Univerza na Primorskem

Fakulteta za matematiko, naravoslovje in informacijske tehnologije

Lorena Mahne

Moduli

Zaključna projektna naloga

Koper, 2010

Mentor: doc. dr. Klavdija Kutnar

Kazalo

Zahvala

Zahvala je namenjena mentorici doc. dr. Klavdiji Kutnar za strokovno pomoč in dobrodošle nasvete pri pripravi zaključne projektne naloge.

Povzetek

V zaključni projektni nalogi je bil namen preučiti lastnosti modulov nad kolobarjem. Na začetku naloge si pogledamo nekaj osnovnih definicij o grupah, kolobarjih in poljih. Ker so moduli posplošitev vektorskih prostorov, so v osrednjem delu zajeti tudi vektorski prostori. Zaključni del projektne naloge sestavljajo moduli, kjer so zajeti vsi trije izreki o izomorfizmu, prosti moduli in direktna vsota. V sledečem podpoglavju pogoji končnosti je poudarek na Noetherianovih in Artinianovih modulih.

Ključne besede:

kolobar, grupa, vektorski prostor, linearna preslikava, vektor, baza, modul, podmodul, homomorfizem modulov, izomorfizem, direktna vsota, Artinianov modul, Noetherianov modul

Poglavje 1

Uvod

Namen projektne naloge je preučiti lastnosti modulov nad kolobarjem s posebnih poudarkom na posebnih družinah modulov, kot so ciklični moduli, prosti moduli. Za teoretično podlago je bila uporabljena strokovna literatura. Zaključna projektna naloga je razdeljena na pet poglavij. Uvodu sledi predstavitev dejstev o osnovnih algebrskih strukturah. To so grupe, kolobarji, obsegi in polja. Sledi podrobnejša predstavitev vektorskih prostorov. V tem poglavju je definirano kaj je linearna preslikava, kdaj je podmnožica vektorskega prostora nad poljem K vektorski podprostor, kaj je linearna ogrinjača, kaj je baza in dimenzija vektorskega prostora. Četrto poglavje je namenjeno predstavitvi modulov. Razdeljeno je na štiri podpoglavja. Prvo podpoglavje govori o homomorfizmu modulov, sledi mu podpoglavje, v katerem so predstavljeni vsi trije izreki o izomorfizmu modulov. V predzadnjem podpoglavju definiramo proste module in direktno vsoto, kjer razširimo koncept baz v vektorskih prostorih na koncept baz v modulih. V zadnjem poglavju, ki govori o pogojih končnosti, so opisani Artinianovi in Noetherianovi moduli.

Poglavje 2

Osnovne algebrske strukture

To poglavje je povzeto iz [2]. Predstavljena so dejstva o osnovnih algebrskih strukturah.

Definicija 2.1. *Naj bo S neprazna množica. Preslikavi $\varphi : S \times S \to S$ rečemo notranja dvomestna operacija na množici S.*

Sliko urejenega para $(a, b) \in S \times S$ s preslikavo φ pišemo $a\varphi b$ (namesto $\varphi(a, b)$) in ji rečemo tudi kompozitum elementov a in b. Pogosto pišemo notranjo dvomestno operacijo z $\circ$ ali $\cdot$. V slednjem primeru notranjo operacijo imenujemo množenje.

Definicija 2.2. *Naj bo $(S, \circ)$ množica z notranjo dvomestno operacijo $\circ$. Operacija $\circ$ je asociativna na množici S, če velja:*

- $\forall a, b, c \in S : (a \circ b) \circ c = a \circ (b \circ c)$.

Operacija $\circ$ je komutativna, če velja:

- $\forall a, b \in S : a \circ b = b \circ a$.

Če je notranja dvomestna operacija $\circ$ na množici S asociativna je element, dobljen s sestavljanjem elementov $a_1, a_2, \ldots, a_n \in S$ enolično določen z vrstnim redom teh elementov in ni odvisen od postavitve oklepajev.

2.1 Grupe

Grupa je najpogostejša algebrska struktura z eno dvomestno notranjo operacijo.

Definicija 2.3. *Naj bo G neprazna množica z notranjo dvomestno operacijo $\cdot$. Strukturi $(G, \cdot)$ pravimo grupa, če so izpoljeni naslednji pogoji:*

(G1) operacija $\cdot$ je asociativna: $\forall a, b, c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$;

(G2) obstaja nevtralni element $1 \in G : 1 \cdot x = x \cdot 1 = x, \forall x \in G$;

(G3) vsak element $a \in G$ je obrnljiv: t.j. $\forall a \in G \exists a^{-1} \in G : a \cdot a^{-1} = 1 = a^{-1} \cdot a$;

Definicija 2.4. *Naj bo $(G, \circ)$ grupa. Potem je podmnožica $H \subseteq G$ glede na operacijo $\circ$ podgrupa grupe G, če je $(H, \circ)$ grupa. Oznaka $H \leq G$.*

Definicija 2.5. *Če je operacija $\cdot$ v grupi $(G, \cdot)$ komutativna, rečemo, da je $(G, \cdot)$ komutativna grupa ali abelska grupa.*

Grupo $(G, \cdot)$ ponavadi označujemo krajše samo z G. Produkt elementa $a \cdot b$, $a, b \in G$, pišemo krajše ab.

Zgledi:

- $(\mathbb{Z}, +)$ je seštevajoča grupa za običajno seštevanje celih števil.
- $(\mathbb{N}, +)$ ni grupa, ker nima nevtralnega elementa.
- $(\mathbb{Q}, +)$ je grupa.
- $(\mathbb{Q}, \cdot)$ ni grupa, ker element 0 ni obrnljiv.

Definicija 2.6. *Naj bosta $(G, \circ)$ in $(H, *)$ grupi. Tedaj je preslikava $f : G \to H$ homomorfizem, če velja:*

$$f(a \circ b) = f(a) * f(b), \forall a, b \in G.$$

Definicija 2.7. *Naj bo $f : G \to H$ homomorfizem grup.*

- *Če je f injektivna preslikava, f imenujemo monomorfizem,*
- *Če je f surjektivna preslikava, f imenujemo epimorfizem,*
- *Če je f bijektivna preslikava, f imenujemo izomorfizem,*
- *Če je $G = H$, f imenujemo endomorfizem,*
- *Če je f endomorfizem in izomorfizem, f imenujemo avtomorfizem.*

2.2 Kolobarji, obsegi in polja

Kolobar je algebrska struktura z dvema notranjima dvomestnima operacijama; eno označimo z $+$ in ji rečemo seštevanje, drugo označimo z $\cdot$ in ji rečemo množenje.

Definicija 2.8. *Naj bo K neprazna množica in $+$ ter $\cdot$ notranji dvomestni operaciji na K. Potem pravimo, da je algebrska struktura $(K, +, \cdot)$ kolobar, če veljajo naslednje lastnosti:*

(K1) $(K, +)$ je komutativna grupa,

(K2) $(K, \cdot)$ je neprazna množica z notranjo dvomestno operacijo, ki je asociativna,

(K3) veljata distributivna zakona: $\forall a, b, c \in K : (a + b)c = ac + bc$, $a(b + c) = ab + ac$.

Kolobar $(K, +, \cdot)$ krajše označujemo s K.

Definicija 2.9. *Kolobar z identiteto (ali enico) je kolobar $(K, +, \cdot)$, v katerem velja:*

$$\exists 1 \in K : 1 \cdot a = a \cdot 1 = a, \quad \forall a \in K.$$

Definicija 2.10. *Naj bo $(K, +, \cdot)$ kolobar. Potem pravimo, da je kolobar K komutativen, če je operacija $\cdot$ na množici K komutativna. Če K premore nevtralni element za operacijo množenja, je K kolobar z identiteto (nevtralni element za operacijo množenja označimo z 1).*

Elemente kolobarja z identiteto, ki imajo inverz za množenje imenujemo *enote*.

Zgledi:

- $\tau = (\{0\}, +, \cdot)$ je najmanjši kolobar, imenujemo ga trivialni kolobar.
- $(\mathbb{Z}, +, \cdot)$ je kolobar, saj je $(\mathbb{Z}, +)$ abelova grupa in $(\mathbb{Z}, \cdot)$ polgrupa. Še več kolobar $(\mathbb{Z}, +, \cdot)$ ima identiteto in je komutativen.
- $(\mathbb{R}^{2\times 2}, +, \cdot)$ je za običajno seštevanje in množenje matrik kolobar z identiteto

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

- $(\mathbb{N}, +\cdot)$ ni kolobar, saj $(\mathbb{N}, +)$ ni komutativna grupa.

Definicija 2.11. *Podmnožica K' kolobarja K je podkolobar kolobarja K, če je $(K', +, \cdot)$ kolobar. Z drugimi besedami, K' je podkolobar če velja:*

- $0_K \in K'$;
- $\forall a, b \in K' : a - b \in K'$;
- $\forall a, b \in K' : ab \in K'$.

Zgled: $2\mathbb{Z}$ je podkolobar kolobarja $\mathbb{Z}$.

Definicija 2.12. *Podmnožica L v kolobarju K je levi ideal, če velja:*

- *(L1) :* $L + L \subseteq L \quad (\forall a, b \in L : a + b \in L)$,
- *(L2):* $xL \subseteq L$, $\forall x \in K \quad (\forall a \in L : xa \in L)$.

Podmnožica D v kolobarju K je desni ideal, če velja:

- *(D1)* $D + D \subseteq D$,
- *(D2)* $Dx \subseteq D, \forall x \in K$.

Če je podmnožica I levi in desni ideal kolobarja K, jo imenujemo (dvostranski) *ideal* kolobarja K.

Zgledi:

- $2\mathbb{Z}$ je ideal kolobarja $\mathbb{Z}$.
- V vsakem kolobarju K sta $\{0\}$ in K ideala. Ideal I v kolobarju K, ki je različen od $\{0\}$ in K, imenujemo pravi ideal.
- Vsak ideal je tudi podkolobar. Narobe pa ni res, da bi bil vsak podkolobar tudi ideal; to nam pove tale zgled: Kolobar $\mathbb{Z}$ je podkolobar kolobarja $\mathbb{Q}$ racionalnih števil. Vendar $\mathbb{Z}$ ni ideal v $\mathbb{Q}$. Produkt števila $1 \in \mathbb{Z}$ s številom $\frac{1}{2} \in \mathbb{Q}$ ni celo število, torej ni v $\mathbb{Z}$. Pogoj (D2) v tem primeru ni izpoljen in zato $\mathbb{Z}$ ni ideal kolobarja $\mathbb{Q}$.

Trditev 2.13. *Če ideal I kolobarja K vsebuje enoto, je I nepravi ideal, t.j. $I = K$.*

Dokaz. Naj bo K kolobar z identiteto $1 \in K$ in I ideal kolobarja K, ki vsebuje enoto $a \in I$. Po lastnosti $(L2)$ vemo, da za vsak $x \in K$ element $x \cdot a \in I$. Torej tudi $1 = a^{-1} \cdot a \in I$. S ponovno uporabo lastnosti $(L2)$ dobimo, da je $x \cdot 1 = x \in I$ za vsak $x \in K$ in zato $I = K$. □

Definicija 2.14. *Obseg je kolobar z identiteto, v katerem je vsak neničelni element obrnljiv. Komutativen obseg je polje, tj. če v obsegu velja $a \cdot b = b \cdot a$ za vse elemente a, b.*

Zgledi:

- $(\mathbb{Z}, +, \cdot)$ ni obseg, ni polje.
- $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ so obsegi in polja.

Poglavje 3

Vektorski prostori

Vektorski prostor je algebrska struktura z dvema binarnima operacijama, eno notranjo in eno zunanjo. Notranja operacija je binarna, zunanja operacija je definirana na kartezičnem produktu polja in vektorskega prostora. Elemente vektorskega prostora imenujemo *vektorji*, elemente polja pa *skalarje*.

Definicija 3.1. *Naj bo K polje. Množica V z notranjo (binarno) operacijo $+$, ki jo imenujemo seštevanje*

$$+ : V \times V \longrightarrow V$$

in zunanjo operacijo $\cdot$, ki jo imenujemo množenje

$$\cdot : K \times V \longrightarrow V$$

je vektorski prostor nad poljem K, če za poljubne elemente $\alpha, \beta \in K$ in $\mathbf{u}, \mathbf{v} \in V$ velja naslednje:

(i) $(V, +)$ *je komutativna grupa za;*

(ii) Množenje vektorja s skalarjem je asociativno,

$$(\alpha \cdot \beta) \cdot \mathbf{v} = \alpha \cdot (\beta \cdot \mathbf{v})$$

in distributivno

$$\begin{aligned} (\alpha + \beta) \cdot \mathbf{v} &= \alpha \cdot \mathbf{v} + \beta \cdot \mathbf{v} \\ \alpha \cdot (\mathbf{u} + \mathbf{v}) &= \alpha \cdot \mathbf{u} + \alpha \cdot \mathbf{v}. \end{aligned}$$

(iii) Za produkt nevtralnega elementa za množenje $1 \in K$ in poljubnega vektorja $\mathbf{v} \in V$ velja:

$$1 \cdot \mathbf{v} = \mathbf{v}.$$

Operaciji v vektorskem prostoru označujemo s $+$ in $\cdot$. Na katero operacijo se dan znak nanaša je navadno enoumno razvidno iz konteksta, v nasprotnem primeru pa dodamo pojasnilo. Na začetku zaradi lažjega razumevanja oznako za zunanjo operacijo pišemo, v

nadaljevanju pa jo izpustimo. Najpomembnejši zgledi vektorskega prostora so realen in kompleksen vektorski prostor končne dimenzije, vektorski prostor matrik in vektorski prostor funkcij.

Zgledi:

(i) $V = \mathbb{R}^n$ je vektorski prostor nad $\mathbb{R}$ za običajno seštevanje po komponentah in množenje s skalarjem: za $\mathbf{u} = (\mathbf{u_1}, \ldots, \mathbf{u_n}) \in \mathbb{R}^n$ in $s \in \mathbb{R}$ je $s \cdot \mathbf{u} = (su_1, \ldots, su_n)$.

(ii) $V = \mathbb{R}^{m \times n}$ je vektorski prostor nad $\mathbb{R}$ za operaciji seštevanje matrik in množenje matrik s skalarjem.

(iii) $V = \mathbb{R}[x]$ je vektorski prostor nad $\mathbb{R}$ za običajno seštevanje polinomov ter množenje s skalarjem, ki je definirano kot množenje polinoma s skalarjem.

Naslednji trditvi veljata v poljubni grupi. Tu ju navajmo za vektorske prostore.

Trditev 3.2. *Vsak vektorski prostor V nad poljem K ima natanko en nevtralni element $\mathbf{0} \in V$ za seštevanje.*

Dokaz. Predpostavimo, da sta $\mathbf{0}$ in $\mathbf{0}'$ aditivni identiteti za vektorski prostor V. Potem velja,

$$\mathbf{0}' = \mathbf{0}' + \mathbf{0} = \mathbf{0}.$$

Prva enakost velja, ker je $\mathbf{0}$ aditivna identiteta. Prav tako drži druga enakost, ker je $\mathbf{0}'$ aditivna identiteta. Torej $\mathbf{0}' = \mathbf{0}$, dokazuje, da ima vsak vektorski prostor V en sam nevtralni element $\mathbf{0}$. □

Trditev 3.3. *Naj bo V vektorski prostor nad poljem K. Za vsak $\mathbf{v} \in V$ obstaja natanko en tak $\mathbf{w} \in V$, da je $\mathbf{v} + \mathbf{w} = \mathbf{0}$.*

Dokaz. Naj bo V vektorski prostor in $\mathbf{v} \in V$. Predpostavimo, da sta elementa za seštevanje $\mathbf{w}$ in $\mathbf{w}'$ nasprotna elementa elementa $\mathbf{v}$. Potem velja:

$$\mathbf{w} = \mathbf{w} + \mathbf{0} = \mathbf{w} + (\mathbf{v} + \mathbf{w}') = \underbrace{(\mathbf{w} + \mathbf{v})}_{\mathbf{0}} + \mathbf{w}' = \mathbf{0} + \mathbf{w}' = \mathbf{w}'.$$

Torej $\mathbf{w} = \mathbf{w}'$. □

Trditev 3.4. *Naj bo V vektorski prostor nad K, $\mathbf{v} \in V$ in $0 \in K$. Potem je $0 \cdot \mathbf{v} = \mathbf{0}$.*

Dokaz. Za vsak element $\mathbf{v} \in V$ imamo

$$0 \cdot \mathbf{v} = (0 + 0) \cdot \mathbf{v} = 0 \cdot \mathbf{v} + 0 \cdot \mathbf{v}.$$

Uporabimo pravilo krajšanja v $(V, +)$ in dobimo željen rezultat. □

V nadaljevanju bomo znak $\cdot$ za množenje vektorjev s skalarjem izpustili.

Definicija 3.5. *Naj bo V vektorski prostor nad poljem K. Potem je podmnožica $U \subseteq V$ vektorski podprostor prostora V, če je zaprta za obe operaciji:*

(i) $(U, +)$ *je podgrupa grupe* $(V, +)$,

(ii) $\alpha \cdot \mathbf{u} \in U$ *za vse* $\alpha \in K$ *in vse* $\mathbf{u} \in U$.

Trditev 3.6. *Podmnožica* $U \subseteq V$ *je vektorski podprostor vektorskega prostora* V *nad poljem* K *natanko tedaj, ko je* $\alpha\mathbf{u} + \beta\mathbf{v}$ *za vse* $\alpha, \beta \in K$ *in vse* $\mathbf{u}, \mathbf{v} \in U$.

Dokaz. Naj bo U vektorski podprostor prostora V. Potem je $\mathbf{u} + \mathbf{v} \in U$ za poljubna $\mathbf{u}, \mathbf{v} \in U$ in $\alpha \cdot \mathbf{u} \in U$ za vsak $\alpha \in K$ in vsak $\mathbf{u} \in U$. Izberemo $\alpha, \beta \in K$ in $\mathbf{u}, \mathbf{v} \in U$. Potem sta po definiciji 3.5 $\alpha \cdot \mathbf{u}$ in $\beta \cdot \mathbf{v}$ elementa vektorskega prostora U in tudi $\alpha\mathbf{u} + \beta\mathbf{v} \in U$. Obratno, naj bo $U \subseteq V$ podmnožica, za katero je $\alpha\mathbf{u} + \beta\mathbf{v} \in U$ za vsaka $\alpha, \beta \in K$ in vsaka $\mathbf{u}, \mathbf{v} \in U$. Izberimo $\alpha = 1$ in $\beta = -1$. Potem je $\mathbf{u} - \mathbf{v} \in U$ za vse $\mathbf{u}, \mathbf{v} \in U$ in zato je $(U, +)$ podgrupa v $(V, +)$. Če vzamemo $\beta = 0$, dobimo, da je $\alpha\mathbf{u} \in U$ za vse $\alpha \in K$ in vse $\mathbf{u} \in U$. Zato je U res vektorski podprostor prostora V. □

Bralec se lahko hitro prepriča sam, da je $\{0\}$ je vektorski podprostor v vsakem vektorskem prostoru. Označimo ga z 0 in imenujemo *trivialni podprostor* ali tudi *ničelni podprostor*. Sliko vektorja $\mathbf{u}$ s preslikavo $\mathcal{A}$ označujemo z $\mathcal{A}\mathbf{u}$ v kolikor ni nevarnosti za nejasnost.

Definicija 3.7. *Naj bosta* U *in* V *vektorska prostora nad poljem* K. *Preslikava* $\mathcal{A} : U \to V$ *je linearna, če velja*

1.) aditivnost: $\mathcal{A}(\mathbf{u}_1 + \mathbf{u}_2) = \mathcal{A}(\mathbf{u}_1) + \mathcal{A}(\mathbf{u}_2)$ *za vse* $\mathbf{u}_1, \mathbf{u}_2 \in U$,

2.) homogenost: $\mathcal{A}(\alpha\mathbf{u}) = \alpha(\mathcal{A}\mathbf{u})$ *za vsak* $\alpha \in K$ *in vsak* $\mathbf{u} \in U$.

Trditev 3.8. *Preslikava* $\mathcal{A} : U \to V$ *med vektorskima prostoroma* U *in* V *nad poljem* K *je linearna, natanko tedaj, ko velja*

$$\mathcal{A}(\alpha\mathbf{u}_1 + \beta\mathbf{u}_2) = \alpha\mathcal{A}\mathbf{u}_1 + \beta\mathcal{A}\mathbf{u}_2$$

za vse $\alpha, \beta \in K$ *in vse* $\mathbf{u}_1, \mathbf{u}_2 \in U$.

Dokaz. Če je $\mathcal{A}$ linearna preslikava, potem iz aditivnosti in homogenosti sledi

$$\mathcal{A}(\alpha\mathbf{u}_1 + \beta\mathbf{u}_2) = \mathcal{A}(\alpha\mathbf{u}_1) + \mathcal{A}(\beta\mathbf{u}_2) = \alpha\mathcal{A}\mathbf{u}_1 + \beta\mathcal{A}\mathbf{u}_2$$

za vse α, $\beta \in K$ in vse $\mathbf{u}_1, \mathbf{u}_2 \in U$.
Obratno, naj bo $\mathcal{A}(\alpha\mathbf{u}_1 + \beta\mathbf{u}_2) = \alpha\mathcal{A}(\mathbf{u}_1) + \beta\mathcal{A}(\mathbf{u}_2)$ za vse $\alpha, \beta \in K$ in vse $\mathbf{u}_1, \mathbf{u}_2 \in U$.

Izberimo $\alpha = \beta = 1$. Potem je $\mathcal{A}(\mathbf{u}_1 + \mathbf{u}_2) = \mathcal{A}\mathbf{u}_1 + \mathcal{A}\mathbf{u}_2$ za vse $\mathbf{u}_1, \mathbf{u}_2 \in U$ in zato je $\mathcal{A}$ aditivna. Če vzamemo $\beta = 0$, dobimo $\mathcal{A}(\alpha\mathbf{u}_1) = \alpha\mathcal{A}\mathbf{u}_1$ in zato je $\mathcal{A}$ tudi homogena. □

Definicija 3.9. *Naj bo* $\mathcal{A} : U \to V$ *linearna preslikava med vektorskima prostoroma* U *in* V *nad poljem* K. *Potem množico*

$$\ker(\mathcal{A}) = \{\mathbf{u} \in U | \mathcal{A}(\mathbf{u}) = \mathbf{0}\},$$

imenujemo jedro linearne preslikave $\mathcal{A}$.

Opomba: Bralec se lahko prepriča sam, da je $\mathcal{A}(\mathbf{0}) = \mathbf{0}$ in zato $\mathbf{0} \in \ker(\mathcal{A})$. Zato je jedro vedno neprazna množica.

Izrek 3.10. *Jedro linearne preslikave $\mathcal{A} : U \to V$ med vektorskima prostoroma U in V nad poljem K je vektorski podprostor prostora U.*

Dokaz. Naj bosta $\mathbf{u}_1, \mathbf{u}_2 \in U$ v jedru $\ker(\mathcal{A})$ linearne preslikave $\mathcal{A}$. Potem je zaradi aditivnosti in homogenosti preslikave $\mathcal{A}$

$$\mathcal{A}(\alpha\mathbf{u}_1 + \beta\mathbf{u}_2) = \alpha\mathcal{A}\mathbf{u}_1 + \beta\mathcal{A}\mathbf{u}_2 = \mathbf{0}.$$

Torej je $\alpha\mathbf{u}_1 + \beta\mathbf{u}_2 \in \ker(\mathcal{A})$ za vse $\alpha, \beta \in K$ in zato je po trditvi 3.6 $\ker(\mathcal{A})$ vektorski podprostor prostora U. □

Definicija 3.11. *Naj bo $\mathcal{A} : U \to V$ linearna preslikava med vektorskima prostoroma U in V nad poljem K. Množico*

$$im(\mathcal{A}) = \{\mathbf{v} \in V | \exists \mathbf{u} \in U : \mathbf{v} = \mathcal{A}\mathbf{u}\}$$

imenujemo slika linearne preslikave $\mathcal{A} : U \to V$.

Definicija 3.12. *Naj bo $\mathcal{A} : U \to V$ linearna preslikava med vektorskima prostoroma U in V nad poljem K.*

- *Če je $\mathcal{A}$ injektivna, $\mathcal{A}$ imenujemo monomorfizem,*
- *Če je $\mathcal{A}$ surjektivna, $\mathcal{A}$ imenujemo epimorfizem,*
- *Če je $\mathcal{A}$ bijektivna, $\mathcal{A}$ imenujemo izomorfizem,*
- *Če je $U = V$, $\mathcal{A}$ imenujemo endomorfizem,*
- *Če je $U = V$ in je $\mathcal{A}$ bijektivna, $\mathcal{A}$ imenujemo avtomorfizem.*

Če je linearna preslikava $\mathcal{A}$ obrnljiva, je njen inverz $\mathcal{A}^{-1}$ tudi linearna preslikava in v tem primeru $\mathcal{A}$ imenujemo izomorfizem. Množico vseh avtomorfizmov vektorskega prostora V nad poljem K skupaj z običajnim komponiranjem preslikav tvori grupo, ki jo označujemo z $GL(V)$.

Definicija 3.13. *Naj bo V vektorski prostor nad poljem K. Potem vektor $\alpha\mathbf{u} + \beta\mathbf{v}$ imenujemo linearna kombinacija vektorjev $\mathbf{u}$ in $\mathbf{v}$. Podobno za $\alpha_1, \alpha_2, \ldots, \alpha_k \in K$ in $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in V$ vektor*

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \ldots + \alpha_k\mathbf{v}_k = \sum_{i=1}^{k} \alpha_i\mathbf{v}_i$$

imenujemo linearna kombinacija vektorjev $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in V$.

Trditev 3.14. *Naj bo V vektorski prostor nad poljem K in $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in V$. Potem je množica vseh linearnih kombinacij teh vektorjev vektorski podprostor prostora V.*

Dokaz. Naj bosta $\sum_{i=1}^{k} \alpha_i \mathbf{v}_i$ in $\sum_{i=1}^{k} \beta_i \mathbf{v}_i$ dve linearni kombinaciji vektorjev $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in V$ in $\gamma, \delta \in K$. Potem je

$$\gamma(\sum_{i=1}^{k} \alpha_i \mathbf{v}_i) + \delta(\sum_{i=1}^{k} \beta_i \mathbf{v}_i) = (\sum_{i=1}^{k} (\gamma\alpha_i + \delta\beta_i)\mathbf{v}_i$$

spet linearna kombinacija vektorjev $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$. Zato je po trditvi 3.6 množica vseh linearnih kombinacij vektorjev $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in V$ vektorski podprostor prostora V. □

Definicija 3.15. *Naj bo V vektorski prostor nad poljem K in $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in V$. Množico vseh linearnih kombinacij vektorjev $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ imenujemo linearna ogrinjača vektorjev $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$. Označimo jo z $\mathcal{L}(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$.*

Po prejšnji trditvi je linearna ogrinjača vektorski podprostor prostora V. Naslednja trditev pa nam pove, da je linearna ogrinjača vektorjev $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ najmanjši vektorski podprostor prostora V, ki vsebuje $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$.

Trditev 3.16. *Naj bo V vektorski prostor nad poljem K in $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in V$. Potem je linearna ogrinjača $\mathcal{L}(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ najmanjši vektorski podprostor prostora V, ki vsebuje vektorje $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$.*

Dokaz. Naj bo U najmanjši tak vektorski podprostor, ki vsebuje vse vektorje $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$. Ker je U vektorski podprostor, vsebuje tudi vektorje $\alpha_1\mathbf{v}_1, \alpha_2\mathbf{v}_2, \ldots, \alpha_k\mathbf{v}_k$ za poljubne skalarje $\alpha_1, \alpha_2, \ldots, \alpha_k \in K$, ter tudi njihovo vsoto $\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \ldots + \alpha_k\mathbf{v}_k$. Torej U vsebuje vse linearne kombinacije vektorjev $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ in zato je

$$\mathcal{L}(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k) \subseteq U.$$

Ker je po trditvi 3.14 $\mathcal{L}(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ vektorski podprostor, zaradi minimalnosti podprostora U sledi, da je $\mathcal{L}(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k) = U$. □

Definicija 3.17. *Naj bodo $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ vektorji iz vektorskega prostora V nad polje K. Rečemo, da so vektorji $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ linearno odvisini, če obstajajo taki skalarji $\alpha_1, \alpha_2, \ldots, \alpha_k$, ne vsi enaki nič, da je $\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \ldots + \alpha_k\mathbf{v}_k = \mathbf{0}$. Če vektorji $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ niso linearno odvisini, potem so linearno neodvisni.*

Trditev 3.18. *Vektorji $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ vektorskega prostora V nad poljem K so linearno neodvisni natanko tedaj, ko iz enakosti $\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \ldots + \alpha_k\mathbf{v}_k = 0$ sledi $\alpha_1 = \alpha_2 = \ldots = \alpha_k = 0$.*

Dokaz iztrditve 3.18 si lahko bralec ogleda v [9] na strani 103.

Trditev 3.19. *Naj bo V vektorski prostor nad poljem K. Če množica $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ vsebuje vektor $\mathbf{0}$, potem so $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ linearno odvisni.*

Dokaz. Recimo, da je $\mathbf{v}_1 = \mathbf{0}$. Potem je $1 \cdot \mathbf{v}_1 + 0 \cdot \mathbf{v}_2 + 0 \cdot \mathbf{v}_3 + \ldots + 0 \cdot \mathbf{v}_k = 0$ in so $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ po trditvi 3.18 linearno odvisni. □

Trditev 3.20. *Naj bo V vektorski prostor nad polje K, $U = \mathcal{L}(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ in naj bo $\mathbf{v}_j$ linearna kombinacija vektorjev $\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_{j+1}, \ldots, \mathbf{v}_k$. Potem je*

$$U = \mathcal{L}(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_{j+1}, \ldots, \mathbf{v}_k).$$

Dokaz. Naj bodo $\mathbf{v}_1, \ldots, \mathbf{v}_k \in \mathcal{L}(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ taki, da je $\mathbf{v}_j$ linearna kombinacija vektorjev $\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_{j+1}, \ldots, \mathbf{v}_k$. Potem obstajajo taki skalarji $\alpha_1, \alpha_2, \ldots, \alpha_k \in K$, ne vsi enaki 0 in $\alpha_j \neq 0$, da je

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \ldots + \alpha_k\mathbf{v}_k = 0.$$

Ker je $\alpha_j \neq 0$, dobimo $\mathbf{v}_j = -\frac{\alpha_1}{\alpha_j}\mathbf{v}_1 - \ldots - \frac{\alpha_{j-1}}{\alpha_j}\mathbf{v}_{j-1} - \frac{\alpha_{j+1}}{\alpha_j}\mathbf{v}_{j+1} - \ldots - \frac{\alpha_k}{\alpha_j}\mathbf{v}_k$ in zato $\mathcal{L}(\mathbf{v}_1, \ldots, \mathbf{v}_k) = \mathcal{L}(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_{j+1}, \ldots, \mathbf{v}_k)$. □

Definicija 3.21. *Naj bo V vektorski prostor nad poljem K. Neprazni množici $M \subseteq V$ rečemo ogrodje vektorskega prostora V, če je linearna ogrinjača $\mathcal{L}(M)$ množice M enaka prostoru V, $\mathcal{L}(M) = V$.*

Enakovredno je lahko reči, da je M ogrodje vektorskega prostora V, če se vsak vektor iz V linearno izraža z vektorji iz M.

Definicija 3.22. *Naj bo V vektorski prostor nad poljem K. Vektorski prostor V je končnorazsežen, če premore končno ogrodje.*

Definicija 3.23. *Množico vektorjev $\mathscr{B} = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ imenujemo baza vektorskega prostora V nad poljem K, če velja*

- *$V = \mathcal{L}(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$,*
- *vektorji $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ so linearno neodvisni.*

Elemente baze $\mathscr{B}$ imenujemo bazni vektorji. Trivialni vektorski prostor $\{0\}$ nima baze.

Trditev 3.24. *Naj bo V vektorski prostor nad poljem K. Množica $\mathscr{B}$ je baza vektorskega prostora V natanko tedaj, ko se vsak vektor prostora V da enolično izraziti kot linearna kombinacija baznih vektorjev.*

Dokaz. Prva lastnost v definiciji baze nam pove, da je vsak vektor linearna kombinacija vektorjev iz baze $\mathscr{B}$. Naj bosta $\mathbf{u} = \sum_{i=1}^{n} \alpha_i\mathbf{v}_i$ in $\mathbf{u} = \sum_{i=1}^{n} \beta_i\mathbf{v}_i$ dva razvoja po bazi. Potem je $\mathbf{0} = \mathbf{u} - \mathbf{u} = \sum_{i=1}^{n}(\alpha_i - \beta_i)\mathbf{v}_i$. Ker so $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ linearno neodvisni, je $\alpha_i - \beta_i = 0$ za vsak $i \in \{1, \ldots, n\}$. Torej $\alpha_i = \beta_i$ za vsak $i \in \{1, \ldots, n\}$ in $\mathbf{u}$ se res da enolično izraziti kot linearna kombinacija baznih vektorjev. □

Izrek 3.25. *Naj bo V vektorski prostor nad poljem K. Vektorji $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m$ naj se dajo vsi linerano izraziti z vektorji $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$. Če je $m > n$, so vektorji $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m$ med seboj linearno odvisni.*

Dokaz. Vektorji $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m$ so gotovo med seboj linearno odvisni, če je eden med njimi enak nič. Zato bomo privzeli, da so vsi $\mathbf{u}_k \neq \mathbf{0}, k \in \{1, \ldots, m\}$. Izrazimo vektor $\mathbf{u}_1$ z vektorji $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$. Ker $\mathbf{u}_1 \neq 0$, niso vsi koeficienti v tem izrazu enaki nič in je zato vsaj eden od vektorjev $\mathbf{v}_i$, brez škode za splošnost, lahko rečemo, da je $\mathbf{v}_1$, linearna kombinacija vektorjev $\mathbf{u}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$.
Prav tako izrazimo $\mathbf{u}_2$ z vektorji $\mathbf{v}_i$, nato pa v tem izrazu še $\mathbf{v}_1$ nadomestimo s pravkar dobljeno linearno kombinacijo vektorjev $\mathbf{u}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$. Tako smo dobili $\mathbf{u}_2$ kot linearno kombinacijo vektorjev $\mathbf{u}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$. Če so v tej linearni kombinaciji koeficienti pri $\mathbf{v}_2, \ldots, \mathbf{v}_n$

vsi enaki nič, se $\mathbf{u}_2$ izraža z $\mathbf{u}_1$. Torej so v tem primeru $\mathbf{u}_1, \ldots, \mathbf{u}_m$ med seboj linearno odvisni. V nasprotnem primeru je en koeficient, naprimer $\mathbf{v}_2$, različen od nič in lahko izrazimo $\mathbf{v}_2$ kot linearno kombinacijo vektorjev $\mathbf{u}_1, \mathbf{u}_2, \mathbf{v}_3, \ldots, \mathbf{v}_n$. Tako nadaljujemo. Če ni noben vektor $\mathbf{u}_k, k \in 2, \ldots, n$, linearna kombinacija vektorjev $\mathbf{u}_1, \ldots, \mathbf{u}_{k-1}$, dobimo nazadnje, da se vektorji $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ izražajo z $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$. Ker je $m > n$, imamo še vektor $\mathbf{u}_{n+1}$. Tudi ta je linearna kombinacija vektorjev $\mathbf{v}_i$. Če v tej linearni kombinaciji izrazimo vektorje $\mathbf{v}_i$ z vektorji $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$, smo vektor $\mathbf{u}_{n+1}$ izrazili kot linearno kombinacijo vektorjev $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$. Torej so res vektorji $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{n+1}$ med seboj linearno odvisni. □

Izrek 3.26. *Naj bosta* $\mathscr{B}_1 = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ *in* $\mathscr{B}_2 = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m\}$ *dve bazi vektorskega prostora* V *nad poljem* K*. Potem je* $m = n$*.*

Dokaz. Vektorji v bazi so med seboj linearno neodvisni in vsak vektor iz V se da z njimi linearno izraziti. Torej so vektorji $\mathbf{u}_k, k \in \{1, \ldots, m\}$ linearne kombinacije vektorjev $\mathbf{v}_i, i \in \{1, \ldots, n\}$. Če bi bil $m > n$, bi bili vektorji $\mathbf{u}_k$ po izreku 3.25 med seboj linearno odvisni, a to ni res. Na enak način se lahko prepričamo, da $n \not> m$ in torej $n = m$. □

Definicija 3.27. *Razsežnost (dimenzija) netrivialnega končnorazsežnega vektorskega prostora je moč katerekoli njegove baze. Oznaka: dim* V*. Razsežnost trivialnega vektorskega prostora je* 0*,* $dim\{0\} = 0$*.*

Poglavje 4

Moduli

To poglavje je povzeto iz [1] , [2] in [6],.

Definicija 4.1. *(Levi modul) Naj bo K kolobar z identiteto (enico) $1 \in K$ in M aditivno pisana komutativna grupa. M je levi modul nad kolobarjem K (oziroma levi K-modul), če vsakemu elementu $\lambda \in K$ in vsakemu elementu $a \in M$ pripada nek element iz M, ki ga pišemo kot produkt $\lambda a \in M$ in veljajo naslednja računska pravila:*

(L1) $\lambda(a+b) = \lambda a + \lambda b$ *za* $\forall \lambda, \mu \in K$ *in* $\forall a, b \in M$,

(L2) $(\lambda + \mu)a = \lambda a + \mu a$ *za* $\forall \lambda, \mu \in K$ *in* $\forall a \in M$,

(L3) $(\lambda\mu)a = \lambda(\mu a)$ *za* $\forall \lambda, \mu \in K$ *in* $\forall a, b \in M$,

(L4) $1 \cdot a = a$ *za* $\forall a \in M$.

Elemente kolobarja K imenujemo skalarne množitelje ali skalarje.

Zgledi:

(i) Direktno iz definicije modula sledi, da v primeru, ko je K polje koncept modulov soupade s konceptom vektorskih prostorov nad polje K.

(ii) Naj bo K komutativna grupa. Potem je

$$K^n = \underbrace{K \times \cdots \times K}_{n-krat}$$

levi K-modul, če skalarno množenje definiramo:

$$\lambda(\lambda_1, \ldots, \lambda_n) = (\lambda\lambda_1, \ldots, \lambda\lambda_n),$$

kjer so $\lambda, \lambda_1, \ldots, \lambda_n \in K$.

(c) Naj bo A komutativen kolobar in K polje matrik razsežnosti $m \times n$ nad kolobarjem A. Naj bo M komutativna grupa n stolpčnega vektorja v A^n. Potem je M levi K-modul, če privzememo, da je množenje matrik skalarno množenje.

Lastnosti 4.2. *Naj bo K kolobar z enico $1 \in K$ in M levi K-modul. Potem velja naslednje:*

- $0_K a = 0_M$, *za vsak* $a \in M$;
- $\lambda 0_M = 0_M$, *za vsak* $\lambda \in K$;
- $(-\lambda)a = -(\lambda a) = \lambda(-a)$, *za vsak* $a \in M$ *in vsak* $\lambda \in K$.

Pravilo (L1) nam pove, da je $x \mapsto \lambda x$ pri izbranem elementu $\lambda \in K$ endomorfizem grupe M. Po pravilu (L4) pripada elementu 1 identični endomorfizem. Ker je M aditivna grupa, vsebuje nevtralni element 0_M. Vsak element $a \in M$ ima nasprotni element $-a$. Kolobar K vsebuje nevtralni element 0_K za seštevanje. Po pravilu (L2) je $\lambda a = (\lambda + 0_K)a = \lambda a + 0_K \cdot a$. Od tu sledi, da je $0_K \cdot a = 0_M$. Nadalje je $0_M = (\lambda - \lambda)a = \lambda a + (-\lambda)a$. Dobimo $(-\lambda)a = -(\lambda a)$. Torej, če pomnožimo poljuben element $a \in M$ s skalarjem $-\lambda$, dobimo nasprotni element produkta λa. Najmanjši modul vsebuje samo element 0. To je modul $\{0\}$. Podobno definiramo desni modul M nad kolobarjem K.

Definicija 4.3. *(Desni modul) Naj bo K kolobar z enico $1 \in K$ in M aditivno pisana komutativna grupa. Potem je M desni modul nad kolobarjem K (oziroma desni K-modul), če vsakemu elementu λ iz K in vsakemu elementu a iz M pripada neki element iz M, ki ga pišemo kot produkt $a\lambda$ in veljajo naslednje lastnosti:*

(D1) $(a + b)\lambda = a\lambda + b\lambda$, $\forall \lambda \in K, \forall a, b \in M$,

(D2) $a(\lambda + \mu) = a\lambda + a\mu$, $\forall \lambda, \mu \in K, \forall a \in M$,

(D3) $a(\lambda\mu) = (a\lambda)\mu$, $\forall \lambda, \mu \in K, \forall a \in M$,

(D4) $a \cdot 1 = a$, $\forall a \in M$.

Razločevanje med levim in desnim modulam ni zgolj formalno. Če pogledamo pravilo (L3) in (D3). Pri produktu elementa λ iz kolobarja K z elementom a iz modula M se (L3) glasi: $a(\lambda\mu) = (a\lambda)\mu$, to pa ni pravilo (D3), če kolobar K ni komutativen. Pri komutativnem osnovnem kolobarju K ni razlike med desnim in levim modulom. Vseeno je ali pišemo λa ali $a\lambda$.
Levi K-modul v nalogi včasih poimenujemo kar samo modul.

Zgledi:

- Vsak kolobar K z enico $1 \in K$ je levi in desni K-modul nad samim seboj.
- Če je G aditivna komutativna grupa, potem lahko $\underbrace{g \times \cdots \times g}_{k-krat}$ pišemo kot kg in tako G postane levi $\mathbb{Z}$-modul, saj za poljubne $k, k_1, k_2 \in \mathbb{Z}$ in poljubne $g, g_1, g_2 \in G$ velja

$$\begin{aligned} k(g_1 + g_2) &= kg_1 + kg_2, \\ (k_1 + k_2)g &= k_1 g + k_2 g, \\ (k_1 k_2)g &= k_1(k_2)g, \\ 1g &= g. \end{aligned}$$

- Naj bo $\mathbb{R}^n$ množica vseh urejenih n-teric

$$(x_1, x_2, \ldots, x_n), \quad x_i \in \mathbb{R}, \text{ kjer je } i \in \{1, \ldots, n\}$$

Množica $\mathbb{R}^n$ je komutativna grupa glede na operacijo seštevanja

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n).$$

Nevtralni element je

$$0 = (0, 0, \ldots, 0),$$

in nasprotni element elementa $(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$ je

$$-(x_1, x_2, \ldots, x_n) = (-x_1, -x_2, \ldots, -x_n).$$

Če definiramo množenje $\mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$ s predpisom

$$\alpha(x_1, x_2, \ldots, x_n) = (\alpha x_1, \alpha x_2, \ldots, \alpha x_n),$$

je $\mathbb{R}^n$ modul nad poljem $\mathbb{R}$, ki ga imenujemo n-dimenzionalni realni vektorski prostor.

Definicija 4.4. *Naj bo K komutativen kolobar z enico $1 \in K$. Potem je K-modul M K-algebra, če je na množici M definirano množenje, ki skupaj s seštevanjem tvori kolobar, in velja:*

$$k(xy) = (kx)y = x(ky)$$

za vse $x, y \in M$ in vsak $k \in K$.

Zgledi:

- Vsak komutativen kolobar K je algebra nad samim seboj.
- Če je K komutativen kolobar, potem sta kolobar polinomov $K[X]$ s koeficienti iz K in cel kolobar matrik $M_n(K)$ primera K-algebr.

Definicija 4.5. *Naj bo K kolobar z enico $1 \in K$ in M modul nad kolobarjem K. Potem je neprazna podmnožica $L \subset M$ podmodul modula M (oziroma K-podmodul modula M), če velja:*

- $x + y \in L, \forall x, y \in L$
- $kx \in L, \forall x \in L$ *in* $\forall k \in K$

Definicija 4.6. *Če je M R-algebra, potem je N podalgebra algebre M, če je N podmodul, ki je podkolobar.*

Zgledi

- Če je I levi ideal kolobarja K, je I podmodul K-modula K.

- Naj bo M K-modul in $x \in M$. Potem je množica

$$Kx = \{kx | k \in K\}$$

podmodul modula M, saj je

$$k_1 x - k_2 x = (k_1 - k_2)x \in Kx$$

$$k_1(k_2 x) = (k_1 k_2)x \in Kx,$$

za vsak $k_1, k_2 \in K$.

Naj bo M K-modul in L podmodul modula M. Potem je L podgrupa aditivne grupe M. Zato eksistira faktorska grupa M/L, ki sestoji iz vseh odsekov $a + L$, $a \in M$. Pomnožimo poljuben element $a + x \in a + L$ s skalarjem λ. Ker je $x \in L$ in je L podmodul , je $\lambda x \in L$ in posledično produkt $\lambda(a + x) = \lambda a + \lambda x$ pripada odseku $\lambda a + L$. Zato v M/L definiramo, da je produkt skalarja λ z odsekom $a + L$ enak odseku $\lambda a + L$. Po tej definiciji je množenje odsekov s skalarji enolično določeno. To množenje ustreza vsem pravilom od (L1) do (L4). Zato je množica odsekov M/L levi K-modul nad kolobarjem K. Imenujemo ga *faktorski modul*.

Opomba: Levi ideal J kolobarja K je levi K-modul. Ker je kolobar K tudi K-modul, je ideal J podmodul modula K. Faktorska množica K/J je prav tako levi K-modul. Če J ni dvostrani ideal, K/J ni kolobar.

Naj bosta L in L' taka podmodula K-modula M, da je

(i) $L \cap L' = \{0\}$

(ii) $L + L' = M$.

V tem primeru imata podmodula L in L' skupen samo element $0 \in M$. Z $L+L'$ označujemo množico vsot $x + y$, ko preteče x ves modul L in y ves modul L'. Ker je po predpostavki (ii) zgoraj vsota $L + L'$ enaka modulu M, se da vsak element $z \in M$ zapisati v obliki vsote

$$z = x + y, x \in L, y \in L'.$$

To izražanje je mogoče samo na en način. Denimo namreč, da je tudi $z = x' + y', x' \in L, y' \in L'$. Potem je $x' + y' = x + y$ oziroma $x' - x = y - y'$. Ker je $x' - x \in L$ in $y - y' \in L'$, pripada razlika $x' - x = y - y'$ preseku $L \cap L'$, ki vsebuje edino element 0. Zato je $x' - x = y - y' = 0$, torej $x' = x$ in $y' = y$.

4.1 Homomorfizem modulov

Definicija 4.7. *Naj bo K kolobar ter M in M' K-modula. Homomorfizem K- modula M v K- modul M' je preslikava $f : M \to M'$, ki ustreza pogojema*

$$f(x + y) = f(x) + f(y), \tag{4.1}$$

$$f(\lambda x) = \lambda f(x), \tag{4.2}$$

kjer sta x in y poljubna elementa modula M in λ poljuben element kolobarja K.

Povratno enoličen homomorfizem imenujemo izomorfizem. Za dva modula med katerima obstaja izomorfizem pa pravimo, da sta izomorfna. Iz enačbe (4.1) je razvidno, da je f homomorfizem za aditivno grupo M. Pogoja (4.1) in (4.2) lahko združimo v eno samo enačbo:

$$f(\lambda x + \mu y) = \lambda f(x) + \mu f(y) \quad \forall x, y \in M \text{ in } \forall \lambda, \mu \in K. \tag{4.3}$$

Iz pogojev (4.1) in (4.2) namreč dobimo $f(\lambda x+\mu y) = f(\lambda x)+f(\mu y) = \lambda f(x)+\mu f(y)$. Naj bo zdaj $f : M \to M'$ preslikava, ki ustreza enačbi (4.3) za vse $x, y \in M$ in $\lambda, \mu \in K$. Če v (4.3) vstavimo naprej $\lambda = \mu = 1$ in nato še $\mu = 0$, dobimo pogoja (4.1) in (4.2). Torej f je homomorfizem. Množico vseh slik označujemo z $f(M)$, ki je podmodul modula M'. Če pa je L' podmodul modula M' je inverzna slika $f^{-1}(L')$, ta sestoji iz vseh elementov modula M, ki se preslikajo v L', podmodul modula M. V posebnem primeru, ko vsebuje L' samo element 0, je inverzna slika $f^{-1}(0)$ podmodul, ki se imenuje *jedro homomorfizma* f. Torej v jedru so vsi elementi modula M, ki se s homomorfizmom f preslikajo v element $0 \in M$.

Množico vseh homomorfizmov modula M v M' označimo s $Hom(M, M')$. Trivialni homomorfizem preslika vsak element modula M v element 0 modula M'. Od tod sklepamo, da množica $Hom(M, M')$ ni nikoli prazna.

Trditev 4.8. *Naj bosta f in g homomorfizma K modula M v K-modulu M', torej $f, g \in Hom(M, M')$. Vsota $f(x) + g(x)$, pri čemer je $x \in M$, je element modula M'. Preslikava, ki priredi elementu $x \in M$ element $f(x)+g(x) \in M'$je homomorfizem iz K-modula M'. Ta homomorfizem imenujemo vsota homomorfizmov f in g in ga označimo z $f + g$, torej*

$$(f + g)(x) = f(x) + g(x). \tag{4.4}$$

Dokaz. Da je vsota $f + g$ homomorfizem ugotovimo takole:

$$\begin{aligned} (f + g)(\lambda x + \mu y) &= f(\lambda x + \mu y) + g(\lambda x + \mu y) = \\ &= \lambda f(x) + \mu f(y) + \lambda g(x) + \mu g(y) = \\ &= \lambda(f + g)(x) + \mu(f + g)(y). \end{aligned}$$

Od tod sledi, da je $f + g \in Hom(M, M')$.

□

4.2 Izreki o izomorfizmu za module

Če je J podmodul K-modula M, potem je J aditivna podgrupa grupe M in lahko tvorimo faktorsko grupo M/J na običajen način. Pravzaprav faktorska grupa postane K-modul, če skalarno množenje definiramo takole:

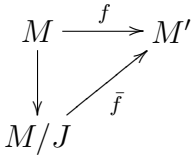
$$r(x + J) = rx + J$$

kjer $r \in K$ in $x \in M$. To množenje je dobro definirano, saj če x pripada podmodulu J potem tudi rx pripada podmodulu J. Ker je skalarno množenje v kvocientnem modulu

M/J definirano preko skalarnega množenja v prvotnem modulu M, se lahko bralec hitro prepriča sam, da M/J zadošča aksiomom z definicije modula (glej tudi stran 19). Kanonična preslikava $f\colon M \to M/J$ je homomorfizem modulov z jedrom J. Tako kot pri teoriji grup in teoriji kolobarjev lahko tudi za module dokažemo osnovne izreke o izomorfizmu.

Trditev 4.9. *Poljuben homomorfizem modulov $f : M \to M'$, katerega jedro vsebuje podmodul J, lahko faktoriziramo preko M/J. Z drugimi besedami, obstaja enolično določen homomorfizem modulov $\bar{f} : M/J \to M'$, za katerega velja $\bar{f}(x+J) = f(x)$. Poleg tega velja*

- *$\bar{f}$ je epimorfizem natanko tedaj, ko je f epimorfizem;*
- *$\bar{f}$ je monomorfizem natanko tedaj, ko je $ker(f) = J$;*
- *$\bar{f}$ je izomorfizem natanko tedaj, ko je f epimorfizem in $ker(f) = J$.*



Bralec si lahko podrobno razlago trditve 4.9 in njenega dokaza ogleda v [10] na strani 46.

Izrek 4.10. *(Prvi izrek izomorfizma modulov) Če je $f : M \to M'$ homomorfizem modulov z jedrom J, je slika homomorfizma f izomorfna faktorskemu modulu M/J.*

Dokaz. Homomorfizem $\overline{f}$ iz trditve 4.10 je zdaj injektiven. Saj, če je odsek $Z = z + J$ v njegovem jedru, iz $f(z) = \overline{f}(Z) = 0$ dobimo, da $z \in J$, torej $Z = J$, to pa je ničelni element faktorskega modula M/J. Vsak element modula $f(M)$ ima obliko $f(x)$ za neki $x \in M$ in je zato slika odseka $X = x + J$. Od tod sledi, da je $\overline{f}$ povratno enoličen, torej izomorfizem med faktorskim modulom M/J in modulom $f(M)$. □

Izrek 4.11. *(Drugi izrek izomorfizma modulov) Naj bosta S in T podmodula modula M nad kolobarjem K in naj bo $S + T = \{x + y : x \in S, y \in T\}$. Potem sta $S + T$ in $S \cap T$ podmodula modula M in obstaja izomorfizem:*

$$\xi : S/(S \cap T) \to (S + T)/T.$$

Dokaz. Definirajmo $f : S \to M/T$ tako, da $f(x) = x + T$. Bralec se lahko hitro prepriča sam, da je f homomorfizem modulov in da je im(f) = (S+T)/T. Poleg tega je

$$\ker(f) = \{x \in S : s + T = 0_{(S+T)/T}\} = \{x \in S : s \in T\} = S \cap T.$$

Zato je po prvem izreku o izmomofizmu modulov (glej izrek 4.10) $S/S \cap T \cong (S+T)/T$. □

Izrek 4.12. *(Tretji izrek izomorfizma modulov) Naj bo M modul nad kolobarjem K ter J in L njegova podmodula. Če je $J \leq L \leq M$, potem obstaja izomorfizem*

$$\eta : (M/J)/(L/J) \to M/L$$

kjer je $\eta((m + J) + L/J) = m + L$, za vsak $m \in M$.

Dokaz. Ker je $J \leq L$, definirajmo preslikavo $f : M/J \to M/L$ tako, da je $f(m+J) = m+L$, za vsak $m \in M$. Naj bosta $m, m' \in M$ taka elementa, da velja $m + J = m' + J$. Potem je $m - m' \in J \leq L$ in zato $m + L = m' + L$ oziroma preslikava f je dobro definirana. Bralec se lahko hitro prepriča sam, da je f pravzaprav homomorfizem modulov z jedrom

$$\begin{aligned} \ker(f) &= \{m + J : m \in M \text{ in } m + L = 0_{M/L}\} \\ &= \{m + J : m \in L\} = L/J, \end{aligned}$$

rezultat sledi iz prvega izreka o izomorfizmu modulov. □

Definicija 4.13. *K-modul M je cikličen, če je generiran z enim samim elementom $x \in M$. Z drugimi besedami,*

$$M = Kx = \{kx : k \in K\}, x \in M.$$

Vsak element cikličnega K-modula M je skalarni mnogokratnik elementa x. (Če je $x = 0$ je $M = \{0\}$, kar imenujemo ničelni modul, pišemo pa kar 0.) Cikličen vektorski prostor nad poljem je eno-dimenzionalen prostor ob predpostavki, da je $x \neq 0$. *Anihilator* elementa y v K-modulu M je množica $I_y = \{k \in K : ky = 0\}$, ki je levi ideal kolobarja K, saj če je $s_1y = 0$ in $s_2y = 0$, potem je $(s_1 + s_2)y = s_1y + s_2y = 0$ in če je $sy = 0$, potem je tudi $(ks)y = k(sy) = 0$ za vsak $k \in K$. Če je K komutativen kolobar in M cikličen modul z generatorjem x, potem je $M \cong K/I_x$. Da to vidimo, uporabimo prvi izrek o izomorfizmu za preslikavo

$$\begin{aligned} K &\to M, \\ k &\mapsto km. \end{aligned}$$

Anhilator za modul M je $I_0 = \{k \in K : ky = 0 \text{ za vsak } y \in M\}$.Naj omenimo še, da je I_0 dvostranski ideal, saj za poljubne $k, l \in I_0$ in $s \in K$ velja:

- $(l + k)y = ly + ky = 0 + 0 = 0$ za vsak $y \in M$ in zato $l + k \in I_0$,
- $(sk)y = s(ky) = s \cdot 0$ za vsak $y \in M$ in zato $sk \in I_0$,
- $(ks)y = k(sy) = 0$ za vsak $y \in M$ in zato $ks \in I_0$.

Ko je K komutativen, je anhilator generatorja cikličnega modula enak annihilatorju celega modula M.

4.3 Prosti moduli in direktna vsota

V tem poglavju bomo razširili koncept baz v vektorskih prostorih na koncept baz v modulih. Naj bo S podmnožica elementov K-modula M. S KS bomo označevali množico vseh končnih vsot oblike $\sum_{i=1}^{n} x_i s_i$, kjer je n pozitivno celo število, $x_i \in K$ in $s_i \in S$ za vsak $i \in \{1, \ldots, n\}$.

Definicija 4.14. *Množico $S = \{s_i\}_{i\in I}$ elementov K-modula M imenujemo množica generatorjev modula M, če je $M = KS$, torej, če lahko vsak element modula M zapišemo kot linearno kombinacijo elementov iz S s koeficienti iz kolobarja K.*

Za vsak modul obstaja sistem generatorjev, saj lahko vzamemo kar $S = M$.

Definicija 4.15. *Pravimo, da je množica $S = \{s_i\}_{i\in I}$ elementov K-modula M linearno neodvisna (ali K-prosta), če za vsako končno linearno kombinacijo elementov iz S s koeficienti iz kolobarja K velja:*

$$\text{če je } r_{i_1}s_{i_1} + r_{i_2}s_{i_2} + \cdots + r_{i_t}s_{i_t} = 0, \quad \text{je} \quad r_{i_1} = r_{i_2} = \cdots = r_{i_t}.$$

Pri $n = 1$ imamo samo en element $a \in M$. Ta element je linearno neodvisen, če velja $\lambda a = 0$ le za $\lambda = 0$. Ko je $\lambda a = 0$ za nek element $\lambda \neq 0$, je a sam sebi linearno odvisen.

Definicija 4.16. *Množica $S = \{s_i\}_{i\in I}$ elementov K-modula M je baza modula M nad K (ali K-baza), če je linearno neodvisna in množica generatorjev modula M.*

Tako kot pri vektorskih prostorih tudi pri modulih lahko dokažemo naslednjo trditev (glej poglavje o vektorskih prostorih).

Trditev 4.17. *Množica $S = \{s_i\}_{i\in I}$ elementov K-modula M je baza natanko tedaj, ko lahko vsak element $m \in M$ na enoličen način izrazimo kot končno linearno kombinacijo*

$$m = r_{i_1}s_{i_1} + r_{i_2}s_{i_2} + \cdots + r_{i_t}s_{i_t},$$

kjer $r_{i_j} \in K$ in $s_{i_j} \in S$ za vsak $j \in \{1, \ldots, t\}$.

Definicija 4.18. *Naj bo $S = \{s_i\}_{i\in I}$ neskončna podmnožica modula M. Množica S je linearno neodvisna natanko takrat, ko je vsaka njena končna podmnožica linearno neodvisna.*

Žal nima vsak modul baze. Na primer, $\mathbb{Z}_6$ kot $\mathbb{Z}$-modul nima baze. O tem se prepričamo takole. Za vsak element $a \in \mathbb{Z}_6$ velja, da je $6a = 0$ in $6 \neq 0$ v $\mathbb{Z}$. Posledično lahko sklepamo, da nobena podmnožica modula $\mathbb{Z}_6$ ni linearno neodvisna in zato $\mathbb{Z}_6$ nima baze.

Definicija 4.19. *Če K-modul M premore bazo, potem pravimo, da je M prost.*

V modulu, ki sestoji iz $n-$teric $(\xi_1, \xi_2, \ldots, \xi_n)$ elementov kolobarja K z enico $1 \in K$, si oglejmo naslednje $n-$terice

$$e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 1).$$

Ti elementi so med seboj linearno neodvisni. Linearna kombinacija

$$\alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_n e_n$$

je namreč enaka n-terici $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ in ta je enaka nič, če so vse komponente enake 0, $\alpha_1 = \alpha_2 = \ldots = 0$. Vsak element $x = (\xi_1, \xi_2, \ldots, \xi_n)$ iz modula n-teric pa lahko zapišemo v obliki vsote

$$\xi_1 e_1 + \xi_2 e_2 + \ldots + \xi_n e_n.$$

Zato je množica $\{e_1, e_2, \ldots, e_n\}$ baza in to pomeni, da je ta modul n-terice prost.

Zgledi:

(i) Za vsak $n > 0$ je K^n prost K-modul.

(ii) Množica $\mathbb{Z}\times\mathbb{Z}$ je prosti modul nad samim seboj z operacijo množenja po komponentah

$$(n, m)(a, b) = (na, mb)$$

in z bazo {(1,1)}. Podmodul $\mathbb{Z} \times \{0\}$ ni prost modul, ker nima linearno neodvisnih elementov in nima baze.

(iii) Kolobar polinomov $K[X]$ je prost K-modul z bazo $1, X, X^2, \ldots$.

Definicija 4.20. *Če v modulu M obstajata podmodula L in L', ki ustrezata pogojema*

(i) $L \cap L' = \{0\}$,

(ii) $L + L' = M$,

pravimo, da je M direktna vsota modulov L in L' in pišemo

$$M = L \oplus L'.$$

Modul M nad kolobarjem $\mathbb{Z}$ je običajna komutativna grupa. V tem primeru govorimo o direktni vsoti grup L in L'.

Definicija 4.21. *Družina $\{M_i\}_{i\in I}$ podmodulov K- modula M je neodvisna, če za vsak indeks $i \in I$ velja*

$$M_i \cap (\sum_{j\neq i} M_j) = (0).$$

Definicija 4.22. *Naj bo $\{M_i\}_{i\in I}$ družina podmodulov K-modula M. Potem je M (notranja) direktna vsota podmodulov družine $\{M_i\}_{i\in I}$, in zapišemo $M = \oplus_{i\in I} M_i$, če je ta družina neodvisna in generira modul M. Z drugimi besedami M je (notranja) direktna vsota podmodulov iz družine $\{M_i\}_{i\in I}$, če velja:*

(i) $\forall i \in I : M_i \cap (\sum_{j\neq i} M_j) = (0)$,

(ii) $M = \sum_{i\in I} M_i$.

Izkaže se, da sta zgornja pogoja ekvivalnetna naslednjemu:

3.) Vsak element a iz modula M lahko enolično zapišemo kot $a = a_{i_1} + a_{i_2} + \cdots + a_{i_t}$, kjer je $a_{i_j} \in M_{i_j}$, $1 \leq j \leq t$.

V primeru, ko $\{a_i\}_{i\in I}$ tvori K-bazo modula M, je M direktna vsota $M = \oplus_{i\in I} Ra_i$.

Definicija 4.23. *Podmodul L K-modula M je direktni sumand, če obstaja tak podmodul L', da je $M = L \oplus L'$. Modul, ki ne vsebuje netrivialnih direktnih sumandov, se imenuje nerazstavljiv modul.*

Lema 4.24. *Naj bo L podmodul K- modula M. Potem je L direktni sumand modula M, če in samo če obstaja endomorfizem $f : M \to M$ za katerega velja: $f \circ f = f$ in $Im(f) = L$.*

Dokaz. Dokaz v $\Rightarrow$:
Naj bo L podmodul K- modula M direktni sumand. Potem obstaja tak podmodul L', tako da je $M = L \oplus L'$. Preslikava

$$M = L \oplus L' \to L$$
$$m = l + l' \mapsto l$$

je homomorfizem modulov, za katerega velja

$$(f \circ f)(m) = f(f(m)) = f(l) = f(l + 0) = l.$$

Dokaz v $\Leftarrow$:
Naj bo $f : M \to M$ endomorfizem za katerega velja: $f \circ f = f$ in $Im(f) = L$. Vemo, da sta $ker(f)$ in $im(f)$ podmodula modula M. Še več, $M/ker(f) \cong im(f)$ in zato zadostuje pokazati, da je $ker(f) \cap im(f) = \{0\}$. V ta namen vzemimo poljubni element $x \in ker(f) \cap im(f) = \{0\}$. Potem $x \in im(f)$ in zato obstaja tak $y \in M$, da je $f(y) = x$. Ker je po predpostavki $f \circ f = f$, dobimo, da je $(f \circ f)(y) = f(f(y)) = f(y) = f(x) = 0$, saj $x \in ker(f)$. Torej je $y \in ker(f)$ in zato iz $f(y) = x$ sledi, da je $x = 0$. □

Homomorfizem $f : M \to M$ v zgornji lemi imenujemo projekcija modula M na podmodul L.

4.4 Pogoji končnosti

Definicija 4.25. *Naj bo M modul nad komutativnem kolobarjem K z enico $1 \in K$. Ker je K komutativen, ni razlike med desnim in levim K-modulom. Pravimo, da modul M zadošča pogoju naraščujočih verig, če vsaka naraščujoča veriga podmodulov modula M*

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_i \subseteq \cdots$$

vsebuje samo končno mnogo različnih členov. Torej, če obstaja tak indeks t, da je $M_t = M_{t+i}$ za vsak $i \geq t$. Če M zadošča pogoju naraščujočih verig pravimo, da je modul M Noetherianov modul. Kolobar K je levo Noetherianov, ko je K kot levi K-modul Noetherianov in desno Noetherianov, ko je K kot desni K-modul Noetherianov.

Opomba: Če je kolobar K desno Noetherianov, ni nujno, da je tudi levo Noetherianov. Primer takšnega kolobarja je matrika 2×2 nad kolobarjem $\mathbb{Q}$ oblike

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix},$$

kjer je element $a \in \mathbb{Z}$ in elementa $b, c \in \mathbb{Q}$. V nadaljevanju bomo obravnavali samo kolobarje, ki so levo Noetherianovi.

Zgled: Ker so vsi ideali v kolobarju $\mathbb{Z}$ glavni (glej [1]) in za poljubne $a, b \in \mathbb{Z}$ velja, da je $a\mathbb{Z} \subset b\mathbb{Z}$ če in samo če b deli a, se lahko bralec hitro prepriča, da je kolobar $\mathbb{Z}$ modul

nad samim seboj in to Noetherianov modul.

Preden spoznamo Zornovo lemo, poglejmo nekaj definiciji, s katerimi bomo razjasnili pojme, kdaj je relacija antisimetrična, kdaj je množica delno urejena, urejena ali linearno urejena množica, kaj je maksimalen, minimalen, največji element, kaj je zgornja in spodnja meja. Definicije so povzete iz [6].

Definicija 4.26. *Relacija R na množici X je antisimetrična, če za poljubne elemente $x, y \in X$ velja:*

$$\text{če } xRy \text{ in } yRx, \text{ potem je } x = y.$$

Relacija deljivosti na množici naravnih števil je antisimetrična. Če je namreč število a deljivo z b, potem obstaja tako število $k \in \mathbb{N}$, da je $a = bk$. Če je tudi b deljiv z a, potem je $b = ak_1$, za nek $k_1 \in \mathbb{N}$. Iz obeh enakosti sedaj sledi, da je $a = akk_1$, torej $kk_1 = 1$ in zato $k = k_1 = 1$ oziroma $a = b$.

Definicija 4.27. *Relacija R na množici X je tranzitivna, če za poljubne elemente $x, y, z \in X$ velja:*

$$\text{če } xRy \text{ in } yRz, \text{ potem je } xRz.$$

Definicija 4.28. *Relacija R na množici X je refleksivna, če za poljuben element $x \in X$ velja:*

$$xRx.$$

Definicija 4.29. *Relacija R na množici X, ki je refleksivna, antisimetrična in tranzitivna se imenuje relacija delne urejenosti. Delno urejena množica je množica z relacijo delne urejenosti R.*

Če je R relacija delne urejenosti in velja aRb, bomo zapisali

$$a \leqq b.$$

Zapis beremo tako: Element a je pod elementom b in element a je vsebovan v elementu b ali kvečjemu enak b. V delno urejeni množici A je za par elementov a, b relacija $a \leqq b$ lahko izpoljena, lahko pa tudi ni izpoljena. Vedno pa velja naslednje:

- $a \leqq a, \forall a \in A$.
- Iz $a \leqq b$ in $b \leqq a$ sledi $a = b$.
- Iz $a \leqq b$ in $b \leqq c$ sledi $a \leqq c$.

Z znakom $\leqq$ so zapisane lastnosti: refleksivnost, antisimetričnost in tranzitivnost.

Zgled:V množici $\mathbb{N}$ naj pomeni $a \leqq b$, da je število a manjše ali kvečjemu enako b. Potem so naravna števila s to relacijo urejena po velikosti.

Včasih je urejenost taka, da sta poljubna elementa iz množice A primerljiva. Elementa a in b sta primerljiva, če $a \leqq b$ ali pa $b \leqq a$. Če sta elementa a in b primerljiva, tedaj velja za vsak par $a, b \in A$ ena izmed relacij $a \leqq b$ ali $b \leqq a$. V tem primeru pravimo, da je množica A *urejana* ali tudi *linerano urejena množica*.

Zgled: Linearno urejana množica so realna števila, ki so urejena po velikosti.

Definicija 4.30. *Naj bo A delno urejena množica. Element $u \in A$, nad katerim ni nobenega drugega elementa, imenujemo maksimalen element. V tem primeru je relacija $u \leqq a$ izpolnjena le za $a = u$.*

Definicija 4.31. *Naj bo A delno urejena množica. Element $v \in A$ imenujemo minimalni element, če ni pod njim nobenega drugega elementa. Torej velja $a \leqq v$ le, če je $a = v$.*

Maksimalen element moramo ločiti od *največjega elementa*. Element m množice A je največji, če so vsi drugi elementi pod njim, torej če velja $a \leqq m$, za vsak $a \in A$. Če obstaja največji element je obenem maksimalen in je vedno en sam. Maksimalnih elementov pa je lahko več. *Najmanjši element* je tak element, da so vsi drugi elementi iz A nad njim. Naj bo B podmnožica delno urejene množice A. Element $u \in A$, za katerega so vsi elementi podmnožice B pod njim, torej da velja $x \leqq u$ za vsak $x \in B$, se imenuje *zgornja meja* podmnožice B. Podobno je $v \in A$ *spodnja meja* podmnožice B, če so vsi elementi iz podmnožice B nad v. Sedaj, ko smo razjasnili pojme lahko zapišemo Zornovo lemo, podroben dokaz Zornove leme si bralec lahko pogleda v [5].

Lema 4.32. *(Zornova lema) Naj bo množica A delno urejena množica. Če ima v množici A vsaka veriga podmnožic (linearno urejeno zaporedje podmnožic) zgornjo mejo, potem množica A vsebuje maksimalen element.*

Za končne množice Zornova lema očitno velja, pogoj o eksistenci zgornje meje je v tem primeru seveda vedno izpoljnena. Ideal I komutativnega kolobarja K z identiteto je maksimalen ideal, če velja :

$$\forall \text{ ideal } J \subseteq K : I \subseteq J \Rightarrow J = I \text{ ali } J = K$$

Več o maksimalnih idealih si lahko ogledate v [9].

Zgledi:

(i) Za množico celih števil ideal (4) ni maksimalen ideal, saj $(4) \subseteq (2) \neq \mathbb{Z}$.

(ii) Ideal $I = 6\mathbb{Z} = \{6n | n \in \mathbb{Z}\}$ v kolobarju $K = 3\mathbb{Z} = \{3n | n \in \mathbb{Z}\}$ je maksimalen. Dokaz: Naj bo J tak ideal v K, da je $I \subseteq J \subseteq K$. Radi bi pokazali, da je $J = I$ ali $J = K$. Če je $J = I$ smo končali. Torej naj bo $J \neq I$. Potem obstaja nek $a \in K : a \in J$ in $a \neq I$, element $a = 6k+3$, za nek $k \in \mathbb{Z}$. Ker je J ideal v K, velja: $J+J \subseteq J$. Ideal J poleg vseh elementov $6n, n \in \mathbb{Z}$ vsebuje tudi vse elemente $6n + 3$. Ideal $J = 3\mathbb{Z} = K$ iz tega sledi, da je ideal $I = 6\mathbb{Z}$ maksimalen ideal v kolobarju $K = 3\mathbb{Z}$.

Lema 4.33. *Kolobar K z enico $1 \in K$ vsebuje pravi maksimalen ideal.*

Dokaz. Naj bo $\mathcal{F}$ množica vseh idealov J kolobarja K, $J \neq K$. Trdimo, da ima vsaka delno urejena podmnožica množice $\mathcal{F}$ zgornjo mejo. Če je $\{J_i\}_{i \in I}$ del takšnih družin, potem pogledamo $\cup_{i \in I} J_i$. Ker je $J_i \neq R$, za vsak $i \in I, 1 \notin J_i, i \in I$ in $1 \neq \cup_{i \in I} J_i$, torej $\cup_{i \in I} J_i \in \mathcal{F}$. Iz Zornove leme sledi, da $\mathcal{F}$ vsebuje maksimalen element. □

Izrek 4.34. *Naj bo M modul nad komutativnim kolobarjem K z enico $1 \in K$. Če modul M vsebuje dve končni bazi $\mathcal{B}_1 = \{v_1, \ldots, v_m\}$ in $\mathcal{B}_2 = \{w_1, \ldots, w_n\}$ sledi, da je $n = m$.*

Dokaz izreka 4.34 si lahko bralec ogleda v [1].

Definicija 4.35. *Naj bo M prost modul nad komutativnem kolobarjem K z enico $1 \in K$ s končno bazo. Potem število elementov v poljubni bazi modula M imenujemo rang modula M.*

Z uporabo Zornove leme bomo v naslednjem izreku karakterizirali Noetherianove module.

Izrek 4.36. *Naj bo M K-modul. Potem so naslednje trditve ekvivalnetne:*

(i) Vsaka neprazna družina podmodulov modula M vsebuje maksimalen element.

(ii) Vsak podmodul modula M je konočno generiran.

(iii) Modul M je Noetherianov.

Dokaz. $(i) \Longrightarrow (ii)$
Dokaz s protislovjem. Predpostavimo, da obstaja tak podmodul N modula M, ki ni končno generiran in naj bo N_0 maksimalen element v družini

$$\mathcal{F} = \{S \subset M : S \text{ je podmodul modula } N,\ S \text{ je končno generiran}\}.$$

Potem je N_0 končno generiran. Naj bo $\{n_1, \ldots, n_t\}$ končna množica generatorjev maksimalnega elementa N_0. Ker podmodul N ni končno generiran, velja $N_0 \neq N$. Torej obstaja element $x \in (N \setminus N_0)$. Naj bo $N_1 = N_0 + Kx$ podmodul modula N generiran z N_0 in elementom x. Potem se lahko hitro prepričamo, da je množica $\{n_1, \ldots, n_t, x\}$ generator modula N_1 in $N_1 \in \mathcal{F}$. Vendar $N_0 \subset N_1$ in $N_1 \neq N_o$. Po predpostavki pa je N_0 maksimalen element in s tem pridemo do protislovja.

$(ii) \Longrightarrow (iii)$
Naj bo

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_i \subseteq \cdots$$

naraščujoča veriga podmodulov modula M. Potem se lahko bralec prepriča sam, da je $N = \bigcup_1^\infty M_i$ podmodul modula M in ker velja (ii) je N končno generiran. Naj bo $\{n_1, \ldots, n_t\}$ končna množica generatorjev podmodula N. Potem vsak od teh elementov pripada nekemu podmodulu zgornje verige, recimo, da $n_i \in M_{ij}, 1 \leq i \leq t$. Če vzamemo, da je $k = max\{i_1, \ldots i_t\}$ je $n_i \in M_k$ za vsak i, $1 \leq i \leq t$. Iz tega sledi, da je $N \subset M_k$. Ker je $M_i \subset M_k$, za vsak i, iz tega sledi, da je $M_k = M_i$, če je $i \geq k$. Torej ima veriga končno mnogo različnih elementov.
$(iii) \Longrightarrow (i)$

Na bo $\mathcal{F}$ zbirka podmodulov modula M. Uporabimo Zornovo lemo za $\mathcal{F}$. Ker je M Noetherianov zadostuje pogoju naraščujočih verig, torej ima vsaka urejena družina podmodulov zbirke $\mathcal{F}$ zgornjo mejo. Po Zornovi lemi $\mathcal{F}$ vsebuje maksimalen element. □

Definicija 4.37. *Pravimo, da K-modul M zadostuje pogoju padajočih verig, če se vsaka veriga podmodula modula M:*

$$M_1 \supseteq M_2 \supseteq \cdots \supseteq M_i \supseteq \cdots$$

konča, to je natanko takrat, ko obstaja tak indeks t, tako da je $M_t = M_{t+i}$, za vsako pozitivno število i. Če podmoduli modula M zadoščajo pogoju padajočih verig, pravimo modulu M Artinianov modul. Kolobar K se imenuje levi Artinian kolobar, če je K kot levi K-modul Artinianov in desno Artinianov, če je K kot desni K-modul Artinianov.

Če je kolobar levo Artinianov ni nujno da je tudi desno Artinianov. Ko govorimo, da je kolobar Artinianov mislimo, da je kolobar levo Artinianov.

Izrek 4.38. *Naj bo M K-modul. Naslednji trditvi sta si ekvivalentni:*

(i.) Vsaka neprazna družina podmodulov modula M vsebuje minimalen element.

(ii.) Modul M je Artinianov.

Dokaz izreka 4.38 si lahko bralec ogleda v [11] na strani 59.

Izrek 4.39. *Naj bo N podmodul K-modula M. Potem je modul M Noetherianov (Artinianov) če in samo če sta N in M/N oba Noetherianova (Artinianova).*

Dokaz. Recimo, da sta oba N in M/N Noetherianova in naj bo

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_i \subseteq \cdots$$

naraščujoča veriga podmodulov modula M. Oglejmo si sledeči verigi:

$$(M_1 \cap N) \subset (M_2 \cap N) \subset \cdots \subset (M_i \cap N) \subset \cdots$$

$$\frac{M_1 + N}{N} \subset \frac{M_2 + N}{N} \subset \cdots \subset \frac{M_i + N}{N} \subset \cdots$$

Ker sta N in M/N Noetherianova se obe verigi končata. Zato lahko določimo pozitivno celo število k tako, da velja:

$$M_i \cap N = M_k \cap N$$

$$M_i + N = M_k + N$$

za vsako pozitivno število $i \geq k$. Vemo, da $M_k \subset M_i$, za $i \geq k$, pokazati pa želimo še, da je $M_k \supset M_i$. Za element $x \in M_i$ nam druga enakost zgoraj pove, da obstaja tak element $y \in M_k$, da je $x + N = y + N$, torej, da je $x - y \in N$. Ker je $M_k \subset M_i$ vidimo, da je $x - y \in M_i \cap N = M_k \cap N$. Torej $x - y \in M_k$ in zato tudi element $x \in M_k$, kot smo želeli dokazati. Posledično je $M_k = M_i$, za vsak $i \geq k$ in veriga se zaključi. Dokaz v nasprotno smer, gre na podoben način kot tudi dokaz v primeru, ko sta N in M/N Artinianova. Dokaz si lahko bralec ogleda v [11] na straneh 60-61. □

Posledica 4.40. *Naj bo $\{M_i\}_{1 \leq i \leq n}$ taka družina podmodulov K-modula M, da je $M = \sum_{i=1}^{n} M_i$. Potem je modul M Noetherianov (Artinianov), če in samo če je vsak podomodul M_i Noetherianov (Artinianov).*

Trditev 4.41. *Končno generiran modul M nad kolobarjem K, ki je Noetherianov (Artinianov) je Noetherianov (Artinianov).*

Dokaz. Naj bo $\{m_1, \dots m_t\}$ končna množica generatorjev modula M nad kolobarjem K. Potem je $M = \sum_{i=1}^{t} Km_i$. Preslikave $f_i : K \to Km_i$ so epimorfizmi, zato je vsak modul Km_i izomorfen kolobarju K in posledično Neoetherianov (Artinianov), $1 \leq i \leq t$. Rezultat tedaj sledi iz posledice (4.40). □

Naj bo M K-modul. Potem M vedno vsebuje verigo podmodulov: $M \supset (0)$. Če je modul M enostaven, torej brez neničelnih pravih podmodulov, je to edina veriga. V nasprotnem primeru, če modul M ni enostaven, pa vsebuje pravi podmodul N in je $M \supset N \supset (0)$ veriga podmodulov v modulu M. Naslednja definicija je posložitev koncepta kompozicijskih vrst s teorije grup [1].

Definicija 4.42. *Veriga podmodulov K-modula M*

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = (0)$$

se imenuje kompozicijska vrsta modula M, če so vsi moduli M_i/M_{i+1} enostavni. Module M_i/M_{i+1} imenujemo faktorji vrste. Število faktorjev vrste imenujemo dolžina vrste. Modulu, ki ima kompozicijsko vrsto pravimo modul končne dolžine.

Prvo si bomo pogledali pogoje za obstoj kompozicijske vrste.

Izrek 4.43. *K-modul M je končne dolžine, če in samo če je Artinianov in Noetherianov.*

Dokaz. Najprej predpostavimo, da je modul M Artinianov in Noetherianov, ker je Noetherianov, družina vseh pravih podmodulov modula M vsebuje maksimalen element M_1. Če je $M_1 \neq 0$ nam, ker je Noetherianov, podoben argument pove, da M_1 vsebuje maksimalen podmodul M_2. S ponavljanjem tega procesa lahko določimo verigo podmodulov:

$$M = M_0 \supset M_1 \supset M_2 \supset \cdots$$

Ker je modul M tudi Artinianov se more veriga zaključiti, torej je $M_n = (0)$ za neko pozitivno celo število n. Potem pa je

$$M = M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_n = (0)$$

kompozicijska vrsta modula M.

Sedaj predpostavimo, da modul M ima kompozicijsko vrsto. Dokaz nadaljujemo z indukcijo glede na dolžino n kompozicijske vrste minimalne dolžine modula M. Če je $n = 1$ potem je modul M enostaven in tako Artinianov in Noetherianov. Predpostavimo sedaj, da je

$$M = M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_n = (0)$$

kompozijska veriga minimalne dolžine modula M. V tem primeru rezultat drži za module z vrsto dolžine $n - 1$. Ker je $M_1 \supset \cdots \supset M_n = (0)$ kompozicijska veriga modula M_1, iz indukcijske predpostavke sledi, da je M_1 tako Artinianov kot Noetherianov. Prav tako, ker je M/M_1 enostaven, je Artinianov in Neotherianov, in posledično po izreku 4.39 je tudi modul M tako Artinianov kot Noetherianov. □

Sedaj predpostavimo, da ima modul M dve ali več kompozicijskih vrst in jih primerjamo med seboj.

Definicija 4.44. *Kompozicijski vrsti*

$$M = M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_n = (0)$$

$$M = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_t = (0)$$

se imenujeta ekvivalentni, če sta enakih dolžin in če obstaja taka bijekcija med faktorji vrst, da so pripadajoči faktorji izomorfni.

Naslednji izrek je posplošitev Jordan-Hölderjevega izreka s teorijo grup. Več o Jordan-Hölderjevem izreku bralec lahko izve v [4].

Izrek 4.45. *(Jordan-Hölder) Dve kompozicijski vrsti K-modula M sta vedno ekivalentni.*

Lema 4.46. *Naj bo L podmodul K-modula M. Potem je modul M končne dolžine, če in samo če sta L in $N = M/L$ končne dolžine. V tem primeru velja:*

$$l(M) = l(L) + l(N).$$

Dokaz. Prva trditev je direktna posledica izreka 4.42 in izreka 4.46 Naj bosta

$$L = L_0 \supset L_1 \supset \cdots \supset L_t = (0)$$

in

$$N = N_0 \supset N_1 \supset \cdots \supset N_r = (0)$$

kompozicijski vrsti za L oziroma N. Ker je $N = M/L$, lahko poiščemo tako zaporedje podmodulov

$$M = M_0 \supset M_1 \supset \cdots \supset M_r = L,$$

da je $M_i/L \simeq N_i$, $1 \leq i \leq r$ in ker velja

$$\frac{M_{i-1}}{M_i} \simeq \frac{M_{i-1}/L}{M_i/L} \simeq \frac{N_{i-1}}{N_i},$$

dobimo, da je vsak podmodul M_i maksimalen v M_{i-1}, $1 \leq i \leq r$. Torej je

$$M = M_0 \supset M_1 \supset \cdots \supset M_r = L_0 \supset L_1 \supset \cdots \supset L_t = (0)$$

kompozicijska vrsta modula M. Zato je $l(M) = r + t$, kar je željen rezultat. □

Poglavje 5

Zaključek

Tekom projektne naloge smo ugotovili, da so moduli nad kolobarjem posplošitev koncepta vektorskih prostor. Medtem ko v vektorskem prostoru skalarji pripadajo nekemu polju, v modulu skalarji pripadajo kolobarju. Teorija modulov obsega veliko lastnosti vektorskih prostorov. Prav tako smo spoznali, da so moduli zelo tesno povezani s teorijo grup. Teorija modulov je obsežna. Namen projektne naloge je bil preučiti lastnosti modulov nad kolobarjem s posebnih poudarkom na posebnih družinah modulov, kot so ciklični moduli, prosti moduli. Veliko več o modulih si lahko bralec ogleda v [7]. Na začetku knjige si lahko bralec pogleda več o prostih modulih, projektivnih modulih. O tenzorskem produktu modulov pa več v [6] in [8].

Literatura

[1] C. P. Milies, S. K. Sehgal, An Introduction to Group Rings, Springer (2002).

[2] R. B. Ash, Abstract Algebra: The Basic Graduate Year, Dover Publications (2006).

[3] J. M. Howie, Fields and Galois Theory, Springer (2006).

[4] J. J. Rotman, Advanced modern Algebra, American Mathematical Society (2010).

[5] R. B. Ash, A primer of abstract mathematics Cambridge University Press (1998).

[6] I. Vidav, Algebra, DMFA- Založništvo, Ljubljana (2003).

[7] J. Dauns, Modules and rings, Cambridge University Press (1994).

[8] K. R. Goodearl, R. B. Warfield, An introduction to noncommutative Noetherian rings, Cambridge University Press (2004).

[9] J. Hefferon, Linear Algebra, Virginia Commonwealth University Mathematics (2009).

[10] F.W. Anderson, C.R. Fuller, Graduate texts in Mathematics, Springer (1992).

[11] M. Hazewinkel, N. M.Gubareni, N. Gubareni, V. V. Kirichenko, Algebras, Rings and Modules, Kluwer Academic Publishers (2004).