UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Jaka Strmčnik

Struktura končno razsežnih algeber

Delo diplomskega seminarja

Mentor: prof. dr. Matej Brešar

Ljubljana, 2020

Kazalo

Struktura končno razsežnih algeber

Povzetek

Besedilo obravnava osnovne vrste kolobarjev, kot so na primer enostavni kolobarji, prakolobarji, polprakolobarji, itd. Sproti se rezultate analogno prilagaja za algebre, saj je glavni cilj besedila dokazati Wedderburnov strukturni izrek za končno razsežne algebre. Precejšen poudarek je na pojmu modula. Potreben je tako za dokaze pomembnih rezultatov, kot tudi za vpeljavo pojma primitivnega kolobarja, ki je ključen pri formulaciji Jacobsonovega izreka o gostoti, na katerem sloni dokaz Wedderburnovega strukturnega izreka.

Structure of Finite Dimensional Algebras

Abstract

This work deals with basic types of rings, such as simple rings, prime and semiprime rings, etc. Along the way, the results are being adjusted to hold also for algebras, since the main goal of the thesis is to prove Wedderburn's structure theorem for finite dimensional algebras. The concept of a module is emphasised in the text. It is often used when proving some of the important results, and, moreover it plays a key role in introducing the notion of a primitive ring. The latter is used in the formulation of Jacobson Density Theorem, which provides the neccessary tool to prove Wedderburn's structure theorem.

Math. Subj. Class. (2010): 16D10, 16D60, 16K20

Ključne besede: Wedderburnov strukturni izrek, Jacobsonov izrek o gostoti, modul

Keywords: Wedderburn's structure theorem, Jacobson Density Theorem, module

1. Uvod

Kot pove že naslov, bodo v tem besedilu obravnavane končno razsežne algebre. Osredotočili se bomo na take s posebno lepimi lastnostmi, ki bodo povod za strukturni Wedderburnov izrek. Slednji igra centralno vlogo v diplomski nalogi. Zavoljo malce širšega spektra teorije v ozadju se bomo dokaza lotili preko modulov in Jacobsonovega izreka o gostoti, kar nas bo postopno pripeljalo do razumevanja uvodnih pojmov in rezultatov s tega področja algebre.

Preden pa se podamo na lov za še ne poznanim, se na kratko spomnimo nekaterih osnovnih pojmov s področja abstraktne algebre.

Definicija 1.1. Kolobar z enoto, v katerem je vsak element razen 0 obrnljiv, se imenuje *obseg*.

Opomba 1.2. V besedilu ne privzemamo, da ima kolobar vedno enoto, ampak ga smatramo kot abelovo grupo za seštevanje ter polgrupo za množenje.

Nedvomno lahko zelo hitro najdemo primere obsegov, ki jih srečujemo že celo življenje.

Primer 1.3. $\mathbb{Q}$ in $\mathbb{R}$ sta primera obsegov, saj lahko poiščemo multiplikativni inverz vsakega elementa, razen 0. Po drugi strani $\mathbb{Z}$ ni obseg, saj sta za množenje obrnljiva le elementa $+1$ in -1. $\diamondsuit$

Naslednja definicija je večini bralcev zagotovo že poznana, a je v tem besedilu ključnega pomena, zato ponovimo tudi to.

Definicija 1.4. Naj bo K kolobar. Podgrupa za seštevanje L se imenuje *levi ideal* kolobarja K, če velja $k \cdot u \in L$ za vse $k \in K, u \in L$. Podgrupa za seštevanje D se imenuje *desni ideal* kolobarja K, če velja $u \cdot k \in D$ za vse $k \in K, u \in D$. Če je podmnožica kolobarja tako levi kot tudi desni ideal, ji pravimo preprosto *ideal*.

Primer 1.5. Najpreprostejši primer ideala so ideali kolobarja celih števil. Ker je kolobar $\mathbb{Z}$ komutativen, ne razlikujemo med levimi in desnimi ideali, zato jim pravimo kar ideali. Ti so natanko podgrupe za seštevanje oblike $n\mathbb{Z}$, kjer je $n \in \mathbb{N}$. Z drugimi besedami so to večkratniki celih števil. Očitno je, da so ideali, zanimivo pa je, kot bralec verjetno že ve, da so to edini ideali kolobarja $\mathbb{Z}$ ([2, primer 4.23]). $\diamondsuit$

Nadaljujmo s še eno ponovitveno definicijo, ki je prav tako za nadaljevanje besedila izjemno pomembna.

Definicija 1.6. Kolobar K se imenuje *enostaven*, če je $K^2 \neq 0$ in če sta 0 in K njegova edina ideala.

V zgornji definiciji $K^2 \neq 0$ pomeni, da obstajata taka $k_1, k_2 \in K$, da velja $k_1 k_2 \neq 0$. V kolobarjih z enoto je to očitno (za k_1, k_2 vzamemo kar enoto), za splošne kolobarje, ki pa so le polgrupe za množenje, to ne velja nujno.

Primer 1.7. Vsak obseg je enostaven kolobar. Res, naj bo K obseg. Ker vsebuje enoto, velja $K^2 \neq 0$. Naj bo $I \neq 0$ ideal. Naj bo $k_1 \in I$ neničeln. Sledi $k_1 k_2 \in I$ za vsak $k_2 \in K$, torej $k_1 k_1^{-1} = 1 \in I$ (inverz elementa k_1 seveda obstaja, saj je neničeln, K pa je obseg). Ko pa je v idealu enkrat enota, je v idealu vse, saj velja $k = k \cdot 1 \in I$. Od tod potem sledi $I = K$. $\diamondsuit$

S tem zaključimo obravnavo uvodnih nekaj ponovitvenih pojmov, ki jih bomo v nadaljevanju besedila pogosto srečevali. Zavoljo novih dogodivščin na poti k Wedderburnovemu strukturnemu izreku pa je čas, da pogledamo tudi nekaj novih definicij in primerov.

2. Prakolobarji in polprakolobarji

Začnimo s pojmom minimalnega ideala, ki ga bomo v besedilu še večkrat srečali.

Definicija 2.1. Levi ideal L kolobarja K se imenuje *minimalen levi ideal*, če velja $L \neq 0$ in če je vsak neničeln levi ideal L', vsebovan v L, enak L. Z drugimi besedami, L je minimalen med levimi ideali glede na inkluzijo.

Opomba 2.2. Analogno bi lahko definirali tudi desni minimalen ideal.

Da se ne bi preveč ustrašili abstraktnosti definicije, si poglejmo že znan primer.

Primer 2.3. Vzemimo spet kolobar celih števil. Kot že vemo, so njegovi edini ideali oblike $n\mathbb{Z}$, za $n \in \mathbb{N}$. Ali je kateri izmed njih minimalen? Vidimo, da ne, saj bi v primeru pritrdilnega odgovora na zastavljeno vprašanje moral obstajati minimalni element med $n\mathbb{Z}$ glede na inkluzijo. V tem primeru bi za neki $n \in \mathbb{N}$ veljalo, da ne obstaja tak $m \in \mathbb{N}$, različen od n, da bi $n\mathbb{Z}$ vseboval $m\mathbb{Z}$. To pa očitno ni res, saj $n\mathbb{Z}$ vedno vsebuje, na primer, $2n\mathbb{Z}$, torej kolobar celih števil nima minimalnega kolobarja. $\diamondsuit$

V nadaljevanju bomo kar nekaj pomembnih rezultatov posvetili algebram, zato je naslednji primer na mestu.

Primer 2.4. Vsaka neničelna končno razsežna algebra vsebuje minimalen levi ideal. Enostavno vzamemo levi ideal najmanjše dimenzije (če kak drug ne obstaja, zadostuje vzeti tudi algebro samo). Naj bo I tak levi ideal algebre A. Če bi potem obstajal še kak drug neničeln levi ideal J te iste dimenzije, vsebovan v I, potem, kot bralec verjetno že ve, sledi $J = I$. $\diamondsuit$

K minimalnim idealom se bomo še vrnili, pred tem pa si poglejmo še eno zanimivo definicijo.

Definicija 2.5. Ideal I kolobarja K se imenuje *nilpotenten ideal*, če obstaja tak $n \in \mathbb{N}$, da velja $I^n = 0$.

Definicija je sama po sebi dokaj intuitivna (sklepamo namreč iz definicije nilpotentnega elementa). Kljub temu je vredno omeniti, da lastnost $I^n = 0$ pomeni, da so vsi produkti n elementov kolobarja ničelni. Kakor bi bralec, vešč linearne algebre, verjetno že pomislil, lahko najpreglednejši primer najdemo pri matrikah.

Primer 2.6. Naj bo K kolobar vseh zgornjetrikotnih $n \times n$ matrik nad obsegom. Naj bo N množica strogo zgornjetrikotnih $n \times n$ matrik v K, torej takšnih, ki imajo tako pod, kakor tudi na diagonali same ničle. Hitro lahko preverimo, da je potem N ideal v K. Še več, N je nilpotenten ideal, saj velja $N^n = 0$. $\diamondsuit$

Prišli smo do dveh zanimivih definicij v svetu kolobarjev. Za osrednji izrek sta zelo pomembni, kot pa bomo videli, sta ti vrsti kolobarjev zanimivi tudi sami po sebi.

Definicija 2.7. Kolobar K se imenuje *prakolobar*, če zadostuje naslednjim ekvivalentnim pogojem:

- Če za $a, b \in K$ velja $aKb = 0$, potem velja $a = 0$ ali $b = 0$.
- Če za njegova ideala I in J velja $IJ = 0$, potem velja $I = 0$ ali $J = 0$.
- Če za njegova leva ideala I in J velja $IJ = 0$, potem veljai $I = 0$ ali $J = 0$.
- Če za njegova desna ideala I in J velja $IJ = 0$, potem velja $I = 0$ ali $J = 0$.

Opomba 2.8. $IJ = 0$ pomeni, da je produkt idealov ničeln, torej, da je $ab = 0$ za vsaka $a \in I, b \in J$.

Preden navedemo nekaj primerov, je treba ekvivalenco seveda dokazati. Dokaz ni zahteven, a pomaga, da se zgornje definicije bralcu bolje vtisnejo v kožo.

Dokaz. Sledimo [1, Lemma 2.17]. Denimo, da velja prva točka (gledano od zgoraj navzdol). Pokažimo, da sledi tretja. Predpostavimo $IJ = 0$, kjer sta I, J leva ideala kolobarja K. Potem velja tudi $IKJ = I(KJ) = 0$, saj je $KJ \subseteq J$. Ker lahko K z leve pomnožimo s poljubnim elementom levega ideala I, z desne s poljubnim elementom levega ideala J, in dobimo vedno ničelni rezultat, po prvi točki sledi, da je $I = 0$ ali $J = 0$.

Podobno dokažemo, da prva točka implicira četrto. Ker je vsak ideal tudi desni in levi ideal, očitno tretja in četrta točka implicirata drugo.

Za konec pokažimo še, da druga točka implicira prvo. Denimo, da sta $a, b \in K$ taka, da velja $aKb = 0$. Množici KaK in KbK sta očitno ideala v K. Njun produkt, $KaKKbK = K(aKKb)K$, je po predpostavki ničeln (velja asociativnost množenja in $KK \subseteq K$). Ker smo predpostavili drugo točko, od tod sledi, da je eden izmed omenjenih idealov ničeln. Denimo $KaK = 0$. To lahko razpišemo kot $KaK = Ka \cdot K = K \cdot aK = 0$. Ka in aK sta torej očitno ideala in iz zgornjega razpisa vidimo, da če na produktu idealov ponovno uporabimo drugo točko iz definicije 2.7, dobimo $Ka = aK = 0$. Če je K kolobar z enoto, smo na tem mestu končali, saj od tod jasno sledi $a = 0$. V kolikor ne, uporabimo dejstvo, da je $\mathbb{Z}a$ očitno ideal kolobarja K. Prav tako zaradi $aK = 0$ velja $\mathbb{Z}a \cdot K = 0$. S ponovnim sklicevanjem na drugo točko definicije 2.7 sledi $\mathbb{Z}a = 0$ in posledično $a = 0$. $\square$

Opomba 2.9. V zgornjem dokazu sta se pojavili množici, označeni s KaK in KbK, kjer sta $a, b \in K$. Z njima seveda označujemo produkta levih idealov Ka in K, oziroma, Kb in K. Prav tako bi lahko ti dve množici obravnavali kot produkta desnih idealov K in aK, oziroma K in bK. Množici KaK in KbK sta torej res (obojestranska) ideala.

Z malo modifikacije lahko definiramo še širši razred kolobarjev.

Definicija 2.10. Kolobar K se imenuje *polprakolobar*, če zadostuje naslednjim ekvivalentnim pogojem:

- Če za $a \in K$ velja $aKa = 0$, potem velja $a = 0$.
- Če za njegov ideal I velja $I^2 = 0$, potem velja $I = 0$.
- Če za njegov levi ideal I velja $I^2 = 0$, potem velja $I = 0$.
- Če za njegov desni ideal I velja $I^2 = 0$, potem velja $I = 0$.
- K nima neničelnih nilpotentnih idealov.

Dokaz. Dokaz ekvivalence prvih štirih točk je zelo podoben dokazu prejšnje ekvivalence o prakolobarjih, zato ga opustimo. Pokažemo še ekvivalenco med četrto in peto točko. Peta točka očitno po definiciji nilpotentnega ideala implicira četrto točko. Obratno, če je I tak ideal kolobarja K, da velja $I^n = 0$ za neko naravno število n, potem očitno drži $(I^{n-1})^2 = 0$. Po četrti točki od tod sledi $I^{n-1} = 0$. Postopek induktivno ponavljamo in dobimo $I = 0$. $\square$

Očitno so vsi prakolobarji tudi polprakolobarji. Prav tako so $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ očitni primeri prakolobarjev. Res, če vzamemo za K katerega koli izmed njih in privzamemo, da velja $aKb = 0$ za neka $a, b \in K$, potem sledi, da je tudi $ab = 0$ (vsi izmed naštetih kolobarjev namreč vsebujejo enoto). Ko pa vidimo takšno enakost v enem izmed teh kokobarjev, že od srednje šole naprej nemudoma sklenemo $a = 0$ ali $b = 0$. Slednja lastnost v kolobarjih ni trivialna, tako da jo posebej definirajmo.

Definicija 2.11. Naj bo K kolobar. Naj bo $x \in K$ različen od nič in naj obstaja tak neničeln $y \in K$, da velja $xy = 0$ ali $yx = 0$. Tedaj x imenujemo *delitelj niča.* Če kolobar K nima takega elementa, torej če za vsaka $x, y \in K$ iz $xy = 0$ sledi $x = 0$ ali $y = 0$, se K imenuje *kolobar brez deliteljev niča.*

Kot zanimivost lahko tako vpeljemo naslednjo trditev.

Trditev 2.12. *Komutativen kolobar je prakolobar natanko tedaj, ko nima deliteljev niča.*

Dokaz. Premisliti je potrebno, da v komutativnem kolobarju K za poljubna $a, b \in K$ $ab = 0$ implicira $aKb = 0$. Res, $aKb = abK$ in z upoštevanjem $ab = 0$ sledi $aKb = 0$. Zdaj je dokaz v obe strani popolnoma trivialen.

Denimo, da je K prakolobar. Naj velja $ab = 0$ za neka $a, b \in K$. Tedaj po zgornjem razmisleku velja tudi $aKb = 0$. Od tod pa po definiciji prakolobarja sledi $a = 0$ ali $b = 0$, torej K res nima deliteljev niča.

Obratno, naj bo K kolobar brez deliteljev niča in naj velja $aKb = 0$ za $a, b \in K$. To pomeni $a(kb) = 0$ za vse $k \in K$. Velja torej $a = 0$ ali $kb = 0$. V prvem primeru smo zaključili, v drugem ponovno uporabimo dejstvo, da K nima deliteljev niča, od koder zaključimo $k = 0$ ali $b = 0$. Ker je bil $k \in K$ poljuben, lahko izberemo neničelnega in potem velja $b = 0$. $\square$

Podobno naslednja trditev porodi kriterij za prepoznavanje polprakolobarjev v komutativnih kolobarjih.

Trditev 2.13. *Komutativen kolobar je polprakolobar natanko tedaj, ko nima neničelnih nilpotentnih elementov.*

Dokaz. Če v kolobarju ni neničelnih nilpotentnih elementov, potem lahko za vsako naravno število n in za vsak neničeln ideal I, v I^n najdemo neničelne elemente (vzamemo lahko kar n-to potenco kateregakoli neničelnega elementa v I). Torej je kolobar po peti točki definicije polprakolobar. Obratno, naj bo K polprakolobar in $a \in K$ tak, da velja $a^n = 0$. Tedaj je aK ideal v K in velja $(aK)^n = a^n K^n = 0$. Sledi $aK = 0$ in posledično tudi $aKa = 0$. Ker pa je K po predpostavki polprakolobar, sledi $a = 0$. $\square$

Povežimo zdaj že poznan pojem enostavnega kolobarja z novima definicijama prakolobarja in polprakolobarja. Očitno je vsak enostaven kolobar prakolobar in posledično tudi polprakolobar. Res, če sta 0 in K edina ideala kolobarja K, je na primer druga točka iz definicije 2.7 izpolnjena, saj smo v definiciji enostavnega kolobarja predpostavili $K^2 \neq 0$. Obratno seveda ne drži. Kolobar celih števil je primer komutativnega kolobarja brez deliteljev niča, ki je po trditvi 2.12 prakolobar. Kljub temu pa $\mathbb{Z}$ ni enostaven kolobar, saj vsebuje neničelne ideale ($n\mathbb{Z}, n \in \mathbb{N}$).

Pred nadaljevanjem pa si poglejmo še primer polprakolobarja, ki ni prakolobar.

Primer 2.14. Kolobar zveznih funkcij na intervalu, $C[a, b]$, kjer sta operaciji seštevanje in množenje po točkah, je polprakolobar, ki ni prakolobar. To lahko premislimo z uporabo zgornjih trditev o polprakolobarjih in prakolobarjih. Vidimo namreč, da je komutativen kolobar polprakolobar in ni prakolobar, če nima neničelnih nilpotentnih elementov, a ima delitelje niča. Premislimo, da to velja za $C[a, b]$. Očitno lahko najdemo taki neničelni funkciji $f, g \in C[a, b]$, da velja $fg = 0$. Za f vzamemo, na primer, funkcijo, ki je ničelna na nekem podintervalu intervala $[a, b]$, za g pa funkcijo, ki je ničelna na komplementu tega podintervala v $[a, b]$. Poiskali smo torej primer neničelnih funkcij, katerih produkt je ničeln.

Denimo sedaj, da ima kolobar $C[a, b]$ nilpotenten element f. Tedaj obstaja tak $n \in \mathbb{N}$, da velja $f^n = (f(x))^n = 0$, za vsak $x \in [a, b]$. Od tod potem sledi $f(x) = 0$ za vsak $x \in [a, b]$. $\diamondsuit$

Pozneje nas bo zanimala struktura direktnih produktov prakolobarjev in polprakolobarjev. Pojem direktni produkt se seveda nanaša na konstrukcijo, ki je bralcu verjetno že poznana, kjer seštevanje in množenje definiramo po komponentah.

Izkaže se, da produkt prakolobarjev ni prakolobar, medtem ko je produkt polprakolobarjev prav tako polprakolobar. Res, če vzamemo K_1, K_2 prakolobarja in pogledamo ideala $I := 0 \times K_2$ in $J := K_1 \times 0$ kot ideala kolobarja $K_1 \times K_2$, vidimo, da velja $IJ = 0$, a sta kljub temu oba ideala neničelna.

Po drugi strani, če sta K_1, K_2 polprakolobarja, lahko uporabimo, na primer, prvo izmed ekvivalentnih definicij polprakolobarja; naj bo $a = (a_1, a_2) \in K_1 \times K_2$ in naj velja $a(K_1 \times K_2)a = 0$. To pomeni, da je $(a_1K_1a_1, a_2K_2a_2) = 0$. Ker sta K_1 in K_2 polprakolobarja, velja $a_1 = a_2 = 0$ in posledično $a = 0$. Torej je tudi $K_1 \times K_2$ polprakolobar.

3. Wedderburnov strukturni izrek

Zaenkrat smo se ukvarjali le s kolobarji, zdaj pa bo več govora o končno razsežnih algebrah, ki so pravzaprav glavna tema tega besedila. Povsem analogno kot za kolobarje lahko vse srečane pojme definiramo za algebre. Gre enostavno za to, da na algebro gledamo kot na kolobar, kar algebra seveda tudi je, in tako ima vse do zdaj povedano smisel tudi pri algebrah.

Definicija 3.1. Pravimo, da je algebra A *obseg*, če je vsak njen neničeln element obrnljiv.

Vprašanje na mestu bi bilo, kako definirati enostavno algebro. Ali imamo v definiciji v mislih ideale algebre, ki so tudi vektorski podprostori, ali zadostuje obravnavati ideale kolobarja? Krajši razmislek pokaže, da je vseeno. Denimo, da je algebra A enostavna v že poznanem smislu, torej kot kolobar. Ker ne vsebuje nobenega netrivialnega ideala kolobarja, očitno ne more vsebovati nobenega netrivialnega ideala algebre, za katerega dodatno zahtevamo, da je vektorski podprostor.

Obratno, če A ne vsebuje nobenega ideala algebre, ali lahko vsebuje kak ideal kolobarja? Denimo, da je I tak netrivialen ideal. Tedaj je AI ideal algebre A (je tudi vektorski podprostor, bralec lahko to zlahka preveri). Ker je A v tem smislu enostavna, velja bodisi $AI = 0$ bodisi $AI = A$. Ker je AI podmnožica I, lahko velja le $AI = 0$. Poglejmo si $J := \{x \in A; Ax = 0\}$. Tudi tokrat lahko bralec po definiciji preveri, da je J ideal algebre A. Ker v definiciji enostavnega kolobarja oziroma algebre predpostavimo $A^2 \neq 0$, mora veljati $J \neq A$, torej $J = 0$ (A je namreč enostavna). Upoštevajoč $AI = 0$ potem sledi $I = 0$.

Tako se izkaže, da pogoj $A^2 \neq 0$, kjer je A algebra, zagotavlja, da je vseeno, ali v definiciji enostavne algebre obravnavamo ideale le kot aditivne podgrupe ali pa tudi kot vektorske podprostore.

Zelo podoben razmislek lahko naredimo za definicijo praalgebre. Če algebro A obravnavamo kot prakolobar, je očitno tudi vsak produkt neničelnih idealov algebre, ki so tudi vektorski prostori, prav tako neničeln. Denimo obratno, torej da je praalgebra definirana s pogojem, ki omejuje zgolj ideale algebre, ki so tudi vektorski podprostori. Vzemimo potem taka I, J ideala algebre A kot ideala kolobarja, da velja $IJ = 0$. Tedaj je očitno tudi produkt linearnih ogrinjač množic I in J ničeln. Tidve množici pa sta ideala algebre A, zato potem velja, da je edna izmed njiju ničelna. Če pa je linearna ogrinjača neke množice ničelna, je ničelna tudi množica sama, zato sledi $I = 0$ ali $J = 0$.

Podobno lahko vidimo, da je tudi pri definiciji polpraalgebre vseeno, ali obravnavamo ideale kot vektorske podprostore ali le kot ideale kolobarja.

S tem smo se že skoraj prebili do formulacije strukturnega izreka, še pred tem pa se spomnimo kolobarja $n \times n$ matrik nad kolobarjem K. Označimo ga z $M_n(K)$. Podobno, če je A algebra, je $M_n(A)$ algebra vseh $n \times n$ matrik nad A. V nadaljevanju bomo $n \times n$ matriko pogosto označili z (a_{ij}), kjer i in j tečeta od 1 do n.

Izkaže se, da če je K obseg, potem $M_n(K)$ dobi prav posebno lastnost.

Trditev 3.2. *Če je K obseg, je $M_n(K)$ enostaven kolobar. Analogno, če je algebra A obseg, je $M_n(A)$ enostavna algebra.*

Preden se lotimo dokaza, naredimo krajši premislek. Naj bo $M_n(K)$ kolobar nad poljubnim kolobarjem z enoto, K. Naj bo $E_{ij} \in M_n(K)$ matrika, ki ima na mestu (i, j) enico in na vseh ostalih ničlo. Z aE_{ij} označimo matriko, ki ima na (i, j)-tem mestu neki $a \in K$. S kratkim premislekom na primeru $n = 2$ lahko vidimo, da velja naslednja enakost: naj bo $A = (a_{ij}) \in M_n(K)$, potem velja $E_{ij}AE_{kl} = a_{jk}E_{il}$ za vse $1 \leq i, j, k, l \leq n$.

Dokaz trditve 3.2. Dokazujemo, da sta 0 in $M_n(K)$ edina ideala kolobarja $M_n(K)$. Naj bo I njegov neničeln ideal. Obstajajo torej taki $(a_{ij}) \in I$ in $1 \leq j, k \leq n$, da je $a_{jk} \neq 0$. Po razmisleku zgoraj velja $E_{ij}(a_{ij})E_{kl} = a_{jk}E_{il} \in I$ za vse i, l. Sledi $(da_{jk}^{-1})E_{ii} \cdot a_{jk}E_{il} = dE_{il} \in I$ za vse $d \in K, 1 \leq i, l \leq n$. Posledično je $I = M_n(K)$. □

Zdaj smo dovolj oboroženi za formulacijo Wedderburnovega strukturnega izreka o končno razsežnih algebrah.

Izrek 3.3 (Wedderburnov strukturni izrek)**.** *Naj bo A končno razsežna neničelna F-algebra, kjer je F polje. Naslednje trditve so ekvivalentne:*

(1) *A je praalgebra.*
(2) *A je enostavna algebra.*
(3) *Obstajata taka $n \in \mathbb{N}$ in F-algebra D, ki je obseg, da velja $A \cong M_n(D)$.*

Premislimo najprej, kako je izrek v eno smer takorekoč trivialen. Potujmo po točkah od spodaj navzgor. Iz tretje v drugo točko smo glavni razmislek že naredili tik pred navedbo izreka. Če je D algebra, ki je obseg, potem vemo, da je $M_n(D)$ enostavna algebra. Ker ji je A izomorfna, je tudi A enostavna algebra.

Iz druge v prvo točko pa tudi pridemo praktično po definiciji praalgebre (oziroma prakolobarja). Ker je A enostavna, in če sta I, J njena ideala (ki sta lahko le 0 ali pa A), potem očitno iz $IJ = 0$ sledi, da je vsaj eden od njiju enak 0 (za enostavno algebro A po definiciji velja $A^2 \neq 0$). To pa pomeni, da je A praalgebra.

V obratno smer pa je izrek pravzaprav zelo presenetljiv; vsako enostavno končno razsežno algebro lahko namreč predstavimo z algebro matrik. Poglejmo si primer tega dognanja preko še enega pomembnega izreka, ki ga je bralec najverjetneje že srečal.

Izrek 3.4 (Frobenius)**.** *Končno razsežna* $\mathbb{R}$*-algebra* A *(algebra nad poljem realnih števil), ki je obseg, je izomorfna* $\mathbb{R}$, $\mathbb{C}$ *ali* $\mathbb{H}$.

Dokaz izpustimo, bralec pa ga lahko najde v [1, Theorem 1.4]. Z uporabo Wedderburnovega izreka lahko zdaj pridemo do naslednjega rezultata.

Posledica 3.5. *Vsaka končno razsežna enostavna* $\mathbb{R}$*-algebra* A *je izomorfna* $M_n(\mathbb{R})$, $M_n(\mathbb{C})$ *ali* $M_n(\mathbb{H})$ *za neki* $n \in \mathbb{N}$

Dokaz. Naj bo A končno razsežna enostavna $\mathbb{R}$-algebra. Po Wedderburnovem izreku je izomorfna algebri matrik nad neko končno razsežno $\mathbb{R}$-algebro D, ki je obseg. Slednja je po Frobeniusovem izreku izomorfna $\mathbb{R}$, $\mathbb{C}$ ali $\mathbb{H}$. Algebra A je torej izomorfna $M_n(\mathbb{R})$, $M_n(\mathbb{C})$ ali $M_n(\mathbb{H})$ za neki $n \in \mathbb{N}$. □

Dokaz Wedderburnovega izreka v obratno smer je presenetljivosti primerno tudi zahtevnejši. Lotili se ga bomo po poti, ki bo predstavljena v kratkem. Pred tem pa še en Wedderburnov izrek, ki karakterizira končno razsežne polpraalgebre.

Izrek 3.6 (Wedderburn)**.** *Naj bo* A *neničelna končno razsežna* F*-algebra. Potem je* A *polpraalgebra natanko tedaj, ko obstajajo taki* $n_1, \ldots, n_r \in \mathbb{N}$ *in* F*-algebre, ki so obsegi,* $D_1, \ldots, D_r$*, da velja* $A \cong M_{n_1}(D_1) \times \ldots \times M_{n_r}(D_r)$.

Tudi ta izrek je v obratni smeri ekvivalence popolnoma trivialen, saj so, kot smo že premislili, vse algebre matrik nad algebrami, ki so obsegi, enostavne, in kot že vemo iz prvega Wedderburnovega izreka, to implicira, da so praalgebre in posledično tudi poplpraalgebre. Prav tako z že znanim premislekom sklenemo, da je tudi direktni produkt algeber matrik (polpraalgeber v tem primeru) polpraalgebra, od koder sledi, da je tudi algebra A iz izreka, ki je izomorfna omenjenemu direktnemu produktu, polpraalgebra.

Povsem drugačna zgodba pa je ponovno v drugi smeri ekvivalence, torej, da je vsaka končno razsežna polpraalgebra v bistvu direktni produkt algeber matrik. Ponovno, kakor je tudi sam rezultat bolj presenetljiv, je tudi dokaz ustrezno bolj zapleten. Ker pa bi nas z vidika tega besedila malce odvrnil od bistva, ga izpustimo in se raje osredotočimo na strukturni izrek. Zainteresirani bralec lahko dokaz zgornjega izreka o polpraalgebrah najde v [1, Theorem 2.64].

Poglejmo si primer, ko nam ta izrek ne pomaga.

Primer 3.7. Izrek torej ne velja za že obravnavani primer, ko je A algebra zgornjetrikotnih $n \times n$ matrik, kjer obstaja nilpotentni ideal, namreč množica strogo zgornjetrikotnih matrik. Tako vidimo, da A ni polpraalgebra in ji zato ne moremo pripisati enostavne strukture, ki jo ponuja izrek. ♢

V naslednjih razdelkih se bomo srečali s teorijo, potrebno za dokaz strukturnega izreka.

4. Moduli in vektorski prostori nad obsegom

Preostanek besedila bomo posvetili konstrukciji celotnega dokaza strukturnega izreka, česar se bomo lotili na zanimiv način. Začnemo z vpeljavo enega izmed pomembnejših konceptov algebre, modula.

Definicija 4.1. Naj bo K kolobar. *Levi K-modul* je aditivna grupa M skupaj s preslikavo iz $K \times M$ v M, $(k, m) \mapsto km$, tako da za vse $k, s \in K$ in vse $m, n \in M$ velja:

- $(k + s)m = km + sm$,
- $k(m + n) = km + kn$,
- $k(sm) = (ks)m$.

Dodatno, če ima K enoto in velja

- $1m = m$

za vse $m \in M$, pravimo, da je M *enotski levi K-modul*.

Podobno lahko definiramo tudi desni K-modul, le da moramo pogoje iz definicije primerno spremeniti, saj tokrat govorimo o preslikavi iz $K \times M$ v M, podani s predpisom $(k, m) \mapsto mk$. V kolikor je K komutativen kolobar, postane vsak levi K-modul desni K-modul, če definiramo $mk := km$ za vse $k \in K, m \in M$.

Seveda je mogoče vse rezultate analogno prilagoditi, tako da veljajo tako za desne, kakor tudi za leve K-module. V nadaljevanju besedila bomo zavoljo boljše preglednosti govorili le o K-modulu, s čimer mislimo levi K-modul.

Bralcu, ki se z moduli še ni srečal, se verjetno zdi definicija zelo podobna tisti, ki jo je srečal pri linearni algebri. Gre seveda za skorajda popoln analog definiciji vektorskega prostora nad poljem, le da pri modulih vlogo polja prevzame poljuben kolobar. Vidimo torej, da je vektorski prostor le poseben primer K-modula, kjer je K polje.

Primer 4.2. Vsak vektorski prostor nad poljem F je F-modul. $\diamondsuit$

Podobno se koncept K-modula skriva še v enem osnovnem primeru.

Primer 4.3. Če vzamemo za kolobar K cela števila in za M poljubno aditivno grupo, postane M enotski $\mathbb{Z}$-modul, kjer ima preslikava $(n, m) \mapsto nm, m \in M, n \in \mathbb{Z}$ običajen pomen. Za $n \geq 0$ to pomeni

$$(n, m) \mapsto nm = m + m + \cdots + m,$$

kjer smo element m sešteli n-krat. Če je $n < 0$, dobimo

$$(n, m) \mapsto nm = (-m) + (-m) + \cdots + (-m),$$

kjer smo tokrat element $-m$ prišteli $|n|$-krat. $\diamondsuit$

Zavoljo uporabe v nadaljevanju besedila navedimo še en primer K-modula.

Primer 4.4. Naj bo K kolobar in I njegov levi ideal. Vidimo, da je I K-modul s preslikavo $(k, u) \mapsto ku$, $k \in K, u \in I$, ki je kar običajen produkt v kolobarju. Očitno so izpolnjeni vsi pogoji iz definicije K-modula. Tako posebej velja, da je K sam K-modul. $\diamondsuit$

Preko krajših dokazov in premislekov bo koncept modula bralcu kmalu postal domač, zato naj se nikar preveč ne ustraši, če se zdi stvar zenkrat še nekoliko neobičajna. Po uvodnih primerih nadaljujemo s še nekaj definicijami, ki nam bodo prav prišle pozneje v besedilu.

Definicija 4.5. Množici

$$\mathrm{ann}_K M := \{k \in K; kM = 0\}$$

pravimo *anihilator* K-modula M. Modulu, ki ima trivialen anihilator (vsebuje samo $0 \in K$), pravimo *zvest* modul.

Pogoj $kM = 0$ v zgornji definiciji seveda pomeni, da je km ničeln za vse $m \in M$.

Vidimo lahko, da je $\mathrm{ann}_K M$ levi ideal kolobarja K. Očitno je podgrupa za seštevanje, prav tako pa velja tudi $xkM = 0$, če je $kM = 0$ za $x, k \in K$. To dejstvo bomo lahko v prihodnjih poglavjih pridoma uporabljali.

Naslednja definicija poda še dodaten argument, ki govori v prid podobnosti med že poznanimi algebraičnimi strukturami ter moduli.

Definicija 4.6. Naj bo M K-modul. Njegova podmnožica L se imenuje *podmodul* modula M, če je podgrupa za seštevanje in če velja $kl \in L$ za vsaka $k \in K, l \in L$.

Nedvomno ima vsak modul vsaj dva podmodula, 0 in samega sebe. Očitno je, da izpolnjujeta kriterije zgornje definicije. Vsekakor pa so, kot ponavadi, bolj zanimivi netrivialni podmoduli.

Primer 4.7. Ponovno se spomnimo, da lahko aditivno grupo obravnavamo kot $\mathbb{Z}$-modul. Tedaj so njegovi podmoduli ravno podgrupe. Res, podgrupe očitno izpolnjujejo prvi pogoj v definiciji podmodula, drugega pa skorajda enako očitno, saj so zaprte za seštevanje, torej ne glede na to, kolikokrat določen element iz podgrupe prištejemo nevtralnemu elementu, rezultat še vedno leži v tej isti podgrupi. $\diamondsuit$

Primer 4.8. Kot že vemo, lahko gledamo na kolobarje kot module. Glejmo torej na kolobar K kot na K-modul. Kaj so njegovi podmoduli? Da odgovorimo na to vprašanje, lahko le slepo sledimo zgornji definiciji podmodula in na ustreznih mestih M nadomestimo s kolobarjem K. Izkaže se, da smo pridelali definicijo levega ideala. Podmoduli K-modula K so torej natanko njegovi levi ideali. $\diamondsuit$

Sedaj pa se posvetimo tistim »dolgočasnim« modulom, ki nimajo netrivialnih podmodulov. Resda ne gre za prav razburljivo lastnost s tega zornega kota, a če se spomnimo enostavnih kolobarjev, se nam lahko dozdeva, da so taki moduli še kako zanimivi.

Definicija 4.9. Naj bo K kolobar. K-modul M se imenuje *enostaven*, če velja $KM \neq 0$ in sta 0 in M njegova edina podmodula.

Pred navedbo kakšnega primera si poglejmo zelo lepo lastnost enostavnih modulov.

Trditev 4.10. *Neničeln K-modul M je enostaven natanko tedaj, ko velja $M = Km$ za vsak neničeln $m \in M$.*

Z drugimi besedami, neničeln modul je enostaven natanko tedaj, ko je generiran z vsakim svojim neničelnim elementom.

Dokaz. Predpostavimo, da je K-modul M enostaven. Vzemimo neničeln $m \in M$ in si oglejmo Km. Trdimo, da je Km podmodul modula M. Očitno je podgrupa za seštevanje (predstavljamo si elemente kolobarja, ki imajo vsi nase pripet še element m, zato deluje seštevanje povsem nemoteno) in če pomnožimo katerikoli element kolobarja z elementom iz Km, leži rezultat ponovno v Km (uporabljamo besedo

»množiti«, čeprav gre za preslikavo v definiciji K-modula). Torej je Km res podmodul. Iz enostavnosti modula M sledi bodisi $Km = 0$ bodisi $Km = M$.

Na tej točki si poglejmo še eno podmnožico modula M, $N := \{m \in M; Km = 0\}$. Tudi ta množica je očitno podgrupa za seštevanje, prav tako ohranja množenje z elementom kolobarja z leve, torej je N podmodul M. Ponovno zaradi enostavnosti M velja $N = 0$ ali $N = M$, kjer nam dodatni pogoj za enostavnost, $KM \neq 0$, slednjo možnost ovrže. Sledi $N = 0$ in posledično Km ne more biti enak 0 za neničeln $m \in M$, zato velja $Km = M$.

Obratno, predpostavimo $M = Km$ za vsak $m \in M$. Denimo, da obstaja neničeln podmodul L modula M. Naj bo $l \in L$ neničeln. Po definiciji podmodula velja $Kl \subseteq L$ in $L \subseteq M$. Po predpostavki pa velja $Kl = M$, torej $M \subseteq L$ in $L \subseteq M$. Sledi $L = M$, oziroma podmodula M sta le M in 0. □

Primer 4.11. Govorili smo že o tem, da je vektorski prostor le poseben primer K-modula, kjer je K polje. Kdaj je torej vektorski prostor enostaven modul? Zgornja trditev nam pove, da natanko tedaj, ko lahko celoten vektorski prostor generiramo z enim samim neničelnim elementom. Verjetno se bralec ob tem spomni, da je v smislu vektorskih prostorov ta pogoj analogen konceptu premice. Res, neničeln vektorski prostor V nad K je enostaven K-modul natanko tedaj, ko velja $\dim_K V = 1$. Očitno lahko v nasprotnem primeru najdemo vsaj enodimenzionalen podprostor, ki pa je, kot že vemo, netrivialen podmodul. ♢

Če se spomnimo že omenjenih minimalnih idealov, lahko pridelamo še eno zanimivo trditev.

Trditev 4.12. *Naj bo K kolobar in naj bo L tak levi ideal v K, da velja $KL \neq 0$. Potem je L enostaven kot K-modul natanko tedaj, ko je L minimalen levi ideal v K.*

Dokaz. Naj bo torej L minimalen levi ideal. Naj bo $l \in L$ neničeln. Pokažimo, da velja $Kl = L$ (alternativna karakterizacija enostavnih modulov). Kl je očitno tudi sam levi ideal kolobarja K, vsebovan v L (po definiciji levega ideala). Ker je L minimalen, je bodisi $Kl = 0$, bodisi $Kl = L$. Oglejmo si sedaj množico

$$J := \{x \in L; Kx = 0\}.$$

Tudi ta množica je očitno levi ideal K, ki je vsebovan v L. Zaradi minimalnosti L ponovno velja $J = 0$ ali $J = L$. Drugo možnost tokrat izključuje predpostavka $KL \neq 0$, torej velja $J = 0$. Vidimo torej, da $Kl = 0$ velja le za $l = 0$, torej za neničeln $l \in L$ velja $Kl = L$. S tem smo dokazali, da je L enostaven kot K-modul.

Obratno, denimo, da je L enostaven K-modul. Naj bo J neničeln levi ideal kolobarja K, vsebovan v L. Kot že vemo, je J potem podmodul K-modula K, ki je vsebovan v L. Zato je J tudi podmodul K-modula L in zaradi enostavnosti L velja $J = L$. Sledi, da je L minimalen levi ideal kolobarja K. □

K enostavnim modulom se bomo v kratkem vrnili, zdaj pa se lotimo preslikav med moduli, ki pogosto, tako kot pri ostalih algebrskih strukturah, igrajo pomembno vlogo.

Definicija 4.13. Naj bosta M, N K-modula. Preslikava $\varphi : M \to N$ se imenuje *homomorfizem K-modulov*, če velja

$$\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2), \varphi(km_1) = k\varphi(m_1)$$

za vse $k \in K$ in $m_1, m_2 \in M$.

Kot bi bilo pričakovati, je jedro homomorfizma, torej $\ker\varphi = \{m \in M; \varphi(m) = 0\}$, podmodul modula M. Prav tako je slika homomorfizma, $\mathrm{im}\varphi = \{\varphi(m); m \in M\}$, podmodul modula N. Ti dve dejstvi sta z uporabo definicije homomorfizma očitni, a ju zavoljo uporabe v nadaljevanju premislimo. Kot že vemo, je $\ker\varphi$ aditivna podgrupa M in $\mathrm{im}\varphi$ aditivna podgrupa N. Če množimo element $m \in \ker\varphi$ z leve s $k \in K$ in izračunamo $\varphi(km)$, z uporabo lastnosti homomorfizma modulov dobimo

$$\varphi(km) = k\varphi(m) = 0.$$

Torej je $\ker\varphi$ res podmodul M. Podobno, če množimo $k \in K$ z $n \in \mathrm{im}\varphi$, velja

$$kn = k\varphi(m_1) = \varphi(km_1) \in im\varphi,$$

kjer smo upoštevali $n = \varphi(m_1)$ za $m_1 \in M$. Tako vidimo, da je tudi $\mathrm{im}\varphi$ podmodul N.

Na tem mestu se spomnimo kolobarja endomorfizmov, tokrat K-modula M. Označimo ga z $\mathrm{End}_K(M)$. Gre seveda za kolobar homomorfizmov iz M v M, kjer je seštevanje definirano po točkah, množenje pa je operacija kompozitum.

Za konec z moduli obarvanega razdelka si poglejmo še koncept linearne neodvisnosti. Kot bi bralec pričakoval, gre tudi tokrat za analog vektorskim prostorom.

Definicija 4.14. Podmnožica X K-modula M je *linearno neodvisna*, če za vse različne elemente $x_1, \ldots, x_n \in X$ in vse $k_1, \ldots, k_n \in K$, iz $k_1x_1 + \cdots + k_nx_n = 0$ sledi $k_i = 0$ za vse $1 \leq i \leq n$. Če X ni linearno neodvisna, potem pravimo, da je *linearno odvisna*.

Vidimo pa lahko, da je v primeru, ko M ni vektorski prostor nad poljem K, temveč je K le kolobar, lahko tudi množica z enim elementom linearno odvisna. Res, če govorimo o vektorskih prostorih nad poljem to seveda ni mogoče, saj iz predpostavke $kx_1 = 0$, kjer je x_1 neničeln, sledi $k = 0$ (lahko množimo na obeh straneh z inverzom elementa k). V primeru, ko obstoj inverza elementa k ni zagotovljen, pa seveda do tega zaključka ne moremo priti. Z drugimi besedami, če modul ni zvest, je že podmnožica z enim elementom linearno odvisna.

Vidimo torej, da bi do zaključkov v smislu obstoja baze in definicije dimenzije modula morali narediti še kar nekaj razmislekov in v procesu naleteli na marsikatero težavo. Kmalu pa bomo videli, da se je smiselno vprašati, kaj lahko povemo o enotskih O-modulih, kjer je O nekomutativen obseg (spomnimo se, za enotski O modul M velja tudi $1m = m$ za vse $m \in M$). Ker se bodo taki moduli v nadaljevanju pojavljali pogosto, jih posebej definirajmo.

Definicija 4.15. Naj bo O obseg. Enotski (levi) O-modul V se imenuje *(levi) vektorski prostor* nad O.

Opomba 4.16. Podobno kot pri modulih bomo tudi tu besedo »levi« spuščali, saj bomo v mislih vedno imeli levi vektorski prostor.

Vidimo, da se pri takih modulih, torej vektorskih prostorih nad obsegi, izognemo linearno odvisnim množicam z enim elementom, na primer. Še več, izkaže se, da ima vsak tak modul bazo. Tega dejstva ne bomo posebej dokazovali. Dokaz lahko bralec najde v [1, Theorem 3.27]). O bazi v smislu modula še nismo govorili, bralec pa si lahko predstavlja, da gre za analogno definicijo baze pri vektorskem prostoru nad poljem.

Definicija 4.17. Linearno neodvisna množica X je *baza* K-modula M, če generira M.

Primer 4.18. Seveda nima vsak modul baze (moral bi najprej vsebovati linearno neodvisno podmnožico, za kar smo videli, da v splošnem ne velja). Če je K enotski kolobar, je K, gledan kot K-modul, modul z bazo 1. Res, iz $k \cdot 1 = 0$ očitno sledi $k = 0$, torej je množica 1 linearno neodvisna. Da pa generira K, je prav tako očitno, saj velja $1 \cdot K = K$. $\diamondsuit$

Podobno lahko za vektorski prostor nad obsegom O definiramo pojme, kot so končna dimenzija, linearna kombinacija in linearna ogrinjača. Tudi pojem podprostora je v tem primeru popolnoma analogen podprostoru vektorskega prostora nad poljem. Gre enostavno za podmnožico, ki je zaprta za seštevanje in množenje z elementi iz O (podmodul ima v tem primeru seveda tudi svojo bazo, saj je sam enotski O-modul.). Ti pojmi za potrebe besedila niso tako pomembni, zato brez dokaza (dokaz je zelo podoben tistemu za vektorske prostore nad poljem) navedimo le še naslednji izrek, ki v bistvu povzema dejstvo, da se vektorski prostori nad obsegom obnašajo zelo podobno tistim nad poljem.

Izrek 4.19. *Naj bo M vektorski prostor nad obsegom. Vsaka linearno neodvisna podmnožica M je vsebovana v bazi M. Naj M vsebuje bazo z n elementi, kjer je $n \in \mathbb{N}$. Potem velja naslednje:*

- *Vsaka baza vektorskega prostora M ima n elementov.*
- *Če je U podmodul M, potem imajo njegove baze kvečjemu n elementov.*
- *Če ima podmodul U modula M bazo z n elementi, potem je $M = U$*

Dokaz izreka, kot rečeno, izpustimo, bralec pa ga lahko najde v [4, 185-187].

Kot omenjeno, nam bo krajši ovinek v smeri nekomutativnih obsegov in njihovih modulov prišel zelo prav v kratkem. Še preden pa nas pot pripelje nazaj do Wedderburnovega strukturnega izreka, moramo narediti nekaj dodatnih razmislekov.

5. Endomorfizmi in kolobar matrik

V tem razdelku sledimo [1, 61–63]. Kot bralec verjetno že ve, obstaja med kolobarjem endomorfizmov končno razsežnega vektorskega prostora V nad poljem F in kolobarjem kvadratnih matrik nad tem poljem izomorfizem. Velja torej

$$\mathrm{End}_F(V) \cong M_n(F),$$

kjer je n dimenzija vektorskega prostora V nad poljem F.

Spomnimo se, da smo kolobar, oziroma algebro $M_n(D)$, kjer je D algebra, ki je obseg, že srečali v Wedderburnovem strukturnem izreku. Če bi bila algebra D dodatno še komutativna, bi lahko končno razsežne enostavne algebre preko zgornjega izomorfizma identificirali tudi z algebro $\mathrm{End}_F(D)$. Ker pa to žal ni vedno res, se lahko vprašamo, če bi lahko podoben rezultat, kot je $\mathrm{End}_F(V) \cong M_n(F)$ izpeljali, namesto za polja in vektorske prostore nad poljem, za vektorske prostore nad nekomutativnim obsegom.

Zastavljeno vprašanje se zdi do neke mere zanimivo, a le, če si uspemo predstavljati, kako bi se endomorfizem obnašal, če bi ga z izomorfizmom transformirali v matriko. Pa poskusimo narediti točno to.

Naj bo M vektorski prostor nad nekomutativnim obsegom O. Konstruirajmo preslikavo

$$\varphi : \mathrm{End}_O(M) \to M_n(O),$$

kjer je n dimenzija M.

Naj bo množica $X := \{x_1, \dots, x_n\}$ baza za M (konec prejšnjega razdelka nam pove, da obstaja). Vzemimo $f \in \mathrm{End}_O(M)$. Sliko vsakega elementa iz M lahko zapišemo kot linearno kombinacijo baznih elementov M. Velja torej

$$f(x_j) = f_{1j}x_1 + \cdots + f_{nj}x_n,$$

za vse $j = 1, \dots, n$, kjer so $f_{ij} \in O$ za $i = 1, \dots, n$.

S pomočjo tega lahko konstruiramo preslikavo φ, ki vzame $f \in \mathrm{End}_O(M)$ in mu priredi element $M_n(O)$. Prirejena matrika v bazi X izgleda tako, da ima v j-tem stolpcu vektor $(f_{1j}, \dots, f_{nj})$ za vse $j = 1, \dots, n$. Z drugimi besedami, na (i, j)-tem mestu prirejene matrike leži element f_{ij}. Očitno je preslikava φ s tem predpisom dobro definirana, tako da preostane preveriti le še, da je izomorfizem.

Premislimo najprej za operacijo seštevanja, ki je seveda v $\mathrm{End}_O(M)$ definirana kot seštevanje po točkah. Izračunajmo torej $\varphi(f + g)$. Za $g \in \mathrm{End}_O(M)$ upoštevamo, da lahko podobno zapišemo $g(x_j) = \sum_{i=1}^n g_{ij}x_i$ za vse $j = 1, \dots, n$. V j-tem stolpcu $\varphi(f + g)$ dobimo vektor koeficientov pred baznimi vektorji pri izračunu $(f + g)(x_j)$ za vse $j = 1, \dots, n$. Iz definicije aditivne operacije v $\mathrm{End}_O(M)$ sledi

$$(f + g)(x_j) = f(x_j) + g(x_j) = \sum_{i=1}^n f_{ij}x_i + \sum_{i=1}^n g_{ij}x_i = \sum_{i=1}^n (f_{ij} + g_{ij})x_i.$$

Koeficienti razvoja $(f + g)(x_j)$ po bazi X so torej enaki vsoti koeficientov razvoja $f(x_j)$ in $g(x_j)$ za vse $j = 1, \dots, n$. Ker seštevanje v $M_n(O)$ poteka običajno, po posameznem vnosu v matriki, velja $\varphi(f + g) = \varphi(f) + \varphi(g)$ in φ je homomorfizem aditivnih grup (množenja še nismo preverjali).

Naprej, preverimo injektivnost. Tega dela se lotimo po poti dokazovanja trivialnosti jedra preslikave φ. Res, če velja $\varphi(f) = 0$, so vsi vnosi v matriki ničelni, kar pomeni, da so vsi koeficienti pri razvoju $f(x_j)$ po bazi X ničelni za vse $j = 1, \dots, n$. Z drugimi besedami, f vse bazne elemente in posledično vse elemente M slika v 0, od koder sledi $f = 0$. Trivialnost jedra nam zagotavlja injektivnost preslikave φ.

Preostane še premislek surjektivnosti. Naj bodo $f_{ij} \in O$ za $i = 1, \dots, n$, $j = 1, \dots, n$. Ali lahko poiščemo tak $f \in \mathrm{End}_O(M)$, da velja

$$\varphi(f) = (f_{ij}),$$

kjer je $(f_{ij}) \in M_n(O)$ matrika, ki ima na (i, j)-tem mestu element f_{ij}? Na drugačen način povedano, iščemo $f \in \mathrm{End}_O(M)$, za katerega velja $f(x_j) = \sum_{i=1}^n f_{ij}x_i$ za vse $j = 1, \dots, n$. Tak f pa očitno obstaja, saj ga prejšnja poved natanko definira. Element $\mathrm{End}_O(M)$ je namreč zaradi linearnosti natanko določen s slikami baznih elementov. Sledi torej, da je φ tudi surjektivna in je zato izomorfizem aditivnih grup $\mathrm{End}_O(M)$ in $M_n(O)$.

Poglejmo si zdaj, kaj preslikava φ naredi s produkti. Želimo se namreč prebiti do izomorfizma kolobarjev, ne le aditivnih grup. Preden izračunamo $\varphi(fg)$, nas zanima, kam produkt fg slika bazne elemente. Ne pozabimo, v $\mathrm{End}_O(M)$ produkt preslikav pomeni njun kompozitum.

$$(fg)(x_j) = f(g(x_j)) = \sum_{k=1}^n g_{kj}f(x_k) = \sum_{k=1}^n g_{kj}\sum_{i=1}^n f_{ik}x_i = \sum_{i=1}^n \left(\sum_{k=1}^n g_{kj}f_{ik}\right) x_i.$$

Uporabili smo $g(x_j) = \sum_{i=1}^n g_{ij}x_i$ in linearnost f. Na (i, j)-tem mestu matrike $\varphi(fg)$ torej leži

$$\sum_{k=1}^n g_{kj}f_{ik}.$$

Posebej izračunamo (i,j)-ti element produkta $\varphi(f)\varphi(g)$. Zanima nas torej skalarni produkt i-te vrstice matrike $\varphi(f)$ in j-tega stolpca matrike $\varphi(g)$. Množimo in dobimo

$$\sum_{k=1}^{n} f_{ik}g_{kj}.$$

Želeli bi si, da bi bili vsoti enaki, torej, da bi bila preslikava φ homomorfizem kolobarjev. Žal v našem primeru, kjer je O nekomutativen obseg, to ne velja. Nedvomno pa sta si zgornji dve vsoti skoraj na las podobni, zato poskusimo zadevo obrniti v naš prid na drugačen način.

Definicija 5.1. Naj bo K kolobar. *Nasprotni kolobar* kolobarja K vsebuje enake elemente kot K, z enako definirano operacijo seštevanja kot v K, množenje definiramo pa na naslednji način:

$$x \cdot y := yx,$$

kjer je yx množenje elementov y in x v K. Nasprotni kolobar kolobarja K označimo s K^o.

Opomba 5.2. Če je K komutativen, velja $K = K^o$.

Hitro lahko vidimo, da je K^o res kolobar, saj se pri strukturi grupe za seštevanje nič ne zatakne (enako kot v K), kar se tiče množenja zahtevamo pa le asociativnost in zaprtost za množenje. Oboje očitno velja. Podobno lahko bralec premisli, da je tudi nasprotni kolobar obsega še vedno obseg.

Poglejmo zdaj, če lahko pojem nasprotnega kolobarja reši našo zagato s preslikavo φ. Vidimo, da jo, če rečemo, da naj φ namesto iz $\mathrm{End}_O(M)$ v $M_n(O)$ slika iz $\mathrm{End}_O(M)$ v $M_n(O^o)$. V tem primeru se zgornji vsoti, kot elementa na (i,j)-tem mestu matrik $\varphi(fg)$ in $\varphi(f)\varphi(g)$, izenačita. Res, na (i,j)-tem mestu matrike $\varphi(f)\varphi(g)$ zdaj dobimo

$$\sum_{k=1}^{n} g_{kj} \cdot f_{ik},$$

kjer $\cdot$ predstavlja množenje v obsegu O^o (v izračunu $\varphi(fg)$ nam ni treba prilagajati operacije množenja, saj gledamo kolobar endomorfizmov še vedno nad obsegom O). Zgornja vsota pa je po definiciji operacije množenja v O^o ravno enaka

$$\sum_{k=1}^{n} f_{ik}g_{kj},$$

kjer je zdaj $f_{ik}g_{kj}$ produkt v O. Premislimo, da modifikacija kodomene preslikave φ ne pokvari že pridelanega izomorfizma aditivnih grup. Očitno ga ne, saj je seštevanje definirano popolnoma enako v obeh, O in O^o. Sledi, da je φ izomorfizem kolobarjev $\mathrm{End}_O(M)$ in $M_n(O^o)$. S tem malo daljšim razmislekom smo tako dokazali za nadaljevanje pomemben izrek.

Izrek 5.3. *Naj bo M n-dimenzionalen vektorski prostor nad O (ima bazo z n elementi), kjer je O (nekomutativen) obseg. Potem sta kolobarja* $\mathrm{End}_O(M)$ *in* $M_n(O^o)$ *izomorfna.*

Na prvi pogled bi se izrek lahko zdel le zanimiv analog že omenjenega izomorfizma med endomorfizmi vektorskega prostora nad polji in prostorom kvadratnih matrik nad poljem. Vidimo pa lahko, da nam pridelani rezultat ponudi alternativen pogled na Wedderburnov izrek o enostavnih algebrah. Spomnimo se, da je bila ena od ekvivalentnih točk izreka o enostavni končno razsežni algebri A naslednja:

$$A \cong M_n(D),$$

kjer je D algebra, ki je obseg. Uporabimo zdaj zgornji razmislek, kjer je O obravnavan zgolj kot obseg, ne pa kot algebra. Zlahka vidimo, da smo uporabljali le dejstvo, da je vsak element obrnljiv, torej četudi bi bila O algebra, ki je obseg, bi zaključki še vedno veljali. Tako lahko dodamo še eno ekvivalentno točko Wedderburnovemu izreku:

$$A \cong \mathrm{End}_{D^o}(M),$$

kjer je D in posledično tudi D^o algebra, ki je obseg (definicija obratne algebre se seveda ne razlikuje od obratnega kolobarja, le da ima dodatno še strukturo vektorskega prostora nad poljem). Modul M je n-dimenzionalen enotski D-modul, kjer je n enak številu n v $M_n(D)$.

6. Primitivni kolobarji

Za potrebe dokaza Wedderburnovega izreka bomo uporabili rezultate, ki so kronološko gledano nastali po tem, ko je Wedderburn objavil dokaz svojega strukturnega izreka. Poslužili se bomo namreč dela njegovega učenca, N. Jacobsona. Še prej pa se vrnimo k enostavnim modulom s precej nezahtevnim, a dokaj pomembnim rezultatom.

Lema 6.1 (Schurova lema [3, Theorem 2.1.1])**.** *Naj bosta M, N enostavna K-modula. Tedaj je vsak neničeln homomorfizem $f : M \to N$ izomorfizem.*

Dokaz. Dokaz sloni na dejstvih, da je $\ker f$ podmodul M in $\mathrm{im} f$ podmodul N. Spomnimo se, da je modul enostaven, kadar nima netrivialnih podmodulov. Sledi torej $\ker f = 0$ ali $\ker f = M$. Druga možnost je izključena, saj je f neničeln, zato velja $\ker f = 0$ in f je injektiven. Podobno velja $\mathrm{im} f = 0$ ali $\mathrm{im} f = N$. Iz istega razloga kot prej izključimo prvo možnost, zato velja $\mathrm{im} f = N$ in f je surjektiven. Sledi, da je f izomorfizem. □

Morda se rezultat sprva zdi malce neumesten, a če dobro pomislimo, vidimo, da nam v drugi luči pokaže nekaj zelo zanimivega.

Posledica 6.2. *Naj bo M enostaven K-modul. Tedaj je $\mathrm{End}_K(M)$ obseg.*

Dokaz. Schurova lema pravi, da so vsi elementi $\mathrm{End}_K(M)$, torej homomorfizmi iz M v M, bodisi ničelni, bodisi izomorfizmi (M je namreč enostaven). Torej ima vsak neničeln element $\mathrm{End}_K(M)$ inverz. □

Dokazano trditev bomo v prihodnje pridoma uporabljali, nadaljujemo pa s še eno lemo, ki nam bo kmalu prišla zelo prav, drugače je pa tudi sama po sebi zanimiva.

Lema 6.3. *Naj bo K enostaven kolobar, ki ima minimalen levi ideal L. Potem je vsak enostaven K-modul izomorfen L.*

Pred dokazom se spomnimo, da je kolobar K enostaven, če velja $K^2 \neq 0$, in če nima netrivialnih idealov, torej različnih od 0 in samega sebe. V zgornji lemi pa predpostavimo, da ima K levi ideal, torej s tem ne kršimo enostavnosti, ki postavi pogoj le za (obojestranske) ideale.

Dokaz leme 6.3. Naj bo torej K enostaven kolobar, M enostaven K-modul in L minimalen levi ideal v K. Poglejmo si levi ideal LK kot produkt levih idealov L in K. Opazimo, da je LK ideal. Podgrupa za seštevanje ostane že iz definicije produkta levih idealov, izkaže pa se, da lahko množimo z elementi iz K tudi z desne, saj je K (obojestranski) ideal. Ker je K enostaven, velja $LK = 0$ ali $LK = K$. Oglejmo si množico

$$J := \{k \in K; kK = 0\},$$

ki je očitno (obojestranski) ideal kolobarja K, zato ponovno velja $J = 0$ ali $J = K$. Slednjo možnost tokrat ovržemo, saj definicija enostavnosti zagotavlja $K^2 \neq 0$. Velja torej $J = 0$ in posledično $LK = K$.

Med drugim definicija enostavnega modula zagotavlja $0 \neq KM$. Naprej, velja $KM = (LK)M = L(KM) \subseteq LM$. Naj bo torej $m \in M$ tak, da velja $Lm \neq 0$. Poskusimo skonstruirati izomorfizem $\varphi : L \to M$. Naj bo $\varphi(l) = lm$. Preslikava je očitno dobro definirana. Preverimo, da je φ homomorfizem K-modulov. Velja

$$\varphi(l + l') = (l + l')m = lm + l'm = \varphi(l) + \varphi(l'), \varphi(kl) = klm = k\varphi(l),$$

kjer $l, l' \in L$, $k \in K$. Vidimo, da je φ res homomorfizem. Kot že vemo, je imφ podmodul K-modula M, torej je enak 0 ali M (M je enostaven). Vemo, da $Lm \neq 0$, torej im$\varphi = M$. Sledi, da je φ surjektiven homomorfizem. Preverimo še injektivnost. Tudi kerφ je podmodul K-modula L. kerφ je tudi podmodul K-modula K. Res, če velja $\varphi(l) = 0$, velja tudi $\varphi(kl) = k\varphi(l) = 0$, za $l \in L, k \in K$. Po premisleku iz četrtega razdelka o podmodulih K-modula K, sledi, da je kerφ levi ideal K, ki pa je seveda vsebovan v L. Iz minimalnosti L sledi ker$\varphi = 0$ ali ker$\varphi = L$. Slednjo možnost spet ovržemo, saj velja $\varphi(L) = Lm \neq 0$. Preslikava φ je torej izomorfizem K-modulov. $\square$

Preden nadaljujemo, si poglejmo pomemben zgled, ki nam bo že v kratkem prišel prav.

Primer 6.4. Spomnimo se že obravnavanega kolobarja kvadratnih matrik nad obsegom, $K := M_n(D)$, kjer je D obseg. Kot smo že premislili zgodaj v besedilu, je v tem primeru, ko je D obseg, K enostaven kolobar. Primer minimalnega levega ideala v tem kolobarju je $L := KE_{11}$. Spomnimo se, E_{11} je $n \times n$ matrika, ki ima na mestu $(1, 1)$ enoto obsega D, drugod same ničle. Torej je L podmnožica K, katere elementi so matrike, ki imajo vse stolpce, razen morda prvega, ničelne. Premislimo, da je L res minimalen levi ideal K. Podgrupa za seštevanje je očitno, prav tako velja, da je $(a_{ij})((x_{ij})E_{11}) = ((a_{ij})(x_{ij}))E_{11} \in L$ za vse $(a_{ij}), (x_{ij}) \in K$, torej je L res levi ideal.

Za dokaz minimalnosti L uporabimo trditev 4.12, ki pravi, da je levi ideal L kolobarja K minimalen natanko tedaj, ko je enostaven kot K-modul. Dodatno zahtevamo še $KL \neq 0$, kar je v tem primeru izpolnjeno, saj je K enotski kolobar. Naj bo $(a_{ij}) \in L$ neničelna matrika, ki ima torej vsaj en neničeln element v prvem stolpcu. Trdimo, da obstaja taka matrika $(b_{ij}) \in K$, da velja $(b_{ij})(a_{ij}) = E_{11}$. Res, vse razen prve vrstice matrike (b_{ij}) naj bodo ničelne, za prvo vrstico pa vzamemo na primer same ničelne vnose na vseh mestih, razen na mestu $(1, j)$, kjer je $1 \leq j \leq n$ tak, da je element matrike (a_{ij}) na mestu $(j, 1)$ neničeln. Na mestu $(1, j)$ matrike (b_{ij}) vzamemo element a_{j1}^{-1}. Potem res velja $(b_{ij})(a_{ij}) = E_{11}$.

Očitno je $K(a_{ij})$ levi ideal kolobarja K in po zgornjem razmisleku velja tudi $E_{11} \in K(a_{ij})$. Posledično je potem tudi $KE_{11} \subseteq K(a_{ij})$. Ker velja tudi $K(a_{ij}) \subseteq KE_{11}$, zaključimo $L = KE_{11} = K(a_{ij})$.

Vidimo, da vsak neničeln element iz L generira cel L, kar po prav tako že dokazani trditvi 4.10 potrjuje enostavnost L kot K-modula.

Ker je torej K enostaven, L pa njegov minimalen ideal, po lemi 6.3 sledi, da je vsak enostaven K-modul izomorfen L. $\diamondsuit$

Prišli smo do pomembne definicije za razvoj teorije Jacobsona, ki jo bomo v besedilu obravnavali.

Definicija 6.5. Kolobar K se imenuje *primitiven*, če obstaja tak K-modul $V \neq 0$, da velja

- $kV \neq 0$ za vsak $0 \neq k \in K$ in
- $Kv = V$ za vsak $0 \neq v \in V$.

Z drugimi besedami bi lahko rekli, da je kolobar K primitiven, če obstaja kak zvest ($\mathrm{ann}_K V = 0$) enostaven K-modul V.

Opomba 6.6. Alternativen pristop je definicija primitivnega ideala, preko katerega potem definiramo tudi primitiven kolobar. V tem besedilu ta definicija ni potrebna, bralec pa si lahko več o tem in sorodnih temah prebere v [5, 45–62].

Kot večina definicij je tudi ta precej abstraktna, zato si je najbolje brž pogledati kakšen primer.

Primer 6.7. Vrnimo se k diskusiji z začetka tega razdelka. Naj bo V vektorski prostor nad obsegom O. Trdimo, da je kolobar $K := \mathrm{End}_O(V)$ primitiven. Premislimo, da je V zvest enostaven K-modul.

Vprašanje na mestu bi bilo, kako sploh definiramo K-modul v tem primeru, ko so elementi K endomorfizmi. Preprosto definiramo $(\varphi, v) \mapsto \varphi(v) \in V$, za $\varphi \in K, v \in V$. Pokažimo najprej, da velja $\mathrm{ann}_K(V) = 0$. Predpostavimo torej $\varphi(V) = 0$ (to je ekvivalentno pogoju $kV = 0$, le da je k tokrat endomorfizem). Vidimo, da je to ekvivalentno $\varphi = 0$, od koder res sledi $\mathrm{ann}_K(V) = 0$ in V je zvest.

Preostane pokazati še enostavnost V kot K-modula. Naj bo $v \in V$ neničeln. Zanima nas Kv. Z drugimi besedami je Kv ovrednotenje vsake preslikave iz K v elementu v. Spomnimo se, da na V lahko gledamo tudi kot na vektorski prostor nad obsegom O. Tedaj ima V bazo. Kot smo že premislili, je vsak element K natanko določen s slikami baznih elementov V. Prav tako vemo, da je v element neke baze vektorskega prostora V (vsak neničeln element iz V je v neki bazi), zato lahko s slikanjem v v različne elemente V dosežemo, da so vsi elementi vsebovani v Kv. Velja torej $Kv = V$, pogoj $KV \neq 0$ iz definicijie enostavnosti modula je pa tudi tako ali tako izpolnjen, saj je K enotski kolobar. $\diamondsuit$

Povežimo zdaj novo definicijo primitivnosti z že znanimi pojmi in jo tako na nek način vpeljimo v osrednje temo tega besedila.

Trditev 6.8. *Naj bo K primitiven kolobar. Tedaj je K prakolobar.*

Dokaz. Uporabili bomo prvo izmed ekvivalentnih točk definicije prakolobarja 2.7, torej iz $aKb = 0$ sledi $a = 0$ ali $b = 0$. Dokazujemo ekvivalentno, da je za a, b neničelna tudi aKb neničeln.

Naj bosta torej $a, b \in K$ neničelna. Ker je K primitiven, obstaja zvest enostaven K-modul V. Velja torej $\mathrm{ann}_K V = 0$, zato obstajata $u, v \in V$, da velja $au \neq 0$ in $bv \neq 0$. Po drugi strani enostavnost V da $Kx = V$ za vsak $x \in V$. Vzemimo $y := bv$. Velja $Ky = Kbv = V$, zato obstaja $k \in K$, da velja $kbv = u$ (u je namreč tudi element V). Velja torej $a(kbv) = (akb)v = au \neq 0$. Od tod sledi $(akb) \neq 0$ in posledično $aKb \neq 0$. $\square$

Obrat trditve ne drži. Za primer vzemimo kolobar celih števil, ki je komutativen brez deliteljev niča, zato po trditvi iz drugega razdelka sledi, da je prakolobar. Vseeno pa ni primitiven. Preden vidimo zakaj, pa si poglejmo naslednjo trditev.

Trditev 6.9. *Prakolobar, ki ima minimalen levi ideal, je primitiven.*

Dokaz. Naj bo K kolobar in L njegov levi minimalen ideal. Trdimo, da je L zvest enostaven K-modul.

Spomnimo se trditve 4.12 iz četrtega razdelka, ki pravi, da je minimalen levi ideal L enostaven kot K-modul, a mora veljati $KL \neq 0$. Na našo srečo je K prakolobar. Tokrat se skličemo na tretjo točko definicije prakolobarja (gledano od zgoraj navzdol), da je produkt neničelnih levih idealov neničeln. V našem primeru sta leva ideala kar K in L. Ker sta oba neničelna, je potem tudi njun produkt KL neničeln. Po že omenjeni trditvi iz četrtega razdelka sledi, da je L enostaven K-modul.

Dokažimo še $\mathrm{ann}_K L = 0$. Spomnimo se,

$$\mathrm{ann}_K L = \{k \in K; kL = 0\}$$

je levi ideal kolobarja K. Poglejmo si produkt levih idealov $\mathrm{ann}_K L \cdot L$. Očitno so po definiciji anihilatorja vsi elementi tega produkta ničelni, torej je produkt sam ničeln. Ker pa je K prakolobar, od tod sledi $L = 0$ ali $\mathrm{ann}_K L = 0$. Ker je L po definiciji minimalnega levega ideala neničeln, velja $\mathrm{ann}_K L = 0$. Torej je L zvest, enostaven K-modul, zato je K primitiven kolobar. □

S to trditvijo lahko potrdimo, da je že večkrat srečani kolobar matrik nad obsegom primitiven.

Primer 6.10. Naj bo $K := M_n(D)$, kjer je D obseg. Kot že vemo iz trditve 3.2, je K enostaven kolobar. Posledično je prakolobar. Prav tako smo v 6.4 že premislili, da K vsebuje minimalen levi ideal (matrike z neničelnim prvim stolpcem, na primer). K je torej prakolobar, ki ima minimalen levi ideal, torej je po zgornji trditvi primitiven.

Lahko pa pomislimo tudi drugače. V začetnem primeru 6.7 smo ugotovili, da je $\mathrm{End}_D(V)$ primitiven kolobar, kjer je D obseg in V vektorski prostor nad D. Ker torej velja, da je kolobar $\mathrm{End}_D(V)$, kjer je D obseg, primitiven in izomorfen $M_n(D^{\mathrm{o}})$, je tudi $M_n(D^{\mathrm{o}})$ primitiven. ♢

V zgornjem primeru smo kar slepo privzeli, da je primitivnost kolobarja lastnost, ki se pri izomorfizmih ohranja. Preverimo, da se res.

Denimo, da velja $K_1 \cong K_2$, kjer sta K_1, K_2 kolobarja. Denimo, da je K_1 primitiven. Tedaj obstaja zvest enostaven K_1-modul V. Definirajmo V kot K_2-modul z množenjem

$$k_2 v := \varphi(k_2)v,$$

kjer je $k_2 \in K_2, v \in V$ in φ izomorfizem iz K_2 in K_1. Leva stran enačbe je torej na novo definirano množenje v K_2-modulu V, desna stran pa predstavlja že poznano množenje v K_1-modulu V. Tako postane V zvest enostaven K_2-modul.

Res, denimo $k_2 V = 0$ za $k_2 \in K_2$. Velja $0 = k_2 V = \varphi(k_2)V$. Ker je $\varphi(k_2)$ element kolobarja K_1, ki je zvest, sledi $\varphi(k_2) = 0$. Preslikava φ je izomorfizem, torej je $k_2 = 0$. Torej je V zvest kot K_2-modul. Preverimo še enostavnost. Naj bo $v \in V$ neničeln. Potem je $K_2 v = \varphi(K_2)v = K_1 v = V$ (zadnja enakost velja zaradi enostavnosti V kot K_1-modula). Velja torej, da je V enostaven kot K_2-modul in posledično je K_2 primitiven.

Zaključimo krajši nabor trditev s še enim zanimivim rezultatom.

Trditev 6.11. *Komutativen primitiven kolobar K je polje.*

Dokaz. Sledimo [1, Lemma 5.7]. Naj bo V zvest enostaven K-modul (obstaja, saj je K primitiven kolobar). Vzemimo neničeln $v \in V$. Trdimo, da za vsak $k \in K$ iz $kv = 0$ sledi $k = 0$. Predpostavimo torej $kv = 0$. Ker je V enostaven, sledi $Kv = V$. Naprej velja $kV = kKv = Kkv = 0$ (K je komutativen). Ker pa je V tudi zvest, iz $kV = 0$ sledi $k = 0$.

Naj bo zdaj $a \in K$ neničeln. Tedaj velja $av \neq 0$, drugače bi moral biti po zgornjem razmisleku a enak 0. Zdaj lahko spet uporabimo enostavnost V, da zapišemo $V = K(av)$. To pa pomeni, da obstaja tak $b \in K$, da velja $v = b(av)$. Od tod izpeljemo $(xba - x)v = 0$ za vse $x \in K$ (velja namreč $(xba - x)v = x(bav) - xv = xv - xv = 0$). Ponovno uporabimo dejstvo, ki smo ga premislili v zgornjem odstavku, in dobimo $xba - x = 0$. Če uporabimo še komutativnost K, dobimo $xba = bax = x$ za vse $x \in K$. Sledi $ba = 1$, torej ima K enoto. Vnovič uporabimo komutativnost K in dobimo $ba = ab = 1$, od koder sledi $b = a^{-1}$. S tem smo pokazali, da je K res polje. □

Zdaj imamo na voljo sredstva, da se lotimo od prej nedokončanega primera kolobarja celih števil.

Primer 6.12. Kot smo že razmislili, je kolobar $\mathbb{Z}$ prakolobar. Vemo, da je komutativen, zato v kolikor bi bil tudi primitiven, bi moral, glede na ravnokar dokazano trditev, biti polje. To pa vemo, da ni, saj sta 1 in -1 edina obrnljiva elementa. Sledi, da $\mathbb{Z}$ ni primitiven kolobar. ♢

7. Jacobsonov izrek o gostoti

Pred nami je verjetno najzahtevnejši, a morda tudi najzanimivejši razdelek. Najbolj se bomo posvetili že omenjenemu izreku o gostoti.

Definicija 7.1. Naj bo V vektorski prostor nad obsegom O. Naj bo K podkolobar kolobarja endomorfizmov $\mathrm{End}_O(V)$. Pravimo, da je K *gost kolobar linearnih operatorjev vektorskega prostora* V, če za vsak $n \in \mathbb{N}$ in vsako podmnožico linearno neodvisnih elementov $\{u_1, u_2, \ldots, u_n\}$ ter vsako podmnožico (ne nujno linearno neodvisnih) elementov $\{v_1, v_2, \ldots, v_n\}$, obstaja tak $f \in K$, da velja

$$f(u_1) = v_1, f(u_2) = v_2, \ldots, f(u_n) = v_n.$$

Zagotovo ena težjih definicij tega besedila, zato lahko namesto nje pogosto uporabimo naslednjo lemo, ki malce bolj jedrnato karakterizira goste kolobarje vektorskega prostora.

Lema 7.2. *Naj bo V vektorski prostor nad obsegom O. Kolobar $K \subseteq \mathrm{End}_O(V)$ je gost kolobar linearnih operatorjev vektorskega prostora V natanko tedaj, ko za vsak $g \in \mathrm{End}_O(V)$ in vsak končno razsežen podprostor U vektorskega prostora V obstaja tak $f \in K$, da velja $f|_U = g|_U$.*

Dokaz. Naj bo K gost kolobar linearnih operatorjev vektorskega prostora V nad obsegom O. Naj bo $g \in \mathrm{End}_O(V)$, naj bo U končno razsežen podprostor V. Naj bo $X := \{u_1, \ldots, u_n\}$ baza U. Vzemimo $v_1 := g(u_1), v_2 := g(u_2), \ldots, v_n = g(u_n)$. Ker je K gost kolobar linearnih operatorjev vektorskega prostora V in so elementi v X linearno neodvisni (so baza podprostora U), po definiciji gostega kolobarja linearnih operatorjev vektorskega prostora obstaja tak $f \in K$, da velja

$$f(u_1) = v_1, f(u_2) = v_2, \ldots, f(u_n) = v_n.$$

Ko vstavimo definicije elementov $v_1, \dots, v_n$, dobimo

$$f(u_1) = g(u_1), f(u_2) = g(u_2), \dots, f(u_n) = g(u_n).$$

Ker se torej preslikavi f, g ujemata na bazi U, velja $f|_U = g|_U$.

Obratno, naj bo $K \subseteq \mathrm{End}_O(V)$ in $X := \{u_1, \dots, u_n\}$ množica linearno neodvisnih elementov V. Naj bo $Y := \{v_1, \dots, v_n\}$ množica (ne nujno linearno neodvisnih) elementov V. Iščemo tak $f \in K$, da velja

$$f(u_1) = v_1, f(u_2) = v_2, \dots, f(u_n) = v_n.$$

Ker je množica X linearno neodvisna, jo lahko smatramo kot bazo linearne ogrinjače množice X. Imenujmo nastali podprostor U. Naj bo $g \in \mathrm{End}_O(V)$ tak, da velja

$$g(u_1) = v_1, g(u_2) = v_2, \dots, g(u_n) = v_n.$$

Po predpostavki leme (zdaj dokazujemo v obratno smer) obstaja tak $f \in K$, da velja $f|_U = g|_U$. Ker je $X \subseteq U$, velja tudi $f|_X = g|_X$ oziroma

$$f(u_1) = v_1, f(u_2) = v_2, \dots, f(u_n) = v_n,$$

kar smo želeli pokazati. $\square$

Primer 7.3. Zlahka vidimo, da je $K := \mathrm{End}_O(V)$ primer gostega kolobarja linearnih operatorjev vektorskega prostora V. Res, za vsak $g \in \mathrm{End}_O(V)$ in vsak podprostor U vektorskega prostora V obstaja $f \in K$ (vzamemo kar $f := g$), da velja $f|_U = g|_U$. $\diamondsuit$

V tej luči ima lema zanimivo posledico za končno razsežne vektorske prostore nad obsegom.

Posledica 7.4. *Naj bo V končno razsežen vektorski prostor nad obsegom O (ima končno bazo). Potem je* $\mathrm{End}_O(V)$ *edini gost kolobar linearnih operatorjev vektorskega prostora V.*

Dokaz. Naj bo K še en (poleg $\mathrm{End}_O(V)$) gost kolobar linearnih operatorjev vektorskega prostora V nad obsegom O. Naj bo $g \in \mathrm{End}_O(V)$ in vzemimo podprostor $U := V$ kot končno razsežen podprostor vektorskega prostora V. Po lemi obstaja tak $f \in K$, da $f|_U = g|_U$, torej $f|_V = g|_V$. Ker pa je V kar celotna domena prelikav f in g (sta namreč elementa kolobarja $\mathrm{End}_O(V)$), sledi $f = g$, oziroma $g \in K$. Ker je bil $g \in \mathrm{End}_O(V)$ poljuben, velja $\mathrm{End}_O(V) \subseteq K$. Po definiciji je tudi $K \subseteq \mathrm{End}_O(V)$, torej zaključimo $K = \mathrm{End}_O(V)$. $\square$

Na tej točki lahko povežemo povsem abstraktno definicijo gostih kolobarjev linearnih operatorjev nad vektorskim prostorom s pojmom primitivnega kolobarja. Rezultat je znano delo na Poljskem rojenega ameriškega matematika Nathana Jacobsona. Pomembnosti primerno bo tudi dokaz izreka med daljšimi v tem besedilu.

Izrek 7.5 (Jacobsonov izrek o gostoti)**.** *Kolobar K je primitiven natanko tedaj, ko je izomorfen gostemu kolobarju linearnih operatorjev vektorskega prostora nad obsegom.*

Dokaz. Sledimo [1, Theorem 5.16]. Najprej premislimo dokaz v obratni smeri. Naj bo K kolobar. Naj bo S gost kolobar linearnih operatorjev vektorskega prostora V nad obsegom O, ki je izomorfen K. Pokažimo, da je K primitiven.

Najprej preverimo, da je S primitiven kolobar. Trdimo, da je V zvest enostaven S-modul. Tudi tokrat so elementi S preslikave, saj je $S \subseteq \mathrm{End}_O(V)$, zato definiramo množenje v modulu preko

$$fv := f(v),$$

kjer je $f \in S, v \in V$. Denimo, da velja $fV = 0$ za neki $f \in S$. Drugače zapisano to pomeni $f(V) = 0$, od koder sledi $f = 0$, saj je V celotna domena preslikave f. V je torej res zvest S-modul.

Preverimo še enostavnost. Naj bo $v \in V$ neničeln. Po definiciji gostega kolobarja linearnih operatorjev vektorskega prostora za vsak $u \in V$ obstaja tak $f \in S$, da velja $f(v) = u$. Ker je bil $v \in V$ poljuben neničeln in ga lahko slikamo v katerikoli element iz V, velja $Sv = V$, oziroma V je enostaven S-modul. Izkaže se torej, da je S primitiven kolobar. Ker mu je K izomorfen, je po premisleku o ohranjanju primitivnosti preko izomorfizmov tudi K primitiven kolobar.

Dokaz izreka v drugo smer bo malce zahtevnejši. Naj bo K primitiven kolobar. Dokazujemo, da je izomorfen gostemu kolobarju linearnih operatorjev vektorskega prostora.

Naj bo V zvest enostaven K-modul (obstaja, saj je K primitiven). Po Schurovi lemi je tedaj $O := \mathrm{End}_K(V)$ obseg. Na ta način lahko tvorimo V kot vektorski prostor nad O (ponovno definiramo $fv := f(v)$ za $f \in O, v \in V$). Prav tako velja $1v = id(v) = v$ za vsak $v \in V$ in očitno so izpolnjeni tudi vsi ostali pogoji iz definicije enotskega modula. Torej je V res vektorski prostor nad O. Za vsak $k \in K$ definiramo preslikavo $k' : V \to V$ s predpisom

$$k'(v) := kv.$$

Množenje na desni strani enakosti seveda ima smisel, saj je V tudi K-modul. Velja

$$k'(v_1 + v_2) = k(v_1 + v_2) = kv_1 + kv_2 = k'(v_1) + k'(v_2),$$

kjer $v_1, v_2 \in V$. Prav tako velja

$$k'(\delta v) = k\delta v = k\delta(v) = \delta(kv) = \delta(k'(v)) = \delta k'(v),$$

kjer sta $v \in V, \delta \in O$. Na kratko premislimo, da zgornje drži. Res, ker je $\delta \in O$, velja $\delta(kv) = k\delta(v)$ za vse $v \in V, k \in K$ po definiciji endomorfizma K-modula V.

S tem smo premislili, da je k' tudi endomorfizem, tokrat O-modula V. Drugače rečeno, $k' \in \mathrm{End}_O(V)$ za vse $k \in K$. Nadaljujmo, naj bo $\psi : K \to \mathrm{End}_O(V)$ preslikava definirana s predpisom

$$\psi : k \mapsto k'.$$

Očitno velja

$$\psi(k_1 + k_2)(v) = (k_1 + k_2)'(v) = (k_1 + k_2)v = k_1 v + k_2 v = \psi(k_1)(v) + \psi(k_2)(v),$$

kjer so $k_1, k_2 \in K, v \in V$. Podobno vidimo, da velja

$$\psi(k_1 k_2)(v) = (k_1 k_2)'(v) = k_1 k_2 v = k_1'(k_2'(v)) = k_1' \cdot k_2'(v),$$

kjer so $k_1, k_2 \in K, v \in V$. Množenje na skrajni desni strani zgornje enačbe je množenje v kolobarju $\mathrm{End}_O(V)$, ki je seveda komponiranje preslikav.

Vidimo torej, da je preslikava ψ homomorfizem kolobarjev. Še več, vidimo lahko, da je ψ injektivna. Res, predpostavimo $\psi(k)(V) = 0$ (nevtralni element za seštevanje v kolobarju $\mathrm{End}_O(V)$ je preslikava, ki celoten V preslika v $0 \in V$). Velja torej

$0 = k'(V) = kV$. Ker je V zvest K-modul, sledi $k = 0$, torej je ψ res injektivna. To pa pomeni, da je K izomorfen $\psi(K)$, oziroma

$$K \cong K' := \{k'; k \in K\} \subseteq \mathrm{End}_O(V).$$

Preostanek dokaza bomo namenili razmisleku, da je K' gost kolobar linearnih operatorjev vektorskega prostora. Razmislimo, da je dokaz v luči osnovne definicije gostega kolobarja linearnih operatorjev vektorskega prostora že načet. S tem mislimo, da za vsak neničeln element $u \in V$ in poljuben element $v \in V$ obstaja tak $k' \in K'$, da velja $k'(u) = ku = v$. Res, dejstvo sledi iz enostavnosti K-modula V, saj velja $Ku = V$, preslikava k' pa je, kot že vemo, definirana kot množenje z elementom k. To izpolnjuje torej pogoj iz definicije gostega kolobarja linearnih operatojev nad vektorskim prostorom za $n = 1$. Težava nastopi, ker mora pogoj držati za poljuben $n \in \mathbb{N}$. Zato trdimo, da namesto tega zadostuje pokazati naslednjo pomožno trditev.

($*$) Naj bo U končno razsežen podprostor K-modula V. Za vsak $w \in V \backslash U$ obstaja tak $k \in K$, da velja $k'(U) = 0$ in $k'(w) \neq 0$.

Premislimo, da je dovolj dokazati zgornjo trditev. Predpostavimo, da drži. Naj bo $n \in \mathbb{N}$ in naj bodo $u_1, u_2, \ldots, u_n$ linearno neodvisni elementi iz V in naj bodo $v_1, v_2, \ldots, v_n$ poljubni elementi iz V. Vzemimo poljuben $1 \leq i \leq n$. Naj bo U linearna ogrinjača elementov $u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n$ in naj bo $w := u_i$. Če zdaj uporabimo trditev ($*$), obstaja tak $k_i \in K$, da velja $k_i'(U) = 0$ (torej tudi $k_i'(u_j) = 0$ za vse $j \neq i$) in $k_i'(w) \neq 0$. Naj bo $a := k_i'(w)$. Premislili smo že, da je pogoj za $n = 1$ v definiciji gostega kolobarja linearnih operatorjev nad vektorskim prostorom izpolnjen za K', zato obstaja tak $s_i' \in K'$, da velja $s_i'(a) = s_i'(k_i'(w)) = v_i$. Definirajmo zdaj

$$k := s_1 k_1 + s_2 k_2 + \cdots + s_n k_n \in K.$$

Vidimo, da velja $k'(u_i) = v_i$. Res,

$$k'(u_i) = ku_i = s_1 k_1 u_i + \cdots + s_{i-1} k_{i-1} u_i + s_i k_i u_i + \cdots + s_n k_n u_i,$$

kjer so vsi sumandi v zgornjem izrazu ničelni razen $s_i k_i u_i = s_i'(k_i'(u_i)) = v_i$. Če nam torej uspe dokazati ($*$), od tod sledi, da je K' gost kolobar linearnih operatorjev vektorskega prostora.

Dokazujemo ($*$) s protislovjem. Denimo, da ($*$) ne velja. Potem lahko brez škode za splošnost predpostavimo, da je U podprostor V z najmanjšo dimenzijo, za katerega ($*$) ne velja (V in U seveda gledamo kot prostora nad O). Očitno je $\dim_O(U) \geq 1$, saj je za $U = 0$ ($*$) očitno izpolnjena. Naprej, naj bo U_0 poljuben podprostor U, da velja $\dim_O(U_0) = \dim_O(U) - 1$. Naj bo

$$L := \{l \in K; l'(U_0) = 0\}.$$

Vzemimo $z \in V \backslash U_0$. Ker po predpostavki ($*$) velja za U_0 (saj ima manjšo dimenzijo od U), obstaja tak $l \in L$, da velja $l'(z) \neq 0$ (prvemu delu trditve ($*$) zadoščajo že vsi elementi množice L). Posledično velja $Lz \neq 0$. Vidimo lahko, da je L očitno levi ideal kolobarja K. Od tod potem sledi, da je Lz podmodul K-modula V. Res, očitno je podgrupa V za seštevanje, prav tako pa velja $KLz \subseteq Lz$, saj je L levi ideal. Ker je V enostaven K-modul in je Lz neničeln, mora veljati

$$Lz = V$$

za vse $z \in V \backslash U_0$.

Naj bo zdaj $w \in V \backslash U$ tak, da zanj ne velja $(*)$, torej ne obstaja tak $k \in K$, da velja $k'(U) = 0$ in $k'(w) \neq 0$. Izberimo zdaj $u \in U \backslash U_0$ in poglejmo preslikavo $\delta : V \to V$ s predpisom

$$\delta(lu) := lw$$

za vse $l \in L$.

Preslikava je definirana na malce nenavaden način, zato preverimo dobro definiranost. Kot že vemo, velja $Lz = V$ za $z \in V \backslash U_0$ in ker je tudi $u \in U \backslash U_0 \subseteq V \backslash U_0$, velja $Lu = V$, torej je domena preslikave δ res cel V. Preslikava δ je očitno homomorfizem aditivnih grup iz V v V, zato nam dobro definiranost zagotavlja pogoj $\delta(0) = 0$. Predpostavimo torej $lu = l'(u) = 0$. Ker je $l \in L$, velja $l'(U_0) = 0$, dodatno, ker u ne leži v U_0 in je dimenzija U le za ena večja od dimenzije U_0, velja $U = U_0 + Ou$, kjer je O že večkrat omenjeni obseg $\mathrm{End}_K(V)$ (na nek način le razširimo vektorski podprostor U_0 s še enim baznim elementom u, katerega linearna ogrinjača je ravno Ou). Ker je $l' \in \mathrm{End}_O(V)$, potem velja

$$l'(U) = l'(U_0 + Ou) = l'(U_0) + Ol'(u) = 0.$$

Potem pa mora nujno veljati tudi $l'(w) = lw = 0$, saj bi drugače tudi za w veljala trditev $(*)$, kar pa smo predpostavili, da ne. Sledi, da je δ dobro definirana. Povsem analogno kot smo to storili že nekajkrat v tem dokazu, gre preveriti, da je δ endomorfizem R-modula V, torej velja $\delta \in O$. Tako lahko predpis preslikave δ zapišemo na malce drugačen način:

$$l(\delta u) = lw$$

za vse $l \in L$. Od tod torej sledi

$$L(\delta u - w) = 0.$$

Vemo, da za vse $z \in V \backslash U_0$ velja $Lz = V$, torej mora veljati

$$\delta u - w \in U_0.$$

Od tod pa potem sledi,

$$w = \delta u - (\delta u - w) \in Ou + U_0 = U,$$

predpostavili pa smo $w \in V \backslash U$. Torej drži $(*)$ in posledično tudi izrek. $\square$

Uspešno smo se prebili skozi malo daljši dokaz Jacobsonovega izreka o gostoti, zdaj pa sledi že dolgo obljubljena povezava med tem izrekom in Wedderburnovim strukturnim izrekom. Še preden se lotimo tega, pa premislimo, kako se izrek o gostoti spremeni, ko so v igri namesto kolobarjev algebre.

Definicija 7.6. Algebra A nad poljem se imenuje *primitivna algebra*, če obstaja zvest enostaven A-modul.

Kaj točno imamo v mislih, ko govorimo o A-modulu, kjer je A algebra nad poljem F? Gre za sorodno konstrukcijo že poznanemu modulu, le da je tokrat v igri še množenje s skalarji. Definicijo modula moramo zato ustrezno prilagoditi: A-modul M je vektorski prostor nad F s preslikavo iz $A \times M \to M$, $(a, m) \mapsto am$, ki izpolnjuje vse že poznane kriterije modula iz definicije 4.1, dodatno pa velja tudi

$$(\lambda a)m = a(\lambda m) = \lambda(am),$$

kjer $a \in A, m \in M, \lambda \in F$.

V celotni diskusiji primitivnih kolobarjev in izreka o gostoti se potem ključni pojmi ustrezno spremenijo. Obseg O nadomesti algebra $O = \mathrm{End}_A(V)$ nad F, ki je obseg (V je A-modul). Podobno postane tudi $\mathrm{End}_O(V)$ algebra nad F in preslikava $\psi : k \mapsto k'$ je zdaj homomorfizem algeber, ne le kolobarjev. Natančna formulacija in preverba pravilnosti teh sprememb je le formalnost, zato jo izpustimo. Kar nas pravzaprav najbolj zanima, je ustrezna prilagoditev Jacobsonovega izreka o gostoti.

Izrek 7.7. *Algebra A je primitivna natanko tedaj, ko je izomorfna gosti algebri linearnih operatorjev vektorskega prostora nad algebro, ki je obseg.*

Opomba 7.8. Besedna zveza vektorski prostor nad algebro, ki je obseg, zveni nenavadno, a gre v bistvu le za enotski A-modul, kjer je A algebra, ki je obseg

Seveda je dokaz izreka popolnoma nepotreben, saj smo ga že naredili pri dokazu izreka za kolobarje (enak je, le z že omenjenimi popravki za algebre). Tako smo zdaj končno dovolj oboroženi s teoretičnim znanjem za dokaz Wedderburnovega strukturnega izreka, ki ga v izpopolnjeni obliki tokrat navedemo le kot posledico.

Posledica 7.9. *Naj bo A neničelna končno razsežna F-algebra. Naslednje trditve so ekvivalentne:*

- *A je praalgebra.*
- *A je enostavna algebra.*
- *Obstaja končno razsežna F-algebra O, ki je obseg in tak končno razsežen vektorski prostor V nad O, da velja $A \cong \mathrm{End}_O(V)$.*
- *A je primitivna algebra.*

Dokaz. Najprej premislimo prehod iz tretje na drugo točko (gledano od zgoraj navzdol). Če velja $A \cong \mathrm{End}_O(V)$, potem smo že premislili (sicer za kolobarje, ampak za algebre velja enako), da velja $A \cong M_n(O^{\mathrm{o}})$, kjer je n dimenzija V nad O. Iz dejstva, da je O^{o} algebra, ki je obseg, sledi, da je $M_n(O^{\mathrm{o}})$ enostavna algebra in je posledično zaradi izomorfnosti tudi A enostavna.

Ob prvi navedbi Wedderburnovega strukturnega izreka v besedilu smo že premislili, da druga točka implicira prvo.

Z uporabo trditve 6.9, ki pravi, da so prakolobarji, ki vsebujejo minimalni levi ideal, primitivni, preidemo s prve na četrto točko. Res, trditev očitno velja tudi za algebre, saj se v dokazu ni nikjer pojavila struktura vektorskega prostora. Prav tako smo v primeru 2.4 premislili, da ima vsaka neničelna končno razsežna algebra minimalen levi ideal.

Da sklenemo krog, nam preostane še dokazati prehod s četrte na tretjo točko. Denimo torej, da je A primitivna algebra nad poljem F. Po priredbi Jacobsonovega izreka o gostoti za algebre potem vemo, da je A izomorfna gosti algebri A' linearnih operatorjev vektorskega prostora V nad algebro O, ki je obseg. Naj bodo $u_1, u_2, \ldots, u_m \in V$ linearno neodvisni nad O. Potem obstajajo taki $f_1, f_2, \ldots f_m \in A'$, da velja $f_i(u_i) \neq 0$ in $f_i(u_j) = 0$, če $i \neq j$. Res, lahko si predstavljamo, da m-krat uporabimo definicijo goste algebre linearnih operatorjev vektorskega prostora. Za poljuben $1 \leq i \leq m$ vzamemo za linearno neodvisne elemente $u_1, u_2, \ldots, u_n \in V$. Potem vzamemo elemente $v_1, v_2, \ldots, v_m \in V$, ki so vsi razen elementa v_i ničelni. Po definiciji obstaja tak $f_i \in A'$, da velja

$$f_i(u_1) = 0, \ldots, f_i(u_{i-1}) = 0, f_i(u_i) = v_i, \ldots, f_i(u_m) = 0.$$

S to konstrukcijo dosežemo linearno neodvisnost $f_1, \ldots, f_m$ nad poljem F. Res, denimo, da velja

$$a_1 f_1 + \cdots + a_m f_m = 0,$$

kjer $a_1, \ldots, a_m \in F$. Če zdaj preslikavo na levi strani zgornje enakosti ovrednotimo v elementu u_i, dobimo

$$a_1 f_1(u_i) + \cdots + a_i f_i(u_i) + \cdots + a_m f_m(u_m) = 0 + \cdots + a_i v_i + \cdots + 0.$$

Dobimo torej $a_i v_i = 0$, od koder, zaradi neničelnosti elementa v_i, sledi $a_i = 0$. Ker je bil i poljuben, velja $a_1 = \ldots = a_m = 0$, kar pomeni, da so $f_1, \ldots, f_m$ linearno neodvisni nad F. Od tod torej sledi $m \leq [A' : F]$. Ker je A končno razsežna nad F, je tudi A' končno razsežna nad F. Posledično mora biti tudi V končno razsežen nad O. Že dokazana posledica tedaj pravi, da je $\mathrm{End}_O(V)$ edina gosta algebra linearnih operatorjev nad vektorskim prostorom V. To pa pomeni $A' \cong \mathrm{End}_O(V)$ in posledično $A \cong \mathrm{End}_O(V)$. Kot smo videli v petem razdelku, potem še dodatno velja $A \cong M_n(O^o)$, kjer je n dimenzija V nad O. □

S tem smo dokazali Wedderburnov strukturni izrek za končno razsežne algebre. Vidimo, da je struktura algebre, pa četudi smo skorajda skozi celotno besedilo govorili o kolobarjih, zelo pomembna. Predvsem dejstvo, da ima vsaka končno razsežna algebra minimalen levi ideal, se je izkazalo za ključno pri obravnavi strukturnega izreka.

Nedvomno na kratko obravnavana veja algebre, ki je bila predstavljena v tem besedilu, ponuja še mnoge zanimivosti. Že s samo teorijo primitivnih kolobarjev bi lahko nadaljevali in prišli do vpeljave primitivnih idealov, Jacobsonovega radkala in še mnogih drugih pojmov ter zanimivih rezultatov. A vse to presega temo tega besedila, v katerem smo glavni cilj, dokazati Wedderburnov strukturni izrek, izpolnili.

Slovar strokovnih izrazov

algebra algebra

annihilator of a module anihilator modula – anihilator K-modula M, kjer je K kolobar, je podmnožica K, v kateri ležijo taki $k \in K$, da velja $kM = 0$

dense ring of linear operators of a vector space gost kolobar linearnih operatorjev vektorskega prostora – podkolobar kolobarja endomorfizmov vektorskega prostora

ideal ideal

opposite ring nasprotni kolobar – nasprotni kolobar kolobarja vsebuje enake elemente kot sam kolobar, z enako definiranim seštevanjem, množenje pa je definirano z $xy = y \cdot x$, kjer s $\cdot$ označimo množenje v prvotnem kolobarju

nilpotent ideal nilpotenten ideal – ideal I kolobarja, za katerega obstaja tako naravno število n, da velja $I^n = 0$

K-module K-modul – abelova grupa M s preslikavo iz $K \times M$ v M, kjer je K poljuben kolobar

semiprime ring polprakolobar – kolobar, ki nima nilpotentnih idealov

prime ring prakolobar – kolobar, v katerem je produkt poljubnih neničelnih idealov neničeln

primitive ring primitiven kolobar – kolobar, ki ima enostaven zvest modul

vector space over a division ring vektorski prostor nad obsegom – enotski modul nad obsegom

Literatura

[1] M. Brešar, *Introduction to noncommutative algebra*, Universitext, Springer International Publishing, Cham, 2014.
[2] M. Brešar, *Uvod v algebro*, Matematični rokopisi **26**, DMFA – založništvo, Ljubljana, 2018; dostopno tudi na `www.fmf.uni-lj.si/~bresar/documents/UvodVAlgebro2018.pdf`.
[3] Y. A. Drozd in V. V. Kirichenko, *Finite dimensional algebras*, Springer-Verlag, Berlin, 1994; dostopno tudi na `www.imath.kiev.ua/~drozd/drozd-kirichenko_en.pdf`.
[4] T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics **73**, Springer, Berlin, 1974.
[5] L. H. Rowen, *Graduate algebra: noncommutative view*, Graduate Studies in Mathematics **91**, American Mathematical Society, Providence, 2008.