n\}\}$. Pri tem je $(a_1, a_2, \ldots, a_n)^\top$ transpozicija $(a_1, a_2, \ldots, a_n)$ in $n \geq 1$. Definiramo:

$$a + b = (a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_n \oplus b_n)^\top$$

in

$$\lambda \cdot a = (\lambda \otimes a_1, \lambda \otimes a_2, \ldots, \lambda \otimes a_n)^\top$$

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. ♢

Definicija 3.3. Levemu (oz. desnemu) polmodulu nad R pravimo *levi moduloid* (oz. desni moduloid), če je $(R, \oplus, \otimes)$ dioid in $(M, +)$ kanonično urejen. Če je $(R, \oplus, \otimes)$ komutativen, opustimo pridevnika levi in desni, saj koncepta sovpadata.

Zgled 3.4. Vrnimo se k zgledu 3.2 in dodatno predpostavimo, da je $(R, \oplus, \otimes)$ dioid. Potem je $(R^n, +)$ kanonično urejen, torej je (levi) moduloid. Da se o tem prepričamo je dovolj, da preverimo lastnosti kanonične urejenosti $\leq_+$ na $(R^n, +)$. Naj bosta $a, b \in R^n$ in denimo, da je $a \leq_+ b$. To bo res natanko tedaj, ko bo obstajal tak $c \in R^n$, da je $b = a + c$ oz. ko bo za vsak $i \in \{1, 2, \ldots, n\}$ veljalo $b_i = a_i \oplus c_i$ oziroma $a_i \leq_\oplus b_i$. Relacija $\leq_+$ podeduje antisimetričnost od $\leq_\oplus$. ♢

3.2. **Homomorfizmi in kvocientne strukture:** Tudi pri polmodulih nas bodo zanimale preslikave, ki ohranjajo algebraično strukturo. Pojavi se tudi vprašanje, ali lahko nad polmoduli tvorimo kvocientne strukture. Oboje bomo obravnavali v tem podpoglavju.

Definicija 3.5. Naj bosta M in N dva (leva) polmodula, oba nad istim (levim) polkolobarjem $(R, \oplus, \otimes)$. Z $+$ in $\boxplus$ označimo notranji operaciji, z $\cdot$ in $\boxdot$ pa množenji s skalarjem. Preslikavi $\phi : M \to N$ pravimo *homomorfizem* levih polmodulov M in N, če zadošča naslednjim pogojem:

(i) $\phi(x + y) = \phi(x) \boxplus \phi(y), \forall x, y \in M$
(ii) $\phi(\lambda \cdot x) = \lambda \boxdot \phi(x), \forall x \in M, \forall \lambda \in R$

Homomorfizmom, ki slikajo iz M nazaj v M pravimo *endomorfizmi*.

Kadar je $(R, \oplus, \otimes)$ dioid in sta M ter N kanonično delno urejena, govorimo o homomorfizmih in endomorfizmih levih moduloidov.

Opomba 3.6. Tako kot elementom x R-polmodula $(R^n, +, \cdot)$, pravimo vektorji, pravimo homomorfizmom med polmoduli kar *linearne preslikave*.

Ker v algebri (tako linearni kot abstraktni) igrajo pomembno vlogo podstrukture in kvocientne strukture, bomo te definirali tudi za polmodule. Spodnji definiciji sta povzeti iz [4].

Definicija 3.7. Naj bo $(M, +, \cdot)$ levi R-polmodul in $\widehat{M}$ neprazna podmnožica v M. Pravimo, da je množica $\widehat{M}$ podpolmodul v M, če vsebuje enoto θ in je zaprta za podedovani operaciji.

Na enak način kot za podstrukture ostalih algebraičnih struktur, kot so grupe, kolobarji, vektorski prostori in moduli, lahko vidimo, da je presek družine $(N_i)_{i\in I}$ R-podpolmodulov R-polmodula M, torej $\cap_{i\in I} N_i$, tudi sam R-podpolmodul v M. Če definiramo vsoto R-podpolmodulov $N_1, N_2 \subseteq M$ s predpisom $N_1 + N_2 = \{n_1 + n_2 \mid n_1 \in N_1 \ \wedge \ n_2 \in N_2\}$, je tudi ta R-podpolmodul v R-polmodulu M.

Definicija 3.8. Naj bo $(M, +, \cdot)$ levi R-polmodul in $(\widehat{M}, +, \cdot)$ (levi) podpolmodul v M. Z $M/\widehat{M}$ označimo kvocientno množico M glede na ekvivalenčno relacijo $\mathcal{E}$:

$$x\mathcal{E}y \iff \exists u, v \in \widehat{M} : x + u = y + v$$

Množici $M/\widehat{M}$ pravimo kvocientni polmodul R-polmodula M nad $\widehat{M}$.

Da se preveriti, da je $\mathcal{E}$ usklajena s $+$ in $\cdot$. Za poljubne elemente $x_1, x_2, y_1, y_2 \in M$ velja $x_1\mathcal{E}y_1$ in $x_2\mathcal{E}y_2$ natanko tedaj, ko obstajajo $u_1, u_2, v_1, v_2 \in \widehat{M}$, da je $x_1 + u_1 = y_1 + v_1$ in $x_2 + u_2 = y_2 + v_2$.

Potem pa velja tudi $(x_1 + x_2)\mathcal{E}(y_1 + y_2)$, saj je $x_1 + x_2 + u_1 + u_2 = y_1 + y_2 + v_1 + v_2$ in $(u_1 + u_2), (v_1 + v_2) \in \widehat{M}$. Dodatno, če je $x + u = y + v$ je tudi $\lambda \cdot (x + u) = \lambda \cdot (y + v)$ za vsak $\lambda \in R$ oz. $\lambda \cdot x + \lambda \cdot u = \lambda \cdot y + \lambda \cdot v$. Ker sta $(\lambda \cdot u), (\lambda \cdot v) \in \widehat{M}$, potem po definiciji $\mathcal{E}$ sledi $(\lambda \cdot x)\mathcal{E}(\lambda \cdot y)$.

Posledično je kanonični epimorfizem φ, ki vsakemu elementu $x \in M$ priredi njegov ekvivalenčni razred v $M/\widehat{M}$, homomorfizem levih R- polmodulov.

3.3. **Generatorji polmodulov in linearna neodvisnost:** V tem podpoglavju bomo definirali generatorje, linearno (ne)odvisnost ter baze v kontekstu (levih) polmodulov. Poleg tega bomo pokazali tudi nekaj zanimivih rezultatov. Več rezultatov na temo baz (levih) polmodulov bomo obravnavali v poglavju o matrikah.

Definicija 3.9. Naj bo $(M, +, \cdot)$ levi R-polmodul in naj bo $X = (x_i)_{i\in I}$ poljubna neprazna družina elementov iz M. Najmanjši (levi) R-podpolmodul, ki vsebuje X, imenujemo (levi) R-podpolmodul generiran z X in ga označimo z $\langle X \rangle$. Če je $\langle X \rangle = M$ pravimo, da X generira M.

V definiciji dopuščamo, da je X končna ali pa neskončna družina. Če je X končna, pravimo, da je M *končno generiran*. Tudi v primeru polmodulov bi želeli definirati t. i. dimenzijo polmodula. Pojem dimenzije, kot jo poznamo iz linearne algebre nad polji, ni ustrezen za polkolobarje, saj kardinalnost baze, kot bomo kasneje videli, ni enolično določena. Zato definiramo rang polmodula po [6, str. 3–4].

Definicija 3.10. *Rang* R-polmodula M, označen z $r(M)$, je enak najmanjšemu številu n, za katerega obstaja množica X velikosti n, ki generira M. Rang vedno obstaja za končno generirane polmodule. Rang polmodula je znan tudi pod imenom *šibka dimenzija polmodula*. Pod tem imenom je definiran kot minimalna kardinalnost šibko linearno odvisnih podmnožic, ki generirajo polmodul.

Rang polmodula bo postal pomemben kasneje v podpoglavju 4.2 o prehodnih matrikah.

V nadaljevanju nam bo prišlo prav, če karakteriziramo podpolmodule generirane z $X \subseteq M$. Ravno to nam da naslednja trditev.

Trditev 3.11. *Naj bo* $(M, +, \cdot)$ *levi* R*-polmodul in* $X = (x_i)_{i \in I}$ *neka poljubna neprazna družina elementov iz* M*. Potem je* $\langle X \rangle = Y$*, kjer je* Y *množica tistih* $y \in M$*, ki so oblike:*

$$y = \sum_{j \in J} \lambda_j \cdot x_j$$

Pri tem je $J \subset I$ *končna podmnožica indeksov in za vsak* $j \in J$ *je* $\lambda_j \in R$*.*

Dokaz. Hitro vidimo, da je $X \subseteq Y$, saj lahko vsak $x_i \in X$ zapišemo kot $\sum_{j \in J} \lambda_j \cdot x_j$ za $J = \{i\}$ in $\lambda_i = 1$. Vidimo tudi, da je θ element Y (vzamemo $J = i$ in $\lambda_i = 0$) ter da je Y zaprt za $+$. Sledi torej, da je Y levi R-podpolmodul v M, ki vsebuje X. Po definiciji je $\langle X \rangle$ najmanjši podpolmodul, ki vsebuje X, torej sledi $\langle X \rangle \subseteq Y$.

Po drugi strani pa vidimo še, da vsak levi R-podpolmodul v M, ki vsebuje X, vsebuje tudi vse linearne kombinacije elementov $x_i \in X$, torej vsebuje Y. V posebnem primeru velja to tudi za $\langle X \rangle$, torej sledi $Y \subseteq \langle X \rangle$. Od tod pa sledi $Y = \langle X \rangle$. Y je torej najmanjši levi R-podpolmodul, ki vsebuje X. □

Ta rezultat seveda ni presenetljiv, saj velja tudi za module in pa vektorske prostore. V slednjem nam je $\langle X \rangle$ znan pod imenom linearne ogrinjače množice vektorjev X.

Sedaj lahko definiramo koncept linearne odvisnosti oz. linearne neodvisnosti v polmodulih. Uporabili bomo definicijo, ki sta jo navedla Minoux in Gondran v [4, Poglavje 5, definicija 2. 5. 1.]. Ta se glasi:

Definicija 3.12. Naj bo $(M, +, \cdot)$ levi R-polmodul in $X = (x_i)_{i \in I}$ neprazna (končna ali števno neskončna) družina elementov iz M. Za vsako podmnožico indeksov $J \subset I$ označimo z X_J poddružino X, ki jo določajo indeksi $j \in J$. Z $\langle X_J \rangle$ označimo R-podpolmodul, ki ga generira X_J.

Pravimo, da je družina X *linearno odvisna* natanko tedaj, ko obstajata dve končni disjunktni podmnožici indeksov $I_1 \subset I$ in $I_2 \subset I$, skupaj s skalarji $\lambda_i \in R \setminus \{0\}; i \in I_1 \cup I_2$, da velja:

$$\sum_{i \in I_1} \lambda_i \cdot x_i = \sum_{i \in I_2} \lambda_i \cdot x_i \tag{1}$$

Če X ni linearno odvisna, pravimo, da je *linearno neodvisna*. Naj bo θ enota v M. Linearna neodvisnost je karakterizirana s pogojem:

$$\forall I_1, I_2 \subset I; I_1 \cap I_2 = \emptyset : \langle X_{I_1} \rangle \cap \langle X_{I_2} \rangle = \{\theta\} \tag{2}$$

V [6, definicija 2. 3.] Tan definira linearno neodvisnost v polmodulih nad polkolobarji drugače. Da bo pojma, za katera se izkaže, da ne sovpadata, lažje razločevati, bomo linearno (ne)odvisnost po Tanu imenovali *šibka linearna (ne)odvisnost*. To poimenovanje črpamo iz [3, definicija 2. 12.]. Definicija se glasi takole:

Definicija 3.13. Naj bo R (levi) polkolobar in M polmodul nad R. Množica $X \subseteq M$ je *šibko linearno neodvisna* v M, če za njo velja

$$\forall x \in X : x \notin \langle X \setminus \{x\} \rangle$$

Hitro lahko vidimo, da če je X linearno neodvisna, bo tudi šibko linearno neodvisna. Naj bo M polmodul nad komutativnim polkolobarjem R, naj bo I končna ali števno neskončna indeksna množica ter naj bo $X = (x_i)_{i \in I}$ podmnožica v M. Če je X linearno neodvisna, potem pogledamo posebni primer $I_1 = \{i\}$ in $I_2 = I \setminus \{i\}$. Če za nek $x \in X$ velja $\langle \{x\} \rangle \cap \langle X \setminus \{x\} \rangle = \{\theta\}$, potem sledi $x \notin \langle X \setminus \{x\} \rangle$. Za $\forall i \in I$ potem v posebnem primeru velja $x_i \notin \langle X \setminus \{x_i\} \rangle$, kar pa je v resnici ravno pogoj iz definicije šibke linearne neodvisnosti. Vsaka linearno neodvisna družina X je torej tudi šibko linearno neodvisna, pojem šibke linearne (ne)odvisnosti pa je posledično širši od pojma linearne (ne)odvisnosti po Gondranu in Minouxu. Nad kolobarji sta oba pojma ekvivalentna.

Izkaže se, da implikacija v drugo smer ne velja. Primer, ki to pokaže, se najde v polmodulu $(\mathbb{R} \cup \{-\infty\})^3$ nad tropskim polkolobarjem $(\mathbb{R} \cup \{-\infty\}, \max, +)$, kot nam pokaže zgled iz [3, zgled 2. 14.]. Kot je v zgledu navedeno, je vsaka družina vektorjev oblike $[x_i, 0, -x_i]$ za $i = \{1, 2, \ldots, m\}$ šibko linearno neodvisna za poljuben m in različne x_i. Po drugi strani pa lahko vidmo, da so vektorji $v_i = \begin{bmatrix} i & 0 & -i \end{bmatrix}^\top ; i = 1, 2, 3, 4$ linearno odvisni, saj velja

$$\begin{aligned} 0 \cdot v_2 + (-1) \cdot v_4 &= \begin{bmatrix} \max\{2+0, 4-1\} & \max\{0+0, 0-1\} & \max\{0-2, -4-1\} \end{bmatrix}^\top \\ &= \begin{bmatrix} 3 & 0 & -2 \end{bmatrix}^\top \\ &= \begin{bmatrix} \max\{1-1, 3+0\} & \max\{0-1, 0+0\} & \max\{-1-1, 0-3\} \end{bmatrix}^\top \\ &= (-1) \cdot v_1 + 0 \cdot v_3 \end{aligned}$$

.

Sedaj s sklicem na [6, Definicija 2. 4.] definiramo t. i. šibko bazo polmodula.

Definicija 3.14. Šibko linearno neodvisni družini X v (levem) R-polmodulu M, ki generira cel M ($\langle X \rangle = M$), pravimo *šibka baza*.

Dodatno se za definicijo baze polmodula obrnemo na [4, poglavje 5, definicija 2. 5. 2.].

Definicija 3.15. Pravimo, da je družina X v R-polmodulu $(M, +, \cdot)$ *baza*, če je linearno neodvisna in generira M.

Opomba 3.16. Ker je vsaka linearno neodvisna množica v polmodulu M hkrati tudi šibko linearno neodvisna, je vsaka baza polmodula M hkrati tudi šibka baza.

V [6, definicija 2. 3.] je definiran tudi pojem proste množice in proste baze. V spodnji definicij povzamemo oboje.

Definicija 3.17. Naj bo R (levi) polkolobar. Pravimo, da je neprazna podmnožica X v R-polmodulu M *prosta množica* v M, če za vsak element v M velja, da če ga lahko zapišemo kot linearno kombinacijo elementov v X, je ta zapis enoličen. Podmnožica X R-polmodula M je *prosta baza* (levega) R-polmodula M, če je prosta množica v M in generira cel M. Polmodulu, ki premore kako prosto bazo, pravimo *prosti polmodul*.

Kratek premislek nam pove, da je vsaka prosta množica v M hkrati tudi (šibko) linearno neodvisna. Da to vidimo, se skličemo na definicijo (šibke) linearne neodvisnosti 3.13, ki smo jo pravkar navedli.

Denimo, da je X prosta množica v R-polmodulu M. Vsak element $x \in X$ lahko zapišemo kot linearno kombinacijo elementov iz X kot $x = 1 \cdot x$. Ker je X prosta, je ta zapis enoličen. Če bi bil $x \in \langle X \setminus \{x\} \rangle$ bi to pomenilo, da obstaja neka linearna kombinacija elementov iz $X \setminus \{x\}$, ki je enaka x in v sebi ne vsebuje nobenega člena oblike $\lambda \cdot x$ za nek $\lambda \in R \setminus \{0\}$ (posebej ne vsebuje $1 \cdot x$). Drugače povedano, v M bi lahko x zapisali kot linearno kombinacijo elementov iz X na dva različna načina, kar pa je v protislovju s predpostavko, da je X prosta množica. Sledi torej, da če je X prosta množica v R-polmodulu M, je v M tudi (šibko) linearno neodvisna.

Opazimo tudi, da je linearna odvisnost družine X nad polkolobarjem R usklajena z linearno odvisnostjo množice vektorjev $(v_k)_{k \in K}$ nad poljem F. To, da so v_k linearno odvisni pomeni, da obstaja neka končna poddružina $(v_l)_{l \in L}; L \subset K$ in skalarji $\mu_l \in F \setminus \{0\}$, da je $\sum_{l \in L} \mu_l v_l = 0$. Ker je L končna indeksna množica, jo lahko zapišemo kot unijo dveh (končnih) disjunktnih podmnožic L_1 in L_2. Potem je

$$\sum_{l \in L_1 \cup L_2} \mu_l v_l = \sum_{l \in L_1} \mu_l v_l + \sum_{l \in L_2} \mu_l v_l = 0$$

oz.

$$\sum_{l \in L_1} \mu_l v_l = -\sum_{l \in L_2} \mu_l v_l = \sum_{l \in L_2} (-\mu_l) v_l = \sum_{l \in L_2} \acute{\mu}_l v_l$$

To pa ravno ustreza definiciji linearne odvisnosti v polmodulih.

Torej, če je $(v_k)_{k \in K} \subset M$ linearno odvisna v smislu vektorskega prostora M nad poljem F, je tudi linearno odvisna v smislu polmodula M nad polkolobarjem F.

Opomba 3.18. Vsaka prosta baza je hkrati tudi šibka baza. Poleg tega ima vsak končno generiran levi polmodul kako končno (šibko) bazo.

Zgled 3.19. Vrnimo se k zgledu 3.2. R-polmodul $(R^n, \oplus, \otimes)$ prepoznamo kot končno generiran prosti R-polmodul. Množica $E = \{e1, e2, \ldots, e_n\}$ tvori prosto bazo za R^n, kjer so $e_1 = (1, 0, 0, \ldots, 0)^\top, e_2 = (0, 1, 0, \ldots, 0)^\top, \ldots, e_n = (0, \ldots, 0, 1)^\top$. Razvidno je tudi, da je $r(R^n) = n$. ♢

Sedaj se lahko lotimo klasifikacije baz polmodulov nad komutativnimi polkolobarji, pri čemer se bomo naslonili na izrek iz Tanovega članka [6, izrek 3. 1.].

Izrek 3.20. *Naj bo R polkolobar in M R-polmodul. Če premore M kako neskončno šibko bazo, so vse njegove šibke baze neskončne.*

Dokaz. Naj bo X neskončna šibka baza za M. Če je Y končna šibka baza za M, lahko vsak element iz Y zapišemo kot linearno kombinacijo nekih elementov iz X. Za vsak $y \in Y$ izberemo reprezentacijo $y = \alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \ldots + \alpha_n \cdot x_n$, kjer so $x_1, x_2, \ldots x_n \in X$ in $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$. Z $y(X)$ označimo množico elementov iz X, s katerimi reprezentiramo y. Torej $y(X) = \{x_1, x_2, \ldots, x_n\}$. Z unijo po $y \in Y$ sestavimo novo šibko bazo: $\acute{Y} = \bigcup_{y \in Y} y(X)$. Velja $\acute{Y} \subseteq X$ in $\acute{Y}$ je končna, torej velja $X \setminus \acute{Y} \neq \emptyset$. Očitno lahko vsak element iz Y izrazimo kot linearno kombinacijo elementov iz $\acute{Y}$. Ker lahko vsak element iz X zapišemo kot linearno kombinacijo elementov iz Y (saj je Y tudi šibka baza), lahko vsak element iz X zapišemo kot linearno kombinacijo elementov iz $\acute{Y}$. Potem pa obstaja $x \in X \setminus \acute{Y} \subseteq S$, da je $x \in \left\langle \acute{Y} \right\rangle \subseteq \langle X \setminus \{x\} \rangle$. Ta zadnji sklep je pa v protislovju s tem, da je X šibko linearno neodvisna. Torej je vsaka druga šibka baza M neskončna. □

Prejšnji izrek nam pove še to, da če ima M končno šibko bazo, so vse njegove šibke baze končne. Ker vsi končno generirani R-polmoduli premorejo vsaj eno končno šibko bazo velja, da je vsaka šibka baza končno generiranega R-polmodula končna.

V nadaljevanju tega podpoglavja se bomo posvetili bazam nad dioidi, kot sta to obravnavala Gondran in Minoux v [4, poglavje 5. 2. 5.]. Za to moramo najprej definirati t. i. »razcepnost« vektorja.

Definicija 3.21. Naj bo $(M, +, \cdot)$ levi polmodul nad polkolobarjem $(R, \oplus, \otimes)$ in denimo, da imamo dano neko množico vektorjev $V = (V_k)_{k\in K}$, kjer je $V_k \in M$ za vsak $k \in K$. Vektor x je *razcepen* na $\langle V\rangle$ natanko tedaj, ko obstajata taka vektorja $y, z \in \langle V\rangle$, ki sta oba različna od x, da velja $x = y + z$. V primeru ko x ni razcepen, pravimo da je *nerazcepen*.

Iz definicije hitro razberemo, da razcepnost implicira vsebovanost v $\langle V\rangle$, od tod pa sledi naslednja trditev.

Trditev 3.22. *Če je x nerazcepen na $\langle V\rangle$, potem zanj velja natanko ena od naslednjih lastnosti:*

(i) $x \notin \langle V\rangle$
(ii) $x = y + z$ *za* $y, z \in \langle V\rangle \Rightarrow x = y$ *ali* $x = z$

S pomočjo trditve 3.22 lahko zapišemo in dokažemo naslednjo trditev.

Trditev 3.23. *Naj bo $(R, \oplus, \otimes)$ dioid in označimo $z\,0$ nevtralni element za $\oplus$ ter $z\,1$ nevtralni element za $\otimes$. Denimo dodatno, da velja: $r \oplus p = 1 \Rightarrow r = 1$ ali $p = 1$. Naj bo $(M, +, \cdot)$ R-moduloid, ki je kanonično urejen glede na $+$. $Z \propto$ označimo kanonično delno urejenost na M. Dodatno predpostavimo, da za $x, y \in M$, ki zadoščata pogojem $x \neq y$ & $y \neq \theta$ in $\lambda \in R$ velja:*

$$y = \lambda \cdot y + x \Rightarrow \lambda = 1$$

Trdimo, da če veljajo omenjene predpostavke, za linearno neodvisno družino $X = (x_i)_{i\in I}$ elementov iz M (kjer velja $x_i \neq \theta\ \forall i \in I$) velja, da je za vsak indeks $j \in I$ element x_j nerazcepen nad $\langle X\rangle$.

Dokaz. Očitno velja za vsak $j \in I$, da je $x_j \in \langle X\rangle$. Denimo, da je $x_j = y + z$ za neka $y, z \in \langle X\rangle$. To implicira $y \propto x_j$ in $z \propto x_j$. Ker je $y \in \langle X\rangle$, sledi, da obstaja indeksna podmnožica $I_1 \subset I$ in skalarji $\lambda_i \in R \setminus \{0\}$, da je $y = \sum_{i\in I_1} \lambda_i \cdot x_i$.

Podobno to, da je $z \in \langle X\rangle$ implicira obstoj podmnožice indeksov $I_2 \subset I$ in skalarjev $\mu_i \in R \setminus \{0\}$, da je $z = \sum_{i\in I_2} \mu_i \cdot x_i$.

Skalarje λ_i in μ_i razširimo na $I_1 \cup I_2$ tako, da določimo $\lambda_i = 0$ za vsak $i \in I_2 \setminus I_1$ ter $\mu_i = 0$ za vsak indeks $i \in I_1 \setminus I_2$. Potem lahko zapišemo naslednjo enakost:

$$x_j = \sum_{i\in I_1\cup I_2} (\lambda_i \oplus \mu_i) \cdot x_i$$

Opazimo, da mora biti $j \in I_1 \cup I_2$, saj sicer pridemo v protislovje s predpostavko, da je X linearno neodvisna. Posledično:

$$x_j = (\lambda_j \oplus \mu_j) \cdot x_j + \sum_{i\in(I_1\cup I_2)\setminus\{j\}} (\lambda_i \oplus \mu_i) \cdot x_i$$

kjer $\lambda_j \oplus \mu_j \neq 0$. Označimo $\lambda = \lambda_j \oplus \mu_j$ in $w = \sum_{i\in(I_1\cup I_2)\setminus\{j\}} (\lambda_i \oplus \mu_i) \cdot x_i$. Vidimo: $w \in \langle X \setminus \{x_j\}\rangle$. Od tod dobimo enakost:

$$x_j = \lambda \cdot x_j + w, \text{ za } \lambda \in R \setminus \{0\} \text{ in } w \in \langle X \setminus \{x_j\}\rangle$$

Vemo, da $x_j \neq \theta$ in zaradi linearne neodvisnosti X vemo tudi, da $w \neq x_j$ in posledično $\lambda \neq 0$. Potem po predpostavki trditve velja, da je $\lambda = 1$ in ker je $\lambda = \lambda_j \oplus \mu_j$ sledi, $\lambda_j = 1$ ali $\mu_j = 1$.

Denimo, da je $\mu_j = 1$. Potem lahko z zapišemo kot $z = x_j + \sum_{i \in I_2 \setminus \{j\}} \mu_i \cdot x_i$. Od tod sledi $x_j \propto z$ in ker je $\propto$ relacija delne urejenosti, sledi, da je $z = x_j$. Podobno, če je $\lambda_i = 1$ pridemo do razultata $y = x_j$.

Po drugi točki posledice 3.22 je potem x_j nerazcepen. □

Sedaj lahko s pomočjo dokazane trditve povemo, kdaj bo moduloid imel enolično določeno bazo.

Trditev 3.24. *Denimo, da veljajo vse predpostavke trditve 3.23 in naj poleg tega velja še* $r, p \in R : r \otimes p = 1 \Rightarrow r = 1$ *in* $p = 1$. *Potem, če ima* $(M, +, \otimes)$ *bazo, je enolično določena.*

Dokaz. Denimo, da ima M dve bazi $X = (x_i)_{i \in I}$ in $Y = (y_j)_{j \in J}$.

To, da sta X in Y bazi nad M implicira, da lahko zapišemo

$$x_i = \sum_{j \in J} \mu_j^i \cdot y_j$$

. Po trditvi 3.23 so potem, ker sta X in Y linearno neodvisni, vsi x_i in prav tako vsi y_j nerazcepni elementi nad $M = \langle X \rangle = \langle Y \rangle$. Posledično obstaja tak indeks $j \in J$, da je $x_i = \mu_j^i \cdot y_j$ za nek $\mu_j^i \in R$ in $y_j \in Y$.

Na enak način pokažemo, da obstaja indeks $k \in I$, da je $y_j = \nu_k^j \cdot x_k$, za nek $\nu_k^j \in R$ in $x_k \in X$.

Torej je $x_i = (\mu_j^i \otimes \nu_k^j) \cdot x_k$. Ker je X linearno neodvisna družina, je nujno $i = k$. Po predpostavki iz trditve 3.23 je tudi $(\mu_j^i \otimes \nu_k^j) = 1$, iz predpostavke te trditve pa potem sledi $\mu_j^i = 1$ in $\nu_k^j = 1$ in posledično $x_i = y_j$.

Torej za vsak $x_i \in X$ lahko najdemo $y_j \in Y$, da je $x_i = y_j$, od koder pa sledi $X = Y$. □

4. Matrike:

Kot smo že videli lahko, podobno kot za vektorske prostore in module, tudi polmodulu pod določenimi pogoji določimo baze in mu tudi dodelimo »dimenzijo« (rang polmodula) preko kardinalnosti najmanjše družine, ki ga generira. V tem poglavju bomo najprej uvedli osnovne definicije in obravnavali obrnljivost matrik, nato bomo obravnavali prehodne matrike med bazami polmodula, na koncu pa bomo nekaj pozornosti posvetili še lastnim vrednostim.

4.1. Definicije in osnove obrnljivosti.

Kot že vemo, lahko tudi nad polmoduli izvajamo linearne preslikave, ki so definirane na enak način, kot na vektorskih prostorih. Preslikava $\mathbb{L} : M \mapsto \grave{M}$ je linearna, če je aditivna in homogena.

Sedaj bomo nad polkolobarjem $(R, +, \cdot)$ uvedli tudi $m \times n$ 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 $A \in M_{m \times n}(R), B \in M_{n \times l}(R)$:

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

Pri množenju moramo seveda biti pozorni na to, da tukaj nimamo komutativnosti. Enota za seštevanje je seveda kar t. i. ničelna matrika 0, kjer je vsak element aditivna

enota iz polkolobarja, za množenje pa je enota kar matrika I, ki ima na diagonali multiplikativno enoto, izven diagonale pa aditivno. K seštevanju in množenju še dodamo množenje s skalarjem: $\lambda \cdot A = [\lambda \otimes a_{ij}]_{ij}$

Hitro se da preveriti, da če je R polkolobar, je tudi množica kvadratnih matrik $M_n(R) = M_{n\times n}$ nad R, opremljena s prej definiranima operacijama, polkolobar. Dodatno, če je R dioid, je tudi $M_n(R)$ dioid.

Vsaki matriki $A \in M_{m\times n}(R)$ lahko tudi priredimo transponiranko na enak način kot v klasični linearni algebri. Označimo jo z $A^\top$.

Definirajmo sedaj, kdaj je matrika nad komutativnim polkolobarjem obrnljiva.

Definicija 4.1. Kvadratna matrika $A \in M_n(R)$ je levo obrnljiva, če obstaja taka matrika $B \in M_n(R)$ za katero velja $B*A = I_n$ in desno obrnljiva, če velja $A*B = I_n$. Če obstaja, matriki B pravimo levi (oziroma desni) inverz matrike A v $M_n(R)$. Če je A hkrati levo in desno obrnljiva, pravimo samo, da je obrnljiva. V tem primeru je levi inverz hkrati tudi desni inverz in v imenu opustimo smeri (torej mu pravimo samo inverz). Ta inverz je očitno enoličen, označimo pa ga z A^{-1}.

Tako kot v klasični linearni algebri se lahko tudi tukaj vprašamo kdaj je neka matrika obrnljiva. Izkaže se, da je odgovor delno odvisen od lastnosti polkolobarja nad katerim tvorimo matriko. Da lahko pridemo do obrnljivosti, bomo potrebovali komutativnost množenja.

Pri obravnavi tega vprašanja nam bosta pomagali že dokazana lema 2.16 ter naslednja lema.

Izrek 4.2. *Naj bo R komutativen polkolobar in naj bosta A in B kvadratni $n \times n$ matriki nad R. Če velja $A * B = I_n$ velja tudi $B * A = I_n$.*

Izreka 4.2 v tem delu ne bomo dokazali, bomo ga pa privzeli kot veljavnega. Dva dokaza se nahajata v [1, poglavje 3 in poglavje 4].

Sedaj lahko zapišemo naslednjo trditev in dokaz, oba povzeta po [6, lema 2. 3.].

Trditev 4.3. *Naj bo R komutativen polkolobar v katerem 1 ni aditivno obrnljiva in velja $1 = u \oplus v \Rightarrow u \in U(R) \vee v \in U(R)\ \forall u, v \in R$. Naj bo $A \in M_n(R)$. Če so diagonalni elementi matrike A multiplikativno obrnljivi v R (torej $a_{ii} \in U(R)\ \forall i \in \{1, \ldots, n\}$) in če so vsi izvendiagonalni elementi v A aditivno obrnljivi ($a_{i,j} \in V(R)\ \forall i, j \in \{1, \ldots, n\}\ ;\ i \neq j$), potem je A obrnljiva.*

Dokaz. Dokaz bomo izvedli po indukciji na n. Za primer, ko je $n = 1$, trditev očitno drži. Naj bo n sedaj poljubno od 1 večje naravno število in denimo, da trditev drži za $n - 1$. Denimo, da je $A \in M_n(R)$ taka, da zadošča zahtevam trditve in z E_{ij} označimo $n \times n$ matriko, ki ima na mestu (i, j) multiplikativno enoto iz R, povsod drugje pa aditivno enoto iz R (torej $a_{ij} = 1$ in $a_{kl} = 0$ za $k \neq i \wedge l \neq j$). Sedaj definiramo matriki P in Q s predpisoma $P = I_n + \sum_{i=2}^{n}((-a_{i1}) \otimes a_{11}^{-1}) \cdot E_{i1}$ ter $Q = I_n + \sum_{j=2}^{n}((-a_{1j}) \otimes a_{11}^{-1}) \cdot E_{1j}$. Hitro se da videti, da sta P in Q obe obrnljivi matriki z inverzoma $P^{-1} = I_n + \sum_{i=2}^{n}(a_{i1} \otimes a_{11}^{-1}) \cdot E_{i1}$ in $Q^{-1} = I_n + \sum_{j=2}^{n}(a_{1j} \otimes a_{11}^{-1}) \cdot E_{1j}$. Sedaj zmnožimo P z A in Q in v zmnožku zapišemo A kot linearno kombinacijo

matrik tipa E_{ij}.

$$
\begin{aligned}
&P * A * Q = \\
&= \left(I_n + \sum_{i=2}^{n}(-a_{i1})a_{11}^{-1} \cdot E_{i1}\right) * \left(\sum_{s,t=1}^{n} a_{st} \cdot E_{st}\right) * \left(I_n + \sum_{j=2}^{n}(-a_{1j})a_{11}^{-1} \cdot E_{1j}\right) = \\
&= \left(\sum_{s,t=1}^{n} a_{st} \cdot E_{st} + \sum_{i=2}^{n}\sum_{t=1}^{n}(-a_{i1})a_{11}^{-1}a_{1t} \cdot E_{it}\right) * \left(I_n + \sum_{j=2}^{n}(-a_{1j})a_{11}^{-1} \cdot E_{1j}\right) = \\
&= \sum_{s,t=1}^{n} a_{st} \cdot E_{st} + \sum_{i=2}^{n}\sum_{t=1}^{n}(-a_{i1})a_{11}^{-1}a_{1t} \cdot E_{it} + \sum_{s=1}^{n}\sum_{j=2}^{n} a_{s1}(-a_{1j})a_{11}^{-1} \cdot E_{sj} + \\
&+ \sum_{i=2}^{n}\sum_{j=2}^{n}(-a_{i1})(-a_{1j})a_{11}^{-1} \cdot E_{it}
\end{aligned}
$$

Na tej točki uporabimo lemo 2.16 znotraj vsot in zamenjamo indekse s z i in t z j v sredinskih dveh vsotah.

$$
\begin{aligned}
&P * A * Q = \\
&= \sum_{i,j=1}^{n} a_{ij} \cdot E_{ij} + \sum_{i=2}^{n}\sum_{j=1}^{n}(-a_{i1}a_{11}^{-1}a_{1j}) \cdot E_{ij} + \\
&+ \sum_{i=1}^{n}\sum_{j=2}^{n}(-a_{i1}a_{1j}a_{11}^{-1}) \cdot E_{ij} + \sum_{i=2}^{n}\sum_{j=2}^{n}(a_{i1}a_{1j}a_{11}^{-1}) \cdot E_{ij} = \\
&= \sum_{i,j=1}^{n} a_{ij} \cdot E_{ij} + \sum_{j=2}^{n}(-a_{1j}) \cdot E_{1j} + \sum_{i=2}^{n}(-a_{i1}) \cdot E_{i1} + \sum_{i=2}^{n}\sum_{j=2}^{n}(-a_{i1}a_{1j}a_{11}^{-1}) \cdot E_{ij} = \\
&= a_{11} \cdot E_{11} + \sum_{i=2}^{n}\sum_{j=2}^{n} a_{ij} \cdot E_{ij} + \sum_{j=2}^{n} a_{1j} \cdot E_{1j} + \sum_{i=2}^{n} a_{i1} \cdot E_{i1} + \\
&+ \sum_{j=2}^{n}(-a_{1j}) \cdot E_{1j} + \sum_{i=2}^{n}(-a_{i1}) \cdot E_{i1} + \sum_{i=2}^{n}\sum_{j=2}^{n}(-a_{i1}a_{1j}a_{11}^{-1}) \cdot E_{ij} = \\
&= a_{11} \cdot E_{11} + \sum_{i=2}^{n}\sum_{j=2}^{n}(a_{ij} \oplus (-a_{i1}a_{1j}a_{11}^{-1})) \cdot E_{ij}
\end{aligned}
$$

Razpišimo sedaj, kar smo dobili, v obliki matrike.

$$
P * A * Q = \begin{bmatrix}
a_{11} & 0 & \cdots & 0 \\
0 & a_{22} \oplus (-a_{21}a_{12}a_{11}^{-1}) & \cdots & a_{2n} \oplus (-a_{21}a_{1n}a_{11}^{-1}) \\
\vdots & \vdots & \ddots & \vdots \\
0 & a_{n2} \oplus (-a_{n1}a_{12}a_{11}^{-1}) & \cdots & a_{nn} \oplus (-a_{n1}a_{1n}a_{11}^{-1})
\end{bmatrix}
$$

Za $A1$ označimo matriko

$$
\begin{bmatrix}
a_{22} \oplus (-a_{21}a_{12}a_{11}^{-1}) & \cdots & a_{2n} \oplus (-a_{21}a_{1n}a_{11}^{-1}) \\
\vdots & \ddots & \vdots \\
a_{n2} \oplus (-a_{n1}a_{12}a_{11}^{-1}) & \cdots & a_{nn} \oplus (-a_{n1}a_{1n}a_{11}^{-1})
\end{bmatrix}
$$

Upoštevamo, da za $i \neq j$ element $a_{ij} \oplus (-a_{i1}a_{1j}a_{11}^{-1})$ pripada $V(R)$, saj je $V(R)$ ideal v R. Označimo tudi $r_i = a_{ii} \oplus (-a_{i1}a_{1i}a_{11}^{-1})$. Potem lahko izračunamo a_{ii} kot $a_{ii} = a_{i1}a_{1i}a_{11}^{-1} \oplus r_i$. Ker je, po predpostavki, $a_{ii} \in U(R)$, lahko enačbo delimo z leve z

a_{ii}^{-1} in dobimo $1 = a_{ii}^{-1}a_{i1}a_{1i}a_{11}^{-1} \oplus a_{ii}^{-1}r_i$, od koder sklepamo, da je eden izmed členov na desni strani enačaja multiplikativno obrnljiv. Denimo, da je $a_{ii}^{-1}a_{i1}a_{1i}a_{11}^{-1} \in U(R)$. Potem je tudi $a_{i1} \in U(R)$, a hkrati je po predpostavki $a_{i1} \in V(R)$. Enačbo $a_{i1} \oplus (-a_{i1}) = 0$ pomnožimo z leve z a_{i1}^{-1} in dobimo $1 \oplus a_{i1}^{-1}(-a_{i1}) = 0$, od koder sledi, da je $1 \in V(R)$, kar pa je v protislovju z eno izmed predpostavk trditve. Sledi, da more biti $a_{ii}^{-1}r_i \in U(R)$ in posledično je tudi $r_i \in U(R)$. Po indukcijski predpostavki je potem $A1$ obrnljiva $(n-1) \times (n-1)$ matrika in velja tudi, da je $\begin{bmatrix} a_{11} & 0 \\ 0 & A1 \end{bmatrix}$ obrnljiva, saj je a_{11} multiplikativno obrnljiv. Uspelo nam je pokazati, da je $P * A * Q = \begin{bmatrix} a_{11} & 0 \\ 0 & A1 \end{bmatrix}$ obrnljiva v $M_n(R)$, torej je tudi $A = P^{-1} * \begin{bmatrix} a_{11} & 0 \\ 0 & A1 \end{bmatrix} * Q^{-1}$ obrnljiva matrika. □

4.2. **Prehodne matrike.** Matrike imajo v klasični linearni algebri pomembno povezavo z bazami, saj je slika vsakega baznega vektorja je spet bazni vektor. Prehajanje med bazami omogoča pogled na določen problem z druge perspektive, kar lahko včasih problem poenostavi. Te prehode tipično izvedemo s t. i. prehodnimi matrikami. Te bomo obravnavali v primeru polmodulov v tem podpoglavju. Pri tem se bomo naslanjali na [6, poglavje 3].

Denimo, da je M končno generiran (levi) R-polmodul in naj bo $T = \{t_1, \ldots, t_n\}$ šibka baza M. Dodatno, naj bo $S \subseteq M$ neka končna podmnožica v M, recimo $S = \{s_1, \ldots, s_m\}$. Za vsak element v S velja, da ga lahko zapišemo kot linearno kombinacijo elementov iz T.

$$\begin{aligned} s_1 &= a_{11}t_1 \oplus a_{21}t_2 \oplus \ldots \oplus a_{n1}t_n \\ s_2 &= a_{12}t_1 \oplus a_{22}t_2 \oplus \ldots \oplus a_{n2}t_n \\ &\ldots \\ s_m &= a_{1m}t_1 \oplus a_{2m}t_2 \oplus \ldots \oplus a_{nm}t_n \end{aligned}$$

Če kvociente a_{ij} združimo v matriko $A \in M : n \times m(R)$ lahko zgornje linearne kombinacije zapišemo v matrični obliki:

$$(s_1, s_2, \ldots, s_m) = (t_1, t_2, \ldots, t_n) * A$$

To nas privede do naslednje definicije.

Definicija 4.4. Naj bo M končno generiran (levi) R-polmodul in naj bosta T in S njegovi šibki bazi. Matriki A, ki slika elemente šibke baze T v S, pravimo prehodna matrika iz šibke baze T v S. Med dvema šibkima bazama lahko obstaja več različnih prehodnih matrik.

Na tej točki definiramo še t. i. faktorski rang matrike, saj bo ta pojem relevanten v naslednji trditvi.

Definicija 4.5. Naj bo $A \in M_{m\times n}(R)$ poljubna $m \times n$ matrika nad komutativnim polkolobarjem R. Najmanjšemu naravnemu številu k, za katerega velja, da je $A = B * C$ za neka $B \in M_{m\times k}(R)$ in $C \in M_{k\times n}(R)$, pravimo faktorski rang matrike A in ga označimo z $\rho_s(A)$.

Za prehodne matrike med bazami končno generiranega R-polmodula M bomo sedaj pokazali, da so njihovi faktorski rangi povezani z $r(M)$.

Izrek 4.6. *Naj bo M R-polmodul ranga r nad komutativnim polkolobarjem R, in naj bosta S in T njegovi šibki bazi. Potem za vsako prehodno matriko A iz T v S velja, da je njen faktorski rang najmanj r, torej $r \leq \rho_s(A)$. Poleg tega med šibkima bazama obstaja prehodna matrika $\widehat{A}$, za katero je $r = \rho_s(\widehat{A})$.*

Dokaz. Naj bo A poljubna $n \times m$ prehodna matrika iz $T = \{t_1, \ldots, t_n\}$ v $S = \{s_1, \ldots, s_m\}$ in naj bo $\rho_s(A) = k$. Potem je, po definiciji faktorskega ranga, $A = B * C$ za neki matriki $B \in M_{n\times k}(R)$ in $C \in M_{k\times m}(R)$. Označimo $\gamma_l = \sum_{j=1}^{n} b_{jl} \cdot t_j$ za vsak $l \in \{1, \ldots, k\}$. Sestavimo množico Γ, ki vsebuje vse γ_l, torej $\Gamma = \{\gamma_1, \ldots, \gamma_k\}$. Očitno je Γ podmnožica v M.

Sedaj zapišemo elemente v S kot linearne kombinacije elementov iz T. Za vsak indeks $i \in \{1, \ldots m\}$ je $s_i = \sum_{j=1}^{n} a_{ji} \cdot t_j$. Sedaj upoštevamo, da lahko A zapišemo kot produkt B in C in dobimo:

$$s_i = \sum_{j=1}^{n} \left(\sum_{l=1}^{k} b_{jl} c_{li} \right) \cdot t_j = \sum_{j=1}^{n} \sum_{l=1}^{k} b_{jl} c_{li} \cdot t_j = \sum_{l=1}^{k} \sum_{j=1}^{n} c_{li} b_{jl} \cdot t_j = \sum_{l=1}^{k} c_{li} \left(\sum_{j=1}^{n} b_{jl} \cdot t_j \right)$$

V oklepaju prepoznamo γ_l, torej nam je uspelo zapisati $s_i = \sum_{l=1}^{k} c_{li}\gamma_l$ za vsak $i \in \{1, \ldots, m\}$. Od tod sledi, da Γ generira S in posledično tudi M, saj S generira M. Potem pa je $r = r(M) \leq k = \rho_s(A)$. in s tem smo pokazali prvi del trditve.

Da dokažemo drugi del trditve, najprej upoštevamo definicijo ranga polmodula. Ker je $r(M) = r$, obstaja neka šibka baza Γ od M, da velja $|\Gamma| = r$. Naj bo $\Gamma = \{\gamma_1, \ldots, \gamma_r\}$ ter naj bo $B \in M_{n\times r}(R)$ prehodna matrika iz T v Γ. Poleg tega naj bo $C \in M_{r\times m}$ prehodna matrika iz Γ v S. Zapis $(\gamma_1, \gamma_2, \ldots, \gamma_r) = (t_1, t_2, \ldots, t_n) * B$ vstavimo v $(s_1, s_2, \ldots, s_m) = (\gamma_1, \gamma_2, \ldots, \gamma_r) * C$ in s tem pridobimo zapis

$$(s_1, s_2, \ldots, s_m) = (t_1, t_2, \ldots, t_n) * B * C$$

Označimo $B * C = \widehat{A}$ in takoj vidimo, da je $\widehat{A}$ prehodna matrika med T in S za katero je $\rho_s(\widehat{A}) \leq r$. Po drugi strani pa nam prvi del trditve pove, da je $r \leq \rho_s(\widehat{A})$. Sledi, da je $\rho_s(\widehat{A}) = r$ in s tem je dokazan tudi drugi del trditve. □

Za naslednjo trditev se spomnimo definicije prostega (levega) R-polmodula v 3.14. Polmodul (levi, desni ali obojestranski) M nad polkolobarjem R je prost, če premore kako prosto bazo.

Trditev 4.7. *Naj bo R komutativen polkolobar in M končno generiran prost R-polmodul. Potem za poljubno šibko bazo S polmodula M in za poljubno prosto bazo T polmodula M velja $|T| \leq |S|$.*

Dokaz. Ker je M končno generiran, ima neko končno šibko bazo, torej sta tako T kot S končni. Naj bo $S = \{s_1, \ldots, s_m\}$ in $T = \{t_1, \ldots, t_n\}$ ter naj bo $A \in M_{n\times m}(R)$ prehodna matrika iz T v S ter $B \in M_{m\times n}(R)$ prehodna matrika iz S v T. Potem je

$$(s_1, s_2, \ldots, s_m) = (t_1, t_2, \ldots, t_n) * A$$

in

$$(t_1, t_2, \ldots, t_n) = (s_1, s_2, \ldots, s_m) * B$$

Ko to dvoje združimo dobimo, da je $(t_1, t_2, \ldots, t_n) = (t_1, t_2, \ldots, t_n) * A * B$ in ker je T prosta baza sledi, da je $A * B = I_n$. Denimo sedaj, da je $m < n$ in naj bosta $O_1 \in M_{n\times(n-m)}(R)$ in $O_2 \in M_{(n-m)\times m}(R)$ ničelni matriki. Sedaj sestavimo matriki $A_1 = \begin{bmatrix} A & O_1 \end{bmatrix}$ in $B_1 = \begin{bmatrix} B \\ O_2 \end{bmatrix}$, ki sta obe kvadratni $n \times n$ matriki nad R. Poleg tega

je tudi $A_1 * B_1 = A * B = I_n$ in ker je R komutativen po izreku 4.2 sledi $B_1 * A_1 = I_n$. Toda če dejansko poračunamo ta produkt, dobimo

$$B_1 * A_1 = \begin{bmatrix} B \\ O_2 \end{bmatrix} * \begin{bmatrix} A & O_1 \end{bmatrix} = \begin{bmatrix} B * A & 0 \\ 0 & 0 \end{bmatrix}$$

ker je po predpostavki $m < n$, dobljena matrika ni enaka I_n. Prišli smo v protislovje, torej more veljati $n \leq m$ oz. $|T| \leq |S|$. □

S pomočjo te trditve bomo sedaj karakterizirali proste baze v končno generiranih polmodulih nad komutativnimi polkolobarji.

Izrek 4.8. *Naj bo R komutativen polkolobar in M naj bo prost R-polmodul z rangom $r(M) = r$ in prosto bazo T. Za poljubno šibko bazo S polmodula M so naslednje trditve ekvivalentne:*

i. S je prosta baza v M
ii. $|S| = r$
iii. prehodna matrika med T in S je enolično določena in obrnljiva

Dokaz. Kombinacija definicije ranga polmodula in trditve 4.7 nam pove, da je $|T| = r(M) = r$ za prosto bazo $T = \{t_1, \ldots, t_r\}$.

$i \Rightarrow ii$: sledi po izreku 4.7.

$ii \Rightarrow iii$: Denimo, da je $|S| = r$ in naj bo potem $S = \{s_1, \ldots, s_r\}$. Naj bo A prehodna matrika med T in S ter naj bo B prehodna matrika med S in T. Na enak način kot v trditvi 4.7 potem vidimo, da velja $(t_1, t_2, \ldots, t_r) = (t_1, t_2, \ldots, t_r) * A * B$, od koder sledi, da je $A * B = I_r$. Ponovno se skličemo na izrek 4.2, po katerem je tudi $B * A = I_r$. Sledi, da je A obrnljiva $r \times r$ matrika nad R. Denimo sedaj, da imamo dve prehodni matriki med T in S, A_1 ter A_2. Potem velja $(s_1, s_2, \ldots, s_r) = (t_1, t_2, \ldots, t_r) * A_1$ in $(s_1, s_2, \ldots, s_r) = (t_1, t_2, \ldots, t_r) * A_2$, od tod pa sklepamo da je $(t_1, t_2, \ldots, t_r) * A_1 = (t_1, t_2, \ldots, t_r) * A_2$. Sledi, da je $A_1 = A_2$, s tem pa smo dokazali iii.

$iii \Rightarrow i$: Denimo, da je prehodna matrika A med šibkima bazama T in S obrnljiva. Potem je $|S| = |T| = r$ in tudi $A \in M_r(R)$. Poleg tega tudi obstaja neka matrika $B \in M_r(R)$, da je $A * B = I_r$, saj je A obrnljiva. Pišemo $S = \{s_1, \ldots, s_r\}$ in potem je $(s_1, s_2, \ldots, s_r) = (t_1, t_2, \ldots, t_r) * A$. Vzemimo nek poljuben element $v \in M$ in ga razvijmo po šibki bazi S na dva načina (saj v splošni šibki bazi nimamo nujno enoličnega zapisa). Torej je $v = \sum_{i=1}^{r} \alpha_i \cdot s_i = \sum_{i=1}^{r} \beta_i \cdot s_i$ za neke skalarje $\alpha_i, \beta_i \in R \forall i \in \{1, \ldots, r\}$. Te linearne kombinacije lahko zapišemo v matrični (v resnici vektorski) obliki:

$$v = (s_1, s_2, \ldots, s_r) * \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_r \end{bmatrix} = (s_1, s_2, \ldots, s_r) * \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_r \end{bmatrix}$$

V ta izraz vstavimo $(s_1, s_2, \ldots, s_r) = (t_1, t_2, \ldots, t_r) * A$ in tako dobimo

$$v = (t_1, t_2, \ldots, t_r) A \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_r \end{bmatrix} = (t_1, t_2, \ldots, t_r) A \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_r \end{bmatrix}$$

in ker je T prosta baza sledi $A * \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_r \end{bmatrix} = A * \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_r \end{bmatrix}$, od koder pa sklepamo, da velja tudi $B*A* \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_r \end{bmatrix} = B*A* \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_r \end{bmatrix}$. Ker je B inverz od A se spomnimo, da je $B*A = I_r$, torej od tod sledi $\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_r \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_r \end{bmatrix}$, torej je $\alpha_i = \beta_i \ \forall i \in \{1, \ldots, r\}$. Pokazali smo torej, da se da vsak element iz M razviti po šibki bazi S na en sam način, torej je S prosta baza. □

Iz izreka 4.8 sledita dve posledici, ki ju bomo sedaj navedli.

Posledica 4.9. *Naj bo R komutativen polkolobar in M končno generiran prost R-polmodul. Naslednji trditvi sta ekvivalentni:*

(1) Vse šibke baze M imajo enako kardinalnost.
(2) Vsaka šibka baza M je prosta baza.

Vemo, da je za komutativen polkolobar R polmodul R^n prost in končno generiran. Iz posledice 4.9 potem sledi naslednja posledica.

Posledica 4.10. *Naj bo R komutativen polkolobar. V R-polmodulu R^n imajo vse šibke baze enako kardinalnost natanko tedaj ko je vsaka šibka baza prosta.*

O bazah nad polmoduli se da povedati še marsikaj, a ker to ni tema te naloge bomo te rezultate, ki so sicer dostopni v [6], opustili.

4.3. **lastne vrednosti.** Spodobi se, da vsaj omenimo lastne vrednosti in lastne vektorje, saj imajo ti izjemen pomen v klasični linearni algebri. V temo se ne bomo preveč poglobili, saj bi lahko tej temi posvetili lastno diplomsko nalogo. Vseeno bomo pa vsaj definirali koncepta in dokazali dva elementarna rezultata. Pri tem se bomo sklicevali na [4, poglavje 6].

Naj bo $(R, \oplus, \otimes)$ polkolobar in obravnavamo R-polmodul $M = R^n$ kot v zgledu 3.2. Naj bo $h : M \to M$ endomorfizem R-polmodulov. Vsak vektor $v \in M$ lahko zapišemo kot linearno kombinacijo $v = \sum_{i=1}^{n} v_i \cdot e_i$, kjer so e_i vektorji, ki imajo na i-tem mestu multiplikativno enoto 1, na vseh ostalih komponentah pa aditivno enoto 0. Vidimo, da je endomorfizem h natanko določen s slikami vektorjev e_i, torej $h(e_1), h(e_2), \ldots, h(e_n)$, oziroma z matriko $A \in M_n(R)$, ki ima za stolpce vektorje $h(e_1), \ldots, h(e_n)$. V tem primeru za vsak $x \in M$ velja zapis $h(x) = A * x$, kjer je produkt med matriko A in vektorjem x definiran s predpisom $\forall i \in \{1, 2, \ldots, n\}$; $(A* x)_i = \sum_{j=1}^{n} a_{ij} \otimes x_j$, kot smo navajeni.

Definicija 4.11. Naj bo R polkolobar in $M = R^n$ R-polmodul. Naj bo $A \in M_n(R)$ matrika, ki pripada endomorfizmu $h : M \to M$. Pravimo, da je λ *lastna vrednost* matrike A, če obstaja tak vektor $v \in M \setminus \{0\}$, da velja $A * v = \lambda \cdot v$. Vektorju v previmo *lastni vektor* matrike A za lastno vrednost λ.

Trditev 4.12. *Naj bo R komutativen polkolobar in naj bo L_λ množica lastnih vektorjev, ki pripadajo lastni vrednosti λ. Potem je $(L_\lambda, +)$ R-podpolmodul v M. L_λ pravimo lastni R-podpolmodul R-polmodula M.*

Dokaz. Vzemimo torej poljubna skalarja $\alpha, \beta \in R$ in poljubna vektorja X in Y iz L_λ ter poglejmo, kaj lahko povemo o vektorju $\alpha \cdot X + \beta \cdot Y$.

$$A(\alpha \cdot X + \beta \cdot Y) = \alpha \cdot A(X) + \beta \cdot A(Y) = \alpha \cdot \lambda \cdot X + \beta \cdot \lambda \cdot Y = \lambda \cdot (\alpha \cdot X + \beta \cdot Y)$$

To pomeni, da je tudi $(\alpha \cdot X + \beta \cdot Y) \in L_\lambda$. Potem je pa očitno $(L_\lambda, +, \cdot)$ t. i. lastni R-polmodul za lastno vrednost λ. Še več, vidimo, da smo v resnici pokazali, da je $(L_\lambda, +, \cdot)$ R-podpolmodul v $(M, +, \cdot)$ in to za vsako lastno vrednost λ poljubne matrike $A \in M_n(R)$. □

Trditev 4.13. *Naj bo R komutativen polkolobar in naj bo $\otimes$ idempotentna operacija (torej $a \otimes a = a \ \forall a \in R$). Naj bo $M = R^n$ R-polmodul in $A : M \to M$ naj bo $n \times n$ matrika, ki pripada nekemu endomorfizmu M. Če je tedaj $v \in M$ lastni vektor za 1, je $\lambda \cdot v$ lastni vektor matrike A za lastno vrednost λ.*

Dokaz. Po predpostavki je $A * v = v$. Hkrati velja $A * (\lambda \cdot v) = \lambda \cdot (A * v) = \lambda \cdot v$. Na tej točki upoštevamo idempotentnost množenja v R in opazimo $\lambda = \lambda \otimes \lambda$. Potem je $\lambda \cdot v = (\lambda \otimes \lambda) \cdot v = \lambda \cdot (\lambda \cdot v)$, torej je $\lambda \cdot v$ lastni vektor matrike A za lastno vrednost λ. □

Za konec še pokažimo, kako lahko matriki nad komutativnim dioidom določimo lastne vrednosti, kot je bilo to storjeno v [4, poglajve 6, izrek 6]

Izrek 4.14. *Naj bo $(R, \oplus, \otimes)$ komutativen dioid in naj bo $A \in M_n(R)$. Za poljubno $\lambda \in R$ definiramo $2n \times 2n$ matriko $\bar{A}(\lambda)$ s predpisom*

$$\begin{bmatrix} A & \lambda \cdot I \\ I & I \end{bmatrix}$$

Potem je λ lastna vrednost matrike A natanko tedaj ko so stolpci matrike $\bar{A}(\lambda)$ linearno odvisni.

Dokaz. Denimo najprej, da imamo nek lastni vektor matrike A, na primer $v = (v_1, v_2, \ldots, v_n)^\top \in R^n$, za lastno vrednost λ. Nato zapišemo $J_1 = \{1, 2, \ldots, n\}$ in $J_2 = \{n+1, n+2, \ldots, 2n\}$. Dodatno definiramo koeficiente μ_j na sledeč način:

$$\mu_j = \begin{cases} v_j & j \in J_1 \\ v_{n-j} & j \in J_2 \end{cases}$$

Po predpostavki je λ lastna vrednost A, torej velja $A * v = \lambda \cdot v$. Če z A_j označimo j-ti stolpec matrike A lahko zapišemo $A * v = \sum_{j=1}^{n} v_j \cdot A_j$ in to je po predpostavki enako $\lambda \cdot v = \lambda \cdot I * v = \sum_{j=1}^{n} (v_j \otimes \lambda) \cdot e_j$. Iz tega sklepamo, da velja enakost

$$\sum_{j \in J_1} \mu_j \cdot \bar{A}(\lambda)_j = \sum_{j \in J_2} \mu_j \cdot \bar{A}(\lambda)_j \tag{3}$$

Sledi, da so stolpci matrike $\bar{A}(\lambda)$ linearno odvisni.

Po drugi strani, denimo, da so stolpci matrike $\bar{A}(\lambda)$ linearno odvisni, in naj bodo $\{\mu_1, \mu_2, \ldots, \mu_n, \mu_{n+1}, \ldots, \mu_{2n}\}$ take uteži na njih, da bo veljala enakost 3 za neki neprazni disjunktni indeksni množici $I_1, I_2 \subseteq \{1, 2, \ldots, 2n\}$, pri čemer velja $\mu_j \neq 0 \ \forall j \in J_1 \cup J_2$ in $\mu_j = 0 \ \forall j \notin J_1 \cup J_2$. Taki množici zagotovo obstajata zaradi linearne odvisnosti stolpcev. V enakosti 3 se sedaj osredotočimo na zadnjih n komponent

in opazimo, da za poljuben indeks $j \in \{1, 2, \ldots, n\}$ velja, da ne more biti v isti indeksni množici (J_1 ali J_2) kot $n + j$. Če bi namreč j in $n + j$ bila skupaj v J_1 (ali v J_2), bi sledilo $\mu_j \oplus \mu_{n+j} = 0$ in ker je R kanonično urejen bi od tod sledilo $\mu_j = \mu_{n+j} = 0$, kar je v protislovju s tem, kako smo definirali uteži μ_j. Če je torej j vsebovan v J_1 nujno sledi $n + j \in J_2$ in iz enakosti 3 sledi $\mu_j = \mu_{n+j}$. Posledično sklepamo $J_1 \subseteq \{1, 2, \ldots, n\}$ in definiramo:

$$v_j = \begin{cases} \mu_j; & j \in J_1 \ \& \ 1 \leq j \leq n \\ 0; & j \in \{1, 2, \ldots, n\} \setminus J_1 \end{cases}$$

Ko vstavimo te nove oznake v 3 zavzame zgornjih n komponent obliko:

$$\sum_{i=1}^{n} \mu_j \cdot A_j = \sum_{j=1}^{n} A_j * v_j = \begin{bmatrix} \lambda \otimes v_1 \\ \lambda \otimes v_2 \\ \vdots \\ \lambda \otimes v_n \end{bmatrix} = \lambda \cdot \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}$$

Ko uvedemo oznako $v = (v_1, v_2, \ldots, v_n)^\top$, postane zgornja enačba kar $\sum_{j=1}^{n} A_j * v_j = \lambda \cdot v$. Od tod sledi, da je λ lastna vrednost matrike A, vektor v pa je njen lastni vektor. □

5. Posplošeni Cayley-Hamiltonov izrek

Eden izmed pomembnih rezultatov linearne algebre nad polji je t. i. Cayley-Hamiltonov izrek. Izkaže se, da ta rezultat ni omejen samo na linearne strukture nad polji, temveč ga lahko, kot je to leta 1964 pokazal Daniel Rutherford v [2], dokažemo v posplošeni obliki tudi za matrike nad komutativnimi polkolobarji. Leta 2011 je to nadgradil Radu Grosu v [5], kjer je razširil rezultat tudi na matrike nad nekomutativnimi polkolobarji. V tem odseku bo predstavljen Cayley-Hamiltonov izrek v tej, najbolj posplošeni obliki. Pri tem bomo snov črpali iz [5].

5.1. **Permutacije:** Za začetek osvežimo svoje znanje o permutacijah, saj bodo te igrale bistveno vlogo v nadaljevanju.

Definicija 5.1. Naj bo $X = \{1, 2, \ldots, n\}$ neka končna množica. Bijekciji $\pi : X \to X$ pravimo *permutacija*. Vsako permutacijo lahko zapišemo kot produkt disjunktnih ciklov. V tem zapisu po navadi ne pišemo ciklov dolžine 1. Ciklu dolžine 2 pravimo *transpozicija*. Vsak cikel lahko razbijemo na produkt transpozicij, torej lahko vsako permutacijo zapišemo kot produkt transpozicij. Če je π sestavljena iz sodega število transpozicij pravimo, da je *soda permutacija*, če je iz lihega števila transpozicij pa pravimo, da je *liha permutacija*. Za parnost permutacije π se tudi uporablja oznaka $sgn(\pi)$. Pri tem velja $sgn(\pi) = 1$, če je π soda in $sgn(\pi) = -1$, če je π liha. S $P(n)$ označimo množico vseh permutacij n elementov, s $P^+(n)$ označimo množico vseh sodih permutacij n elementov, s $P^-(n)$ pa množico lihih permutacij n elementov. 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.

Delno permutacijo σ množice $S \subseteq X$ lahko tudi razširimo na cel X:

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

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

Za dano permutacijo π s $\bar{\pi}$ označimo zaporedje $(1, \pi(1)), (2, \pi(2)), \ldots, (n, \pi(n))$. Za dano zaporedje $w = w_1 w_2 \ldots w_n$ lahko permutacijo π razširimo po komponentah, tako da je $\pi(w) = w_{\pi(1)} w_{\pi(2)} \ldots w_{\pi(n)}$.

Poglejmo en konkreten primer za vse navedene pojme.

Zgled 5.2. $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$ je permutacija 5 elementov. Zapišemo jo lahko kot produkt disjunktnih ciklov $\pi = (12)(354) = (1\ 2)(5\ 3)(4\ 5)$. Ker je sestavljena iz treh transpozicij, je liha permutacija. Po drugi strani pa je $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$ soda permutacija, saj je $\sigma = (1\ 2)(4\ 5)$. Velja $sgn(\pi) = -1$ in $sgn(\sigma) = 1$. Permutacija $\varphi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ je delna permutacija množice 5 elementov. Razširimo jo lahko do permutacije množice 5 elementov s predpisom $\hat{\varphi} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$.

Vzemimo sedaj zaporedje $w = oprs$š. Potem je $\sigma(w) = por$šs in $\pi(w) = pos$šr. Dodatno je $\sigma(\bar{\pi}) = (2,1)(1,2)(3,5)(5,4)(4,3)$. ♢

Za konec navedemo še eno definicijo, ki bo prišla prav v naslednjem podpoglavju.

Definicija 5.3. Naj bo $w = w_1 w_2 \ldots w_n$ neko zaporedje dolžine $n \in \mathbb{N}$. Vsoti $\sum_{\pi \in P(n)} \pi(w)$ pravimo *permutacijsko zaprtje* zaporedja w in ga označimo z $[\![w]\!]$.

5.2. **Pideterminanta:** Za dano permutacijo π množice z n elementi lahko permutacijsko zaporedje $\bar{\pi}$ uporabimo tudi na dani $n \times n$ matriki A na naslednji način:

$$\bar{\pi}(A) = (1, \pi(1))(2, \pi(2)) \ldots (n, \pi(n))(A) = A_{1\pi(1)} A_{2\pi(2)} \ldots A_{n\pi(n)}$$

Pri tem je A_{ij} element matrike A, ki se nahaja v i-ti vrstici in j-tem stolpcu. Sedaj se spomnimo definicije determinante nad polji.

Definicija 5.4. Naj bo F polje in $A \in M_n(F)$ kvadratna matrika nad F. Potem je determinanta matrike A definirana s predpisom:

$$det(A) = \sum_{\pi \in P(n)} sgn(\pi) a_{1\pi(1)} a_2 \pi(2) \ldots a_{n\pi(n)}$$

Formulo iz definicije lahko skrajšamo s pomočjo uporabe permutacijskega zaporedja $\bar{\pi}$ na matriki A. Dodatno lahko še permutacije $\pi \in P(n)$ ločimo glede na parnost. Nova formula ima obliko

$$det(A) = \sum_{\pi \in P(n)} sgn(\pi) \bar{\pi}(A) = \sum_{\pi \in P^+(n)} \bar{\pi}(A) - \sum_{\pi \in P^-(n)} \bar{\pi}(A)$$

Vsoto po sodih permutacijah označimo z $det^+(A)$, vsoto po lihih permutacijah pa z $det^-(A)$. Potem lahko determinanto matrike A zapišemo tudi kot

$$det(A) = det^+(A) - det^-(A)$$

Definicija 5.5. Naj bo R nek polkolobar in $A \in M_n(R)$ kvadratna matrika. Urejeni dvojici podani s predpisom

$$pdt(A) = \Big(\sum_{\substack{\pi \in P^+(n) \\ \sigma \in P(n)}} \sigma(\bar{\pi})(A), \sum_{\substack{\pi \in P^-(n) \\ \sigma \in P(n)}} \sigma(\bar{\pi})(A) \Big)$$

pravimo *pideterminanta* matrike A.

Ko v definiciji prepoznamo permutacijsko zaprtje, lahko formulo zapišemo tudi kot $pdt(A) = (\llbracket det^+(A) \rrbracket, \llbracket det^-(A) \rrbracket)$.

Slovar strokovnih izrazov

base of a semimodule baza polmodula – linearno neodvisna podmnožica v polmodulu, ki ga generira
complete set polna množica
dioid dioid
eigenvalue lastna vrednost
eigenvector lastni vektor
endomorphism endomorfizem – homomorfizem, ki ima isto domeno in kodomeno
factor rank faktorski rang
finitely generated semimodule končno generiran polmodul – polmodul, za katerega obstaja končna množica, ki ga generira
free semimodule prosti polmodul – polmodul, ki premore kako prosto bazo
free set in a semimodule prosta množica v polmodulu – podmnožica v polmodulu za katero velja, da lahko vsak element iz polmodula zapišemo kot linearno kombinacijo njenih elementov na največ en način
free base of a semimodule prosta baza polmodula – prosta podmnožica v polmodulu, ki generira polmodul
homomorphism (of semirings, dioids, semimodules, moduloids, ...) homomorfizem (polkolobarjev, dioidov, polmodulov, moduloidov, ...)
ideal of a semiring ideal polkolobarja
infimum infimum
lower bound spodnja meja
linear independence linearna neodvisnost
linear combination linearna kombinacija
moduloid moduloid
partial permutation delna permutacija
permutation permutacija
Perron-Frobenius Theorem Perron-Frobeniusov izrek – Pod to ime spada več rezultatov o realnih matrikah s samimi pozitivnimi ali nenegativnimi vrednostmi (pozitivne oz. nenegativne realne matrike), ki sta jih dokazala Oskar Perron (za pozitivne matrike), in Georg Frobenius (za nenegativne matrike)
positivity condition pogoj pozitivnosti – struktura v kateri velja sklep, da če je t.i. vsota dveh elementov enaka nevtralnemu elementu oz. »ničli«, sta potem oba elemeneta enaka nevtralnemu elementu, zadošča pogoju pozitivnosti
pre-semiring pred-polkolobar
semifield polpolje
semimodule polmodul
semiring polkolobar
supremum supremum
the element $0 \in R$ is absorbing for $\otimes$ element $0 \in R$ izniči operacijo $\otimes$, torej $\forall a \in R; a \otimes 0 = 0 \otimes a = 0$
the greatest element zadnji element
the least element prvi element
transition matrix prehodna matrika
transposition transpozicija

upper bound zgornja meja

weak dimension of the R-semimodule M šibka dimenzija R-polmodula M – minimalna kardinalnost šibko linearno neodvisnih množic, ki generirajo M.

weak linear independence šibka linearna neodvisnost

weak base of a semimodule šibka baza polmodula

Literatura

[1] C. Reutenauer in H. Straubing, *Inversion of matrices over a commutative semiring*, Journal of Algebra **88** (1984) 350–360.

[2] 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.

[3] 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.

[4] 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`.

[5] 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.

[6] Y. J. Tan, *Bases in semimodules over commutative semirings*, v: Linear Algebra Appl. **443** (2014) 139–152.

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

[8] Y. J. Tan, *On invertible matrices over commutative semirings*, Linear Multilinear Algebra **61** (2013) 710–714.

[9] *Semiring*, v: Wikipedia, The Free Encyclopedia, [ogled 15. 2. 2022], dostopno na `https://en.wikipedia.org/wiki/Semiring`.