Vaje iz Algebre 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 Evklidski, glavni in kolobarji z enolično faktorizacijo

Lema 1.1

Naj bo K komutativni kolobar z multiplikativno normo. Če imata elementa $a, b \in K$ največji skupni delitelj velja

$$N(\gcd(a,b)) \mid \gcd(N(a), N(b)).$$

Z nekaj računanja lahko ovržemo morebitno domnevo, da je

$$N(\gcd(a,b)) = \gcd(N(a), N(b)),$$

opazujemo lahko namreč elementa 5 in $7+i$ v $\mathbb{Z}[i]$.

Dokaz. Očitno. □

Naloga 1.2. *Določi največji skupni delitelj elementov* $3-4i$ *in* $1-3i$ *v kolobarju* $\mathbb{Z}[i]$.

Rešitev. Poslužimo se Evklidovega algoritma (kolobar $\mathbb{Z}[i]$ je namreč Evklidski z evklidsko funkcijo $\delta : a+bi \mapsto a^2+b^2$) kjer upoštevamo, da je kvocient v Evklidovem algoritmu tisti element $\mathbb{Z}[i]$, ki ga dobimo, ko komponenti $\frac{3-4i}{1-3i}$ zaokrožimo do najbližjega celega števila. □

Komentar 1.3

Druga možnost je, da upoštevamo multiplikativnost norme v $\mathbb{Z}[i]$ (norma je podana z $N(a+bi) = a^2+b^2$), kar vodi do ugotovitve

$$N(\gcd(a,b)) \mid \gcd(N(a), N(b)).$$

V našem primeru $N(\gcd(a,b)) \mid 5$, kar pomeni, da za $\gcd(a,b) = x+iy$ velja bodisi $x^2+y^2 = 1$ ali $x^2+y^2 = 5$, kar da razmeroma malo možnosti.

Naloga 1.4

Pokaži, da elementa 6 in $2+2\sqrt{5}$ nimata največjega skupnega delitelja v $\mathbb{Z}[\sqrt{-5}]$.

Rešitev. Vemo, da največji skupni delitelj obstaja v vseh komutativnih domenah enolične faktorizacije. Sledeči dokaz med drugim pokaže, da $\mathbb{Z}[\sqrt{-5}]$ ni domena enolične fakto-

rizacije. Opazimo, da tuja si elementa 2 in $1+\sqrt{-5}$ delita elementa. Njuni normi sta zaporedoma 4 in 6, kar pomeni, da mora norma največjega skupnega delitelja (če ta obstaja) biti deljiva z 12. Obenem velja $N(\gcd(a,b)) \mid \gcd(N(a),N(b))$, kar pomeni, da norma največjega skupnega delitelja deli $\gcd(36,24)=14$ (norma elementa $a+b\sqrt{-5}$ je namreč a^2+5b^2). Sledi, da je norma največjega skupnega delitelja enaka 12. To ni mogoče, saj diofantska enačba $12=a^2+5b^2$ ni rešljiva v celih številih. □

Naloga 1.5. *V komutativnih domenah enolične faktorizacije obstaja največji skupni delitelj, ki je določen do asociiranosti natančno.*

Dokaz. Očitno. □

Naloga 1.6. *Kolobar $\mathbb{Z}[\sqrt{-2}]$ je Evklidski.*

Rešitev. Trdimo, da je evklidska funkcija $\delta : a+b\sqrt{-2} \mapsto a^2+2b^2$. Ko delimo dva elementa $\mathbb{Z}[\sqrt{-2}]$ (kot kompleksni števili) dobimo število oblike $x+i\sqrt{-2}$. Za kvocient vzamemo tisti element kolobarja, ki ga dobimo, ko x ter y zaokrožimo do najbližjega celega števila. Ostanek ima tako evalvacijo največ $\delta(\frac{1}{2}+\frac{1}{2}\sqrt{-2})=\frac{3}{4}<1$, kar smo želeli pokazati. □

Naloga 1.7. *Pokaži, da je $1+\sqrt{-3}$ nerazcepen v $\mathbb{Z}[\sqrt{-3}]$, ni pa praelement.*

Rešitev. Definiramo normo $N(a+\sqrt{-3}b)=a^2+3b^2$. Vidimo, da je $N(1+\sqrt{-3})=4$. Če bi bil razcepen bi veljalo, da je norma enega izmed faktorjev enaka 2 (elementi norme 1 so namreč enote). To očitno ni mogoče.

Opazimo, da je

$$(1+\sqrt{-3})(1-\sqrt{-3})=4=2\cdot 2.$$

Vidimo, da bi v primeru $1+\sqrt{-3} \mid 2$ sledi, da sta $1+\sqrt{-3}$ in 2 asociirana, saj imata enako normo. To seveda ni res.

Sledi, da $\mathbb{Z}[\sqrt{-3}]$ ni GCD domain, specifično ni niti DEF. □

Komentar 1.8: Obstoj norme

Za vsak $d \in \mathbb{Z}$, ki ni popolen kvadrat, obstaja homomorfizem monoidov iz $\mathbb{Z}[\sqrt{d}]$ v $\mathbb{Z}$, podan z

$$N(a+\sqrt{d}b)=a^2-db^2.$$

Algebraične lastnosti $\mathbb{Z}[\sqrt{d}]$ kot so na primer UFD, PID, GCD domain niso relevantne, saj je to dejstvo le posledica identitete Brahmagupte.

2 Kolobar polinomov nad domeno enolične faktorizacije

Definicija 2.1

Cel kolobar K je *kolobar z enolično faktorizacijo* (DEF, UFD), če za vsak $k \in K$, ki je neničelen in neobrnljiv, velja

- obstajajo taki nerazcepni elementi p_i, da je $k = \prod p_i$.
- zgornja faktorizacija je enolična do asociiranosti in vrstnega reda faktorjev natančno.

Naloga 2.2

Pokaži, da je $K[X]$ domena enolične faktorizacije natanko tedaj, ko je K domena enolične faktorizacije.

Rešitev. Če je $K[X]$ domena enolične faktorizacije vemo, da so konstantni polinomi, ki so pravzaprav le elementi K, produkt nerazcepnih elementov iz $K[X]$. Slednji so seveda konstantni, saj se pri produktu polinomov stopnje seštevajo. Sledi, da je K DEF.

Najprej pokažemo, da ima vsak element $K[X]$ končen razcep na nerazcepne elemente.

Denimo, da je K domena enolične faktorizacije in naj bo $f \in K[X]$. Če je f nerazcepen smo končali. Drugače je $f = kg$ za $k, g \in \mathbb{K}[X]$, kjer je seveda $\deg(k), \deg(g) < \deg(f)$. Če je stopnja obeh polinomov v razcepu neničelna nadaljujemo z indukcijo na stopnji polinomov, kjer bazo indukcije pokrije dejstvo, da je K DEF.

V nasprotnem primeru je $f = k_1 \cdot \ldots \cdot k_n g(x)$. Ker ima vodilni koeficient f končen razcep na nerazcepne elemente vemo, da mora imeti g končno mnogo nerazcepnih faktorjev, saj vodilni koeficienti polinomov v razcepu g delijo vodilni koeficient f, slednji pa ima končen razcep nad K.

V zgornjem dokazu smo implicitno uporabili naslednjo lemo

Lema 2.3

V domenah enolične faktorizacije nerazcepni elementi in praelementi sovpadajo.

Sedaj pokažemo enoličnost razcepa na nerazcepne elemente. Za to da bi to sledilo je zadosti pokazati, da je vsak nerazcepen element tudi praelement kolobarja $K[X]$.

Definicija 2.4. Naj bo $f(X) = a_n X^n + \ldots + a_0 \in K[X]$. Njegovo *vsebino* definiramo kot

$$\operatorname{cont}(f) = \gcd(a_n, \ldots, a_0).$$

Lema 2.5 (Lema o vsebini). *Za $f, g \in K[X]$ je*

$$\mathit{cont}(fg) = \mathit{cont}(f) \cdot \mathit{cont}(g) \qquad \textit{do asociiranosti natančno.}$$

Dokaz. Obravnavamo primer $\text{cont}(f) = \text{cont}(g) = 1$. Denimo, da $p \mid \text{cont}(fg)$ za praelement $p \in K$. Sledi, da je $fg = 0$ v kolobarju $K[X]/\langle p \rangle$.

Zaradi naslednje trditve je eden izmed f in g ničelen v $K[X]/\langle p \rangle$, kar pomeni, da vsebina enega izmed nju ni enaka 1.

Trditev 2.6. *Kvocient komutativnega kolobarja s praidealom je domena.*

Dobili smo protislovje, zato je $\text{cont}(fg) = 1$.

Lotimo se še splošnega problema, kar dosežemo z reduciranjem polinomov po njuni vsebini ter nadaljni uporabi leme o vsebini v zgornjem specifičnem primeru.

□

Lema 2.7 (Gauss). *Naj bo $f \in K[X]$ ter $\mathbb{F}$ polje ulomkov K.*

$$f \text{ nerazcepen v } K[X] \implies f \text{ nerazcepen v } \mathbb{F}[X].$$

Lemi uporabimo za dokaz naslednje trditve.

Trditev 2.8. *Če je K DEF, potem praelementi in nerazcepni elementi v $K[X]$ sovpadajo.*

Dokaz. Naj bo f nerazcepen. Denimo, da $f \mid pq$ za $p, q \in K[X]$. Želimo pokazati, da f deli enega izmed q, p.

Po Gaussovi lemi je $f \in \mathbb{F}[X]$ nerazcepen. Ker je $\mathbb{F}[X]$ evklidski je $\mathbb{F}[X]$ UFD in posledično je f praelement v $\mathbb{F}[X]$. Brez škode za splošnost velja $f \mid p$ v $\mathbb{F}[X]$, oziroma obstaja $h \in \mathbb{F}[X]$, da je $p = hf$. Obenem je $h = \frac{g}{k}$, kjer je $k \in K$ ter $g \in K[X]$. Sledi, da je

$$g(X)f(X) = k \cdot p(X).$$

Po lemi o vsebini je

$$\text{cont}(g) \cdot \text{cont}(f) = k \cdot \text{cont}(p)$$

Želimo pokazati, da je k enota. V nasprotnem primeru za vsak $p_i \mid k$ velja $p_i \mid \text{cont}(g)$ ali $p_i \mid \text{cont}(f)$. Druga opcija je nemogoča, saj potem f ni nerazcepen, saj ga lahko zapišemo kot produkt dveh neobrnljivih elementov $K[X]$, namreč praštevila in še nekega polinoma.

Sledi, da lahko k pokrajšamo in dobimo, da $f \mid p$ nad $K[X]$, kar smo želeli. □

□

Naloga 2.9

Pokaži, da je $K[X]$ glavni kolobar natanko tedaj, ko je K polje.

Dokaz. Če je K polje je $K[X]$ evklidski, sledi, da je glavni.

Denimo, da je $K[X]$ glavni. Naj bo $a \in K \setminus \{0\}$. Poglejmo ideal $\langle a, X \rangle$. Očitno ga ne generira noben polinom stopnje 1 ali več, zato ga generira element $a' \in K$.

Ker je $X \in \langle a' \rangle$ obstaja $f \in K[X]$, da je $a'f = X$. Stopnja f je največ 1. Vodilni koeficient f je inverz a'. Sledi, da je a' obrnljiv, kar pomeni$\langle a, X \rangle = K[X]$. Ker je $1 \in K[X]$ linearna kombinacija elmentov X in a dobimo inverz a. □

3 Glavni kolobar, ki ni evklidski

Za $\omega = \frac{1+\sqrt{-19}}{2}$ je $Z[\omega]$ podkolobar $\mathbb{C}$. Normo definiramo s predpisom

$$N(a+b\omega) = |a+b\omega|^2 = a^2 + ab + 5b^2.$$

Trditev 3.1.

- *Elementa* 2 *in* 3 *sta nerazcepna nad* $\mathbb{Z}[\omega]$.
- ± 1 *sta edini enoti* $\mathbb{Z}[\omega]$.

Dokaz. Poljuben obrnljiv element ima normo ± 1. Ker je $4N(a+b\omega) = 4a^2 + 4ab + b^2 + 19b^2 = (2a+b)^2 + 19b^2$ sledi, da je element obrnljiv natanko tedaj, ko je $a^2 = 1$ ter $b = 0$, kar poda želeno. Če je element $x \in \mathbb{Z}$ razcepen obstajata $a, b \in \mathbb{Z}$, da velja $4x = (2a+b)^2 + 19b^2$. Za $x \in \{2, 3\}$ ta diofantska enačba očitno nima rešitev. □

Trditev 3.2

Kolobar $\mathbb{Z}[\omega]$ ni evklidski.

Dokaz. Denimo, da je $\mathbb{Z}[\omega]$ evklidski z evklidsko funkcijo $\delta : \mathbb{Z}[\omega] \setminus \{0\} \to \mathbb{N}_0$. Naj bo x neničelen neobrnljiv element z minimalno stopnjo. Zanj velja $2 = qx + r$, kjer je $r = 0$ ali pa je r obrnljiv, po predpostavki minimalnosti.

- Če je $r = 0$, potem $x \mid 2$, kar pomeni $x = \pm 2$.
- Če je $r = 1$ je x obrnljiv, kar ni mogoče.
- Če je $r = -1$, potem $x \mid 3$, kar pomeni $x = \pm 3$.

Obenem lahko delimo $\omega = q'x + r'$. Podobno ugotovimo, da je $r = 0$ ali pa je r obrnljiv.

- Če je $r = 0$ bi sledilo, da $x \in \{\pm 2, \pm 3\}$ deli ω, kar ni mogoče.
- Če je $r = \pm 1$ sledi, da $x \mid \mp 2 + \omega$. To seveda ni mogoče v primeru $x \in \{\pm 2, \pm 3\}$.

□

Trditev 3.3

Kolobar $\mathbb{Z}[\omega]$ je glavni.

Dokaz.

Lema 3.4. *Za vsak* $\alpha \in \mathbb{C} \setminus \mathbb{Z}[\omega]$ *obstajata* $p, q \in \mathbb{Z}[\omega]$*, da velja*

$$0 < |p\alpha - q| < 1.$$

Dokaz. Naj bo $\alpha = a + b\omega$ za $a, b \in \mathbb{R}$. Brez škode za splošnost obravnavamo zgolj primer $a, b \in [0, 1]$. □

□

4 Prva domača naloga

Naloga 4.1

Naj bo $d \in \mathbb{N}$ kongruenten $1 \pmod 4$. Pokaži, da $\mathbb{Z}[\sqrt{d}]$ nima enolične faktorizacije.

Rešitev. Trditev ni pravilna, saj v primeru, ko je d popolen kvadrat dobimo kolobar $\mathbb{Z}$, ki seveda ima enolično faktorizacijo.

Trditev je pravilna v primeru, ko je $d = 1 \pmod 4$ naravno število, ki ni popolni kvadrat.

Trditev 4.2. 2 *je nerazcepni element kolobarja* $\mathbb{Z}[\sqrt{d}]$.

Dokaz. Kolobar ima multiplikativno normo podano z $N(x + \sqrt{d}y) = x^2 - dy^2$. Velja $N(2) = 4$. Ker so elementi z normo ± 1 enote, je edini razcep 2 kot produkt dveh ne-enot razcep na produkt dveh elementov norme ± 2. Če bi tak razcep obstajal bi obstajala $a, b \in \mathbb{Z}$, da je $a^2 - db^2 = \pm 2$. Taki celi števili ne obstajata, kar lahko vidimo upoštevajoč $d = 1 \pmod 4$ ter to, da so kvadrati kongruentni 0 ali 1 po modulu 4. □

Trditev 4.3. 2 *ni praelement kolobarja* $\mathbb{Z}[\sqrt{d}]$.

Dokaz. Ker je $d = 1 \pmod 4$ je $1 - d$ sodo število. Sledi, da je deljivo z 2 nad $\mathbb{Z}[\sqrt{d}]$, saj je deljivo z 2 nad podkolobarjem $\mathbb{Z}$. Denimo, da bi 2 bilo praštevilo v $\mathbb{Z}[\sqrt{d}]$. Ker je $1 - d = (1 + \sqrt{d})(1 - \sqrt{d})$ bi 2 moralo deliti enega izmed faktorjev. Če bi 2 delilo $1 \pm \sqrt{d}$ bi obstajala $a, b \in \mathbb{Z}$, da je

$$1 \pm \sqrt{d} = 2(a + \sqrt{d}b) = 2a + 2b\sqrt{d}.$$

Ker d ni popolni kvadrat bi iz $\mathbb{Z}$-linearne neodvisnosti sledilo, da je $2a = 1$, kar je seveda nemogoče. Sledi, da 2 ni praštevilo v $\mathbb{Z}[\sqrt{d}]$. □

Vemo, da v kolobarjih z enolično faktorizacijo nerazcepni elementi ter praelementi sovpadajo. Pokazali smo, da to ne velja za $\mathbb{Z}[\sqrt{d}]$, če je $d = 1 \pmod 4$ naravno število, ki ni popolni kvadrat, kar pomeni, da slednji ni kolobar enolične faktorizacije. □

Naloga 4.4

Naj bo K komutativen kolobar. Pokaži, da je množica vseh polinomov iz $K[X]$ z ničelno vsoto koeficientov glavni ideal kolobarja $K[X]$, in poišči njegov generator.

Rešitev. Opazimo, da ima polinom f vsoto koeficientov enako 0 natanko tedaj, ko je $f(1) = 0$.

Naj bo $I = \{f \in K[X] | f(1) = 0\}$ množica polinomov, vsota koeficientov katerih je enaka 0. Pokažemo, da je

$$I = \langle X - 1 \rangle_{K[X]},$$

kar pokaže, da je I glavni ideal, generiran z $X-1$. Zelo očitno velja inkluzija $\langle X-1 \rangle_{K[X]} \subseteq I$, saj ima vsak element leve množice ničlo v točki 1.

Inkluzijo $I \subseteq \langle X - 1 \rangle_{K[X]}$ pokažemo z uporabo naslednjega izreka, ki smo ga dokazali pri Algebri 2.

Izrek 4.5: Faktorski izrek

Naj bo K komutativen kolobar ter $p \in K[X]$. Tedaj je $p(a) = 0 \iff (X - a) \mid p(X)$.

Naj bo $f \in I$ poljuben. Ker je $f(1) = 0$ po zgornjem izreku obstaja $f' \in K[X]$, da je $f(X) = (X - 1)f'(X)$. Sledi, da je $f \in \langle X - 1 \rangle_{K[X]}$. Tako sledi druga inkluzija.

Pokazali smo, da je I glavni ideal kolobarja $K[X]$ ter, da je generiran z $X - 1$. □

Naloga 4.6

Pokaži, da $\mathcal{L} = \{f \in \mathcal{C}(\mathbb{R}) | f(0) = 0\}$ ni končno generiran ideal kolobarja zveznih funkcij $\mathcal{C}(\mathbb{R})$.

Rešitev. Denimo, da bi bil ideal $\mathcal{L}$ končno generiran nad $\mathcal{C}(\mathbb{R})$ z elementi $f_1, \ldots, f_n$. Naj bo $g(x) = \sqrt{\sum_{i=1}^{n} |f_i(x)|} \in \mathcal{L}$. Sledi, da obstajajo $\{h_i\}_{i=1}^{n} \subset \mathcal{C}(\mathbb{R})$, da je

$$g = \sum_{i=1}^{n} h_i f_i.$$

Sledi

$$g = \left| \sum_{i=1}^{n} h_i f_i \right| \leq \sum_{i=1}^{n} |h_i| \, |f_i| \leq \sqrt{\left(\sum_{i=1}^{n} h_i^2 \right) \left(\sum_{i=1}^{n} f_i^2 \right)},$$

kjer prva enakost velja, saj je g po definiciji nenegativna funkcija, druga neenakost pa sledi po Cauchy-Schwarzevi neenakosti. Prav tako velja, da je

$$\sqrt{\sum_{i=1}^{n} f_i^2} \leq \sum_{i=1}^{n} |f_i| \, .$$

Funkcija $t(x) = \sqrt{\sum_{i=1}^{n} h_i(x)^2}$ je zvezna na kompaktu $[-1, 1]$, posledično je tam omejena $0 \leq t(x) < M$. Če združimo vse dosedajšnje ugotovitve dobimo, da je

$$g < Mg^2$$

na intervalu $[0, 1]$. Sledi, da je na intervalu $[-1, 1]$ g bodisi enaka 0, bodisi večja od $\frac{1}{M}$. Po izreku o vmesni vrednosti ter dejstvu, da je $g(0) = 0$, je to možno zgolj, če je $g = 0$ na celotnem intervalu $[-1, 1]$.

Ker na $[-1, 1]$ velja $g = 0$ ter $0 = g(x)^2 = \sum_{i=1}^{n} |f_i|$, sledi, da so vse izmed funkcij f_i ničelne na intervalu $[-1, 1]$. Sledi, da so vse funkcije v $\mathcal{L}$ ničelne na intervalu $[-1, 1]$. To seveda ne velja, protiprimer je funkcija $x \mapsto x$, ki je gotovo element $\mathcal{L}$.

Dosegli smo protislovje, kar pomeni, da ideal $\mathcal{L}$ ni končno generiran. □

Komentar 4.7

Ideal ni niti števno generiran! Skoraj identičen tip argumenta na funkciji

$$g(x) = \sqrt{\sum_{i=1}^{\infty} \frac{|g_i|\,(x)}{2^i}},$$

kjer so

$$g_i = \frac{f_i}{\max\left(\sup_{[-1,1]}(|f_i|), 1\right)}$$

normalizirani generatorji (če zamenjamo f_i-je z g_i-ji očitno ohranimo generiranje) dobi protislovje z istim argumentom.
Ta argument je bolj tehnično zahteven, obstajata vsaj dve znatni razliki. Kot prvič je g s to vrsto definirana samo na intervalu $[-1, 1]$, kjer lahko zagotovimo enakomerno konvergenco po Weierstrassovem M-testu. Zunaj kompakta g dopolnimo z ustrezno konstantno funkcijo, ki zagotovi zveznost.
Prav tako moramo biti pazljivi, saj števna generiranost pomeni, da za vsakega izmed elementov ideala izberemo le končno mnogo generatorjev, ki ga generirajo. Z analogno uporabo Cauchy-Schwarzeve neenakosti ter neenakosti $g(x)^2 \geq \frac{|g_i|(x)}{2^i} \implies |g_i| \leq 2^i g^2$ ugotovimo

$$g(x) \leq \sum_{i=1}^{m} |h_i(x)|\,|g_i(x)| \leq \left(\sum_{i=1}^{m} |h_i(x)|\,2^i\right) g(x)^2.$$

Ustrezna pomožna funkcija je tedaj

$$t(x) = \sum_{i=1}^{m} |h_i(x)|\,2^i,$$

nadaljni argument pa poteka kot v dokazu zgoraj.

Del II

Moduli

I naj bo levi ideal kolobarja K. I je obenem tudi levi modul nad K, kar označmo z ${}_K I$.

Primer 4.8.

- $K = \mathbb{F}$ *polje, modul je tedaj vektorski prostor.*
- $\mathbb{Z}$*-moduli so Abelove grupe.*
- $\mathbb{F}[X]$ *so vektorski prostori z linearno preslikavo.*

Lema 4.9

Naj bo M K-modul ter K' podkolobar K. Potem je M tudi K' modul.

Naloga 4.10. *Naj bo K kolobar 2×2 zgornjetrikotnih matrik nad poljem $\mathbb{F}$. Naj bo M množica 2×1 stolpcev. M je K modul. Poišči vse podmodule M.*

Rešitev. $\mathbb{F}$ je podkolobar K, saj je izomorfen skalarnim večkratnikom identitete. Po zgornji lemi sledi, da so podmoduli K pravzaprav vektorski prostori. Sledi, da so vsi kandidati za leve K-module trivialni modul ter polni modul ($\mathbb{F}^2$), prav tako pa enodimentionalni prostori $\left\{ \lambda \begin{bmatrix} a \\ b \end{bmatrix} \mid \lambda \in \mathbb{F} \right\}$.

Prva dva sta zelo očitno podmodula, sedaj preverimo tretjo opcijo. Sledi, da za vse $a, b, c, \lambda \in \mathbb{F}$ za fiksna $u, v \in \mathbb{F}$ velja, da je

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \lambda \begin{bmatrix} u \\ v \end{bmatrix} = \lambda \begin{bmatrix} au + bv \\ vc \end{bmatrix} \in M,$$

kar pomeni, da je slednji oblike $\mu \begin{bmatrix} u \\ v \end{bmatrix}$. Dobimo sistem enačb $\lambda(au + bv) = \mu u$ ter $\lambda cv = \mu v$, kar more veljati za vse $a, b, c \in \mathbb{F}$. Če je $v \neq 0$ hitro najdemo podmodul, sedaj obravnavamo samo še $v = 0$. Tedaj dobimo $u = 0$. □

Naloga 4.11. *Naj bo $M = {}_{\mathbb{Z}}\mathbb{Z}_{12}$. Poišči vse $\mathbb{Z}$-podmodule modula M. Kateri so enostavni?*

Rešitev. Ker so podmoduli tudi podgrupe za seštevanje so kandidati samo podgrupe. Vemo, da je $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_4$. Kandidati za podgrupe so $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$, seveda pa trivialni in polni podmodul. Od teh sta samo $\mathbb{Z}_2$ ter $\mathbb{Z}_3$ enostavna. □

Naloga 4.12. *Določi $Hom_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_{12})$, $Hom_{\mathbb{Z}}(\mathbb{Z}_3, \mathbb{Z}_4)$ in $Hom_{\mathbb{Z}}(\mathbb{Z}_{12}, \mathbb{Z}_{12})$.*

Rešitev. Ker so homomorfizmi linearni nam slika enice pove slike vsega. Natančneje je $\varphi(n) = \varphi(n \cdot 1) = n\varphi(1)$. Poglejmo katere vrednosti so ustrezne za $\varphi(1)$.

$$\varphi(1)\,(au + bv) = \varphi(au + bv) = \varphi(1)au + \varphi(1)bv.$$

Sledi, da je $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_{12}) = \{\varphi(x) = x \cdot a\}$.

Poglejmo $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_3, \mathbb{Z}_4)$. Ponovno iz cikličnosti $\mathbb{Z}_3$ sledi, da slika enice določi slike vseh elementov. Vemo, da ima 1 red 3 v $\mathbb{Z}_3$, kar pomeni, da moramo 1 slikati v element z redom deljivim z 3. V $\mathbb{Z}_4$ je tak element samo 0, sledi, da je edini homomorfizem ničelni homomorfizem.

Poglejmo $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_{12}, \mathbb{Z}_{12})$. Vemo, da je jedro vsake preslikave iz $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_{12})$ vsebovano v $12 \cdot \mathbb{Z}$. Izrek o izomorfizmu nam pove, da vsaka preslikava iz $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_{12})$ inducira preslikavo med ${}_{\mathbb{Z}}\mathbb{Z}/_{\mathbb{Z}}12\mathbb{Z}$ in ${}_{\mathbb{Z}}\mathbb{Z}_{12}$. Po definiciji lahko preverimo, da je inducirana preslikava injektivna in surjektivna, kar pomeni, da dobimo izomorfizem. □

Trditev 4.13

Naj bo K kolobar ter ${}_KM$ levi modul. Sledi, da je

$$\mathrm{Hom}_K(K, M) = \{\varphi : K \to M, \varphi(x) = xm \mid m \in M\} \cong {}_KM$$

Trditev 4.14. *Naj bo $\varphi : A \to B$ morfizem in obstaja $C \leq A$, da velja $\varphi(C) = 0$, potem obstaja induciran $\overline{\varphi}$, ki slika $\overline{\varphi} : A/C \to B$*

Naloga 4.15

Pokaži, da je ${}_KK$ je enostaven natanko tedaj, ko je K obseg.

Rešitev. Naj bo $\varphi \in \mathrm{End}_K(K, K)$ poljuben. Vemo, da so vsi podmoduli realizirani kot jedra. Če je K obseg in φ slika neničelen element v 0, potem slika vse elemente v 0, saj slika enko v 0 (obrnljivost). Če nima podmodulov, potem je jedro vsakega endomorfizma bodisi cel modul, bodisi trivialen modul. Sledi, da je vsaka preslikava bodisi trivialna, bodisi avtomorfizem. Potem so tudi vsi endomorfizmi $\varphi_a(x) = ax$ ter $\psi_a(x) = xa$ avtomorfizmi, kar pomeni, da je 1 v sliki, kar implicira obrljivost a. □

Trditev 4.16

Naj bo N podmodul K-modula M. Potem obstaja $\varphi : M \to M$, za katerega velja $\ker(\varphi) = N$