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, 2023

Kazalo

1. Uvod 4
2. Monoidi, polkolobarji in dioidi 5
2.1. Monoidi 5
2.2. Polkolobarji 7
2.3. Dioidi 9
3. Polmoduli in moduloidi 13
3.1. Definicije in elementarni primeri 13
3.2. Homomorfizmi in kvocientne strukture 14
3.3. Generatorji polmodulov in linearna neodvisnost 15
4. Matrike 20
4.1. Definicije in osnove obrnljivosti 21
4.2. Prehodne matrike 23
4.3. Lastne vrednosti 27
5. Posplošeni Cayley-Hamiltonov izrek 29
5.1. Permutacije 29
5.2. Pideterminanta in karakteristični pipolinom 30
5.3. Cayley-Hamiltonov izrek nad polkolobarji 32
Slovar strokovnih izrazov 36
Literatura 37

Linearna algebra nad polkolobarji

Povzetek

Delo obravnava algebraično strukturo polkolobarja z dodatno pozornostjo dano na posebni primer dioida. 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 v povezavi s temi strukturami, s stališča linearne algebre, že ima 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, lastnosti in obrnljivost matrik nad polkolobarjem R ter Cayley-Hamiltonov izrek.

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 some time now and most of the classical questions relating to the structures, from the perspective of linear algebra, have already been answered. From among those, this paper will present some of the more elementary results. In particular, the focus will be on properties of semirings and dioids and on generalizations of concepts from classical linear algebra over fields such as the existence and properties of bases of an R-semimodule, the properties and invertibility of a matrix over a semiring R and the Cayley-Hamilton theorem.

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

Ključne besede: Linearna algebra, algebra, polkolobar, polmodul, dioid, pideterminanta, karakteristični pipolinom, posplošeni Cayley-Hamiltonov izrek

Keywords: Linear algebra, algebra, semiring, semimodule, dioid, pideterminant, characteristic pipolynomial, generalized Cayley-Hamilton theorem

1. Uvod

Polkolobarji so algebraična struktura, s katero se srečamo takoj ko začnemo obravnavati številske množice. Med primere spadajo nenegativni odseki celih, racionalnih ter realnih števil (opremljeni s standardnim seštevanjem in množenjem), t. i. tropski polkolobarji, ki se uporabljajo za ocenjevanje učinkovitosti v podjetjih itd. Uporabo imajo tudi v teoretičnem računalništvu in kriptografiji.

Kljub njihovi uporabnosti in pogostemu 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 polji.

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 in dioidi ter razne trditve o njih, 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, na primer vprašanje obstoja in kardinalnosti baze. Sledila bo definicija linearnih preslikav in matrik nad polkolobarji ter obravnava lastnosti le teh v četrtem razdelku. V zadnjem poglavju pa bomo obravnavali posplošitev determinante in karakterističnega polinoma ter navedli Cayley-Hamiltonov izrek.

Za začetek obravnavajmo motivacijski primer, ki nam bo pokazal, da četudi operaciji $\oplus$ in $\otimes$ na neki algebrajski strukturi $(R, \oplus, \otimes)$ 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 [2, str. 1 – 2].

Zgled 1.1. Množico nenegativnih realnih števil $\mathbb{R}_+$ opremimo s standardnima operacijiama seštevanja in množenja in to strukturo označimo z $(\mathbb{R}_+, +, \cdot)$. 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 lastni 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 in

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 [2, 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, a ni nujno, v neki zvezi z operacijo na monoidu. 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, da je $x = y$, 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 podpoglavja 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

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

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, da je $z \oplus w = 0$. 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 lotimo polkolobarjev.

Definicija 2.10. Za neprazno množico R, ki je opremljena z notranjima binarnima operacijama $\oplus$ in $\otimes$, pravimo, da je *polkolobar*, če izpolnjuje naslednje pogoje:

(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 definiramo *levi polkolobar* na enak način kot polkolobar, le da zahtevamo samo levo distributivnost. 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).

Po hitrem premisleku vidimo, da 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 2.13. Naj bo X neprazna množica in $P(X)$ potenčna množica množice X. Z $\cup$ označimo operacijo unije, s $\cap$ pa operacijo preseka. 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 povzemamo iz [6, str. 3].

Definicija 2.14. 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, da multiplikativna enota ni nujno vsebovana v $V(R)$. Da to vidimo, je dovolj vzeti polkolobar iz zgleda 2.13, 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 2.15. *Naj bo $(R, \oplus, \otimes)$ komutativen polkolobar.*

Potem za vsaka $p, q \in V(R)$ in za vsak $r \in R$ velja, da je $(-p) \otimes r = -(p \otimes r)$ & $(-p) \otimes (-q) = p \otimes q$.

Dokaz. Naj bosta $p, q \in V(R)$ in naj bo $r \in R$. Očitno velja, da je $-p \in V(R)$ 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 je $(-p) \otimes r = -(p \otimes r)$. 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 2.16. 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 vidimo, da so elementi iz R 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 omenjeni 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 2.17. Naj bo $(R, \oplus, \otimes)$ polkolobar. Neprazna množica P je podpolkolobar v R, če je podmnožica v R in če je $(P, \oplus_{|P}, \otimes_{|P})$ polkolobar. Pri tem sta $\oplus_{|P}$ in $\otimes_{|P}$ zožitvi $\oplus$ in $\otimes$ na P.

Iz zgornje definicije hitro sledi naslednja trditev.

Trditev 2.18. *Naj bo $(R, \oplus, \otimes)$ polkolobar in $P \subseteq R$ neprazna podmnožica v R. Tedaj je P podpolkolobar v R, čim je zaprt za zoženi operaciji $\oplus_{|P}$ in $\otimes_{|P}$ ter 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 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 polkolobar, torej je tudi podpolkolobar v R. $\square$

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 pripadajočemu dokazu za kolobarje.

Sedaj preidemo na preslikave med polkolobarji, specifično homomorfizme. Ti so definirani na skoraj enak način kot homomorfizmi kolobarjev, kar pokaže spodnja definicija.

Definicija 2.19. Naj bosta $(R, \oplus, \otimes)$ in $(P, \boxplus, \boxtimes)$ polkolobarja. Naj bo 0 nevtralni element in 1 enota v R ter e nevtralni element in ε enota 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, ne da bi samo definicijo bistveno spremenili.

Definicija 2.20. Neprazni podmnožici I polkolobarja $(R, \oplus, \otimes)$ pravimo *levi ideal*, če zanjo 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. Dodatno, če imamo nek komutativen polkolobar R, nam lema 2.15 pove, da je $V(R)$ ideal R.

2.3. **Dioidi.** Kot smo že napovedali v prejšnjem podpoglavju, zahvaljujoč 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 2.21. 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 izrek 2.9 lahko klasificiramo dioide kot polkolobarje, ki so, glede na $\oplus$, okrajšljivi in zadoščajo pogoju pozitivnosti.

Opomba 2.22. 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.

Preprost 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 $(\mathbb{N}_0, +, \cdot)$ služi 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. To bo tudi pokazal naslednji zgled.

Zgled 2.23. 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 $+\infty$, v primeru drugega pa $-\infty$. V obeh primerih je enota 0 in vse tri operacije so komutativne ter asociativne. Med max in $+$ ter min in $+$ tudi očitno velja distributivnost in tako ∞ kot $-\infty$ izničita $+$. 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 zgolj ko je $c = +\infty = d$, torej je $a = b$. Na enak način pokažemo antisimetričnost kanonične urejenosti definirane preko max.

Oba polkolobarja sta torej res dioida. Na enak način vidimo, da sta tudi $(\mathbb{R} \cup \{\infty\}, \min, +)$ in $(\mathbb{R} \cup \{-\infty\}, \max, +)$ dioida. Slednja, odvisno od konteksta, imenujemo tropska polkolobarja oz. tropska dioida. $\diamondsuit$

Trditev 2.24. *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 vsak $x \in R$ 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 $\otimes$. $\square$

Tudi pri dioidih lahko obravnavamo strukturo njihovih produktov. Vrnimo se k zgledu 2.16, v katerem smo že premislili, da je $(R, \oplus, \otimes)$ polkolobar. 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 $x \leq y \iff x_1 \leq_1 y_1 \ \& \ \ldots \ \& \ x_m \leq_m y_m$.

Splača se obravnavati tudi vprašanje podstruktur dioidov. 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 2.25. Neprazna množica P je poddioid dioida $(R, \oplus, \otimes)$, če je podmnožica v R 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 2.26. *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 še omenimo 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 2.26 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 [2, 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 [2, definicija 6. 1. 8.].

Definicija 2.27. Dioid $(R, \oplus, \otimes)$ je *poln*, 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 *vrhnji element* kar vsoto vseh elementov dioida $T = \bigoplus_{r\in R} r$. Za vrhnji element polnega dioida T in za vsak $r \in R$ velja $T \oplus r = T$ in $T \otimes 0 = 0$.

Zgled 2.28. Tropska dioida $(\mathbb{R}\cup\{-\infty\}, \max, +)$ in $(\mathbb{R}\cup\{+\infty\}, \min, +)$ nista polna. Da postaneta polna, jima moramo dodati njuna vrhnja elementa. Za prvi dioid je to $T = +\infty$., za drugi dioid pa je $T = -\infty$. Dioida nad $\bar{\mathbb{R}}$ iz zgleda 2.23 sta torej polna dioida. ♢

Opomba 2.29. Omenimo še dualni pojem *infimuma* množice, kot je definiran v [2, 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 uporabe dioidov, navedimo še en zgled, ki ni vezan na znane številske množice. Zgleda 2.30 in 2.31 v nadaljevanju sta povzeta iz [2, poglavje 6. 2.].

Zgled 2.30. Naj bo $(R, +)$ kanonično urejen komutativen monoid z enoto 0. Na množici E endomorfizmov R potem uvedemo operaciji $\oplus$ in $\otimes$ na sledeč način:

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

kjer je $\circ$ navadno komponiranje preslikav. Hitro vidimo, da je $(E, \oplus, \otimes)$ dioid. Pri tem je nevtralni element v E kar ničeln endomorfizem s predpisom $0(r) = 0;\ \forall r \in R$, enota pa je identični endomorfizem s predpisom $id_R(r) = r;\ \forall r \in R$. ♢

Naslednji zgled, nam demonstrira praktično aplikacijo zgleda 2.30.

Zgled 2.31. Vsebino zgleda 2.30 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 je $f(\min\{t, \acute{t}\}) =$

$\min\{f(t), f(\acute{t})\}$ 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 2.31.

Na koncu izpostavimo še eno povezavo med polkolobarji in dioidi. Kot lahko vidimo v [2, 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, je razkrito v [2, trditev 6. 9. 1.], kar tudi navajamo spodaj.

Trditev 2.32. *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 s predpisom:*

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

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 $\widehat{R}$. Nevtralni element v $\widehat{R}$ je $[0]$, torej ekvivalenčni razred, ki pripada nevtralnemu elementu 0 iz R. Podobno je enota v $\widehat{R}$ kar $[1]$, torej ekvivalenčni razred enote 1 iz R. Ker aditivna enota 0 v $(R, \oplus, \otimes)$ izniči $\otimes$, sledi da v $(\widehat{R}, \oplus, \otimes)$ razred $[0]$ 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. Sledi, da je $(\widehat{R}, \oplus, \otimes)$ dioid. $\square$

Opomba 2.33. V [2, poglavje 1, definicija 5. 2. 3.] vidimo, da lahko definiramo še strukturo, ki jo imenujemo *polpolje*, kot polkolobar v katerem je vsak od 0 različen element obrnljiv glede na $\otimes$. 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 bomo pozornost posvetili vprašanju baz. V večji meri se bomo pri tem sklicevali na vir [2, 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 nevtralnim elementom 0 in enoto 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 za vsaka $\lambda, \mu \in R$ in vsaka $m, n \in M$ zadošča naslednjim pogojem:

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 $\lambda \cdot \theta = \theta = 0 \cdot m$

Na enak način definiramo desni R-polmodul, le da tam množenje s skalarjem izvajamo z desne, torej $\cdot : M \times R \to M$. Elementom polmodula pravimo vektorji. Polmodule (leve, desne in obojestranske) bomo na kratko označevali z $(M, +, \cdot)$ ali kar $(M, +)$.

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 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. Želimo pokazati, da je $(R^n, +)$ kanonično urejen. 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 $\leq_\oplus$, torej je $(R^n, +)$ res kanonično urejen in od tod sledi, da je $(R^n, +, \cdot)$ (levi) moduloid. ♢

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 $(M, +, \cdot)$ in $(N, \boxplus, \boxdot)$ oba polmodula nad istim polkolobarjem $(R, \oplus, \otimes)$. Preslikavi $\phi : M \to N$ pravimo *homomorfizem* R-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 R-moduloidov.

Opomba 3.6. Tako kot elementom x R-polmodula $(R^n, +, \cdot)$, pravimo vektorji, pravimo homomorfizmom med R-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 [2].

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

Hitro se da preveriti, da je neprazna množica $\widehat{M} \subseteq M$ podpolmodul v M čim vsebuje enoto $\theta \in M$ 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 M.

Definicija 3.8. Naj bo $(M, +, \cdot)$ R-polmodul in $(\widehat{M}, +, \cdot)$ 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 $\varphi : M \to M/\widehat{M}$, s predpisom $\varphi(x) = [x]$, ki vsakemu elementu $x \in M$ priredi njegov ekvivalenčni razred $[x] \in M/\widehat{M}$, homomorfizem R-polmodulov.

3.3. **Generatorji polmodulov in linearna neodvisnost.** V tem podpoglavju bomo definirali generatorje, linearno (ne)odvisnost in baze v kontekstu polmodulov ter pokazali nekaj zanimivih rezultatov v zvezi s temi koncepti. Več rezultatov na temo baz (levih) polmodulov bomo obravnavali v naslednjem poglavju v razdelku 4.2. Začnimo kar z definicijo generiranega polmodula.

Definicija 3.9. Naj bo $(M, +, \cdot)$ R-polmodul in naj bo $X = (x_i)_{i \in I}$ poljubna neprazna družina elementov iz M. Najmanjši R-podpolmodul, ki vsebuje X, imenujemo 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. Izkaže se, da pojem dimenzije, kot ga poznamo iz linearne algebre nad polji, ni ustrezen za polkolobarje, saj lahko linearno neodvisnost definiramo na več različnih načinov, ki pogojujejo različne definicije »baz«. Temu problemu se izognemo tako, da 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.

Takoj opazimo, da rang vedno obstaja za končno generirane polmodule. Sam pojem bo postal pomemben kasneje v podpoglavju 4.2 o prehodnih matrikah.

V nadaljevanju nam bo prišlo prav, če karakteriziramo podpolmodule generirane z $X \subseteq M$.

Trditev 3.11. *Naj bo* $(M, +, \cdot)$ 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 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 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 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 [2, poglavje 5, definicija 2. 5. 1.]. Ta se glasi:

Definicija 3.12. Naj bo $(M, +, \cdot)$ 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 [1, definicija 2. 12.]. Definicija se glasi takole:

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

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

Opomba 3.14. Rang polmodula, ki smo ga definirali v 3.10 je znan tudi pod imenom *šibka dimenzija polmodula*. Pod tem imenom je definiran kot minimalna kardinalnost šibko linearno neodvisnih podmnožic, ki generirajo polmodul.

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 $I_1 = \{i_0\}$ in $I_2 = I \setminus \{i_0\}$ za poljuben $i_0 \in I$. Zaradi linearne neodvisnosti X za vsak $i_0 \in I$ velja $\langle \{x_{i_0}\} \rangle \cap \langle X \setminus \{x_{i_0}\} \rangle = \{\theta\}$, od tod pa sledi $x_{i_0} \notin \langle X \setminus \{x_{i_0}\} \rangle$. To je v resnici ravno pogoj iz definicije šibke linearne neodvisnosti. Vsaka linearno neodvisna družina X je torej tudi šibko linearno neodvisna. Posledično je pojem šibke linearne (ne)odvisnosti širši od pojma linearne (ne)odvisnosti. Nad polji sta oba pojma ekvivalentna.

Izkaže se, da ni vsaka šibko linearno neodvisna množica hkrati tudi linearno neodvisna. Primer, ki to demonstrira, se najde v polmodulu $(\mathbb{R} \cup \{-\infty\})^3$ nad tropskim polkolobarjem $(\mathbb{R} \cup \{-\infty\}, \max, +)$, kar nam pove [1, zgled 2. 14.]. Kot je tam navedeno, je vsaka družina vektorjev $[x_i, 0, -x_i] \in (\mathbb{R} \cup \{-\infty\})^3$ za $i = \{1, 2, \ldots, m\}$ šibko linearno neodvisna za poljuben m in različne x_i. Po drugi strani pa lahko vidimo, da so vektorji $v_i = \begin{bmatrix} i & 0 & -i \end{bmatrix}^\top$ za $i = 1, 2, 3, 4$ 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 3.15. 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 [2, poglavje 5, definicija 2. 5. 2.].

Definicija 3.16. Pravimo, da je družina X v R-polmodulu $(M, +, \cdot)$ *baza*, če je linearno neodvisna in generira M.

Opomba 3.17. 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 3.18. Naj bo R 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* 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.

Opomba 3.19. Vsaka prosta baza je hkrati tudi šibka baza. Poleg tega ima vsak končno generiran polmodul kako končno šibko bazo.

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 vektorji 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 in če je linearno odvisna v smislu polmodula M nad polkolobarjem F, je linearno odvisna tudi v smislu vektorskega prostora M nad poljem F.

Zgled 3.20. Vrnimo se k zgledu 3.2 in R-polmodul $(R^n, \oplus, \otimes)$ prepoznamo kot končno generiran prosti polmodul. Množica $E = \{e_1, e_2, \ldots, e_n\}$ 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 [6, izrek 3. 1.].

Izrek 3.21. *Naj bo R polkolobar in M naj bo 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 $x \in X \setminus \acute{Y} \subseteq X$, 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 polmodul M končno šibko bazo, so vse njegove šibke baze končne. Posledično je vsaka šibka baza končno generiranega polmodula končna, saj ta polmodul premore vsaj eno končno šibko bazo.

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

Definicija 3.22. Naj bo $(M, +, \cdot)$ levi polmodul nad polkolobarjem $(R, \oplus, \otimes)$ in denimo, da imamo dano neko množico vektorjev $X = (x_k)_{k \in K}$, kjer je $x_k \in M$ za vsak $k \in K$. Vektor x je *razcepen* na $\langle X \rangle$ natanko tedaj, ko obstajata taka vektorja $y, z \in \langle X \rangle$, 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 na $\langle X \rangle$ implicira vsebovanost v $\langle X \rangle$, od tod pa sledi naslednja trditev.

Trditev 3.23. *Če je x nerazcepen na $\langle X \rangle$, potem zanj velja natanko ena od naslednjih lastnosti:*

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

S pomočjo trditve 3.23 lahko zapišemo in dokažemo naslednjo trditev.

Trditev 3.24. *Naj bo $(R, \oplus, \otimes)$ dioid in označimo z 0 njegov nevtralni element ter z 1 njegovo enoto. 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 poljuben $\lambda \in R$ velja:*

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

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

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 obstajajo 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 velja enakost

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

kjer je $\lambda_j \oplus \mu_j \neq 0$. Uvedemo oznaki $\lambda = \lambda_j \oplus \mu_j$ in $w = \sum_{i \in (I_1 \cup I_2) \setminus \{j\}} (\lambda_i \oplus \mu_i) \cdot x_i$ ter vidimo, da je $w \in \langle X \setminus \{x_j\} \rangle$. 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 je $x_j \neq \theta$ in zaradi linearne neodvisnosti X vemo tudi, da je $w \neq x_j$. Posledično velja, da je $\lambda \neq 0$. Potem po predpostavki trditve velja, da je $\lambda = 1$ in ker je $\lambda = \lambda_j \oplus \mu_j$ sledi, da je $\lambda_j = 1$ ali pa je $\mu_j = 1$.

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, da je $x_j \propto z$ in ko to združimo z dejstvom, da je $z \propto x_j$ in upoštevamo, da je $\propto$ relacija delne urejenosti, sledi, da je $z = x_j$. Podobno, če predpostavimo, da je $\lambda_i = 1$, pridemo do rezultata $y = x_j$.

Po drugi točki posledice 3.23 je potem x_j nerazcepen. □

Primer moduloida, ki ustreza pogojem in predpostavkam trditve, je $\mathbb{N}_0^n$ za dioid $\mathbb{N}_0$ opremljen s standardnim seštevanjem in množenjem. Sedaj lahko s pomočjo dokazane trditve povemo, kdaj bo moduloid imel enolično določeno bazo.

Trditev 3.25. *Denimo, da veljajo vse predpostavke trditve 3.24 in naj poleg tega velja še sklep $r, p \in R : r \otimes p = 1 \Rightarrow r = 1$ in $p = 1$. Potem, če ima $(M, +, \otimes)$ bazo, je enolično določena.*

Dokaz. Denimo, da ima R-moduloid 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 $x_i = \sum_{j \in J} \mu_j^i \cdot y_j$ za neke skalarje $\mu_j^i \in R$. Ker sta X in Y linearno neodvisni, po trditvi 3.24 sledi, da so vsi x_i in prav tako vsi y_j nerazcepni elementi na $M = \langle X \rangle = \langle Y \rangle$. 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 $x_i = \mu_j^i \cdot (\nu_k^j \cdot x_k) = (\mu_j^i \otimes \nu_k^j) \cdot x_k$. Ker je X linearno neodvisna družina, je nujno $i = k$. Po predpostavki iz trditve 3.24 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 tod pa sklepamo da je $X = Y$. □

Tudi tukaj lahko za primer vzamemo $\mathbb{N}_0^n$ nad $\mathbb{N}_0$ opremljenim s standardnim seštevanjem in množenjem.

4. Matrike

Kot smo že videli, lahko, podobno kot za vektorske prostore in module, tudi polmodulu pod določenimi pogoji določimo različne vrste baz ter mu tudi dodelimo neke vrste »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 šibkimi 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 $(R, \oplus, \otimes)$ uvedli tudi $m \times n$ matrike, za poljubna $m, n \in \mathbb{N}$. Za $A \in M_{m\times n}(R), B \in M_{n\times l}(R)$ definiramo seštevanje na enak način kot za matrike nad obsegi, torej po komponentah, množenje pa na sledeč način:

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

Predpis množenja matrik tukaj zapišemo eksplicitno zato, da poudarimo vrstni red množenja, saj R ni nujno komutativen. Enota za seštevanje je seveda kar t. i. ničelna matrika 0, kjer je vsak element aditivna enota polkolobarja $0 \in R$, za množenje pa je enota kar matrika I, ki ima na diagonali multiplikativno enoto polkolobarja $1 \in R$, izven diagonale nevtralni element polkolobarja 0. 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 $M_n(R) = M_{n\times n}$, opremljena s prej definiranima operacijama seštevanja in množenja, polkolobar. Dodatno, če je $(R, \oplus, \otimes)$ dioid za svojo kanonično delno urejenost, je tudi $(M_n(R), +, *)$ dioid za svojo kanonično šibko urejenost.

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 obstaja taka matrika $C \in M_n(R)$, da velja $A * C = I_n$. Če obstaja, matriki B pravimo levi inverz matrike A, matriki C pa 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 2.15 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 [4, 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 sklep $1 = u \oplus v \Rightarrow u \in U(R) \vee v \in U(R)$ za vse $u, v \in R$. 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 $n-1$. Naj bo $A \in M_n(R)$ taka matrika, da zadošča zahtevam trditve in z E_{ij} označimo $n \times n$ matriko, ki ima na mestu (i,j) multiplikativno enoto polkolobarja $1 \in R$, povsod drugje pa aditivno enoto polkolobarja $0 \in R$. 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 2.15 znotraj vsot in zamenjamo indekse s z indeksi i in indekse t z indeksi 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.

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

Z A_1 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 različna indeksa i in 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 izrazimo 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 $1 = a_{ii}^{-1}a_{i1}a_{1i}a_{11}^{-1} \oplus a_{ii}^{-1}r_i$. Sedaj po predpostavki lastnosti polkolobarja R 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 $a_{i1}a_{1i} \in U(R)$, hkrati pa je $a_{i1}a_{1i} \in V(R)$, ker je $V(R)$ ideal. Enačbo $a_{i1}a_{1i} \oplus (-a_{i1}a_{1i}) = 0$ pomnožimo z leve z $(a_{i1}a_{1i})^{-1}$ in dobimo enakost $1 \oplus (a_{i1}a_{1i})^{-1}(-a_{i1}a_{1i}) = 0$. Iz te enakosti sledi, da je $1 \in V(R)$, kar pa nas privede v protislovje s predpostavko, da 1 ni aditivno obrnljiva v R. 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 A_1 obrnljiva $(n-1) \times (n-1)$ matrika in velja tudi, da je $\begin{bmatrix} a_{11} & 0 \\ 0 & A_1 \end{bmatrix}$ obrnljiva, saj je $a_{11} \in U(R)$. Njen inverz je ravno matrika $\begin{bmatrix} a_{11}^{-1} & 0 \\ 0 & A_1^{-1} \end{bmatrix}$. Ker je $P * A * Q = \begin{bmatrix} a_{11} & 0 \\ 0 & A_1 \end{bmatrix}$ obrnljiva v $M_n(R)$, je tudi $A = P^{-1} * \begin{bmatrix} a_{11} & 0 \\ 0 & A_1 \end{bmatrix} * Q^{-1}$ obrnljiva matrika v $M_n(R)$. □

4.2. **Prehodne matrike.** Matrike imajo v klasični linearni algebri pomembno povezavo z bazami, saj je slika vsakega baznega vektorja tudi sama bazni vektor v zalogi vrednosti. Prehajanje med bazami omogoča pogled na določen problem z druge perspektive, kar lahko včasih ta 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 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.

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

Če koeficiente a_{ij} združimo v $n \times m$ matriko A nad polkolobarjem 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 R-polmodul ter naj bosta T in S njegovi šibki bazi. Matriki A, ki slika elemente šibke baze T v elemente šibke baze S, pravimo prehodna matrika iz 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 poljubna $n \times m$ matrika nad komutativnim polkolobarjem R. Najmanjšemu naravnemu številu $k \in \mathbb{N}$, za katerega velja, da je $A = B * C$ za neko $n \times k$ matriko B nad R in neko $k \times m$ matriko C nad 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 polmodul ranga r nad komutativnim polkolobarjem R, ter naj bosta S in T njegovi šibki bazi. Potem za vsako prehodno matriko A iz T v S velja, da je njen faktorski rang $\rho_s(A)$ najmanj r. 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 neko matriko B velikosti $n \times k$ in neko matriko C velikosti $k \times m$. Uvedemo oznako $\gamma_l = \sum_{j=1}^{n} b_{jl} \cdot t_j$ za vsak $l \in \{1, \ldots, k\}$ in 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 $s_i = \sum_{j=1}^{n} a_{ji} \cdot t_j$. 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 generira tudi M, saj S generira M. Potem pa je $r = r(M) \leq k = \rho_s(A)$. 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 R-polmodula M, da velja $|\Gamma| = r$. Naj bo $\Gamma = \{\gamma_1, \ldots, \gamma_r\}$ ter naj bo B neka $n \times r$ prehodna matrika iz T v Γ. Poleg tega naj bo C neka $r \times m$ 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. $\square$

Za naslednjo trditev se spomnimo definicije prostega R-polmodula v 3.15. 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, so vse njegove šibke baze končne, 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 neka $n \times m$ prehodna matrika iz T v S ter B neka $m \times n$ 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 $(t_1, t_2, \ldots, t_n) = (t_1, t_2, \ldots, t_n) * A * B$. Ker je T prosta baza sledi, da je $A * B = I_n$. Denimo, da je $m < n$ in naj bo O_1 ničelna matrika velikosti $n \times (n - m)$, O_2 pa ničelna matrika velikosti $(n - m) \times n$. 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, da je $B_1 * A_1 = I_n$. 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 lahko vidimo, da je kardinalnost vsake proste baze T polmodula M nad komutativnim polkolobarjem enaka $r(M)$. S pomočjo tega rezultata in trditve 4.7 bomo sedaj karakterizirali proste baze v končno generiranih polmodulih nad komutativnimi polkolobarji.

Izrek 4.8. *Naj bo R komutativen polkolobar in naj bo M 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. Spomnimo se torej, da za poljubno prosto bazo T polmodula M velja $|T| = r(M) = r$ in jo lahko zapišemo kot $T = \{t_1, \ldots, t_r\}$. Implikacija $i \Rightarrow ii$ sledi po izreku 4.7. Da dokažemo implikacijo $ii \Rightarrow iii$ za začetek denimo, da je $|S| = r$. Dodatno naj bo $S = \{s_1, \ldots, s_r\}$ in naj bo A prehodna matrika med T in S ter 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 $(t_1, t_2, \ldots, t_r) * A_1 = (t_1, t_2, \ldots, t_r) * A_2$. Ker je T prosta baza sledi, da je $A_1 = A_2$, s tem pa smo dokazali iii. Da dokažemo

implikacijo $iii \Rightarrow i$, predpostavimo, da je prehodna matrika A med šibkima bazama T in S enolično določena in 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 $S = \{s_1, \ldots, s_r\}$. Potem je $(s_1, s_2, \ldots, s_r) = (t_1, t_2, \ldots, t_r) * A$. Sedaj vzamemo nek poljuben element $v \in M$ in ga razvijemo po šibki bazi S na dva načina. To lahko storimo, ker v splošni šibki bazi nimamo nujno enoličnega zapisa. Pišemo torej $v = \sum_{i=1}^{r} \alpha_i \cdot s_i = \sum_{i=1}^{r} \beta_i \cdot s_i$ za neke skalarje $\alpha_i, \beta_i \in R \; \forall i \in \{1, \ldots, r\}$. Te linearne kombinacije lahko zapišemo v matrični 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

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

Ker je T prosta baza iz prejšnje enakosti sledi, da je $A * \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_r \end{bmatrix} = A * \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_r \end{bmatrix}$, od koder sklepamo, da velja tudi enakost $B * A * \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_r \end{bmatrix} = B * A * \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_r \end{bmatrix}$. Ker je B inverz od A, je $B * A = I_r$, torej sledi, da je $\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_r \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_r \end{bmatrix}$ oz. $\alpha_i = \beta_i$ za vsak $i \in \{1, \ldots, r\}$. 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 prosti 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 ji lahko posvetili lastno diplomsko nalogo. Vseeno bomo pa vsaj definirali oba koncepta in dokazali tri elementarne rezultate. Pri tem se bomo sklicevali na [2, poglavje 6].

Naj bo $(R, \oplus, \otimes)$ polkolobar in obravnavamo R-polmodul $M = R^n$ iz zgleda 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 $1 \in R$, na vseh ostalih komponentah pa aditivno enoto $0 \in R$. 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 $M = R^n$ polmodul nad R. 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 $v \in M \setminus \{\theta\}$, 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 matrike $A \in M_n(R)$. Potem je L_λ R-podpolmodul v M. Podpolmodulu L_λ pravimo lastni polmodul matrike A za λ.*

Dokaz. Naj bo A poljubna matrika iz $M_n(R)$, ki pripada nekemu endomorfizmu h R-polmodula M in naj bo λ poljubna lastna vrednost te matrike. Vzemimo poljubna skalarja $\alpha, \beta \in R$ ter poljubna vektorja $x, y \in L_\lambda$ in vidimo, da velja:

$$A(\alpha \cdot x + \beta \cdot y) = \alpha \cdot Ax + \beta \cdot Ay = \alpha \cdot \lambda \cdot x + \beta \cdot \lambda \cdot y = \lambda \cdot (\alpha \cdot x + \beta \cdot y)$$

To pomeni, da je tudi $(\alpha \cdot x + \beta \cdot y) \in L_\lambda$. Potem je $(L_\lambda, +, \cdot)$ R-podpolmodul v M, saj je zaprt za podedovani operaciji seštevanja in množenja s skalarjem ter vsebuje θ. To velja za vsako lastno vrednost λ matrike A. □

Vrnimo se k polmodulu $\mathbb{N}_0^n$ in tokrat poglejmo primer diagonalnih matrik $A = \lambda \cdot I$ ter $B = diag(d_1, d_2, \ldots, d_n)$ za $\lambda, d_1, d_2, \ldots, d_n \in \mathbb{N}_0$. Trivialno je videti, da je λ lastna vrednost matrike A za poljuben vektor, torej je $L_\lambda = \mathbb{N}_0^n$. Po drugi strani so $d_1, d_2, \ldots, d_n$ lastne vrednosti matrike B. Lastni vektor za lastno vrednost d_i je kar e_i in $L_{d_i} = \{\mu \cdot e_i;\ \mu \in \mathbb{N}_0\}$ za vsak $i \in \{1, 2, \ldots, n\}$.

Trditev 4.13. *Naj bo R komutativen polkolobar in naj bo $\otimes$ idempotentna operacija (torej $a \otimes a = a$ za vse $a \in R$). Naj bo $M = R^n$ R-polmodul in $A : M \to M$ naj bo $n \times n$ matrika, ki pripada nekemu endomorfizmu h R-polmodula 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 $Av = v$. Hkrati velja $A(\lambda \cdot v) = \lambda \cdot (Av) = \lambda \cdot v$. Na tej točki upoštevamo idempotentnost množenja v R in opazimo $\lambda = \lambda \otimes \lambda$. Potem je $\lambda \cdot v = (\lambda \otimes \lambda) \cdot v = \lambda \cdot (\lambda \cdot v)$. Sledi, da je $\lambda \cdot v$ lastni vektor matrike A za lastno vrednost λ. □

Za konec tega poglavja še pokažimo, kako lahko matriki nad komutativnim dioidom določimo lastne vrednosti, kot je bilo to storjeno v [2, poglavje 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*

$$\bar{A}(\lambda) = \begin{bmatrix} A & \lambda \cdot I \\ I & I \end{bmatrix}$$

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 $J_2 = \{n+1, n+2, \ldots, 2n\}$ ter definiramo koeficiente μ_j na sledeč način:

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

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

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

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

Po drugi strani pa 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 teh stolpcih, da bo veljala enakost (3) za neki neprazni disjunktni indeksni množici $J_1, J_2 \subseteq \{1, 2, \ldots, 2n\}$, pri čemer velja $\mu_j \neq 0$ za vse $j \in J_1 \cup J_2$ in $\mu_j = 0$ za vse $j \notin J_1 \cup J_2$. 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, da je $\mu_j = \mu_{n+j} = 0$, 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, da je $J_1 \subseteq \{1, 2, \ldots, n\}$ 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 vrstic enakosti naslednjo obliko:

$$\sum_{j=1}^{n} v_j \cdot A_j = \sum_{j=1}^{n} v_j \cdot (\lambda \cdot e_j) \tag{4}$$

Opazimo, da je $\sum_{j=1}^{n} v_j \cdot (\lambda \cdot e_j) = \begin{bmatrix} \lambda \otimes v_1 \\ \lambda \otimes v_2 \\ \vdots \\ \lambda \otimes v_n \end{bmatrix} = \lambda \cdot \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}$. Ko dodatno uvedemo oznako $v = (v_1, v_2, \ldots, v_n)^\top$, se zgornja enakost (4) spremeni v enakost oblike $\sum_{j=1}^{n} v_j \cdot A_j = \lambda \cdot v$. Upoštevamo, da je $Av = \sum_{j=1}^{n} v_j \cdot A_j$ in vidimo, 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 [5], dokažemo v posplošeni obliki tudi za matrike nad komutativnimi polkolobarji. Leta 2011 je to nadgradil Radu Grosu v [3], 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 [3].

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 števila 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. Poljubni permutaciji $\pi \in P(n)$ pripada asociiran graf $G(\pi) = (\{1, 2, \ldots, n\}, \{(i, \pi(i));\ i \in \{1, 2, \ldots, n\}\})$. Z asociiranega grafa lahko hitro razberemo parnost permutacije ter tudi njeno dekompozicijo na produkt disjunktnih ciklov. Za dano permutacijo π s $\bar{\pi}$ označimo zaporedje $(1, \pi(1)), (2, \pi(2)), \ldots, (n, \pi(n))$. Na danem produktu $w = w_1 w_2 \ldots w_n$ lahko permutacijo π uporabimo po komponentah, tako da je $\pi(w) = w_{\pi(1)} w_{\pi(2)} \ldots w_{\pi(n)}$. Permutacijo lahko uporabimo tudi na končnih zaporedjih $s = s_1 s_2 \ldots s_n$ dolžine n, tako da i-ti člen zaporedja s_i premaknemo na $\pi(i)$-to mesto.

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 $w = oprs\check{s}$. Potem je $\sigma(w) = por\check{s}s$ in $\pi(w) = po\check{s}rs$. Dodatno je $\sigma(\bar{\pi}) = (2,1)(1,2)(3,5)(5,4)(4,3)$. $\diamondsuit$

5.2. **Pideterminanta in karakteristični pipolinom.** V tem odseku bosta predstavljeni posplošitvi konceptov determinante in karakterističnega polinoma matrike, t. i. *pideterminanta* in *karakteristični pipolinom*.

Najprej se spomnimo, da lahko vsaki kvadratni matriki $X \in M_n(F)$ nad poljem F določimo asociiran usmerjen utežen graf $G(X) = (V, E, X)$, kjer je $V = \{1, 2, \ldots, n\}$ množica vozlišč, $E = \{(i,j) \in V^2;\ x_{ij} \neq 0\}$ pa množica povezav z utežmi X_{ij}. Zaporedju povezav $p_1 p_2 \ldots p_n$ iz E za katerega velja, da je za vsak $i \in \{1, 2, \ldots, n-1\}$ konec povezave p_i hkrati tudi začetek povezave p_{i+1} pravimo *sprehod*. Sprehodu pravimo *pot*, če je omejen in so vozlišča, ki jih obišče, različna, razen morda prvega in zadnjega. Utež poti je enaka produktu uteži povezav, ki jih pot vsebuje. Sklenjeni poti pravimo *cikel*. Sedaj se spomnimo definicije determinante za matrike nad polji.

Definicija 5.3. Naj bo $(F, \oplus, \otimes)$ polje in $X \in M_n(F)$ kvadratna matrika nad F. Potem je determinanta matrike X definirana s predpisom:

$$det(X) = \bigoplus_{\pi \in P(n)} sgn(\pi) x_{1\pi(1)} x_{2\pi(2)} \ldots x_{n\pi(n)}$$

Formulo iz definicije lahko skrajšamo s pomočjo uporabe permutacijskih zaporedij, sprehodov in asociiranih uteži poti na matriki X na naslednji način: Za dano permutacijo π množice z n elementi in permutacijsko zaporedje $\bar{\pi}$ je $\bar{\pi}(X) = (1, \pi(1))(2, \pi(2)) \ldots (n, \pi(n))(X) = X_{1\pi(1)} X_{2\pi(2)} \ldots X_{n\pi(n)}$. Pri tem je X_{ij} element matrike X, ki se nahaja v i-ti vrstici in j-tem stolpcu. Dodatno lahko še permutacije $\pi \in P(n)$ ločimo glede na parnost. Nova formula ima obliko

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

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

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

Oznaki $det^+(X)$ in $det^-(X)$ bosta prišli prav pri obravnavi zapisa pideterminante, katere definicijo navajamo spodaj.

Definicija 5.4. Naj bo R nek polkolobar in $X \in M_n(R)$ kvadratna matrika. Urejeni dvojici podani s predpisom

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

pravimo *pideterminanta* matrike X.

V definiciji pideterminante opazimo, da nastopa dvojna vsota. Posebej za prvo komponento dvojice vidimo, da je $\bigoplus_{\substack{\pi \in P^+(n) \\ \sigma \in P(n)}} \sigma(\bar{\pi}(X)) = \bigoplus_{\sigma \in P(n)} \bigoplus_{\pi \in P^+(n)} \sigma(\bar{\pi}(X))$ in podobno tudi za drugo komponento. Če razumemo uporabo permutacije σ na vsoti produktov $x_{11}x_{12}\ldots x_{1n} \oplus x_{21}x_{22}\ldots x_{2n} \oplus \ldots \oplus x_{n1}x_{n2}\ldots x_{nn}$, torej

$$\sigma(x_{11}x_{12}\ldots x_{1n} \oplus x_{21}x_{22}\ldots x_{2n} \oplus \ldots \oplus x_{n1}x_{n2}\ldots x_{nn})$$

kot vsoto s σ premešanih produktov

$$\sigma(x_{11}x_{12}\ldots x_{1n}) \oplus \sigma(x_{21}x_{22}\ldots x_{2n}) \oplus \ldots \oplus \sigma(x_{n1}x_{n2}\ldots x_{nn})$$

potem lahko vsoto v prvi komponenti zapišemo kot $\bigoplus_{\sigma\in P(n)} \sigma\Big(\bigoplus_{\pi\in P^+(n)} \bar{\pi}(X)\Big) = \bigoplus_{\sigma\in P(n)} \sigma(det^+(X))$. Ko je $\sigma = id$, dobimo v tej vsoti kar $det^+(X)$. Ostale permutacije $\sigma \in P(n)$ nam v resnici dajo podobne vsote, s tem da premešajo vrstne rede faktorjev v členih. V komutativnih polkolobarjih so vse te vsote enake, torej dobimo $n! \cdot det^+(X) = \underbrace{det^+(X) \oplus \ldots \oplus det^+(X)}_{n!\text{-krat}}$. Podobno se v tem primeru zgodi tudi na drugi komponenti. Ko to dvoje združimo dobimo, da je pideterminanta $n \times n$ matrike X nad komutativnim polkolobarjem enaka $pdt(X) = n! \cdot (det^+(X), det^-(X))$. Za produkt ali vsoto produktov w uvedemo še eno oznako:

$$[\![w]\!] = \bigoplus_{\pi\in P(n)} \pi(w)$$

Uporaba te oznake nam omogoča naslednji zapis pideterminante:

$$pdt(X) = ([\![det^+(X)]\!], [\![det^-(X)]\!]) = (pdt^+(X), pdt^-(X))$$

Dodatno, za matriko X nad nekim poljem $(F, \oplus, \otimes)$ velja

$$det(X) = det^+(X) \ominus det^-(X) = \frac{1}{n!}(pdt^+(X) \ominus pdt^-(X))$$

Naslednji zgled bo pokazal uporabo uvedenih pojmov.

Zgled 5.5. Naj bo $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ neka 2×2 matrika nad poljubnim polkolobarjem R. Vemo, da je $P(2) = \{id, (1\ 2)\}$. Pri tem sta $P^+(2) = \{id\}$ in $P^-(2) = \{(1\ 2)\}$. Označimo $\sigma = (1\ 2)$. Za izračun pideterminante bomo najprej potrebovali $det^+(A)$ in $det^-(A)$. Velja:

$$det^+(A) = A_{11}A_{22} = a_{11}a_{22}$$
$$det^-(A) = A_{12}A_{21} = a_{12}a_{21}$$

Sedaj poračunajmo še $[\![det^+(A)]\!]$ in $[\![det^-(A)]\!]$:

$$[\![det^+(A)]\!] = id(a_{11}a_{22}) \oplus \sigma(a_{11}a_{22}) = a_{11}a_{22} \oplus a_{22}a_{11}$$
$$[\![det^-(A)]\!] = id(a_{12}a_{21}) \oplus \sigma(a_{12}a_{21}) = a_{12}a_{21} \oplus a_{21}a_{12}$$

Sledi, da je $pdt(A) = (a_{11}a_{22} \oplus a_{22}a_{11}, a_{12}a_{21} \oplus a_{21}a_{12})$ ♢

Preden definiramo karakteristični pipolinom matrike nad polkolobarjem se spomnimo, kaj je karakteristični polinom matrike nad poljem.

Definicija 5.6. Naj bo F polje in $X \in M_n(F)$ kvadratna matrika nad njim. Karakteristični polinom $p_X(\lambda)$ matrike X je polinom v spremenljivki λ, ki ga določa predpis $p_X(\lambda) = det(X \ominus \lambda \cdot I)$.

Po zgledu determinante lahko tudi karakteristični polinom $p_X(\lambda)$ razdelimo na razliko dveh polinomov:

$$p_X(\lambda) = p_X^+(\lambda) \ominus p_X^-(\lambda)$$

To storimo tako, da vse »pozitivno« predznačene člene $p_X(\lambda)$ označimo s $p_X^+(\lambda)$, pri ostalih pa izpostavimo $\ominus$ in dobljeno vsoto označimo s $p_X^-(\lambda)$. Sedaj definirajmo karakteristični pipolinom matrike nad polkolobarjem.

Definicija 5.7. Naj bo R polkolobar in $X \in M_n(R)$ kvadratna matrika nad njim. *Karakteristični pipolinom* $pp_X(\lambda)$ matrike X v spremenljivki λ je urejen par polinomov definiran s predpisom:

$$pp_X(\lambda) = ([\![p_X^+(\lambda)]\!], [\![p_X^-(\lambda)]\!]) = (pp_X^+(\lambda), pp_X^-(\lambda))$$

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

Definicijo dopolnimo z naslednjim zgledom.

Zgled 5.8. Vrnimo se k matriki A iz zgleda 5.5 in poračunajmo njen karakteristični pipolinom. Tega lahko poračunamo tako, da se najprej pretvarjamo, da delamo nad poljem, nato pa seštejemo »pozitivne« člene v p_A^+, »negativne« pa v p_A^-. Če bi R bil polje, bi karakteristični polinom matrike A imel predpis $P_A(\lambda) = a_{11}a_{22} \oplus \lambda^2 \ominus (a_{11} \oplus a_{22})\lambda \ominus a_{12}a_{21} = a_{11}a_{22} \oplus \lambda^2 \ominus ((a_{11} \oplus a_{22})\lambda \oplus a_{12}a_{21})$. Sledi, da je potem $p_A^+(\lambda) = a_{11}a_{22} \oplus \lambda^2$ in $p_A^-(\lambda) = (a_{11} \oplus a_{22})\lambda \oplus a_{12}a_{21}$. Sedaj lahko poračunamo $pp_A^+(\lambda)$ in $pp_A^-(\lambda)$.

$$\begin{aligned}
pp_A^+(\lambda) &= [\![\lambda^2 \oplus a_{11}a_{22}]\!] = \lambda^2 \oplus a_{11}a_{22} \oplus \sigma(\lambda^2) \oplus \sigma(a_{11}a_{22}) \\
&= \lambda^2 \oplus a_{11}a_{22} \oplus \lambda^2 \oplus a_{22}a_{11} \\
pp_A^-(\lambda) &= [\![(a_{11} \oplus a_{22})\lambda \oplus a_{12}a_{21}]\!] \\
&= (a_{11} \oplus a_{22})\lambda \oplus a_{12}a_{21} \oplus \sigma((a_{11} \oplus a_{22})\lambda) \oplus \sigma(a_{12}a_{21}) \\
&= (a_{11} \oplus a_{22})\lambda \oplus a_{12}a_{21} \oplus \lambda(a_{11} \oplus a_{22}) \oplus a_{21}a_{12}
\end{aligned}$$

Sledi, da je karakteristični pipolinom matrike A enak

$$pp_A(\lambda) = (\lambda^2 \oplus a_{11}a_{22} \oplus \lambda^2 \oplus a_{22}a_{11}, (a_{11} \oplus a_{22})\lambda \oplus a_{12}a_{21} \oplus \lambda(a_{11} \oplus a_{22}) \oplus a_{21}a_{12})$$

♢

Opazimo, da je za matriko X nad nekim poljem F karakteristični polinom enak

$$p_X(\lambda) = \frac{1}{n!}(pp_X^+(\lambda) \ominus pp_X^-(\lambda))$$

Sedaj lahko končno preidemo na obravnavo posplošenega Cayley-Hamiltonovega izreka, kar bomo storili v naslednjem poglavju.

5.3. **Cayley-Hamiltonov izrek nad polkolobarji.** V tem podpoglavju bomo navedli posplošeni Cayley-Hamiltonov izrek in demonstrirali veljavnost na 2×2 kvadratnih matrikah. Dodatno bomo navedli idejo dokaza izreka, dokaz pa bo opuščen.

Izrek 5.9 (Cayley-Hamilton)**.** *Naj bo F polje in $X \in M_n(F)$ neka kvadratna matrika in naj bo $p_X(\lambda)$ njen karakteristični polinom. Potem je $p_X(X) = 0$.*

Seveda, če upoštevamo zapis $p_X(\lambda) = p_X^+(\lambda) \ominus p_X^-(\lambda)$ iz izreka sledi $p_X^+(X) = p_X^-(X)$. Pri vstavljanju matrike X v $p_X(\lambda)$ sledimo konvenciji in vsako potenco λ^n nadomestimo z X^n, vsako konstanto $c \in F$ pa s $c \cdot I$. Poleg tega vsak produkt tipa $c \cdot \lambda$ nadomestimo s $c \cdot X$. Posebej omenimo, da $\oplus$ zamenjamo s $+$.

V primeru matrike $X = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}$ nad poljem F, vemo, da je njen karakteristični polinom $p_X(\lambda) = \lambda^2 \ominus (x_{11} \oplus x_{22})\lambda \oplus (x_{11}x_{22} \ominus x_{12}x_{21})$, torej je potem $p_X(X) = X^2 \ominus (x_{11} \oplus x_{22}) \cdot X \oplus (x_{11}x_{22} \ominus x_{12}x_{21}) \cdot I = 0$.

V primeru karakterističnega pipolinoma moramo biti malce bolj previdni. Razlog za to lahko vidimo že v primeru 2×2 matrike A iz zgledov. Posebej poglejmo razliko med $[\![p_A^+(\lambda)]\!]$ in $[\![p_A^+(A)]\!]$. V primeru $[\![p_A^+(\lambda)]\!] = [\![\lambda^2 \oplus a_{11}a_{22}]\!]$ nastopa člen $\sigma(\lambda^2)$, kjer je $\sigma = (1\ 2)$. Tukaj uporaba σ na λ^2 preprosto pomeni zamenjavo vrstnega reda množenja. V $[\![p_A^+(A)]\!]$ pa nastopa člen $\sigma(A^2)$, ki pa potrebuje pravilno interpretacijo. V prvi vrsti se zavedajmo, da bo, za vsako matriko X nad nekim polkolobarjem in za vsak $n \in \mathbb{N}$, vsaka komponenta matrike X^n vsota produktov n elementov. Obe komponenti $pp_X(\lambda)$ bosta polinoma stopnje največ n. Ko v kateregakoli od teh polinomov vstavimo X, bomo dobili vsoto $n \times n$ matrik, ki bodo, po tem ko poračunamo skalarno množenje vsakega člena, v vsaki komponenti imele vsote produktov n elementov. Ko potem na kakem izmed teh členov uporabimo permutacijo $\mu \in P(n)$, to storimo po komponentah:

$$\mu(X^n) = \left[\mu(X_{ij}^n)\right]_{ij}$$

Tukaj tudi upoštevamo, da ko uporabimo permutacijo μ na vsoti produktov n elementov, to razumemo kot vsoto produktov, katerih faktorji so bili premešani z μ. Dodatno za potrebe permutiranja vsak člen oblike a_{ij}^k razumemo kot $\underbrace{a_{ij}a_{ij}\ldots a_{ij}}_{k\text{-krat}}$.

Poglejmo si to na konkretnem primeru.

Zgled 5.10. Ponovno se vrnimo k matriki A iz zgledov 5.5 in 5.8. Vemo že, da je $pp_A(\lambda) = ([\![\lambda^2 \oplus a_{11}a_{22}]\!], [\![(a_{11} \oplus a_{22})\lambda \oplus a_{21}a_{12}]\!])$. Vstavimo A v njen karakteristični pipolinom in dobimo $pp_A(A) = (pp_A^+(A), pp_A^-(A)) = ([\![A^2 + a_{11}a_{22} \cdot I]\!], [\![(a_{11} \oplus a_{22}) \cdot A + a_{21}a_{12} \cdot I]\!])$. Poračunajmo vsako komponento posebej.

$$\begin{aligned}
A^2 &= \begin{bmatrix} a_{11}^2 \oplus a_{12}a_{21} & a_{11}a_{12} \oplus a_{12}a_{22} \\ a_{21}a_{11} \oplus a_{22}a_{21} & a_{21}a_{12} \oplus a_{22}^2 \end{bmatrix} \\
\sigma(A^2) &= \sigma\left(\begin{bmatrix} a_{11}^2 \oplus a_{12}a_{21} & a_{11}a_{12} \oplus a_{12}a_{22} \\ a_{21}a_{11} \oplus a_{22}a_{21} & a_{21}a_{12} \oplus a_{22}^2 \end{bmatrix} \right) \\
&= \begin{bmatrix} \sigma(a_{11}^2) \oplus \sigma(a_{12}a_{21}) & \sigma(a_{11}a_{12}) \oplus \sigma(a_{12}a_{22}) \\ \sigma(a_{21}a_{11}) \oplus \sigma(a_{22}a_{21}) & \sigma(a_{21}a_{12}) \oplus \sigma(a_{22}^2) \end{bmatrix} \\
&= \begin{bmatrix} a_{11}^2 \oplus a_{21}a_{12} & a_{12}a_{11} \oplus a_{22}a_{12} \\ a_{11}a_{21} \oplus a_{21}a_{22} & a_{12}a_{21} \oplus a_{22}^2 \end{bmatrix}
\end{aligned}$$

Od tod sledi

$$\begin{aligned}
pp_A^+(A) &= [\![A^2 + a_{11}a_{22} \cdot I]\!] = A^2 + \sigma(A^2) + a_{11}a_{22} \cdot I + \sigma(a_{11}a_{22} \cdot I) \\
&= \begin{bmatrix} a_{11}^2 \oplus a_{12}a_{21} & a_{11}a_{12} \oplus a_{12}a_{22} \\ a_{21}a_{11} \oplus a_{22}a_{21} & a_{21}a_{12} \oplus a_{22}^2 \end{bmatrix} + \begin{bmatrix} a_{11}^2 \oplus a_{21}a_{12} & a_{12}a_{11} \oplus a_{22}a_{12} \\ a_{11}a_{21} \oplus a_{21}a_{22} & a_{12}a_{21} \oplus a_{22}^2 \end{bmatrix} \\
&+ \begin{bmatrix} a_{11}a_{22} & 0 \\ 0 & a_{11}a_{22} \end{bmatrix} + \begin{bmatrix} a_{22}a_{11} & 0 \\ 0 & a_{22}a_{11} \end{bmatrix}
\end{aligned}$$

Ko vse matrike seštejemo, dobimo

$$\begin{bmatrix} 2a_{11}^2 \oplus a_{21}a_{12} \oplus a_{12}a_{21} \oplus a_{11}a_{22} \oplus a_{22}a_{11} & a_{11}a_{12} \oplus a_{12}a_{22} \oplus a_{12}a_{11} \oplus a_{22}a_{12} \\ a_{21}a_{11} \oplus a_{22}a_{21} \oplus a_{11}a_{21} \oplus a_{21}a_{22} & a_{21}a_{12} \oplus a_{12}a_{21} \oplus 2a_{22}^2 \oplus a_{11}a_{22} \oplus a_{22}a_{11} \end{bmatrix}$$

Poračunajmo še $pp_A^-(A)$. Da nam bo lažje najprej poračunamo člene:

$$\begin{aligned}(a_{11} \oplus a_{22}) \cdot A &= \begin{bmatrix} a_{11}^2 \oplus a_{22}a_{11} & a_{11}a_{12} \oplus a_{22}a_{12} \\ a_{11}a_{21} \oplus a_{22}a_{21} & a_{11}a_{22} \oplus a_{22}^2 \end{bmatrix} \\ \sigma((a_{11} \oplus a_{22}) \cdot A) &= \begin{bmatrix} \sigma((a_{11} \oplus a_{22})a_{11}) & \sigma((a_{11} \oplus a_{22})a_{12}) \\ \sigma((a_{11} \oplus a_{22})a_{21}) & \sigma((a_{11} \oplus a_{22})a_{22}) \end{bmatrix} \\ &= \begin{bmatrix} a_{11}(a_{11} \oplus a_{22}) & a_{12}(a_{11} \oplus a_{22}) \\ a_{21}(a_{11} \oplus a_{22}) & a_{22}(a_{11} \oplus a_{22}) \end{bmatrix} \\ &= \begin{bmatrix} a_{11}^2 \oplus a_{11}a_{22} & a_{12}a_{11} \oplus a_{12}a_{22} \\ a_{21}a_{11} \oplus a_{21}a_{22} & a_{22}a_{11} \oplus a_{22}^2 \end{bmatrix}\end{aligned}$$

$$\begin{aligned}pp_A^-(A) &= [\![(a_{11} \oplus a_{22}) \cdot A + a_{21}a_{12} \cdot I]\!] \\ &= (a_{11} \oplus a_{22}) \cdot A + \sigma((a_{11} \oplus a_{22}) \cdot A) + a_{21}a_{12} \cdot I + \sigma(a_{21}a_{12} \cdot I) \\ &= (a_{11} \oplus a_{22}) \cdot A + A \cdot (a_{11} \oplus a_{22}) + a_{21}a_{12} \cdot I + a_{12}a_{21} \cdot I \\ &= \begin{bmatrix} a_{11}^2 \oplus a_{22}a_{11} & a_{11}a_{12} \oplus a_{22}a_{12} \\ a_{11}a_{21} \oplus a_{22}a_{21} & a_{11}a_{22} \oplus a_{22}^2 \end{bmatrix} + \begin{bmatrix} a_{11}^2 \oplus a_{11}a_{22} & a_{12}a_{11} \oplus a_{12}a_{22} \\ a_{21}a_{11} \oplus a_{21}a_{22} & a_{22}a_{11} \oplus a_{22}^2 \end{bmatrix} \\ &+ \begin{bmatrix} a_{21}a_{12} \oplus a_{12}a_{21} & 0 \\ 0 & a_{21}a_{12} \oplus a_{12}a_{21} \end{bmatrix}\end{aligned}$$

Ko seštejemo vse člene tokrat dobimo

$$\begin{bmatrix} 2a_{11}^2 \oplus a_{11}a_{22} \oplus a_{22}a_{11} \oplus a_{21}a_{12} \oplus a_{12}a_{21} & a_{12}a_{11} \oplus a_{12}a_{22} \oplus a_{11}a_{12} \oplus a_{22}a_{12} \\ a_{21}a_{11} \oplus a_{21}a_{22} \oplus a_{11}a_{21} \oplus a_{22}a_{21} & a_{22}a_{11} \oplus 2a_{22}^2 \oplus a_{11}a_{22} \oplus a_{21}a_{12} \oplus a_{12}a_{21} \end{bmatrix}$$

oziroma

$$\begin{bmatrix} 2a_{11}^2 \oplus a_{21}a_{12} \oplus a_{12}a_{21} \oplus a_{11}a_{22} \oplus a_{22}a_{11} & a_{11}a_{12} \oplus a_{12}a_{22} \oplus a_{12}a_{11} \oplus a_{22}a_{12} \\ a_{21}a_{11} \oplus a_{22}a_{21} \oplus a_{11}a_{21} \oplus a_{21}a_{22} & a_{21}a_{12} \oplus a_{12}a_{21} \oplus 2a_{22}^2 \oplus a_{11}a_{22} \oplus a_{22}a_{11} \end{bmatrix}$$

Spotoma smo torej pokazali, da je $pp_A^+(A) = pp_A^-(A)$. ♢

Izkaže se, da sklep na koncu zgleda 5.10 velja tudi v splošnem za poljubno kvadratno matriko nad polkolobarjem. Temu rezultatu pravimo *Cayley-Hamiltonov izrek nad polkolobarji*. Formalno zapišimo ta izrek in nato navedimo idejo dokaza.

Izrek 5.11. *Naj bo R poljuben polkolobar in $X \in M_n(R)$ neka kvadratna matrika nad R. Potem je $pp_X^+(X) = pp_X^-(X)$.*

V zgledu 5.10 smo pokazali izrek za $n = 2$ tako, da smo direktno poračunali komponenti pipolinoma, v dokazu pa bomo postopoma skonstruirali obe komponenti na tak način, da bo veljala enakost iz izreka. Dodatno ta pristop utemeljimo s pomočjo matriki asociiranih grafov, kot so definirani v [3, poglavje 4].

Definicija 5.12. Naj bo R nek polkolobar in $X \in M_n(R)$ matrika. Matriki X *asociiran usmerjen utežen graf* je graf $G(X)$, za katerega je $V = \{1, 2, \ldots, n\}$ množica vozlišč in $E = \{(i, j) \in V(X)^2;\ X_{ij} \neq 0\}$ množica povezav. Vsaki povezavi $e_{ij} \in E$ pripada utež X_{ij}.

Demonstrirajmo postopek konstrukcije na primeru $n = 2$. Z LS_i označimo levo stran enakosti v i-tem koraku, z DS_i pa desno stran enakosti v i-tem koraku. Naj bo R polkolobar in $X \in M_2(R)$ s predpisom $X = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}$. Za LS_0 določimo

$LS_0 = X^2 = \begin{bmatrix} x_{11}x_{11} \oplus x_{12}x_{21} & x_{11}x_{12} \oplus x_{12}x_{22} \\ x_{21}x_{11} \oplus x_{22}x_{21} & x_{21}x_{12} \oplus x_{22}x_{22} \end{bmatrix}$. Opazimo, da je vsaka komponenta X^2 vsota produktov dolžine 2, kjer je vsak produkt enak uteži na neki poti v asociiranem grafu $G(X)$. Ker ima $G(X)$ n vozlišč more biti vsaj ena od teh poti cikel. Z $diag_s(X^2)$ označimo skrčitev diagonale matrike X^2 na produkte, ki predstavljajo utež nekega cikla v $G(X)$, s $Tr_s(X^2)$ pa označimo vsoto produktov iz $diag_s(X^2)$. Vidimo, da sta $diag_s(X^2) = \{x_{12}x_{21}, x_{21}x_{12}\}$ in $Tr_s(X^2) = x_{12}x_{21} \oplus x_{21}x_{12}$. S pomočjo tega določimo začetno desno stran enakosti $DS_0 = Tr_s(X^2) \cdot I$. Vse uteži ciklov v $Tr_s(X^2)$ so permutacije uteži cikla, ki izhaja v vozlišču 1. V tem primeru sta to $\pi_1 = id$ in $\pi_2 = (1\ 2)$. Drugače povedano, $DS_0 = \sum_{i=1}^{2} \pi_i(x_{12}x_{21}) \cdot I = \begin{bmatrix} x_{12}x_{21} \oplus x_{21}x_{12} & 0 \\ 0 & x_{12}x_{21} \oplus x_{21}x_{12} \end{bmatrix}$. Posledica množenja z matrično identiteto I nam vsili »odvečne« uteži na določenih mestih. Posebej, v $(X^2)_{11}$ imamo člen $x_{12}x_{21}$, nimamo pa člena $x_{21}x_{12}$. Ta problem rešimo tako, da levo stran spremenimo v vsoto teh enakih permutacij $LS_1 = \sum_{i=1}^{2} \pi_i(X^2) = \begin{bmatrix} x_{11}x_{11} \oplus x_{12}x_{21} \oplus x_{11}x_{11} \oplus x_{21}x_{12} & x_{11}x_{12} \oplus x_{12}x_{22} \oplus x_{12}x_{11} \oplus x_{22}x_{12} \\ x_{21}x_{11} \oplus x_{22}x_{21} \oplus x_{11}x_{21} \oplus x_{21}x_{22} & x_{21}x_{12} \oplus x_{22}x_{22} \oplus x_{12}x_{21} \oplus x_{22}x_{22} \end{bmatrix}$. Seveda to vsili nove odvečne uteži na levi strani, kar popravimo tako, da uteži na ciklih dolžine 1 dodamo na desno stran in to potem uravnotežimo na levi strani. Edina prava cikla dolžine 1 imata uteži x_{11} in x_{22}. Če iz LS_1 odmislimo elemente, ki so že v DS_0, nam ostane matrika

$$\begin{bmatrix} x_{11}x_{11} \oplus x_{11}x_{11} & x_{11}x_{12} \oplus x_{12}x_{22} \oplus x_{12}x_{11} \oplus x_{22}x_{12} \\ x_{21}x_{11} \oplus x_{22}x_{21} \oplus x_{11}x_{21} \oplus x_{21}x_{22} & x_{22}x_{22} \oplus x_{22}x_{22} \end{bmatrix}$$
$$= \begin{bmatrix} x_{11}x_{11} & x_{11}x_{12} \\ x_{11}x_{21} & 0 \end{bmatrix} + \begin{bmatrix} x_{11}x_{11} & x_{12}x_{22} \oplus x_{12}x_{11} \oplus x_{22}x_{12} \\ x_{21}x_{11} \oplus x_{22}x_{21} \oplus x_{21}x_{22} & x_{22}x_{22} \oplus x_{22}x_{22} \end{bmatrix}$$
$$= \begin{bmatrix} x_{11}x_{11} & x_{11}x_{12} \\ x_{11}x_{21} & 0 \end{bmatrix} + \begin{bmatrix} 0 & x_{22}x_{12} \\ x_{22}x_{21} & x_{22}x_{22} \end{bmatrix} + \begin{bmatrix} x_{11}x_{11} & x_{12}x_{22} \oplus x_{12}x_{11} \\ x_{21}x_{11} \oplus x_{21}x_{22} & x_{22}x_{22} \end{bmatrix}$$
$$= \begin{bmatrix} x_{11}x_{11} & x_{11}x_{12} \\ x_{11}x_{21} & 0 \end{bmatrix} + \begin{bmatrix} 0 & x_{22}x_{12} \\ x_{22}x_{21} & x_{22}x_{22} \end{bmatrix} + \begin{bmatrix} x_{11}x_{11} & x_{12}x_{11} \\ x_{21}x_{11} & 0 \end{bmatrix} + \begin{bmatrix} 0 & x_{12}x_{22} \\ x_{21}x_{22} & x_{22}x_{22} \end{bmatrix}$$

Opazimo, da se prva in tretja matrika razlikujeta samo v tem, da so produkti v komponentah premešani. Enako opazimo za drugo in četrto matriko v vsoti. Poleg tega lahko v vsaki matriki izpostavimo en faktor. Ko to storimo, izgleda vsota tako:

$$x_{11} \cdot \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & 0 \end{bmatrix} + x_{22} \cdot \begin{bmatrix} 0 & x_{12} \\ x_{21} & x_{22} \end{bmatrix} + \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & 0 \end{bmatrix} \cdot x_{11} + \begin{bmatrix} 0 & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \cdot x_{22}$$

Matrike, ki preostanejo, so zelo blizu matriki X, zato bomo na desno stran prišteli $x_{11} \cdot X + x_{22} \cdot X + X \cdot x_{11} + X \cdot x_{22} = (x_{11} \oplus x_{22}) \cdot X + X \cdot (x_{11} \oplus x_{22}) = \sum_{i=1}^{2} \pi_i((x_{11} \oplus x_{22}) \cdot X)$. Torej je $DS_1 = \sum_{i=1}^{2} \pi_i((x_{11} \oplus x_{22}) \cdot X) + \sum_{i=1}^{2} \pi_i(x_{12}x_{21}) \cdot I = \sum_{i=1}^{2} \pi_i((x_{11} \oplus x_{22}) \cdot X + x_{12}x_{21} \cdot I) = [\![(x_{11} \oplus x_{22}) \cdot X + x_{12}x_{21} \cdot I]\!] = pp_X^-(X)$. Ko iz matrike DS_1 odmislimo vse člene, ki se nahajajo v LS_1, nam ostane matrika

$$\begin{bmatrix} x_{11}x_{22} \oplus x_{22}x_{11} & 0 \\ 0 & x_{11}x_{22} \oplus x_{22}x_{11} \end{bmatrix} = \begin{bmatrix} x_{11}x_{22} & 0 \\ 0 & x_{11}x_{22} \end{bmatrix} + \begin{bmatrix} x_{22}x_{11} & 0 \\ 0 & x_{22}x_{11} \end{bmatrix}$$

LS_1 je treba torej prišteti še $\sum_{i=1}^{2} \pi_i(x_{11}x_{22} \cdot I)$. Sledi, da je $LS_2 = \sum_{i=1}^{2} \pi_i(X^2) + \sum_{i=1}^{2} \pi_i(x_{11}x_{22} \cdot I) = \sum_{i=1}^{2} \pi_i(X^2 + x_{11}x_{22} \cdot I) = [\![X^2 + x_{11}x_{22} \cdot I]\!] = pp_X^+(X)$. V tem zadnjem koraku nismo pridobili nobenih »odvečnih« uteži, torej se postopek tukaj zaključi in sledi enakost $pp_X^+(X) = LS_2 = DS_1 = pp_X^-(X)$.

Enak postopek lahko uporabimo za poljubno $n \times n$ matriko $X \in M_n(R)$. Začnemo torej z $LS_0 = X^n$ in $DS_0 = Tr_s(X^n) \cdot I$ oziroma $LS_1 = [\![X^n]\!]$ ter $DS_1 = [\![Tr_s(X^n) \cdot I]\!]$. Nato izmenično na vsaki strani »popravimo« t. i. »odvečne« člene v komponentah, dokler ne dosežemo, da je na desni strani $pp_X^-(X)$, na levi pa $pp_X^+(X)$.

Na koncu navedemo opazko, da je Cayley-Hamiltonov izrek nad polkolobarji res posplošitev Cayley-Hamiltonovega izreka za matrike nad polji. Res, če je R polje in $X \in M_n(R)$ kvadratna matrika, potem iz Cayley-Hamiltonovega izreka nad polkolobarji seveda sledi enakost $pp_X^+(A) = pp_X^-(A)$ iz nje pa sledi $p_X(A) = \frac{1}{n!}(pp_X^+(A) \ominus pp_X^-(A)) = 0$.

Slovar strokovnih izrazov

base of a semimodule baza polmodula – linearno neodvisna podmnožica v polmodulu, ki ga generira
cancellative element okrajšljiv element
canonical preorder relation kanonična relacija šibke urejenosti
canonical order relation kanonična relacija delne urejenosti
canonically ordered set kanonično urejena množica
characteristic pipolynomial karakteristični pipolinom
characteristic polynomial karakteristični polinom
complete dioid poln dioid
complete for the dual order set dualno polna množica
complete lattice polna mreža
complete set polna množica
cycle cikel
determinant determinanta
dioid dioid
directed graph usmerjen graf
eigen-semimodule lastni polmodul
eigenvalue lastna vrednost
eigenvector lastni vektor
endomorphism endomorfizem
factor rank faktorski rang
finitely generated semimodule končno generiran polmodul
free semimodule prosti polmodul
free set in a semimodule prosta množica v polmodulu
free base of a semimodule prosta baza polmodula
homomorphism (of semirings, dioids, semimodules, moduloids, ...) homomorfizem (polkolobarjev, dioidov, polmodulov, moduloidov, ...)
ideal of a semiring ideal polkolobarja
left dioid levi dioid
left ideal levi ideal
left semimodule levi polmodul
left semiring levi polkolobar
lower bound spodnja meja
linear combination linearna kombinacija
linear independence linearna neodvisnost
linear transformation linearna preslikava

matrix associated weighted directed graph matriki asociiran utežen usmerjen graf
moduloid moduloid
ordered set urejena množica
partial order relation relacija delne urejenosti
partial permutation delna permutacija
partially ordered set delno urejena množica
path pot
path weight utež poti
permutation permutacija
pideterminant pideterminanta
positivity condition pogoj pozitivnosti
pre-semiring pred-polkolobar
quotient semimodule kvocientni polmodul
rank of a semimodule rang polmodula
reducible vector razcepen vektor
right dioid desni dioid
right ideal desni ideal
right semimodule desni polmodul
right semiring desni polkolobar
semifield polpolje
semimodule polmodul
semiring polkolobar
sign of a permutation parnost permutacije
subdioid poddioid
subsemimodule poldpomodul
subsemiring podpolkolobar
supremum supremum
the Cayley-Hamilton theorem Cayley-Hamiltonov izrek
the element $0 \in R$ is absorbing for $\otimes$ element $0 \in R$ izniči operacijo $\otimes$
the Perron-Frobenius Theorem Perron-Frobeniusov izrek
top-element vrhnji element
transition matrix prehodna matrika
transposition transpozicija
weak dimension of a semimodule šibka dimenzija polmodula
weak linear independence šibka linearna neodvisnost
weak base of a semimodule šibka baza polmodula
weighted graph utežen graf
weighted path utežena pot

Literatura

[1] 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.

[2] 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`.

[3] 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.
[4] C. Reutenauer in H. Straubing, *Inversion of matrices over a commutative semiring*, Journal of Algebra **88** (1984) 350–360.
[5] 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.
[6] Y. J. Tan, *Bases in semimodules over commutative semirings*, v: Linear Algebra Appl. **443** (2014) 139–152.