

# Algebra 3

Hugo Trebše ([hugo.trebse@gmail.com](mailto:hugo.trebse@gmail.com))

12. november 2025

Which should I learn, analysis or  
algebra?

Do you want to be deaf or blind?

---

*Michael Atiyah*

# Kazalo

<b>I</b>	<b>Komutativni kolobarji</b>	<b>3</b>
1	Deljivost v komutativnih kolobarjih	3
2	Glavni kolobarji	4
3	Enolična faktorizacija	6
<b>II</b>	<b>Moduli</b>	<b>8</b>
4	Uvod v module	8
5	Osnovni pojmi teorije modulov	11
5.1	Podmoduli . . . . .	11
5.2	Homomorfizmi modulov . . . . .	11
5.3	Kolobarji endomorfizmov . . . . .	13
5.4	Kvocietni moduli . . . . .	14
5.5	Direktne vsote modulov . . . . .	15
5.6	Generatorji modulov . . . . .	16
6	Prosti moduli	17
7	Eksaktna zaporedja	20
7.1	Projektivni moduli . . . . .	23
8	Tenzorski produkt modulov	25
8.1	Linearne preslikave nad tenzorskim produktom . . . . .	28

## Del I

# Komutativni kolobarji

## 1 Deljivost v komutativnih kolobarjih

**Definicija 1.1.** Naj bo  $K$  komutativen kolobar.

- Element  $b \neq 0$  *deli* element  $a \in K$ , če obstaja  $q \in K$ , da je  $a = bq$ .
- Neničelna elementa  $a, b \in K$  sta *asociirana*, če  $a \mid b$  in  $b \mid a$ . Ekvivalentno obstaja enota  $u$ , da je  $a = ub$ .
- *Največji skupni delitelj* elementov  $a, b$ , ki nista ničelna, je tak element  $d$ , da velja

$$\dagger \quad d \mid a \text{ in } d \mid b.$$

$$\dagger \quad c \mid a \text{ in } c \mid b \implies c \mid d.$$

- Element  $p$  je *nerazcepen*, če je neničelen ter neobrnljiv ter  $p = ab \implies a$  ali  $b$  obrnljiv.

**Definicija 1.2.** Kolobar je *cel*, če je komutativen in

$$xy = 0 \implies x = 0 \vee y = 0.$$

**Definicija 1.3.**

- Element celega kolobarja je *nerazcepen*, če ni enota ter ni produkt elementov, ki niso enote.
- Element  $p$  komutativnega kolobarja  $K$  je *praelement*, če je  $K/pK$  cel kolobar, oziroma iz  $ab \in pK$  sledi  $a \in pK$  ali  $b \in pK$ .

### Komentar 1.4

V celih kolobarjih je vsak praelement nerazcepen, kar preverimo z lahkoto. Ni pa vsak nerazcepen element praelement, vsaj ne v celih kolobarjih.

Implikacija  $\text{nerazcepen} \implies \text{praelement}$  je pravilna v celih kolobarjih, v katerih imata vsaka dva elementa največji skupni delitelj. Slednje gotovo velja v vseh celih kolobarjih z enolično faktorizacijo.

Od sedaj naprej so vsi kolobarji celi in komutativni.

**Trditev 1.5.** *Neničelna elementa sta asociirana natanko tedaj, ko se razlikujeta smao za obrnljiv faktor.*

*Dokaz.* Očitno. □

## 2 Glavni kolobarji

**Definicija 2.1.**

- $I \subseteq K$  je *ideal* ( $I \trianglelefteq K$ ), če je  $I$  aditivna podgrupa  $K$  ter velja

$$IK, KI \subseteq I.$$

- Za  $a \in K$  je  $\langle a \rangle = \{ax | x \in K\}$  *glavni ideal* generiran z  $a$ .

**Trditev 2.2.**

- $b \mid a \iff \langle a \rangle \subseteq \langle b \rangle$ .
- $a$  in  $b$  asociirana  $\iff \langle a \rangle = \langle b \rangle$ .
- $\langle a \rangle = K \iff a$  obrnljiv.

*Dokaz.* Očitno. □

**Definicija 2.3.** Ideal je *končno generiran*, če je generiran s končno mnogo elementi. Opazimo

$$\langle a_1, \dots, a_n \rangle = \langle a_1 \rangle + \dots + \langle a_n \rangle = \{a_1x_1 + \dots + a_nx_n \mid x_i \in K\}.$$

**Primer 2.4.**

- Edini ideali  $Z$  so  $nZ$ , saj je  $Z$  evklidski.
- Naj bo  $I$  množica polinomov s sodim konstantnim členom.  $I = \langle 2, X \rangle \trianglelefteq \mathbb{Z}[X]$ , a  $I$  ni glavni.

**Definicija 2.5.**

- Cel kolobar je *glavni*, če je vsak njegov ideal glavni.
- Cel kolobar  $K$  je *evklidski*, če obstaja funkcija  $\delta : K \setminus \{0\} \rightarrow \mathbb{N}_0$ , za katero velja
  - †  $\forall a, b \in K, b \neq 0$  obstajata  $q, r \in K$ , da je  $a = qb + r$  ter je  $r = 0$  ali  $\delta(r) < \delta(b)$ .
  - †  $\delta(a) \leq \delta(ab) \forall a, b \in K \setminus \{0\}$ .
- 

**Primer 2.6 (Primeri evklidskih kolobarjev).**

- $\mathbb{Z}$
- $\mathbb{F}[X]$ , kjer je  $\mathbb{F}$  polje.
- $\mathbb{Z}[i]$

### Izrek 2.7

Vsak evklidski kolobar je glavni kolobar.

*Dokaz.* Razen v trivialnem primeru kolobar vsebuje neničelen element, ki ima najmanjšo evklidsko valuacijo izmed vseh elementov ideala. Če ta element ni generator celotnega ideala lahko delimo ter najdemo element z manjšo evklidsko valuacijo.  $\square$

**Izrek 2.8.** *Naj sta  $a$  in  $b$  elementa glavnega kolobarja  $K$ , ter nista oba ničelna. Potem njin največji skupni delitelj  $d$  obstaja, ter je oblike  $d = ax + by$  za  $x, y \in K$ .*

*Dokaz.* Ideal  $\langle a, b \rangle$  je glavni, zato ima generator  $d$ .  $d$  je najmanjši skupni delitelj, saj zelo lahko preverimo, da je vsak drug delitelj elementov tudi v idealu. Oblika  $d$  je tedaj očitna.  $\square$

**Izrek 2.9.** *Naj bo  $p \neq 0$  element glavnega kolobarja. Naslednji pogoji so ekvivalentni:*

- $p$  je nerazcepen.
- $\langle p \rangle$  je maksimalni ideal.
- $K/\langle p \rangle$  je polje.

*Dokaz.* Drugi in tretji pogoj sta ekvivalentna iz Algebre 2. Ekvivalenco med prvim in drugim pogojem preverimo z lahkoto.  $\square$

### 3 Enolična faktorizacija

**Lema 3.1.** Naj bo  $K$  cel kolobar. Denimo, da element  $a \in K$  ni produkt nerazcepnih elementov, je neničelen ter neobrnljiv. Potem  $K$  vsebuje zaporedje elementov  $a_1 = a, a_2, a_3, \dots$ , da velja

$$\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \langle a_3 \rangle \subsetneq \dots$$

*Dokaz.* Iz  $a$  odstranjujemo nerazcepne elemente, ki jih nikoli ne zmanjka, saj bi v nasprotnem primeru  $a$  bil produkt nerazcepnih elementov.  $\square$

#### Definicija 3.2

Komutativen kolobar  $K$  je *Noetherski*, če vsaka naraščajoča veriga idealov terminira.

**Trditev 3.3.** Vsak glavni kolobar je noetherski kolobar.

*Dokaz.* Naj bo  $I_1 \subseteq I_2 \subseteq \dots$  nestrogo naraščajoča veriga. Sledimo definicijam ter preverimo, da je  $I = \bigcup_{n \in \mathbb{N}} I_n$  ideal. Ker je kolobar glavni je  $I$  generiran z nekim elementom, na katerim lahko uporabimo zgornjo lemo.  $\square$

**Komentar 1.** Zgornji trditvi implicirata, da je v glavnem kolobarju vsak element produkt nerazcepnih elementov.

#### Izrek 3.4: Hilbertov izrek o bazi

Če je  $K$  Noetherski kolobar je  $K[X]$  Noetherski kolobar.

*Dokaz.* Izpustimo, čeprav ni zahteven.  $\square$

**Lema 3.5.** V celih kolobarjih je vsak praelement nerazcepen. V glavnih kolobarjih velja obrat.

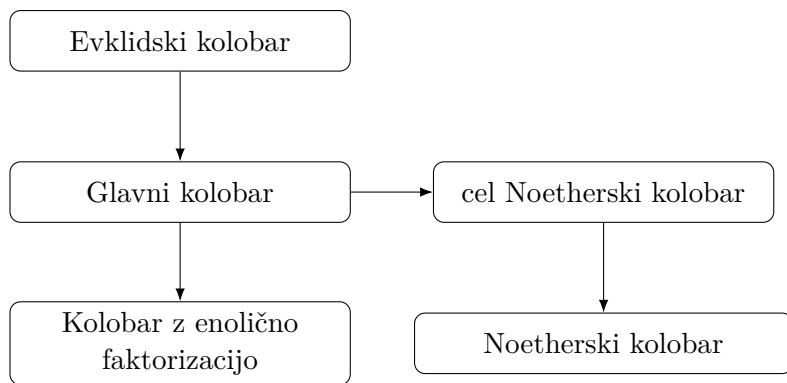
*Dokaz.* Očitno.  $\square$

#### Definicija 3.6

Cel kolobar  $K$  imenujemo kolobar z enolično faktorizacijo (UFD), če za vsak neničelni neobrnljiv element  $a$  obstajajo nerazcepni elementi, katerih produkt je  $a$ , ter je taka faktorizacija enolična do asociiranosti in vrstnega reda faktorjev natančno.

**Trditev 3.7.** Vsak glavni kolobar je kolobar z enolično faktorizacijo.

*Dokaz.* Vemo, da ima vsak neničelen neobrnljiv element v celim kolobarju nerazcepne elemente, ki ga delijo. Teh je končno, saj je vsak glavni kolobar Noetherski. Enoličnost razcepa pokažemo upoštevajoč sovpadanje praelementov in nerazcepnih elementov, ki velja v glavnih kolobarjih.  $\square$



**Hilbertov izrek:** če je  $K$  Noetherski, je tudi  $K[X]$  Noetherski.

Vsi kolobarji v glavni (navpični) verigi so po definiciji *celi kolobarji*.

## Del II

# Moduli

## 4 Uvod v module

Od sedaj dalje kolobarji niso več nujno komutativni.

**Motivacija:** Pojem modula nad kolobarjem je naravna nadgraditev pojma delovanja grupe na množici.

Cayleyjev izrek nam pove, da je vsaka grupa pravzaprav podgrupa simetrične grupe, ter si jo lahko konkretno predstavljamo kot množico permutacij. Sedaj bomo pokazali, da si lahko tudi kolobarje predstavljamo bolj konkretno.

### Izrek 4.1

Naj bo  $M$  aditivna grupa ter  $\text{End}(M)$  množica vseh endomorfizmov grupe  $M$ .  $\text{End}(M)$  je kolobar, če vpeljemo seštevanje na naraven način ter množenje kot kompozicijo.

**Izrek 4.2.** Vsak kolobar lahko vložimo v kolobar endomorfizmov neke aditivne grupe.

*Dokaz.* Naj bo  $K$  kolobar. Tvorimo preslikavo  $\ell_a : x \mapsto ax$ . Očitno je  $\ell_a$  aditivna. Sledi, da je  $\ell_a$  endomorfizem aditivne grupe  $K$ . Tako je  $\varphi : K \rightarrow \text{End}(K)$  definirana z  $\varphi(x) = \ell_x$ . Ostane še vprašanje multiplikativnosti  $\varphi$ , kar je očitno. Da ohranja enoto je prav tako očitno.

Trivialnost jedra vložitve sledi, saj je

$$a \in \ker(\varphi) \iff \ell_a = 0 \implies \ell_a(1) = a \cdot 1 = 0.$$

□

Na filozofskem nivoju smo sedaj pokazali, da si lahko elemente kolobarjev predstavljamo kot aditivne funkcije, podobno kot si lahko elemente grupe predstavljamo kot permutacije.

Na podoben način izpeljemo naslednji izrek.

**Izrek 4.3.** Vsako algebro nad poljem  $\mathbb{F}$  lahko vložimo v algebro endomorfizmov nekega vektorskega prostora nad  $\mathbb{F}$ .

Filozofsko sledi, da si elemente algebre pravzaprav lahko predstavljamo kot linearne preslikave.

V primeru končnodimenzionalnih algeber sledi, da lahko  $A$  vložimo v algebro matrik nad poljem.

$$A \hookrightarrow \text{End}_{\mathbb{F}}(A) \cong M_n(\mathbb{F})$$

Tako sledi, da si lahko elemente algebre predstavljamo kot matrike.

#### Naloga 4.4

Naj bo  $A$  končnodimenzionalna algebra nad poljem  $\mathbb{F}$ . Ali lahko  $A$  vsebuje elementa  $s, t$ , da je

$$st - ts = 1.$$

*Rešitev.* Odgovor je ne v poljih s karakteristiko 0, saj lahko elementa zapišemo kot matriki, nakar dobimo  $0 = n$ . V poljih s praštevilsko karakteristiko obstajajo primeri matrik, ki zadostijo pogoju naloge.  $\square$

**Nauk:** Komutator matrik  $\implies$  sled.

#### Definicija 4.5: Modul

Naj bo  $K$  kolobar. Množica  $M$  skupaj z zunanjo binarno operacijo  $(a, u) \mapsto au$  med množicama  $K \times M \rightarrow M$  in notranjo binarno operacijo  $(u, v) \mapsto u + v$  je *modul nad kolobarjem*  $K$  ali  *$K$ -modul*, če je

- $(M, +)$  je Abelova grupa.
- $(a + b)u = au + bu \quad \forall a, b \in K, \forall u \in M$ .
- $a(u + v) = au + av \quad \forall a \in K, \forall u, v \in M$ .
- $(ab)u = a(bu) \quad \forall a, b \in K, \forall u \in M$ .
- $1u = u \quad \forall u \in M$ .

Operaciji  $(a, u) \rightarrow au$  pravimo množenje s skalarji.

Po domače je modul vektorski prostor nad kolobarjem. To seveda ni popolnoma natančno, saj izgubimo možnost krajšanja skalarjev.

Opomnimo, da smo definirali levi modul nad kolobarjem, s skalarjem množimo namreč z leve.

Pojem delovanja grupe na množici je ekvivalenten pojmu homomorfizma iz grupe v simetrično grupo. Podobno je pojem  $K$ -modula ekvivalenten pojmu homomorfizma kolobarjev iz  $K$  v  $\text{End}(M)$ . Za  $K$ -modul  $M$  je  $\varphi : K \rightarrow \text{End}(M)$  definiran z  $\varphi(a)(u) = \ell_a(u) = au$  ustrezen homomorfizem. Obratno za homomorfizem  $\varphi$ , ki slika iz  $K$  v  $\text{End}(M)$ , definiramo množenje s skalarjem preko  $a \cdot u = \varphi(a)(u)$ , po čem dobimo modul.

#### Primer 4.6 (Primeri modulov).

- Če je  $K = \mathbb{F}$  je  $\mathbb{F}$ -modul vektorski prostor nad  $\mathbb{F}$ .
- Pojem  $\mathbb{Z}$ -modula sovpada s pojmom aditivne grupe.
- Vsak kolobar  $K$  postane  $K$ -modul, če definiramo produkt v modulu kot običajni produkt elementov v  $K$ .
- Naj bo  $I$  levi ideal kolobarja  $K$ .  $I$  je  $K$ -modul, če definiramo modulsko množenje kot množenje elementov v kolobarju.

- Naj bo  $K \leq K'$ .  $K'$  je  $K$ -modul, če definiramo modulsko množenje kot množenje v  $K'$ .
- $K = M_n(\mathbb{F})$  ter  $M = \mathbb{F}^n$ .  $M$  postane  $K$ -modul z običajnim množenjem matrike z vektorjem.
- Trivialni modul je  $\{0\}$ .

## 5 Osnovni pojmi teorije modulov

### 5.1 Podmoduli

**Definicija 5.1.** *Podmodul* je podmnožica modula, ki je za isti operaciji sama modul. Ekvivalentno je  $N \subseteq M$  podmodul modula  $M$ , če je:

- $N \leq M$  kot aditivna grupa ( $u, v \in N \implies u - v \in N$ )
- $KN \subseteq N$ , kar zagotovi zaprtost za množenje.

**Primer 5.2.**

- V primeru vektorskih prostorov kot modulov so podmoduli podprostori.
- Podmodul  $\mathbb{Z}$ -modula je podgrupa za seštevanje.
- Podmodul  $K$ -modula  $K$  je levi ideal kolobarja  $K$ .

**Trditev 5.3.**

- Če sta  $N_1$  in  $N_2$  podmodula je  $N_1 \cap N_2$  prav tako podmodul.
- Vsota podmodulov je prav tako podmodul.

**Definicija 5.4.** Lahko se zgodi, da ima modul samo dva podmodula, namreč modul sam ter trivialni modul  $\{0\}$ . Če sta to tudi edina podmodula in  $M$  ni trivialni modul je  $M$  enostaven modul.

**Primer 5.5.**

- Vektorski prostor je enostaven kot modul natanko tedaj, ko je enorazsežen.
- Aditivna grupa je enostavna kot  $\mathbb{Z}$ -modul natanko tedaj ko je izomorfna  $\mathbb{Z}_p$ .
- $K = M_n(\mathbb{F})$  ter  $M = \mathbb{F}^n$ . Za  $N \subseteq \mathbb{F}^n$  je lahko  $N = \{0\}$ , v nasprotnem primeru pa je seveda  $N = M$ , saj fiksni neničelni vektor množimo s poljubno matriko in lahko dobimo poljuben vektor iz  $\mathbb{F}^n$  po Frobenius-Cappelijevem izreku o rešitvah linearnih enačb.

### 5.2 Homomorfizmi modulov

**Definicija 5.6.** Naj sta  $M$  in  $N$  modula nad kolobarjem  $K$ .  $\varphi : M \rightarrow N$  je homomorfizem  $K$ -modulov, če velja

$$\varphi(au + bv) = a\varphi(u) + b\varphi(v) \quad \forall a, b \in K, \forall u, v \in M$$

Pravimo jim tudi  $K$ -linearne preslikave.

**Definicija 5.7.**

- $\ker \varphi = \{u \in M \mid \varphi(u) = 0\}$
- $\operatorname{im} \varphi = \{\varphi(u) \mid u \in M\}$

sta zaporedoma podmodula  $M$  in  $N$ .

**Trditev 5.8.**

- $\ker \varphi = \{0\} \iff \varphi$  *injektiven*.
- $M \cong N$ , če obstaja izomorfizem med njima.

**Primer 5.9 (Homomorfizmi modulov).**

- Naj bo kolobar  $K$  polje. Tedaj so homomorfizmi modulov nad  $K$  linearne preslikave.
- Če je  $K = \mathbb{Z}$  so homomorfizmi modulov aditivne preslikave oz. homomorfizmi aditivnih grup.
- Naj bo  $I \trianglelefteq K$  levi ideal ter  $u_0 \in I$ .  $\varphi : I \rightarrow I$  s predpisom  $\varphi(u) = u \cdot u_0$ . Aditivnost je posledica distributivnosti, homogenost pa je zagotovljena, saj smo definirali desno množenje. V primeru levega množenja homogenost ne bi bila izpolnjena, saj je

$$\varphi(au) = (au)u_0 = a\varphi(u).$$

### 5.3 Kolobarji endomorfizmov

V primeru vektorskega prostora  $V$  je  $\text{End}_{\mathbb{F}}(V)$  kolobar (celo algebra).

**Definicija 5.10.** Množica endomorfizmov  $K$ -modula  $M$   $\text{End}_K(M)$  postane kolobar, če definiramo seštevanje po točkah ter množenje kot komponiranje.

**Komentar 2.** Če bi v zgornji definiciji definirali množenje kot množenje po točkah bi naredili napako, saj bi homogenost tedaj velela

$$(\varphi \cdot \psi)(au) = a\varphi(u) \cdot a\psi(u) \neq a\varphi(u)\psi(u).$$

Podobno bi zmotno trdili, da je  $\text{End}_K(M)$  algebra nad  $K$ , saj če bi definirali

$$(a\varphi)(u) = a\varphi(u) \implies (a\varphi)(bu) = ab\varphi(u) \neq ba\varphi(u) = b \cdot (a\varphi)(u).$$

V primeru komutativnosti  $K$  pa bi zgornja trditev veljala.

#### Lema 5.11: Schur

Če je  $M$  enostaven  $K$ -modul je  $\text{End}_K(M)$  obseg.

*Dokaz.* Slika ter jedro sta podmodula. □

## 5.4 Kvocientni moduli

### Definicija 5.12

Naj bo  $M$   $K$ -modul ter  $N \leq M$  podmodul. Na množici

$$M/N = \{u + N \mid u \in M\}$$

definiramo seštevanje ter množenje s skalarji kot

- $(u + N) + (v + N) = (u + v) + N$
- $a(u + N) = au + N$

Z definiranimi operacijama postane  $M/N$   $K$ -modul, ki ga imenujemo *kvocientni modul*.

Opazimo, da za razliko od grup ter kolobarjev ne zahtevamo nobene posebne lastnosti od  $N$ , kot so na primer podgrupe edinke ali ideali.

### Primer 5.13.

- Če je  $K = \mathbb{F}$  so kvocientni moduli kvocientni vektorski prostori.
- Če je  $K = \mathbb{Z}$  so kvocientni moduli kvocientne grupe (normalnost podgrupe je zagotovljena zaradi komutativnosti).
- Naj bo  $I \trianglelefteq K$  levi ideal. Tokrat na množici odsekov ne definiramo operacij enako kot pri kvocientnem kolobarju (tedaj med drugim potrebujemo tudi dvostranskost ideala), seštevanje je enako, množenje s elementi iz  $K$  (skalarno množenje) pa definiramo kot  $a(b + I) = ab + I$ .

### Izrek 5.14: O izomorfizmu

Naj bo  $\varphi : M \rightarrow N$  homomorfizem modulov. Tedaj je

$$M/\ker \varphi \cong \operatorname{im} \varphi$$

*Dokaz.* Dokaz je standarden. □

## 5.5 Direktne vsote modulov

**Definicija 5.15.** Naj so  $M_1, \dots, M_s$   $K$ -moduli. Množica

$$M_1 \times \dots \times M_s$$

postane  $K$  modul s seštevanjem po komponentah in množenje s skalarji, ki je homogeno v vseh komponentah.

Temu modulu pravimo *direktna vsota* modulov  $M_1, \dots, M_s$  ter pišemo

$$M_1 \oplus \dots \oplus M_s.$$

Natančneje zgornji konstrukciji pravimo zunanja direktna vsota.

**Definicija 5.16.** Naj bo  $M$  modul in  $N_1, \dots, N_s$  njegovi podmoduli. Pravimo, da je  $M$  *notranja direktna vsota* modulov  $N_i$ , če

•

$$M = N_1 + \dots + N_s$$

•

$$N_i \cap \sum_{j \neq i} N_j = \{0\}$$

Omenimo, da drugo točko ekvivalentno zapišemo, kot linearno neodvisnost elementov  $N_i$ :

$$\sum_{i=1}^s v_i = 0 \implies \forall i \ v_i = 0.$$

**Komentar 3.** Zunanje in notranje direktne vsote so pravzaprav skoraj enake, saj če je  $M$  notranja direktna vsota  $N_i$ , potem je  $M \cong \oplus_{i=1}^s N_i$ . Podobno so  $\{(0, 0, \dots, v_i, \dots, 0) | v_i \in M_i\}$  podmoduli modula  $\oplus_{i=1}^s M_i$ , ki seveda izpolnjujejo oba pogoja notranje direktne vsote. Sledi, da je vsaka zunanja vsota tudi notranja vsota.

**Definicija 5.17.** Naj bo  $N$  podmodul  $M$ . Pravimo, da je  $N$  *direktni sumand*  $M$ , če obstaja  $N' \leq M$ , da je

$$M = N \oplus N'.$$

**Primer 5.18.**

- Če je  $K = \mathbb{F}$  so vsi podprostorji vektorskega prostora direktni sumandi.
- Če je  $K = \mathbb{Z}$  sta direktna sumanda le cel modul ter trivialni modul.

## 5.6 Generatorji modulov

**Definicija 5.19.** Naj bo  $M$   $K$ -modul in  $u \in M$ .  $Ku = \{au | a \in K\}$  je najmanjši modul  $M$ , ki vsebuje  $u$ . Pravimo, da je  $Ku$  generiran z  $u$ .

**Definicija 5.20.** Podmodul generiran z enim samim elementom se imenuje *ciklični podmodul*.

**Trditev 5.21.** Vsak enostaven modul je cikličen. Obrat trditve ne velja.

*Dokaz.* Očitno. □

**Primer 5.22.**

- Če je  $K = \mathbb{F}$  so ciklični podmoduli 1-razsežni podprostori ter  $\{0\}$ .
- Če je  $K = \mathbb{Z}$  so ciklični  $\mathbb{Z}$ -moduli ciklične podgrupe.
- Naj bo  $K$  komutativen kolobar. Vemo, da so levi ideali nad  $K$  levi  $K$ -moduli. Ciklični podmoduli  $K$ -modula  $K$  so glavni ideali.
- Naj bo  $I \trianglelefteq K$  levi ideal ter opazujemo modul  $K/I$ .  $K/I$  je ciklični modul generiran z  $1 + I$ , saj je  $a + I = a(1 + I)$ .

**Definicija 5.23.** Naj bo  $X \subseteq M$ . Podmodul, generiran s  $X$ , je množica vseh **končnih** linearnih kombinacij elementov  $X$ .

**Definicija 5.24.**  $M$  je *končno generiran*, če je generiran s kakšno končno množico.

### Naloga 5.25

Naj bo  $n$  naravno število. Določi največji  $M \in \mathbb{N}$ , za katerega velja, da za vsako množico naravnih števil  $A = \{a_1, \dots, a_n\}$  z  $n$  elementi, vsota katerih je enaka  $M$ , obstajajo koeficienti  $b_i \in \{-2, -1, 0, 1, 2\}$ , ki niso vsi 0, da velja

$$\sum_{i=1}^n a_i b_i = 0.$$

## 6 Prosti moduli

### Definicija 6.1

Podmnožica  $B$   $K$ -modula  $M$  je *linearno neodvisna*, če za vse različne  $e_1, \dots, e_s \in B$  in vse  $a_1, \dots, a_s \in K$  velja

$$\sum_{i=1}^s a_i e_i = 0 \implies \forall i \ a_i = 0.$$

Če je  $B$  linearno neodvisna in generira  $M$  pravimo, da je  $B$  baza  $M$ .

**Komentar 4.** Če je  $B$  baza modula  $M$ , za vsak  $u \in M$  obstajajo  $e_1, \dots, e_s \in B$ , da je

$$u = \sum_{i=1}^s a_i e_i,$$

kjer so  $a_i \in K$  enolično določeni

### Primer 6.2.

- $K = \mathbb{F}$  - vsi vektorski prostori imajo bazo.
- $K = \mathbb{Z}$  ter  $G$  končna Abelova grupa. Za vsak  $u \in G$  množica  $\{u\}$  ni linearno neodvisna, saj ima element  $u$  končen red. Sledi, da je v tem primeru edina linearno neodvisna množica prazna množica.
- $K = \mathbb{Z}$  ter  $G = \mathbb{Z}$ . Bazi sta natanko  $\{1\}$  ter  $\{-1\}$ .

**Definicija 6.3.** Modul, ki ima bazo se imenuje *prosti modul*.

### Primer 6.4.

- Vsak vektorski prostor je prost, kot  $\mathbb{F}$ -modul.
- Naj bo  $K$  poljuben kolobar. Struktura  $K^s = K \oplus \dots \oplus K$  je  $K$ -modul. Natančneje je  $K^s$  prosti  $K$ -modul, z bazo  $\{e_i\}_{i=1}^s$ .

**Definicija 6.5.** Prosta Abelova grupa je Abelova grupa, ki je kot  $\mathbb{Z}$ -modul prost.

**Primer 6.6.**  $\mathbb{Z}^s = \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$  je prosta Abelova grupa.

### Komentar 6.7: Patologije modulov

Med vektorskimi prostori in moduli obstajajo znatne razlike:

- Vsak modul ni prost. Glej primer končne Abelove grupe, kot  $\mathbb{Z}$  modul.
- Podmodul prostega modula ni nujno prost. Primer: vsak kolobar  $K$  je prost kot  $K$ -modul (baza  $\{1\}$ ). Levi podmoduli so levi ideali. Točni protiprimer je kolobar  $\mathbb{Z}_4$  ter njegov levi podmodul  $2\mathbb{Z}_4$ , ki nima linearno neodvisne podmnožice, saj 2 uniči element 2.
- Če obstaja baza z  $n$  elementi ni res, da je vsaka druga linearno neodvisna množica z  $n$  elementi baza.
- Baze imajo lahko različno kardinalnost. Lahko se celo zgodi, da je za kolobar  $K$ ,  $K^s \cong K^t$  za  $s \neq t$ . To se sicer ne zgodi v primeru komutativnih  $K$ , a obstajajo protiprimeri.
- Kvocientni modul dveh prostih modulov ni nujno prost.

Naj bo  $B$  poljubna množica in  $K$  kolobar. Ali obstaja prost modul nad  $K$  z bazo  $B$ ?

**Izrek 6.8.** *Za vsako množico  $B$  in vsak kolobar  $K$  obstaja  $K$ -modul z bazo  $B$ .*

*Dokaz.* Vzamemo množico vseh končnih formalnih linearnih kombinacij elementov  $B$  in vpeljemo seštevanje in skalarno množenje na samoumeven način. Na tak način dobimo prosti modul izomorfen  $K^{|B|}$ .  $\square$

**Izrek 6.9.** *Naj bo  $M$  prosti  $K$ -modul in  $N$  poljuben  $K$ -modul. Vsako funkcijo  $f : B_M \rightarrow N$  iz baze  $B_M$  modula  $M$  lahko enolično razširimo do homomorfizma med  $M$  in  $N$ .*

*Dokaz.* Očitno.  $\square$

**Trditev 6.10.** *Vsak modul je homomorfna slika prostega modula.*

*Dokaz.* Naj bo  $B$  podmnožica  $N$ , ki generira  $N$ . Sedaj uporabimo zgornji izrek.  $\square$

Očitno sledi, da je vsak modul kvocient po prostem modulu.

**Definicija 6.11.** Modul nad obsegom  $D$  imenujemo *vektorski prostor* nad  $D$ .

**Lema 6.12 (Zorn).** *Naj bo  $S$  množica z delno urejenostjo  $\leq$  (operacija je refleksivna, antisimetrična ter tranzitivna). Naj bo  $V$  veriga v  $S$  (linearno urejena podmnožica  $S$ ). Če ima vsaka veriga  $V$  zgornjo mejo ima  $S$  maksimalni element.*

**Izrek 6.13.** *Vsaka linearno neodvisna podmnožica vektorskega prostora  $V$  nad obsegom  $D$  je vsebovana v neki bazi  $V$ .*

*Dokaz.* Naj bo  $T$  linearno neodvisna množica. Naj bo  $S$  množica vseh linearno neodvisnih podmnožic  $V$ , ki vsebujejo  $T$ .  $S$  delno uredimo glede na inkluzijo. Naj bo  $\mathcal{V}$  veriga v  $S$ .

Ta ima zgornjo mejo

$$\mathcal{Z} = \bigcup_{\mathcal{M} \in \mathcal{V}} \mathcal{M}.$$

Preverimo, da  $\mathcal{Z}$  vsebuje  $T$  in da je element  $S$ . Naj so  $\{z_i\}_{i=1}^n$  različni elementi  $\mathcal{Z}$ . Vemo, da je  $z_i \in \mathcal{M}_i$  za  $\mathcal{M}_i \in \mathcal{V}$ . Ker je  $\mathcal{V}$  veriga ter so  $\mathcal{M}_i \in \mathcal{V}$  vemo, da eden izmed  $\{\mathcal{M}_i\}$  vsebuje vse ostale, naj bo to  $\mathcal{M}_j$ . Sledi, da je  $\{z_i\}_{i=1}^n \subseteq \mathcal{M}_j$ , sepravi so  $\{z_i\}_{i=1}^n$  linearno neodvisni, kar pomeni, da je  $\mathcal{Z} \in S$ .

Zornova lema pove, da ima  $S$  maksimalni element  $\mathcal{B}$ . Vemo, da je  $\mathcal{B}$  linearno neodvisna ter vsebuje  $T$ . Naj bo  $v \in V$ . Če je  $v \in \mathcal{B}$  smo končali, zato predpostavimo, da  $v \notin \mathcal{B}$ . Zaradi maksimalnosti  $\mathcal{B} \cup \{v\} \notin S$ . Ker  $\mathcal{B} \cup \{v\}$  ni linearno neodvisna sledi, da lahko zapišemo  $v$  kot linearno kombinacijo elementov  $\mathcal{B}$ . Pokazali smo, da je  $\mathcal{B}$  linearno neodvisna ter ogrodje, kar pokaže, da je  $\mathcal{B}$  baza.  $\square$

**Trditev 6.14.** *Vsak vektorski prostor ima bazo.*

*Dokaz.* V zgornjem izreku izberemo  $T = \emptyset$ .  $\square$

Tudi v primeru vektorskih prostorov nad obsegom govorimo o pojmu dimenzije. Ne pojavijo se patologije, vsaki dve bazi imata enako kardinalnost. V primeru modulov nad komutativnim kolobarjem, ko se ne pojavijo baze različnih razsežnosti, namesto o dimenziji modula govorimo o *rangu* modula.

## 7 Eksaktna zaporedja

**Komentar 5.** Problem, ali je podmodul direktni sumand je v splošnem zahteven in zanimiv. Kratka eksaktna zaporedja v ozadju študija tega problema.

### Definicija 7.1: Eksaktno zaporedje

Naj so  $\{M_i\}_{i=0}^s$  moduli nad kolobarjem  $K$ . Množica homomorfizmov  $\{\varphi_i\}_{i=1}^s$ , kjer je  $\varphi_i : M_{i-1} \rightarrow M_i$ , pravimo *eksaktno zaporedje*, če je  $\text{im}(\varphi_i) = \ker(\varphi_{i+1})$ .

$$M_0 \xrightarrow{\varphi_0} M_1 \xrightarrow{\varphi_1} \dots \xrightarrow{\varphi_{s-1}} M_{s-1} \xrightarrow{\varphi_s} M_s$$

### Primer 7.2.

- Zaporedje  $0 \rightarrow L \xrightarrow{\varphi} M$  je eksaktno, kadar je  $\varphi$  inektiven.
- Zaporedje  $M \xrightarrow{\varphi} N \rightarrow 0$  je eksaktno, kadar je  $\varphi$  surjektiven.
- $0 \rightarrow L \xrightarrow{\varphi} M \rightarrow 0$  je eksaktno, kadar je  $\varphi$  izomorfizem.

### Definicija 7.3: Kratko eksaktno zaporedje

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$$

je eksaktno, kadar je  $\varphi$  inektiven,  $\psi$  surjektiven, ter je  $\text{im}(\varphi) = \ker(\psi)$ . Posledično velja, da je  $\psi \circ \varphi = \{0\}$ . Temu rečemo *kratko eksaktno zaporedje*.

### Primer 7.4.

- Naj bo  $L$  podmodul  $M$ . Imamo kratko eksaktno zaporedje

$$0 \longrightarrow L \xrightarrow{\iota_L} M \xrightarrow{\pi} M/L \longrightarrow 0,$$

kjer je  $\iota_L$  vložitev  $L$  v  $M$  ter  $\pi$  kanonični epimorfizem.

- Za modula  $L$  in  $N$  imamo kratko eksaktno zaporedje

$$0 \longrightarrow L \xrightarrow{\iota_L} L \oplus N \xrightarrow{\pi_N} N \longrightarrow 0,$$

kjer je  $\iota_L(t) = (t, 0)$  ter  $\pi(t, v) = v$ .

### Definicija 7.5: Kratko razpadno eksaktno zaporedje

Kratkemu eksaktnemu zaporedju

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$$

pravimo *razpadno*, če obstaja izomorfizem  $\sigma : M \rightarrow L \oplus N$ , da naslednji diagram komutira.

$$\begin{array}{ccccccc} 0 & \longrightarrow & L & \xrightarrow{\varphi} & M & \xrightarrow{\psi} & N \longrightarrow 0 \\ & & \downarrow id & & \downarrow \sigma & & \downarrow id \\ 0 & \longrightarrow & L & \xrightarrow{\iota_L} & L \oplus N & \xrightarrow{\pi_N} & N \longrightarrow 0. \end{array}$$

Komutiranje zgornjega diagrama je ekvivalentno enakostima  $\sigma\varphi = \iota_L$  ter  $\pi_N = \psi\sigma^{-1}$ .

Komutiranje diagrama je ekvivalentno enakostima, saj moramo skrbeti le za komutiranje kvadratov. Uporaba dveh zaporednih kolinearnih homomorfizmov je namreč enaka trivialni preslikavi v  $\{0\}$ .

Od sedaj dalje uporabimo oznake  $t \in L$ ,  $u \in M$ ,  $v \in N$ .

**Komentar 6.** Razpadnost eksaktnega zaporedja nam na filozofskem nivoju pove, da je  $L$  direktni sumand  $M$ , čeprav na formalnem nivoju ni niti podmodul.

**Izrek 7.6.** Za kratko eksaktno zaporedje

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$$

so naslednji pogoji ekvivalentni

- Zaporedje je razpadno.
- Obstaja tak homomorfizem  $\varphi' : M \rightarrow L$ , da je  $\varphi'\varphi = id_L$ .
- Obstaja homomorfizem  $\psi' : N \rightarrow M$ , da je  $\psi\psi' = id_N$ .

*Dokaz.* Pokažimo, da druga toča implicira prvo. Izomorfizem  $\sigma$  definiramo kot  $\sigma(u) = (\varphi'(u), \psi(u))$ . Ni dvoma, da je  $\sigma$  homomorfizem.

Naj bo  $u \in \ker(\sigma)$ . Sledi, da je  $\varphi'(u) = 0$  in  $\psi(u) = 0 \implies u \in \ker(\psi) = \text{im}(\varphi)$ . Sledi, da obstaja  $t \in L$ , da je  $u = \varphi(t)$ . Posledično je  $\varphi'(\varphi(t)) = 0$ , ker pa je  $\varphi'\varphi = id_L$  sledi  $t = 0$ , kar dokaže injektivnost.

Dokažimo še surjektivnost  $\sigma$ . Naj bo  $(t, v) \in L \oplus N$ . Želimo torej najti tak  $u \in M$ , da je  $(t, v) = (\varphi'(u), \psi(u))$ .  $\psi$  je surjektiven, zato obstaja  $u_0 \in N$ , da je  $\psi(u_0) = v$ . Ker je  $\psi(u_0 + \varphi(\ell)) = v$  za vse  $\ell \in L$  moramo poiskati tak  $\ell$ , da je  $\varphi'(u_0 + \varphi(\ell)) = t$ . Upoštevajoč aditivnost homomorfizmov dobimo

$$\varphi'(u_0) + \ell = t \implies \ell = t - \varphi'(u_0),$$

kar pomeni, da lahko vedno izberemo ustrezn  $\ell \in L$ , kar dokaže surjektivnost.

Preko podanih ekvivalentnih pogojev preverimo, da je  $\sigma$  tak, da diagram komutira. Velja

$$\sigma(\varphi(t)) = (\varphi'(\varphi(t)), \psi(\varphi(t)) = (t, 0),$$

kar smo želeli. Drugi pogoj je

$$\pi_N \sigma = \psi,$$

kar je očitno ustrezno po definiciji  $\sigma$ .

Pokažimo, da tretja točka implicira prvo. Naj bo  $\psi' : N \rightarrow M$ , da je  $\psi\psi' = \text{id}_N$ .

Definirajmo  $\sigma' : L \oplus N \rightarrow M$  s predpisom  $\sigma'(t, v) = \varphi(t) + \psi'(v)$ . Jasno je  $\sigma'$  homomorfizem. Pokažemo, da je  $\sigma'$  bijektiven.

Denimo, da je  $(t, v) \in \ker(\sigma')$ . Vemo, da je  $\varphi(t) + \psi(v) = 0 \implies \psi(\varphi(t)) + v = 0$ . Prvi člen vsote je vedno 0, sledi, da je  $v = 0$ . Začetna formula iz jedra pokaže, da je  $\varphi(t) = 0$ , kar pomeni, da je  $t = 0$ , saj je  $\varphi$  inektiven.

Naj bo  $u \in M$ . Želimo pokazati, da je  $u = \varphi(t) + \psi'(v)$ . Sledi, da je  $\psi(u) = 0 + v \implies v = \psi(u)$ . Sledi, da je  $\varphi(t) = u - \psi'(\psi(u))$ . Radi bi pokazali, da je  $u - \psi'(\psi(u)) \in \text{im}(\phi) = \ker(\psi)$ . Izračunamo

$$\psi(u - \psi'(\psi(u))) = \psi(u) - \psi(\psi'(\psi(u))) = \psi(u) - \psi(u) = 0,$$

kar pokaže surjektivnost.

Ker je  $\sigma'$  izomorfizem definiramo  $\sigma = \sigma'^{-1}$ . Preverimo še dva ekvivalentna pogoja za komutiranje diagrama. Očitno je

$$\varphi(t) = \sigma'(t, 0).$$

Prav tako je

$$\psi(\sigma'(t, v)) = \psi(\varphi(t) + \psi'(v)) = v,$$

kar pokaže komutativnost diagrama.

Dokažemo še najlažji del, da prva točka implicira drugo in tretjo. Definiramo funkciji  $\varphi' = \pi_L \sigma$  ter  $\psi' = \sigma^{-1} \iota_N$  ter preprosto preverimo, da sta pogoja izpolnjena.  $\square$

## 7.1 Projektivni moduli

### Definicija 7.7

Modul  $P$  je *projektiven*, če za vsak homomorfizem  $\varphi : P \rightarrow N$  in vsak epimorfizem  $\psi : M \rightarrow N$  obstaja tak homomorfizem  $\theta : P \rightarrow M$ , da je  $\psi\theta = \varphi$ .

Ekvivalentno za vsaka  $\varphi, \psi$  obstaja  $\theta$ , da komutira diagram.

$$\begin{array}{ccc}
 & P & \\
 \theta \swarrow & & \searrow \varphi \\
 M & \xrightarrow{\psi} & N \longrightarrow 0
 \end{array}$$

**Lema 7.8.** Vsak prosti modul je projektiven.

*Dokaz.* Naj bo  $P$  prosti modul z bazo  $\mathcal{B}$ .  $\varphi(e) \in N$  za vsak  $e \in \mathcal{B}$ . Ker je  $\psi$  surjektiven obstaja  $u_e \in M$ , da je  $\varphi(e) = \psi(u_e)$ . Definiramo  $\theta(e) = u_e$ .  $\theta$  je z delovanjem na bazi enolično določen. Za bazne elemente  $P$  je pogoj o kompozicijo očitno izpolnjen, kar pomeni, da je izpolnjen za vse elemente  $P$ .  $\square$

**Izrek 7.9.** Za modul  $P$  so naslednje trditve ekvivalentne:

- $P$  je projektiven.
- Vsako kratko eksaktno zaporedje

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} P \longrightarrow 0$$

razpade.

- Obstaja tak modul  $L$ , da je modul  $L \oplus P$  prost.

*Dokaz.* Pokažemo, da prva točka implicira drugo.  $P$  je projektivni modul, kar pomeni, da naslednji diagram komutira.

$$\begin{array}{ccccccc}
 & & & & P & & \\
 & & & & \downarrow id & & \\
 & & \theta \swarrow & & & \searrow \psi & \\
 0 & \longrightarrow & L & \xrightarrow{\varphi} & M & \longrightarrow & P \longrightarrow 0
 \end{array}$$

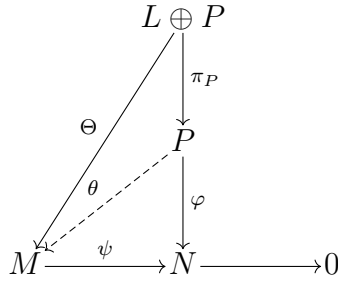
Razpadnost sledi po ekvivalentni karakterizaciji razpadnosti, saj lahko definiramo  $\phi' = \theta$ , kar poda  $id_P = \phi\theta = \phi\phi'$ .

Pokažemo, da druga točka implicira tretjo. Vemo, da je vsak modul homomorfna slika prostega modula. Naj bo  $P$  homomorfna slika prostega modula  $M$ . Imamo kratko eksaktno zaporedje.

$$0 \longrightarrow \ker(\psi) \xrightarrow{id} M \xrightarrow{\psi} P \longrightarrow 0$$

Sledi, da je  $M \cong L \oplus P \implies L \oplus P$  je prost.

Pokažemo, da tretja točka implicira prvo. Naj bo  $L$  tak, da je  $L \oplus P$  prost.



Ker  $L \oplus P$  prost je projektiven, zato obstaja  $\Theta$ . Definiramo  $\theta = \Theta \iota_P$ , kjer je  $\iota_P : P \rightarrow L \oplus P$  vložitev. Preverimo, da je  $\theta$  ustrezen za projektivnost  $P$ . Res velja:

$$\psi\theta = \phi\Theta\iota_P = \varphi\pi_P\iota_P = \varphi.$$

□

### Primer 7.10: Projektiven modul ni nujno prost

Naj bo  $K$  komutativen kolobar, ki ima netrivialni idempotent  $e$ . Opazimo, da je  $K$  prost kot modul nad samim sabo.

$P = eK$  je podmodul oziroma ideal. Trdimo, da je  $P$  projektiven, saj je namreč direktni sumand  $K = eK \oplus (1-e)K$ . Vsota modulov je enaka  $K$ , saj je  $x = ex + (1-e)x$ .

Naj bo  $ex = (1-e)y$  element preseka  $eK$  in  $(1-e)K$ . Sledi  $ex = e^2x = e(1-e)x = (e - e^2)x = 0x = 0$ . Vsota je torej direktna, kar utemelji projektivnost  $P$ .

$P$  ni prost, saj enojec  $\{ex\}$  za poljuben  $x \in K$  ni linearno neovisen, velja namreč  $(1-e)ex = 0$ .

Konkretno lahko za komutativna kolobarja  $K_1, K_2$  dobimo netrivialni idempotent kot element  $(1, 0) \in K_1 \times K_2$ .

Opomnimo tudi, da obstoj netrivialnega idempotenta  $e$  pove, da je kolobar  $K$  »sestavljen iz dveh delov«, namreč

$$K = eK \oplus (1-e)K.$$

## 8 Tenzorski produkt modulov

»Predstavljajte si največjo stvar na svetu, ki ste je kadarkoli videli. Modul z bazo  $M \times N$  je večji.«

prof. dr. Matej Brešar

### Komentar 8.1: Motivacija tenzorskega produkta

Tenzorski produkt končnodimenzijskih vektorskih prostorov  $U$  in  $V$  nad poljem  $\mathbb{F}$  je vektorski prostor dimenzije  $\dim(U) \cdot \dim(V)$ . V primeru modulov nad komutativnim kolobarjem pa je konstrukcija malo zahtevnejša.

**Tenzorski produkt je magično orodje, ki nam bilinearne preslikave pretvori v linearne preslikave.**

Od sedaj naprej obravnavamo module nad komutativnim kolobarjem  $K$ .

**Definicija 8.2 (Tenzorski produkt).** Naj sta  $M, N$   $K$ -modula. Opazujemo prosti modul  $\mathcal{F}$ , ki ima množico  $M \times N$  za bazo. Naj bo  $\mathcal{R}$  podmodul generiran z vsemi elementi oblike

$$(au + a'u', v) - a(u, v) - a'(u', v) \text{ ter } (u, av + a'v') - a(u, v) - a'(u, v').$$

*Tenzorski produkt* modulov  $M$  in  $N$  je modul  $\mathcal{F}/\mathcal{R}$ . Označimo ga kot  $M \otimes N$ .

K sreči lahko na to definiciji zelo hitro pozabimo. Navedemo jo zato, da pokažemo, da tak modul obstaja ter je enolično določen.

**Definicija 8.3 (Bilinearna preslikava).** Preslikava  $\Phi : M \times N \rightarrow L$  je *bilinearna*, če je linearna v vsakem argumentu. Na daljše to zapišemo kot

$$\begin{aligned}\Phi(au + a'u', v) &= a\Phi(u, v) + a'\Phi(u', v) \\ \Phi(u, av + a'v') &= a\Phi(u, v) + a'\Phi(u, v')\end{aligned}$$

### Primer 8.4.

- *Skalarni produkt, vektorski produkt v  $\mathbb{R}^3$ .*
- *Produkt v vsaki algebri  $A$  - bilinearne vsebuje obe distributivnosti ter homogenost. To pomeni, da je bilinearne množenja skoraj ekvivalentno aksiomom množenja v algebri, edino kar manjka je asociativnost množenja.*
- *Produkt matrik je bilinearne preslikava.*

Ključna je sledeča karakteristična lastnost tenzorskega produkta.

### Izrek 8.5: Univerzalna lastnost tenzorskega produkta

Za vsaka modula  $M, N$  nad komutativnim kolobarjem  $K$  obstaja taka bilinearna preslikava  $M \times N \rightarrow M \otimes N$ ,  $(u, v) \mapsto u \otimes v$ , za katero velja

† za vsako bilinearno preslikavo  $\Phi : M \times N \rightarrow L$  obstaja enolično določena linearna preslikava  $\varphi : M \oplus N \rightarrow L$ , da je

$$\varphi(u \oplus v) = \Phi(u, v).$$

S to lastnostjo je tenzorski produkt modulov do izomorfizma natančno enolično določen.

Ekvivalentno??? obstaja enolično določena inducirana linearna preslikava  $\varphi$ , da komutira naslednji diagram.

$$\begin{array}{ccc} M \times N & \xrightarrow{\otimes} & M \otimes N \\ & \searrow \Phi & \downarrow \varphi \\ & & L \end{array}$$

*Dokaz.* Vpeljemo

$$u \oplus v = (u, v) + \mathcal{R},$$

kjer je  $\mathcal{R}$  definiran enako kot v definiciji tenzorskega produkta. Iz lastnosti  $\mathcal{R}$  sledi

$$(au + a'u', v) \otimes v = a(u \otimes v) + a'(u' \otimes v).$$

Podobno vpeljemo linearnost  $\otimes$  v drugem argumentu.  $\Phi : M \times N \rightarrow L$  naj bo bilinearna preslikava.  $\mathcal{F}$  je prosti modul z bazo  $M \times N$ . Zato lahko  $\Phi$  razširimo do linearne preslikave  $F : \mathcal{F} \rightarrow L$ . Torej velja

$$F(u, v) = \Phi(u, v).$$

Ker je  $\Phi$  linearna obstaja  $\ker(F)$ . Opazimo, da  $\mathcal{R} \subseteq \ker(F)$ , kar preverimo z vsebovanostjo generatorjev  $\mathcal{R}$ .

Zato je  $\varphi : M \otimes N \rightarrow L$  definirana s predpisom

$$\varphi(x + \mathcal{R}) = F(x)$$

dobro definirana. Ker je  $F$  linearna takoj sledi, da je  $\varphi$  linearna. Res  $\varphi$  deluje na predpisan način, hitro preverimo  $\varphi(u \otimes v) = \Phi(u, v)$ .

Preverimo enoličnost  $\varphi$ . Vsak element v  $\mathcal{F}$  je (končna) linearna kombinacija baznih elementov  $(u, v)$ . Vsak element  $M \otimes N = \mathcal{F}/\mathcal{R}$  je tako enak linearni kombinaciji elementov oblike  $u \otimes v$ . Sledi, da je vsak element  $M \otimes N$  oblike

$$a_1(u_1 \oplus v_1) + \cdots + a_n(u_n \oplus v_n) = (a_1 u_1) \oplus v_1 + \cdots + (a_n u_n) \oplus v_n.$$

Sledi, da je vsak element  $M \oplus N$  vsota *enostavnih tenzorjev*. Ker se  $\varphi$  in  $\Psi$  ujemata na generatorjih sledi enoličnost preslikave  $\varphi$ .

Ostane le še dokaz enolične karakterizacije tenzorskega produkta z univerzalno lastnostjo.

Naj bo  $T$  modul z enako lastnostjo. Po predpostavki sta  $\Phi$  in  $\odot$  bilinearni. Uporabimo predpostavko na bilinearni preslikavi  $\Phi = \otimes$ . Sledi, da obstaja  $\varphi(u \otimes v) = u \odot v$ .

Sedaj uporabimo univerzalno lastnost na  $\otimes$ . Sledi, da obstaja  $\psi : T \rightarrow M \otimes N$ , da je  $\psi(u \odot v) = u \otimes v$ .

Sledi, da je  $(\psi\varphi)(u \otimes v) = u \otimes v$  ter  $(\varphi\psi)(u \odot v) = u \odot v$ . Izomorfizem sledi.  $\square$

**Komentar 7.** Sporočilo izreka je, da če definiramo  $\varphi(u \otimes v) = \Phi(u, v)$ , potem je  $\varphi$  dobro definirana ter velja

$$\varphi\left(\sum_{i=1}^n u_i \otimes v_i\right) = \sum_{i=1}^n \Phi(u, v).$$

Profesor opomni, da pri bilinearnih preslikavah pri bilinearnih preslikavah pogosteje dokažemo izomorfizem s konstruiranjem bijekcije, kot pa z drugimi metodami.

Točna definicija tenzorskega produkta je nekoliko zapletena. Podano naslednjo bolj praktično »definicijo« tenzorskega produkta.

### Definicija 8.6: Praktična definicija Tenzorskega produkta

Naj sta  $M$  in  $N$  modula nad komutativnim kolobarjem  $K$ . *Tenzorski prdukt* modulov  $M$  in  $N$  je modul  $M \otimes N$ . Velja:

- Za vsaka  $u \in M$ ,  $v \in N$  obstaja element  $u \otimes v \in M \otimes N$ , ki ga imenujemo *enostavni tenzor*. Vsak element v  $M \otimes N$  je vsota enostavnih tenzorjev

$$u_1 \otimes v_1 + \cdots + u_n \otimes v_n.$$

•

$$\begin{aligned}(u + u') \otimes v &= u \otimes v + u' \otimes v \\ u \otimes (v + v') &= u \otimes v + u \otimes v' \\ (au) \otimes v &= u \otimes (av) = a(u \otimes v),\end{aligned}$$

posledično je  $0 \otimes v = u \otimes 0 = 0$ .

- Univerzalna lastnost: Za vsako bilinearno  $\Phi$  obstaja enolično določena linearna  $\varphi$ , da diagram komutira.

$$\begin{array}{ccc} M \times N & \xrightarrow{\otimes} & M \otimes N \\ & \searrow \Phi & \downarrow \varphi \\ & & L \end{array}$$

## 8.1 Linearne preslikave nad tenzorskim produktom

**Definicija 8.7 (Tenzorski produkt preslikav).** Za linearni preslikavi  $\varphi : M \rightarrow M'$  ter  $\psi : N \rightarrow N'$  konstruiramo bilinearno preslikavo iz  $M \times N$  v  $M' \otimes N'$ , definirano s predpisom  $(u, v) \mapsto \varphi(u) \otimes \psi(v)$ .

Posledično obstaja linearna preslikava, ki jo označimo z  $\varphi \otimes \psi$ , z lastnostjo

$$(\varphi \otimes \psi)(u \otimes v) = \varphi(u) \otimes \psi(v).$$

Preslikavo  $\varphi \otimes \psi$  imenujemo *tenzorski produkt preslikav*  $\varphi$  in  $\psi$ . Za tenzorski produkt preslikav velja:

$$\begin{aligned} (\varphi_1 + \varphi_2) \otimes \psi &= \varphi_1 \otimes \psi + \varphi_2 \otimes \psi \\ \varphi \otimes (\psi_1 + \psi_2) &= \varphi \otimes \psi_1 + \varphi \otimes \psi_2 \\ a\varphi \otimes \psi &= \psi \otimes a\psi = a(\varphi \otimes \psi) \\ (\varphi_1 \otimes \varphi_2) \circ (\psi_1 \otimes \psi_2) &= \varphi_1 \circ \psi_1 \otimes \varphi_2 \circ \psi_2 \end{aligned}$$

**Trditev 8.8.**

$$\begin{aligned} \varphi, \psi \text{ izomorfizma} &\implies \varphi \otimes \psi \text{ bijektivna} \\ (\varphi \otimes \psi)^{-1} &= \varphi^{-1} \otimes \psi^{-1} \end{aligned}$$

**Izrek 8.9.** Naj so  $M, N, R$   $K$ -moduli. Velja

- $M \otimes N \cong N \otimes M$
- $(M \otimes N) \otimes R \cong M \otimes (N \otimes R)$
- $(M \oplus N) \otimes R \cong (M \otimes R) \oplus (N \otimes R)$ .
- $M \otimes K \cong M$

*Dokaz.* Pri prvi točki vzamemo naravni izomorfizem  $u \otimes v \mapsto v \otimes u$ . Standardni postopek je, da opazujemo preslikavo iz  $M \times N$  v  $N \oplus V$  definirano s predpisom  $(u, v) \mapsto v \oplus u$ . Sedaj z univerzalno lastnostjo dobimo izomorfizem. Inverz preslikave je na dlani.

Pri drugi točki bi želeli dobro definirano preslikavo  $(u \otimes v) \otimes w \mapsto u \otimes (v \otimes w)$ . Zelo očitno je njen inverz  $u \otimes (v \otimes w) \mapsto (u \otimes v) \otimes w$ . Začasno fiksiramo  $w \in R$ . Gledamo preslikavo  $(u, v) \mapsto u \otimes (v \otimes w)$ . Ta je bilinearna, zato obstaja dobro definirana linearna preslikava  $\alpha : u \otimes v \mapsto u \otimes (v \otimes w)$ . Zato lahko definiramo  $\Phi : (M \otimes N) \otimes R \rightarrow M \otimes (N \otimes R)$  s predpisom

$$\Phi \left( \sum u_i \otimes v_i, w \right) = \sum u_i \otimes (v_i \otimes w).$$

Stvar nadaljujemo na očiten način.

Dokaz tretje točke izpustimo.

Četrto točko dokažemo z preslikavo  $u \otimes a \mapsto au$ . Inveržno je  $u \mapsto u \otimes 1$

□

**Komentar 8.** Če pozabimo na module in si predstavljamo vektorske prostore zgornji izrek postanejo očitni upoštevajoč dimenzijske razmisleke. Izrek tako ni pretirano presenetljiv.

#### Komentar 8.10

Čeprav zgornji izrek ni presenetljiv si je vredno zapomniti kako poteka dokaz. Skoraj vedno definiramo preslikavo iz direktnega produkta modulov v tenzorski produkt, nato pa dobimo inducirano preslikavo iz tenzorskega produkta v tenzorski produkt. Ta je dobro definirana po univerzalnem izreku.

Čeprav so izomorfizmi »očitni« je dokazovanje dobre definiranosti nadležno. To nadležnost odpravi zgornji pristop ter uporaba univerzalne lastnosti.