UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Jimmy Zakeršnik

Linearna algebra nad polkolobarji

Delo diplomskega seminarja

Mentor: prof. dr. Tomaž Košir

Ljubljana, 2021/22

Kazalo

Linearna algebra nad polkolobarji

Povzetek

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

Linearn algebra over semirings

Abstract

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

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

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

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

1. Uvod

Polkolobarji so algebraična struktura, s katero se srečamo, čim začnemo obravnavati številske množice. Med primere spadajo množica nenegativnih celih števil, množica nenegativnih racionalnih števil, množica nenegativnih realnih števil, razne strukture nad množicami, ki se izkažejo kot uporabne v topologiji, t. i. tropski polkolobarji, ki se uporabljajo za ocenjevanje učinkovitosti zaposlenih itd. Uporabo imajo tudi v teoretični računalniški znanosti in kriptografiji.

Kljub njihovi uporabnosti in pogostem pojavljanju, tako polkolobarji kot strukture nad njimi v sklopu standardne matematične izobrazbe eksplicitno ne prejmejo kaj dosti pozornosti. Poleg popolnoma praktičnih motivacij za obravnavo teh struktur se izkaže, da nas obravnava polkolobarjev oz. linearne algebre nad njimi privede tudi do bistva definicij določenih lastnosti in konceptov v klasični linearni algebri nad vektorskimi prostori.

V tem delu bom obravnaval nekaj razmeroma osnovnih lastnosti polkolobarjev (in v manjši meri tudi dioidov) ter linearne algebre nad njimi. V drugem razdelku bom na kratko definiral in obravnaval polkolobarje, njihove posebne primere in trditve, ki jih lahko dokažemo o njih. Nato bom v tretjem razdelku definiral polmodule – posplošitve modulov. Pri polmodulih bom obravnaval tipična vprašanja, ki se nanašajo na vektorske prostore v klasični linearni algebri, kot so vprašanje obstoja baze, obstoja dimenzije, itd. Sledila bo definicija linearnih preslikav in matrik nad polkolobarji ter obravnava lastnosti le teh v četrtem razdelku. Posebej bom pozornost posvetil posplošitvam konceptov determinante v petem razdelku in karakterističnega polinoma v šestem razdelku. Na koncu bom v sedmem razdelku obravnaval posplošen Cayley-Hamiltonov izrek.

Za začetek obravnavajmo motivacijski primer, ki nam bo pokazal, da četudi operaciji $\oplus$ in $\otimes$ na neki algebrajski strukturi $(E, \oplus, \otimes)$ nista obrnljivi, še vedno lahko rešujemo določene tipe enačb. Primer je povzet iz [2].

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

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

$\diamondsuit$

Izkaže se, da lahko nad polkolobarji počnemo več kot le reševanje preprostih enačb. Da to vidimo je dovolj, da obravnavamo kvadratne matrike nad $\mathbb{R}_+$. Perron-Frobeniusov izrek nam namreč zagotovi, da bo vsaka kvadratna matrika $A \in \mathbb{R}_+^{n \times n}$ imela pozitivno realno lastno vrednost, torej $\lambda \in \mathbb{R}_+ \setminus \{0\}$ in da bo pripadajoč lasten vektor imel vse koeficiente iz $\mathbb{R}_+ \setminus \{0\}$. Torej lahko govorimo ne samo o rešitvah enačb, ampak tudi o matrikah in lastnih vrednostih, čeprav niti $(\mathbb{R}_+, +, \cdot)$ niti $(\mathbb{R}_+ \setminus \{0\}, +, \cdot)$ nista polji. Ta tip matrik (in prej omenjen izrek) je relevanten v verjetnosti, predvsem v teoriji dinamičnih sistemov. Struktura $(\mathbb{R}_+, +, \cdot)$ tudi igra fundamentalno vlogo v teoriji mere in v verjetnosti.

2. Monoidi, polkolobarji in dioidi:

V tem razdelku bomo obravnavali definicije pojmov, ki jih bomo obravnavali skozi celo nalogo. Za začetek bomo osvežili znanje o že znanih monoidih, preden se lotimo novih konceptov kot so polkolobarji in dioidi.

2.1. **Monoidi:**

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*.

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*.

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

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

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

Opomba 2.4. Če je $(R, \oplus)$ komutativen monoid, mu lahko priredimo t. i. kanonično šibko urejenost na sledeč način:

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

Ta relacija je zaradi obstoja nevtralnega elementa refleksivna, poleg tega je pa tudi tranzitivna:

$$a \leq b \text{ in } b \leq c \Rightarrow \exists d, e \in R : b = a \oplus d \text{ in } c = b \oplus e$$
$$\text{torej je } c = a \oplus d \oplus e = a \oplus (d \oplus e) \text{torej } a \leq c.$$

Kanonična šibka urejenost že zadošča pogoju usklajenosti s komutativno notranjo operacijo $\oplus$, ki je zapisana v definiciji urejenega (komutativnega) monoida:

$$a \leq b \Rightarrow \exists c \in R : b = a \oplus c$$
$$\forall d \in R : b \oplus d = a \oplus c \oplus d = a \oplus d \oplus c$$
$$\text{torej velja } a \oplus d \leq b \oplus d.$$

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.

Definicija 2.5. Za komutativen monoid $(R, \oplus)$, ki je kanonično šibko urejen z $\leq$, pravimo, da je *kanonično* urejen, če je $\leq$ delna urejenost (torej, če je antisimetrična).

Sedaj se lahko lotimo prvega zanimivega rezultata, ki nam bo pomagal s klasifikacijo monoidov.

Izrek 2.6. *Monoid ne more hkrati biti grupa in kanonično urejen.*

Dokaz. Naj bo $(E, \oplus)$ grupa in za vsak element $a \in E$ označimo njegov inverz kot a^{-1}. Denimo, da je ta grupa tudi kanonično urejena in naj bosta a ter b dva poljubna različna elementa iz E (torej $a \neq b$).
Ker je $(E, \oplus)$ grupa obstaja tak $c \in E$, da je $a = b \oplus c$, torej je $b \leq a$ (zadošča, da vzamemo $c = b^{-1} \oplus a$). Poleg tega obstaja tak $d \in E$, da je $b = a \oplus d$ (vzamemo kar $d = a^{-1} \oplus b$), torej je $a \leq b$. Potem po antisimetričnosti sledi $a = b$, torej smo prišli v protislovje. □

Opomba 2.7. Izrek 2.6 nas, kot je bilo že prej omenjeno, privede do klasifikacije monoidov. Razred vseh monoidov lahko 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 pa imajo še eno zanimivo lastnost, ki nam je znana iz aritmetike nad nenegativnimi celimi števili $\mathbb{N}_0$.

Trditev 2.8. *V kanonično urejenem monoidu $(E, \oplus)$ velja naslednje:*

$$\forall a, b \in E : a \oplus b = 0 \Rightarrow a = 0 \ \& \ b = 0$$

Dokaz. Denimo, da velja $a \oplus b = 0$. Od tod sledi $a \leq 0$ in $b \leq 0$. Hkrati pa velja $a = 0 \oplus a$ in $b = 0 \oplus b$, torej velja tudi $0 \leq a$ in $0 \leq b$. Po antisimetričnosti potem sledi $a = 0$ in $b = 0$. □

Opomba 2.9. Če v strukturi $(E, \oplus)$ velja $\forall a, b \in E : a \oplus b \Rightarrow a = 0 = b$ pravimo, da je brez vsote nič. Tipičen primer, ki zadošča tej lastnosti, je $(\mathbb{N}_0, +)$. Opazimo lahko tudi, da v komutativnem monoidu ta lastnost implicira antisimetričnost kanonične šibke urejenosti. Res, denimo $a \leq b$ in $b \leq a$. Potem $\exists c, d \in E$, da velja $b = a \oplus c$ in $a = b \oplus d$. Ko prvo enakost vstavimo v drugo, dobimo $a = (a \oplus c) \oplus d = a \oplus (c \oplus d)$, od tod pa sklepamo $d \oplus d = 0$. Po predpostavki sledi $c = 0$ in $d = 0$, torej $a = b$.

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

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

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

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

Opomba 2.11. Če je $1 = 0$, potem je avtomatsko $R = \{0\}$. Ker nas ta trivialen primer ne zanima, predpostavimo $1 \neq 0$ od zdaj naprej.

Opomba 2.12. Dodatno lahko definirano *levi polkolobar* na enak način kot polkolobar, le da zahtevamo samo levo distributivnost in analogno lahko definiramo tudi *desni polkolobar*. $(R, \oplus, \otimes)$ je potem polkolobar če je hkrati levi in desni polkolobar.

Opomba 2.13. 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.

Zgled 2.14. 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. ♢

Zgled 2.15. V tem zgledu bomo obravnavali poseben tip polkolobarja, ki se definira na (pod)množicah: Naj bo X neprazna množica in $S \subseteq P(X)$ neprazen nabor podmnožic množice X. Nabor S je polkolobar (pod)množic za operaciji unije in preseka, če zanj velja:

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

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

Definicija 2.16. 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.

Hitro se da videti, da če je $(R, \oplus, \otimes)$ polkolobar, je $(V(R), \oplus, \otimes)$ kolobar. Če je R komutativen polkolobar, je $V(R)$ komutativen kolobar.

Lema 2.17. *Naj bo $(R, \oplus, \otimes)$ komutativen polkolobar.*
Potem velja $\forall p, q \in V(R), \forall r \in R : (-p) \otimes r = -(p \otimes r)$ & $(-p) \otimes (-q) = p \otimes q$.

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

Razred polkolobarjev lahko s pomočjo izreka 2.6 naravno razdelimo na disjunktne podrazrede, glede na to, ali $\oplus$ opremi množico R s strukturo abelove grupe ali s strukturo kanonično urejenega monoida ali pa z nobeno od prej navedenih struktur. Prej omenjen izrek 2.6 nam namreč pove, da $(R, \oplus, \otimes)$ (oziroma $(R, \oplus)$) ne more hkrati zadostiti prvi in drugi lastnosti. 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.

Zgled 2.18. Denimo, da imamo m polkolobarjev $(R_i, \oplus_i, \otimes_i)$; $i \in \{1, 2, \ldots, m\}$. Potem označimo $R = R_1 \times \ldots \times R_m$ in elementi iz R so oblike $x = \begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix}$. Za

$\forall x, y \in R$ definiramo operaciji $\oplus$ in $\otimes$ na naslednji način:

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

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

Tako kot pri ostalih algebraičnih strukturah, lahko tudi tukaj definiramo podstrukture, torej podpolkolobarje.

Definicija 2.19. Naj bo $(R, \oplus, \otimes)$ levi polkolobar. Neprazna množica P je podpolkolobar v R, če je podmnožica v R in če je tudi sama polkolobar za operaciji $\oplus_{|P}$ in $\otimes_{|P}$, ki jih podeduje od R. Operaciji $\oplus_{|P}$ in $\otimes_{|P}$ sta torej zožitvi $\oplus$ in $\otimes$ na P.

Trditev 2.20. *Naj bo $(R, \oplus, \otimes)$ levi polkolobar in $P \subseteq R$ neprazna podmnožica v R. Tedaj je P podpolkolobar v R, čim je zaprt za zoženi operaciji in vsebuje obe enoti.*

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

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 pripadajoćemu dokazu za kolobarje.

Za konec omenimo še preslikave med polkolobarji, specifično homomorfizme, ki so definirani na skoraj enak način kot homomorfizmi kolobarjev.

Definicija 2.21. Naj bosta $(R, \oplus, \otimes)$ in $(P, \boxplus, \boxtimes)$ leva polkolobarja. Naj bosta 0 in 1 enoti v R ter e in ε enoti v P. Preslikava $\phi : R \to P$ je homomorfizem polkolobarjev, če zadošča naslednjim pogojem:

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

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

Tako kot za kolobarje lahko tudi za polkolobarje definiramo ideale, brez da bi samo definicijo bistveno spremenili.

Definicija 2.22. Neprazni podmnožici I polkolobarja $(R, \oplus, \otimes)$ pravimo *levi ideal*, če za njo velja

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

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

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

2.3. **Dioidi.** Kot smo že napovedali v prejšnjem podpoglavju, zahvaljujoč se izreku 2.6, lahko obravnavamo podkolobarje, ki so opremljeni s kanonično delno ureditvijo. Tem strukturam pravimo dioidi. Vseeno zapišimo definicijo bolj formalno preden se lotimo obravnave.

Definicija 2.23. Polkolobarju $(R, \oplus, \otimes)$, na katerem je kanonična relacija šibke urejenosti (definirana preko $\oplus$) delna urejenost, pravimo *dioid*.

Opomba 2.24. Upoštevajoč opombo 2.9 lahko klasificiramo dioide kot polkolobarje brez vsote nič.

Opomba 2.25. 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.

Zgled 2.26. Množica nenegativnih celih števil $\mathbb{N}_0$, opremljena z navadnim seštevanjem in množenjem ter kanonično delno (celo linearno) urejenostjo, je dioid. Enako velja za nenegativna racionalna števila $\mathbb{Q}_+$ in nenegativna realna števila $\mathbb{R}_+$. $\diamondsuit$

V zgledu omenjene množice, opremljene s standardnim seštevanjem in množenjem, nam služijo kot prototip dioidov, na podoben način kot je množica celih števil $\mathbb{Z}$ s standardnim seštevanjem $+$ prototip za abelove grupe. Seveda dioidi niso omejeni zgolj na osnovne operacije. Znane množice lahko opremimo tudi z manj pogostimi operacijami in tako pridobimo dioide, kot bo pokazal naslednji zgled.

Zgled 2.27. Z $\bar{\mathbb{R}}$ označimo množico $\mathbb{R} \cup \{-\infty, +\infty\}$. Potem sta $(\bar{\mathbb{R}}, \min, +)$ in $(\bar{\mathbb{R}}, \max, +)$ dioida. V primeru prvega dioida je nevtralni element $+\infty$, enota pa je 0, v primeru drugega pa sta enoti $-\infty$ in 0. V obeh primerih sta obe operaciji komutativni in asociativni, med njima tudi očitno velja distributivnost in aditivna enota izniči $+$. Obravnavani strukturi sta torej komutativna polkolobarja.

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

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

Trditev 2.28. *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 opombe 2.4. Pokažimo torej enako še za $\otimes$. Vemo, da velja $a \leq b \iff \exists c \in R : b = a \oplus c$. Potem iz $a \leq b$ za $\forall x \in R$ sledi $(a \oplus c) \otimes x = b \otimes x$. Po distributivnosti potem sledi $(a \otimes x) \oplus (c \otimes x) = b \otimes x$. Potem je pa $a \otimes x \leq b \otimes x\ \forall x \in R$. Torej je $\leq$ usklajena z $\otimes$. Podobno pokažemo tudi $x \otimes a \leq x \otimes b$. $\square$

Tako kot prej s polkolobarji, lahko tudi z dioidi sestavimo produkte, ki imajo tudi strukturo dioida. Torej če imamo m dioidov $(R_i, \oplus_i, \otimes_i)$, jih sestavimo v $R = R_1 \times \ldots \times R_m$ in na to množico vpeljemo operaciji $\oplus$ in $\otimes$ na naslednji način:

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

in

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

V zgledu 2.18 smo že premislili, da je $(R, \oplus, \otimes)$ polkolobar. Poleg tega hitro vidimo, da je $\oplus$ usklajena s kanonično delno ureditvijo na R.

Seveda lahko tudi v primeru dioidov obravnavamo podstrukture, t. i. poddioide. Njihov obstoj nam namigujejo prototipni dioidi $\mathbb{N}_0 \subseteq \mathbb{Q}_+ \subseteq \mathbb{R}_+$.

Definicija 2.29. Neprazna množica P je poddioid dioida $(R, \oplus, \otimes)$, če je podmnožica v R, ki vsebuje obe enoti, in če je tudi sama dioid za operaciji, ki ju podeduje od $(R, \oplus, \otimes)$.

Hitro se da opaziti, da v preverjanju, ali je P poddioid, ni treba direktno obravnavati urejenosti. Razlog za to je, da se kanonična urejenost (v resnici antisimetričnost kanonične relacije urejenosti) prenese na podmnožico skupaj z operacijama. Iz tega razloga je dovolj, da za podmnožico P v dioidu R preverimo, ali je polkolobar.

Trditev 2.30. *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: $a \leq b \iff \exists c \in P;\ b = a \oplus c$. Ker je kanonična šibka urejenost na R antisimetrična, ima to lastnost tudi na P, torej je $\leq$ na P v resnici kanonična delna urejenost. Sledi, da je P dioid, torej je poddioid v R. □

Pri obravnavi dioidov se težko izognemo vprašanju preslikav. Izkaže se, da v resnici ni treba uvesti ničesar novega - 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 $\phi(a) \leq_P \phi(b)$. 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 2.30 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], je

delna 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 2.31. Dioid $(R, \oplus, \otimes)$ je *poln* oz. *kompleten*, če je za kanonično delno urejenost $\leq$ urejena množica $(R, \leq)$ polna in če poleg tega ustreza še t.i. posplošeni distributivnosti:

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

in

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

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

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

.

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

Zgled 2.32. Dioida $(\mathbb{R} \cup \{-\infty\}, \max, +)$ in $(\mathbb{R} \cup \{+\infty\}, \min, +)$ nista polna. Da postaneta polna, jima moramo dodati njuna zadnja elementa. Za prvi dioid je to $T = +\infty$., za drugi dioid pa je $T = -\infty$. Tropska dioida iz zgleda 2.27 sta torej polna dioida. ♢

Opomba 2.33. Omenimo še dualni pojem *infimuma* množice:
Element $r \in R$ je infimum $P \subseteq R$ ko je spodnja meja P ($\forall p \in P$ velja $r \leq p$) in $\forall q \in R$ velja sklep (q je spodnja meja $P \Rightarrow q \leq r$). Če ima v $(R, \leq)$ vsaka podmnožica infimum, pravimo, da je $(R, \leq)$ dualno polna. Urejeni množici $(R, \leq)$, ki je hkrati polna in dualno polna, pravimo *polna mreža*.

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

Zgled 2.34. Naj bo $(R, +)$ kanonično urejen komutativen monoid z enoto 0. Na množici E endomorfizmov R potem uvedemo operaciji $\oplus$ in $\otimes$ na sledeč način:

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

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

Naslednji zgled, povzet iz [2], nam demonstrira praktično aplikacijo obravnavane teorije.

Zgled 2.35. Vsebino zgleda 2.34 lahko uporabimo v teoriji grafov v iskanju časovno najkrajše poti. Denimo, da imamo graf $G = (V, E)$ in da vsaki povezavi (i, j) pripada preslikava h_{ij}, ki nam poda čas prihoda t_j v vozlišče j, če zapustimo vozlišče i ob času t_i. Torej $t_j = h_{ij}(t_i)$. Iščemo najkrajši čas, da prispemo iz vozlišča t_1 v izbrano vozlišče t_i.

Za ta problem vzamemo $R = \mathbb{R} \cup \{+\infty\}, \oplus = \min, 0 = +\infty$. Za množico E vzamemo množico nepadajočih funkcij $f : R \mapsto R$, za katere gre $f(t) \to +\infty$ ko se t bliža $+\infty$. Te funkcije so endomorfizmi nad $(\mathbb{R} \cup \{+\infty\}, \min)$, saj $f(\min\{t, \acute{t}\}) = \min\{f(t), f(\acute{t})\}$ in $f(+\infty) = +\infty$. Na enak način kot v prejšnjem zgledu sestavimo dioid $(E, \oplus, \otimes)$.

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

Na koncu izpostavimo še eno povezavo med polkolobarji in dioidi: Vsakemu polkolobarju pripada nek dioid. Pri določanju tega dioida bo seveda ključno to, da kanonični šibki urejenosti na izbranem polkolobarju dodamo antisimetričnost. Kako to naredimo, nam pove naslednji izrek.

Izrek 2.36. *Naj bo $(R, \oplus, \otimes)$ polkolobar v katerem kanonična relacija šibke urejenosti $\leq$ ni antisimetrična (torej ni delna ureditev). Naj bo $\mathcal{E}$ ekvivalenčna relacija definirana na R:*

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

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

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

Opomba 2.37. Dodatno lahko definiramo še eno strukturo, t. i. 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 $(\mathbb{R}, \min, +)$ in $(\mathbb{R}, \max, +)$. To omenimo zgolj kot zanimivost, saj nas v nadaljevanju polpolja ne bodo kaj preveč zanimala.

3. Polmoduli in moduloidi:

3.1. **Definicije in elementarni primeri:** 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. Nekoliko bolj presenetljive rezultate bomo obravnavali pri strukturah nad dioidi.

Definicija 3.1. Naj bo $(R, \oplus, \otimes)$ polkolobar z nevtralnima elementoma 0 in 1.
Levi R-polmodul je komutativen monoid $(M, +)$ z aditivno identiteto θ, na katerem je definirana zunanja operacija $\cdot : R \times M \to M$, ki jo imenujemo množenje s skalarjem. Množenje s skalarjem zadošča naslednjim pogojem za vsaka $\lambda, \mu \in R$ in vsaka $m, n \in M$:

A1 $\lambda \cdot (m + n) = \lambda \cdot m + \lambda \cdot n$

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

Analogno definiramo desni R-polmodul.

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

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

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

in

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

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

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

Zgled 3.4. Vrnimo se k zgledu 3.2 in dodatno predpostavimo, da je $(R, \oplus, \otimes)$ dioid. Potem je $(R^n, +)$ kanonično urejen, torej je (levi) moduloid. ♢

3.2. **Homomorfizmi in kvocientne strukture:** Tako kot pri vektorskih prostorih, nas tudi pri polmodulih zanimajo preslikave, ki ohranjajo algebraično strukturo. Pojavi se tudi vprašanje, ali lahko nad polmodulih tvorimo kvocientne strukture. Oboje bomo obravnavali v tem podpoglavju.

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

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

Homomorfizmom iz M nazaj vase pravimo *endomorfizmi*.

Kadar je $(R, \oplus, \otimes)$ dioid, govorimo o homomorfizmih in endomorfizmih levih moduloidov.

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

Tako v linearni algebri vektorskih prostorov in modulov kot v splošni abstraktni algebri igrajo pomembno vlogo podstrukture in kvocientne strukture. Oboje lahko definiramo tudi za polmodule. Spodnji definiciji sta povzeti iz [2].

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

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

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

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

Množici $M/\widehat{M}$ pravimo kvocientni polmodul 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, iz $x\mathcal{E}y \iff \exists u, v \in \widehat{M} : x + u = y + v$ sledi tudi $\lambda \cdot (x + u) = \lambda \cdot (y + v)$ za vsak $\lambda \in R$. Od tod pa vidimo:

$$\lambda \cdot x + \lambda \cdot u = \lambda \cdot y + \lambda \cdot v$$

Ker $(\lambda \cdot u), (\lambda \cdot v) \in \widehat{M}$, potem velja $(\lambda \cdot x)\mathcal{E}(\lambda \cdot y)$.

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

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

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

Opomba 3.10. V definiciji dopuščamo, da je X končna ali pa neskončna družina. Če je X končna, pravimo, da je M končno generiran.

Definicija 3.11. Rang R-polmodula M, označen z $r(M)$, je enak najmanjšemu številu n, za katerega obstaja množica X velikosti n, ki generira M. Rang vedno obstaja za končno generirane polmodule.

Trditev 3.12. *Naj bo $(M, +, \cdot)$ levi R-polmodul in $X = (x_i)_{i\in I}$ neka poljubna neprazna družina elementov iz M. Potem je $\langle X \rangle = Y$, kjer je Y množica tistih $y \in M$, ki so oblike:*

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

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

Dokaz. Takoj vidimo, da je množica Y, kot je definirana zgoraj, levi R-polmodul. To je zato, ker je $(Y,+)$ komutativen monoid z enoto θ in $(M,+,\cdot)$ zadošča vsem aksiomom $A1$–$A5$ iz definicije 3.1.

Dodatno vidimo, da velja $X \subseteq Y$, 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 $\lambda_i = 0$). Sledi torej, da je Y levi R-podpolmodul v M, ki vsebuje X, od tod pa sklepamo $\langle X\rangle \subseteq Y$.

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

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

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

Definicija 3.13. Naj bo $(M,+,\cdot)$ levi R-polmodul in $X = (x_i)_{i\in I}$ neprazna (končna ali 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:

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

Če X ni linearno odvisna, pravimo, da je *linearno neodvisna*. Linearna neodvisnost je karakterizirana s pogojem:

$$\forall I_1, I_2 \subset I; I_1 \cap I_2 = \emptyset : \langle X_{I_1}\rangle \cap \langle X_{I_2}\rangle = \{\theta\} \tag{1}$$

oziroma ekvivalentno:

$$\forall x_i \in X : x_i \notin \langle X \setminus \{x_i\}\rangle \tag{2}$$

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.

Kratek premislek nam pove, da je vsaka prosta množica v M hkrati tudi linearno neodvisna. Da to vidimo, se skličemo na ekvivalentno definicijo 2 linearne neodvisnosti, 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 linearno neodvisna.

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

Sedaj lahko končno definiramo bazo polmodula.

Definicija 3.14. Pravimo, da je družina X v (levem) R-polmodulu $(M, +, \cdot)$ *baza* M, če je linearno neodvisna in generira cel M ($\langle X\rangle = M$). Družina X je *prosta baza* (levega) R-polmodula M, če je prosta množica v M in generira cel M. Polmodulu, ki premore kako prosto množico, pravimo *prosti polmodul*.

Opomba 3.15. Vsaka prosta baza je hkrati tudi baza. Poleg tega ima vsak končno generiran levi polmodul kako bazo.

Definicija 3.16. Naj bo $(M, +, \cdot)$ levi R-polmodul. Z $r(M)$ označimo najmanjše tako naravno število n, za katerega obstaja množica X v M, kardinalnosti n, ki generira M. To število očitno obstaja za vsak končno generiran M.

Zgled 3.17. Vrnimo se k zgledu 3.2. R-polmodul $(R^n, \oplus, \otimes)$ prepoznamo kot končno generiran prosti R-polmodul. Množica $E = \{e1, e2, \ldots, e_n\}$ tvori prosto bazo za R^n, kjer so $e_1 = (1, 0, 0, \ldots, 0)^\top, e_2 = (0, 1, 0, \ldots, 0)^\top, \ldots, e_n = (0, \ldots, 0, 1)^\top$. Razvidno je tudi, da je $r(R^n) = n$. ♢

Sedaj se lahko lotimo klasifikacije baz levih polmodulov, pri čemer se bomo naslonili na Tanov članek [3].

Izrek 3.18. *Naj bo R komutativen polkolobar in M R-polmodul. Če premore M kako neskončno bazo, so vse njegove baze neskončne.*

Dokaz. Naj bo X neskončna baza za M. Če je Y končna 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 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 baza), lahko vsak element iz X zapišemo kot linearno kombinacijo elementov iz $\acute{Y}$. Potem pa obstaja $x \in X \setminus \acute{Y} \subseteq S$, da je $x \in \left\langle \acute{Y} \right\rangle \subseteq \langle X \setminus \{x\}\rangle$. Ta zadnji sklep je pa v protislovju s tem, da je X linearno neodvisna. Torej je vsaka druga baza M neskončna. □

Opomba 3.19. Prejšnji izrek nam pove še to, da če ima M končno bazo, so vse njegove baze končne. Ker vsi končno generirani R-polmoduli premorejo vsaj eno končno bazo velja, da je vsaka baza končno generiranega levega R-polmodula končna.

Definicija 3.20. Naj bo $(M, +, \cdot)$ levi polmodul nad polkolobarjem $(R, \oplus, \otimes)$ in denimo, da imamo dano neko množico vektorjev $V = (V_k)_{k \in K}$, kjer je $V_k \in M$ za vsak $k \in K$. Vektor x je *razcepen* na $\langle V \rangle$ natanko tedaj, ko obstajata taka vektorja $y, z \in \langle V \rangle$, ki sta oba različna od x, da velja $x = y + z$. V primeru ko x ni razcepen, pravimo da je *nerazcepen*.

Opomba 3.21. Takoj se da videti, da razcepnost implicira vsebovanost v $\langle V \rangle$: x razcepen na $\langle V \rangle \Rightarrow x \in \langle V \rangle$

Iz zgornje opombe takoj sledi naslednja posledica:

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

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

Sedaj lahko zapišemo in dokažemo naslednjo trditev:

Trditev 3.23. *Naj no $(R, \oplus, \otimes)$ dioid in označimo z 0 nevtralni element za $\oplus$ ter z 1 nevtralni element za $\otimes$. Denimo dodatno, da velja: $r \oplus p = 1 \Rightarrow r = 1$ ali $p = 1$. Naj bo $(M, +, \cdot)$ R-moduloid, ki je kanonično urejen glede na $+$. $Z \propto$ označimo kanonično delno urejenost na M. Dodatno predpostavimo, da za $x, y \in M$, ki zadoščata pogojem $x \neq y$ & $y \neq \theta$ in $\lambda \in R$ velja:*

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

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

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

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

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

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

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

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

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

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

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

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

Po drugi točki posledice 3.22 je potem x_j nerazcepen. □

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

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

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

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

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

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

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

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

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

4. Matrike:

4.1. **Definicije in obrnljivost.** Kot smo že videli lahko, podobno kot za vektorske prostore in module, tudi za polmodule pod določenimi pogoji definiramo baze in jim tudi določimo »dimenzije« (rang polmodula) preko kardinalnosti najmanjše baze. Na njih lahko tudi izvajamo linearne preslikave, ki so definirane na enak način, kot na vektorskih prostorih - $\mathbb{L} : M \mapsto \grave{M}$ more biti aditivna in homogena.

Sedaj bomo nad polkolobarjem $(R, +, \cdot)$ definirali tudi mxn matrike, za poljubna $m, n \in \mathbb{N}$. Pri tem seštevanje definiramo enako kot za matrike nad obsegi (po komponentah), množenje pa na sledeč način za $A \in M_{m\times n}(R), B \in M_{n\times l}(R)$:

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

Pri množenju moramo seveda biti pozorni na to, da tukaj nimamo komutativnosti. Enota za seštevanje je seveda kar t. i. ničelna matrika, kjer je vsak element aditivna enota iz polkolobarja, za množenje pa je enota kar matrika, ki ima na diagonali multiplikativno enoto, izven diagonale pa aditivno.

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

Definicija 4.1. Naj bo $A \in M_{m\times n}(R)$ poljubna $m \times n$ matrika nad polkolobarjem R. Najmanjšemu naravnemu številu k, za katerega velja, da je $A = B * C$ za neka $B \in M_{m\times k}(R)$ in $C \in M_{n\times l}(R)$, pravimo faktorski rang matrike A in ga označimo z $\rho_S(A)$.

Definirajmo sedaj, kdaj je matrika nad polkolobarjem obrnljiva,

Definicija 4.2. Kvadratna matrika $A \in M_n(R)$ je obrnljiva, če obstaja taka matrika $B \in M_n(R)$ za katero velja $A * B = B * A = I_n$. Če obstaja, matriki B pravimo inverz matrike A v $M_n(R)$. 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 2.17 ter naslednja lema.

Lema 4.3. *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 $B * A = I_n$.*

Leme 4.3 v tem delu ne bomo dokazali, bomo jo pa privzeli kot veljavno. Dva dokaza se nahajata v [6].

Sedaj se lahko zapišemo naslednjo trditev in dokaz, oba povzeta po [3].

Trditev 4.4. *Naj bo R komutativen polkolobar v katerem 1 ni aditivno obrnljiva in velja $1 = u \oplus v \Rightarrow u \in U(R) \vee v \in U(R)\ \forall u, v \in R$. Naj bo $A \in M_n(R)$. Če so diagonalni elementi matrike A multiplikativno obrnljivi v R (torej $a_{ii} \in U(R)\ \forall i \in \{1, \ldots, n\}$) in če so vsi izvendiagonalni elementi v A aditivno obrnljivi ($a_{i,j} \in V(R)\ \forall i, j \in \{1, \ldots, n\}\ ;\ i \neq j$), potem je A obrnljiva.*

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

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

Na tej točki uporabimo lemo 2.17 znotraj vsot in zamenjamo indekse s z i in t z j v sredinskih dveh vsotah.

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

Razpišimo sedaj, kar smo dobili, v obliki matrike.

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

Za $A1$ označimo matriko

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

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

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

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

Zgornje linearne kombinacije lahko tudi zapišemo v matrični obliki:

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

Pri tem je $A = (a_{ij}) \in M : n \times m(R)$. To nas privede do naslednje definicije.

Definicija 4.5. Naj bo M končno generiran (levi) R-polmodul in naj bosta T in S njegovi bazi. Matriki A, ki slika elemente baze T v S, pravimo prehodna matrika iz baze T v S. Med dvema bazama lahko obstaja več različnih prehodnih matrik.

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

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

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

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

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

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 M, saj S generira M. Potem pa je $r = r(M) \leq k = \rho_S(A)$. in s tem smo pokazali prvi del trditve.

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

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

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

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

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

Dokaz. Opomba 3.19 nam pove, da sta tako T kot S končni. Naj bo $S = \{s_1, \ldots, s_m\}$ in $T = \{t_1, \ldots, t_n\}$ ter naj bo $A \in M_{n\times m}(R)$ prehodna matrika iz T v S ter $B \in M_{m\times n}(R)$ prehodna matrika iz S v T. Potem je

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

in

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

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

je tudi $A_1 * B_1 = A * B = I_n$ in ker je R komutativen po lemi 4.3 sledi $B_1 * A_1 = I_n$. Toda če dejansko poračunamo ta produkt, dobimo

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

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

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

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

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

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

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

$ii \Rightarrow iii$: Denimo, da je $|S| = r$ in naj bo potem $S = \{s_1, \ldots, s_r\}$. Naj bo A prehodna matrika med T in S ter naj bo B prehodna matrika med S in T. Na enak način kot v trditvi 4.7 potem vidimo, da velja $(t_1, t_2, \ldots, t_r) = (t_1, t_2, \ldots, t_r) * A * B$, od koder sledi, da je $A * B = I_r$. Ponovno se skličemo na lemo 4.3, po kateri je tudi $B * A = I_r$. Sledi, da je A obrnljiva $r \times r$ matrika nad R. Denimo sedaj, da imamo dve prehodni matriki med T in S, A_1 ter A_2. Potem velja $(s_1, s_2, \ldots, s_r) = (t_1, t_2, \ldots, t_r) * A_1$ in $(s_1, s_2, \ldots, s_r) = (t_1, t_2, \ldots, t_r) * A_2$, od tod pa sklepamo da je $(t_1, t_2, \ldots, t_r) * A_1 = (t_1, t_2, \ldots, t_r) * A_2$. Sledi, da je $A_1 = A_2$, s tem pa smo dokazali iii.

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

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

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

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

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

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

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

(1) Vse baze M imajo enako kardinalnost.
(2) Vsaka 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 baze enako kardinalnost natanko tedaj ko je vsaka 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 [3], opustili.

4.3. **lastne vrednosti.** V naslednjem zgledu se bomo srečali s konceptoma lastnih vektorjev in lastnih vrednosti kvadratnih matrik nad komutativnimi polkolobarji. Oba koncepta bomo bolj podrobno obravnavali v naslednjem poglavju, o matrikah.

Zgled 4.11. Naj bo $(R, \oplus, \otimes)$ komutativen polkolobar in $A \in M_n(R)$ kvadratna $n \times n$ matrika s koeficienti iz R. Naj bosta $V \in R^n$ in $\lambda \in R$ takšna, da velja $A \times V = \lambda \cdot V$. Vektorju V previmo lastni vektor matrike A za lastno vrednost λ. Naj bo L_λ množica lastnih vektorjev, ki pripadajo lastni vrednosti λ. Hitro se da preveriti, da je potem tudi $(L_\lambda, +)$ R-polmodul.

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

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

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

5. Posplošitve determinante:

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

Definicija 5.1. Naj bo $X = \{1, 2, \ldots, n\}$ neka končna množica. Pravimo, da je σ *delna permutacija* X, če je permutacija neke podmnožice $S \subseteq X$. Na enak način kot za navadne permutacije tudi za delne definiramo parnost.

Oznaka: $Per(n)$ je množica vseh permutacij množice $\{1, 2, \ldots, n\}$, $Per^+(n)$ množica vseh sodih permutacij na isti množici in analogno $Per^-(n)$ množica vseh lihih permutacij na tej množici. Na enak način označimo $Part(n)$ kot množico vseh delnih permutacij množice $\{1, 2, \ldots, n\}$ in na enak način kot prej tudi $Part^+(n)$ ter $Part^-(n)$.

Delno permutacijo σ lahko tudi razširimo na cel X:

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

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

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

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

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

6. Karakteristični bipolinom:

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

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

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

To pa nas privede do zadnje in najbolj zanimive točke:

7. Posplošen Cayley-Hamiltonov izrek:

Izrek 7.1. *Naj bo A neka $n \times n$ matrika nad komutativnim polkolobarjem z nevtralnim elementom 0 in enoto 1 in naj bo $(P_A^+(\lambda), P_A^-(\lambda))$ bipolinom, ki pripada matriki A. Tedaj velja:*

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

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

Slovar strokovnih izrazov

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

Literatura

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

[2] Gondran in M. Minoux, *Graphs, dioids and semirings: New models and algorithms*, Operations Research/Computer Science Interfaces **41**, Springer, Boston, 2008; dostopno tudi na `https://www.researchgate.net/publication/266193429_Graphs_Dioids_and_Semirings_New_Models_and_Algorithms`.

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

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

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

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

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