Algebra 3

Hugo Trebše (hugo.trebse@gmail.com)

29. oktober 2025

Which should I learn, analysis or algebra?

Do you want to be deaf or blind?

Michael Atiyah

Kazalo

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 obstja enota u, da je $a = ub$.
- *Največji skupni delitelj* elementov a, b, ki nista ničelna, je tak element d, da velja

  † $d \mid a$ in $d \mid b$.

  † $c \mid a$ 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 nerazcepen $\implies$ 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
$$\langle a_1, \ldots, a_n \rangle = \langle a_1 \rangle + \ldots + \langle a_n \rangle = \{a_1 x_1 + \ldots a_n x_n \mid x_i \in K\}.$$

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 $\delta : K \setminus \{0\} \to \mathbb{N}_0$, 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. □

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. □

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. □

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 $a_1 = a, a_2, a_3, \ldots$, da velja*

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

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

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 $I_1 \subseteq I_2 \subseteq \ldots$ 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. □

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. □

Definicija 3.5

Naj bo K komutativen kolobar. $p \in K$ je *praelement*, če je p neničelen in neobrnljiv, ter velja

$$p \mid ab \implies p \mid a \text{ ali } p \mid b.$$

Lema 3.6. *V celih kolobarjih je vsak praelement nerazcepen. V glavnih kolobarjih velja obrat.*

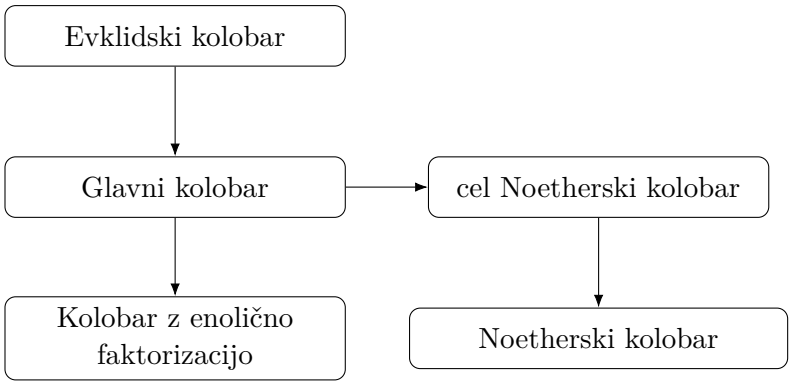
Dokaz. Očitno. □

Definicija 3.7

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 3.8. *Vsak glavni kolobar je kolobar z enolično faktorizacijo.*

Dokaz. Vemo, da ima vsak neničelen neobrnljiv element v celem 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. □



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 $\mathrm{End}(M)$ množica vseh endomorfizmov grupe M. $\mathrm{End}(M)$ 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 ℓ_a aditivna. Sledi, da je ℓ_a endomorfizem aditivne grupe K. Tako je $\varphi : K \to \mathrm{End}(K)$ definirana z $\varphi(x) = \ell_x$. Ostane še vprašanje multiplikativnosti φ, 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.

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

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. □

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 $K \times M \to M$ in notranjo binarno operacijo $(u, v) \mapsto u + v$ je *modul nad kolobarjem* K ali K*-modul*, če je

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

Operaciji $(a, u) \to au$ 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 $\mathrm{End}(M)$. Za K-modul M je $\varphi : K \to \mathrm{End}(M)$ definiran z $\varphi(a)(u) = \ell_a(u) = au$ ustrezen homomorfizem. Obratno za homomorfizem φ, ki slika iz K v $\mathrm{End}(M)$, definiramo množenje s sklararjem 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. $\varphi : M \to N$ je *homomorfizem K-modulov*, če velja

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

Pravimo jim tudi K-linearne preslikave.

Definicija 5.7.

- $\ker \varphi = \{u \in M | \varphi(u) = 0\}$
- $\text{im}\varphi = \{\varphi(u) | u \in M\}$

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 $u_o \in I$. $\varphi : I \to I$ 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 $\mathrm{End}_{\mathbb{F}}(V)$ kolobar (celo algebra).

Definicija 5.10. Množica endomorfizmov K-modula M $\mathrm{End}_K(M)$ 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 $\mathrm{End}_K(M)$ 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 $\mathrm{End}_K(M)$ 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

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

definiramo seštevanje ter množenje s skalarji kot

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

Z definiranima operacija 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 $\varphi : M \to N$ homomorfizem modulov. Tedaj je

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

Dokaz. Dokaz je standarden. □

5.5 Direktne vsote modulov

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

$$M_1 \times \ldots \times M_s$$

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

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

$$M_1 \oplus \ldots \oplus M_s.$$

Natančneje zgornji konstrukciji pravimo zunanja direktna vsota.

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

- $$M = N_1 + \ldots + N_s$$
- $$N_i \cap \sum_{j \neq i} N_j = \{0\}$$

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 $\{(0, 0, \ldots, v_i, \ldots, 0) | v_i \in M_i\}$ 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 podprostori 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 opazujmo 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 $A = \{a_1, \ldots, a_n\}$ 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 $e_1, \ldots, e_s \in B$ in vse $a_1, \ldots, a_s \in K$ 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 $e_1, \ldots, e_s \in B$, 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* $K^s = K \oplus \ldots \oplus K$ *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. $\mathbb{Z}^s = \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$ *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 $K^{|B|}$. □

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

Dokaz. Očitno. □

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

Dokaz. Naj bo B podmnožica N, ki generira N. Sedaj uporabimo zgornji izrek. □

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, antisimetična 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. □

Trditev 6.14. *Vsak vektorski prostor ima bazo.*

Dokaz. V zgornjem izreku izberemo $T = \emptyset$. □

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

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 $\varphi_i : M_{i-1} \to M_i$, pravimo *eksaktno zaporedje*, če je $\text{im}(\varphi_i) = \ker(\varphi_{i+1})$.

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

Primer 7.2.

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

Definicija 7.3: Kratko eksaktno zaporedje

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

je eksaktno, kadar je φ inektiven, ψ 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 ι_L *vložitev* L *v* M *ter* π *kanonični epimorfizem.*
- $$0 \longrightarrow L \xrightarrow{\iota_L} L \oplus N \xrightarrow{\pi_N} N \longrightarrow 0,$$

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

Definicija 7.5: Kratko razpadno eksaktno zaporedje

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

imenujemo *razpadno kratko eksaktno zaporedje*, če obstaja izomorfizem $\sigma : M \to L \oplus N$, da naslednji diagram komutira.

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