UNIVERZA V MARIBORU
FAKULTETA ZA NARAVOSLOVJE IN MATEMATIKO
Oddelek za matematiko in računalništvo

Diplomsko delo

JORDAN - HÖLDERJEV IZREK

Mentor:
dr. Dominik Benkovič
izredni profesor

Kandidatka:
Ana Skok

Maribor, 2012

Zahvala

Najprej se iskreno zahvaljujem svojim staršem, ki so mi omogočili študij in me na tej poti spodbujali. Zahvala gre tudi mentorju dr. Dominiku Benkoviču za njegove nasvete in pomoč pri izdelavi diplomskega dela.

UNIVERZA V MARIBORU
FAKULTETA ZA NARAVOSLOVJE IN MATEMATIKO
Oddelek za matematiko in računalništvo

Izjava

Podpisana Ana Skok, rojena 2.2.1987, študentka Fakultete za naravoslovje in matematiko Univerze v Mariboru, smer matematika, izjavljam, da je diplomsko delo z naslovom

Jordan - Hölderjev izrek

pri mentorju izred. prof. dr. Dominiku Benkoviču avtorsko delo. V diplomskem delu so uporabljeni viri in literatura korektno navedeni; teksti niso prepisani brez navedbe avtorjev.

Ptuj, maj 2012 Ana Skok

Program diplomskega dela: Jordan - Hölderjev izrek

V diplomskem delu naj bo predstavljen Jordan - Hölderjev izrek in obravnavane naj bodo osnovne lastnosti kompozicijskih vrst, verižnih pogojev in eksaktnih zaporedij na strukturi modulov.

Osnovni viri:

- T. W. Hungerford, *Algebra*, Springer-Verlag, 1989.
- N. Jacobson, *Basic Algebra II*, W. H. Freeman & Company, 1989.
- L. Rowen, *Ring Theory*, Academic Press, Inc, 1988.

izred. prof. dr. Dominik Benkovič

SKOK, A. : Jordan - Hölderjev izrek

Diplomsko delo, Univerza v Mariboru, Fakulteta za naravoslovje in matematiko, Oddelek za matematiko in računalništvo, 2012.

Izvleček

V diplomskem delu je predstavljen Jordan - Hölderjev izrek na strukturi modulih. Na začetku so na kratko predstavljeni osnovni pojmi kolobarjev, idealov in modulov. Nato se seznanimo še z verižnimi pogoji, eksaktnimi zaporedji in kompozicijskimih vrstami, ki so potrebni za razumevanje celotnega diplomskega dela. Na koncu je predstavljen Jordan - Hölderjev izrek, ki ga dokažemo na dva različna načina. Pri prvem načinu si pomagamo s pomočjo pojma dolžina modula, medtem ko se pri drugem načinu dokazovanja opremo na Schreierjev izrek.

Ključne besede: kolobar, modul, verižni pogoj, eksaktno zaporedje, kompozicijska vrsta, Jordan - Hölderjev izrek.

Math. Subj. Class. (2010): 16D10, 16P20, 16P40.

SKOK, A.: The Jordan - Hölder theorem.

Graduation Thesis, University of Maribor, Faculty of Natural Sciences and Mathematics, Department of Mathematics and Computer Science, 2012.

Abstract

In graduation thesis the Jordan - Hölders theorem on modules is presented. At the begining we introduce the basics of rings, modules and ideals. Next we consider the chain conditions, exact sequence and composition series, which are nessesery to understand the hole thesis. In the end part of the thesis we present the Jordan - Hölders theorem, which we can prove on two different ways. In the first way we help ourselves with the definition of length, and in the second way we depend on Schreiers theorem.

Key words: ring, module, chain condition, exact sequence, composition series, the Jordan - Hölder theorem.

Math. Subj. Class. (2010): 16D10, 16P20, 16P40.

Kazalo

Poglavje 1

Uvod

Diplomsko delo obsega uvodno in še tri poglavja. Osrednja tema diplomskega dela je Jordan - Hölderjev izrek na strukturi modulov.

V drugem poglavju predstavimo že znane osnovne pojme iz algebre. Predstavljeni so kolobarji, ideali in moduli, njihove lastnosti in primeri, ter osnovni izreki, ki so potrebni za razumevanje nadaljnih poglavij.

V tretjem poglavju se seznanimo z verižnimi pogoji, eksaktnimi zaporedji in kompozicijskimi vrstami. Pri verižnih pogojih se ukvarjamo z artinskimi in noetherskimi kolobarji, maksimalnimi in minimalnimi pogoji ter njihovimi lastnostmi in povezavami. Za lažje razumevanje artinskih in noetherskih kolobarjev so podani tudi zgledi. Jordan - Hölderjev izrek je lahko formuliran, ko je opredeljen pojem kratkih eksaktnih zaporedij, ki pa je zaporednje modulskih homomorfizmov. Pri kompozicijskih vrstah podamo definicijo normalne vrste, kaj so to faktorji, dolžina vrste ter kaj pomeni nadaljevanje vrste.

Če ima grupa kompozicijsko vrsto, potem sta poljubni dve njeni kompozicijski vrsti izomorfni. Camille Jordan in Otto Hölder sta raziskovala grupe v povezavi s problemom rešljivosti enačb z radikali (Galoiseva teorija). Jordan je predstavil, da so indeksi dveh vrst enakega tipa (to so indeksi podgrup) enaki, razen njihovega reda. Z drugimi besedami, bilo je dokazano, da je zaporedje redov kvocientov dveh kompozicijskih vrst enako do permutacije. Hölder je dokazal, da so ustrezni faktorji izomorfni. Schreier je dokazal močnejšo trditev: Vsaki dve normalni vrsti poljubne grupe imata izomorfno nadaljevanje. Jordan-Hölderjev izrek je bil prav tako dokazan za grupe z operatorji, od koder sledi analogen izrek za invariantne in popolnoma neodvisne vrste. Kasnejše posplošitve so šle v več smeri, Jordan - Hölderjev izrek je bil razširjen na vrste idealov v kolobarjih in druge algebraične strukture.

Četrto poglavje vsebuje dokaz Jordan - Hölderjev izreka, ki pravi, da sta dve poljubni kompozicijski vrsti ekvivalentni. Ta izrek dokažemo na dva načina. Pri prvem načinu si pomagamo z definicijo dolžine.modula po analogiji z dimenzijo vektorskega prostora. Vpeljemo lastnosti dolžine levega K-modula in definiramo število $d(M)$ kot dolžino maksimalne verige podmodulov modula M. Potem na podlagi treh primerov dokažemo izrek. Pri drugem načinu, moramo najprej vpeljati Zassenhausovo lemo, da lahko dokažemo Schreierjev izrek, na katerega se moramo opreti, da lahko dokažemo Jordan - Hölderjev izrek, namreč Jordan - Hölderjev izrek je posledica Schreirjevega izreka.

Poglavje 2

Osnovni pojmi

V tem poglavju bomo navedli nekatere že znane pojme iz algebre. Omejili se bomo le na tiste osnovne pojme kolobarjev, idealov in modulov, ki jih bomo potrebovali v nadaljevanju.

2.1 Kolobarji in ideali

Kolobar je ime za algebrsko strukturo, v kateri je možno brez omejitev seštevati, odštevati in množiti. Oznaka: $(K, +, \cdot)$.

Definicija 2.1 *Kolobar je neprazna množica K skupaj z binarnima operacijama $+ : K \times K \to K$ in $\cdot : K \times K \to K$, za kateri velja*

(i) komutativnost seštevanja: $a + b = b + a$ za vse $a, b \in K$;

(ii) asociativnost seštevanje: $a + (b + c) = (a + b) + c$ za vse $a, b, c \in K$;

(iii) obstaj nevtralnega elementa za seštevanje: $a + 0 = a$ za vsak $a \in K$;

(iv) obstoj nasprotnega elementa: $a + (-a) = 0$ za vsak $a \in K$;

(v) asociativnost množenje: $a(bc) = (ab)c$ za vse $a, b, c \in K$;

(vi) distributivnost: za vse $a, b, c \in K$ velja

$$a(b + c) = ab + ac \quad \textit{in} \quad (a + b)c = ac + bc.$$

Zaradi lastnosti *(i)-(iv) je kolobar K* Abelova grupa za seštevanje. Kolobar K je *komutativen*, če je množenje komutativno, torej $ab = ba$ za vse $a, b \in K$. *Center* kolobarja je množica tistih elementov, ki komutirajo z vsakim elementom iz kolobarja K

$$Z(K) = \{c \in K | ca = ac \text{ za vsak } a \in K\}.$$

Nevtralni element za množenje (če seveda obstaja) imenujemo *enota* kolobarja ali identiteta kolobarja. Označujemo ga s simbolom 1; torej velja $1a = a1 = a$ za vsak $a \in K$. Element $a \in K$ imenujemo *(levi) delitelj niča*, če je $ab = 0$ za neki $b \neq 0 \in K$. Kolobar K je *cel kolobar*, če nima pravih deliteljev niča; torej iz $ab = 0$ sledi $a = 0$ ali $b = 0$. V celih kolobarjih velja pravilo krajšanja; če je $ab = ac$ in $a \neq 0$, potem je $b = c$.

Element $b \in K$ je *desni inverz* elementa $a \in K$, če je $ab = 1$. V tem primeru je tudi a *levi inverz* elementa b. Element, ki je hkrat levi in desni inverz elementa a, imenujemo *inverz* elementa a in ga označimo z a^{-1}(t.j. $aa^{-1} = a^{-1}a = 1$). Element a je *obrnljiv*, če obstaja inverz a^{-1}. Vpeljimo $K^* = \{a \in K | a \text{ obrnljiv}\}$. Očitno je K^* grupa, ki se imenuje grupa vseh obrnljivih elementov kolobarja K. Kolobar K z enoto $1 \neq 0$ imenujemo *obseg*, če je vsak njegov neničelni element obrnljiv (t.j. $K^* = K \backslash \{0\}$).

Podmnožica K' kolobarja K je *podkolobar*, če iz $x, y \in K'$ sledi $x+y, -x, xy \in K'$. Torej , če je K' za isti operaciji tudi sama kolobar. Algebra $A = (A, +, *, \cdot)$ je kolobar $(A, +, *)$, ki je hkrati vektorski prostor $(A, +, \cdot)$ nad komutativnim obsegom F.

Naj bosta K in K' kolobarja. Preslikavi $\varphi : K \to K'$ pravimo *homomorfizem* (kolobarjev), če za vse $x, y \in K$ velja

$$\varphi(x + y) = \varphi(x) + \varphi(y) \qquad \text{in} \qquad \varphi(xy) = \varphi(x) \cdot \varphi(y).$$

Bijektivni homomorfizem se imenuje *izomorfizem*. Kolobarja K in K' sta si *izomorfna*, če med njima obstaja izomorfizem $\varphi : K \to K'$. *Endomorfizem* je homomorfizem, ki slika iz kolobarja K vase. *Avtomorfizem* je bijektivni endomorfizem, *monomorfizem* je injektivni homomorfizem in z *epimorfizmom* označujemo surjektivni homomorfizem. Naj bo $\varphi : K \to K'$ homomorfizem, tedaj je *jedro homomorfizma* množica

$$\ker \varphi = \{x \in K | \varphi(x) = 0\} \subseteq K$$

in *slika homomorfizma* φ je množica

$$\operatorname{im} \varphi = \{\varphi(x) | x \in K\} \subseteq K'.$$

Ideal (tudi ideal kolobarja) je v teoriji kolobarjev posebna podmnožica kolobarjev. Podmnožica L kolobarja K je *levi ideal* kolobarja K, če velja:

(i) L je Abelova grupa za seštevanje (t.j. $\forall u, v \in L : u \pm v \in L$),

(ii) za vsak $x \in K$ in za vsak $u \in L$ je $xu \in L$.

Podobno definiramo *desni ideal* D, le da v točki (ii) zahtevamo $DK \subseteq D$. Podmnožica $I \subseteq K$, ki je hkrati levi in desni ideal, se imenuje *ideal* kolobarja K. Neposredno z računom lahko preverimo, da je jedro vsakega homomorfizma $\ker \varphi$ ideal kolobarja K.

Naj bo I ideal kolobarja K, če v množico vseh odsekov

$$K/I = \{x + I | x \in K\}$$

vpeljemo seštevanje in množenje takole:

$$(x + I) + (y + I) = (x + y) + I,$$
$$(x + I)(y + I) = xy + I,$$

postane K/I kolobar. Kolobar K/I imenujemo *kvocientni ali faktorski kolobar.* Preslikava $q : K \to K/I$, definirana s predpisom $q(x) = x + I$ je homomorfizem kolobarjev. To sledi iz definicije seštevanja in množenja v K/I. Homomorfizem q imenujemo *kvocientna preslikava* ali *kvocientni homomorfizem.*

Naj bo $S \subseteq K$. Zaradi enostavnosti, naj bo $1 \in K$. Najmanjši levi ideal kolobarja K, ki vsebuje množico S, se imenuje levi ideal *generiran* z S in je enak

$$KS = \{x_1 s_1 + x_2 s_2 + ... + x_n s_n | x_i \in K, s_i \in S, n \in \mathbb{N}\}.$$

Podobno je desni ideal kolobarja K generiran z množico S enak

$$SK = \{s_1 x_1 + s_2 x_2 + ... + s_n x_n | x_i \in K, s_i \in S, n \in \mathbb{N}\}$$

in (dvostranski) ideal generiran z S je

$$KSK = \{x_1 s_1 y_1 + ... + x_n s_n y_n | x_i, y_i \in K, s_i \in S, n \in \mathbb{N}\}.$$

Ideal generiran z enim samim elementom imenujemo *glavni ideal.* Če je K komutativen kolobar z enoto, je vsak glavni ideal oblike

$$aK = \{ax | x \in K\}.$$

Običajna oznaka za glavni ideal generiran z elementom a je (a).

Kolobar K z netrivialnim množenjem imenujemo *enostavni kolobar*, če sta njegova edina (dvostranska) ideala 0 in K. Levi ideal M kolobarja K je *maksimalni levi ideal*, če $M \neq K$ in če ne obstaja tak levi ideal L, da bi veljalo $M \subsetneq L \subsetneq K$.

Izrek 2.2 *Naj bo I ideal kolobarja K. Preslikava $\pi : K \to K/I$, podana z $\pi(k) = k + I$, je surjektiven kolobarski homomorfizem z jedrom I.*

Dokaz. Dejstvo, da preslikava π ohranja seštevanje in množenje sledi iz definicije seštevanja in množenja pri K/I. Homomorfizem π je surjektiven, saj je poljuben odsek $k+I$ slika $k \in K$. Jedro je množica vseh $k \in K$, tako da je $\pi(k) = 0 + I$, ničelni element iz K/I. Ampak $k+I = 0+I$ natanko tedaj, ko je $k \in I$. Torej je jedro homomorfizma π enako I. $\square$

Izrek 2.3 *Naj bo $f : K \to S$ poljuben homomorfizem kolobarjev in naj bo $N = \ker f$. Potem je N ideal v K.*

Dokaz. Vemo, da je $0 \in N$, torej $N \neq \emptyset$. Naj bosta $a, b \in N$. Potem je $f(a) = f(b) = 0$, tako da je $f(a-b) = f(a) - f(b) = 0$. Za poljuben $k \in K, f(ka) = f(k)f(a) = f(k) \cdot 0 = 0$. Podobno, $f(ak) = f(a)f(k) = 0$. Torej so $a-b, ka$ in ak tudi v K, zato je N ideal. $\square$

Izrek 2.4 *Naj bo $f : K \to S$ poljuben homomorfizem kolobarjev z jedrom N. Potem je f injektiven natanko tedaj, ko je $N = (0)$.*

Dokaz. Vemo, da je $f(0) = 0$. Če je $f(k)$ enak 0, potem je $k = 0$, saj je f injektiven. Zato je $N = (0)$.

Obratno, predpostavimo da je $f(a) = f(b)$. Potem je $f(a-b) = f(a) - f(b) = 0$, torej $a - b \in N = (0)$, zato je $a - b = 0$ in $a = b$, torej je f injektiven. $\square$

Kadar je $f : K \to S$ surjektivni homomorfizem, rečemo da je S homomorfna slika kolobarja K. V naslednjem izreku bomo vidli, da vsak surjektivni homomorfizem res deluje kot $K \to K/I$.

Izrek 2.5 ***(Osnovni izrek o izomorfizmih)*** *Naj bo $f : K \to S$ surjektivni homomorfizem kolobarjev z jedrom N. Potem je kvocientni kolobar K/N izomorfen kolobarju S.*

Dokaz. Definirajmo preslikavo $\Phi : K/N \to S$ z $\Phi(k+N) = f(k)$. Preveriti moramo, da je Φ dobro definirana. Predpostavimo, da je $k + N = t + N$; potem je $k - t \in N$, tako da je $f(k) = f(k-t+t) = f(k-t) + f(t) = 0 + f(t) = f(t)$. Torej je Φ dobro definiran. Zdaj še preverimo, da je Φ homomorfizem:

$$\begin{aligned}
\Phi((k+N) + (t+N)) &= \Phi((k+t) + N) \\
&= f(k+t) = f(k) + f(t) \\
&= \Phi(k+N) + \Phi(t+N)
\end{aligned}$$

in

$$\begin{aligned}\Phi((k+N)(t+N)) &= \Phi((kt)+N)\\ &= f(kt) = f(k)f(t)\\ &= \Phi(k+N)\Phi(t+N)\end{aligned}$$

Za poljuben $s \in S$ vemo, da je za nek $k \in K$ z $f(k) = s$ in zato je $\Phi(k+N) = s$. S tem smo pokazali, da je Φ surjektiven. Da vidimo, da je Φ injektiven, moramo pokazati, da je $\ker \Phi$ enako nič v K/N: če je $\Phi(k+N) = 0$, potem je $f(k) = 0$, torej $k \in N$, zato je $k+N = 0+N$. S tem smo dokazali, da je $\Phi : K/N \to S$ izomorfizem. $\square$

2.2 Moduli

Definicija modula je formalno enaka, kot definicija vektorskega prostora, le da vlogo skalarjev zamenjajo elementi poljubnega kolobarja.

Definicija 2.6 *Množica M je levi modul nad kolobarjem K (ali levi K-modul), če velja:*

1. *M je Abelova grupa za seštevanje $+$.*
2. *Definirana je operacija $K \times M \to M, (x, m) \to xm \in M$ (modulsko množenje), za katero velja:*

   $(x+y)m = xm + ym$ *za vse $x, y \in K$ in vsak $m \in M$,*

   $x(m+n) = xm + xn$ *za vsak $x \in K$ in vse $m, n \in M$,*

   $(xy)m = x(ym)$ *za vse $x, y \in K$ in vsak $m \in M$.*

Če je K kolobar z enoto in velja tudi $1 \cdot m = m$ za vsak $m \in M$, potem M imenujemo *enotski modul*.

Primeri:

1. Vektorski prostor V nad poljem F je F-modul.
2. Vsaka Abelova grupa A je $\mathbb{Z}$-modul, če definiramo: $n \cdot a = a + \cdots + a$, $0 \cdot a = 0$ in $(-n) \cdot a = -(a + \cdots + a)$.

3. Naj bo L levi ideal kolobarja K. Potem levi ideal L lahko obravnavamo kot levi K-modul, če vzamemo za modulsko množenje kar običajno množenje $kl \in L$.

4. Spet naj bo L levi ideal kolobarja K. V množici vseh odsekov $K/L = \{k + L | k \in K\}$ vpeljimo seštevanje in modulsko množenje:

$$\begin{aligned} (k+L)+(k'+L) &= (k+k')+L \\ k(k'+L) &= kk'+L \end{aligned}$$

   za vse $k, k' \in K$. S tem množica K/L postane levi K-modul.

5. Naj bo V vektorski prostor nad poljem F in $K = End(V)$ kolobar linearnih operatorjev vektorskega prostora V. Potem lahko vektorski prostor V obravnavamo kot levi K-modul, če definiramo:

$$\begin{aligned} Av &= A(v) \in V, \\ (A+B)v &= Av + Bv, \\ A(v+w) &= Av + Aw, \\ (AB)v &= A(Bv) \end{aligned}$$

   za vse $v, w \in V$ in vse $A, B \in K$.

Množica M je *desni modul* nad kolobarjem K (ali *desni K-modul*), če velja:

1. M je Abelova grupa za seštevanje.

2. Definirana je operacija $M \times K \to M, (m, x) \to mx \in M$ (modulsko množenje), za katero velja:

   $m(x + y) = mx + my \quad$ za vse $x, y \in K$ in vsak $m \in M$,

   $(m + n)x = mx + nx \quad$ za vsak $x \in K$ in vse $m, n \in M$,

   $m(xy) = (mx)y \quad$ za vse $x, y \in K$ in vsak $m \in M$.

Na desni ideal D kolobarja K lahko gledamo kot na desni K-modul, ne pa tudi kot levi K-modul. *Bimodul* nad kolobarjem K (ali *K-bimodul*) je levi K-modul, ki je hkrati desni K-modul in v katerem velja

$$(xm)y = x(my) \quad \text{za vse } x, y \in K, m \in M.$$

Primera

1. Če je I ideal kolobarja K, lahko na I gledamo kot na K-bimodul.
2. Če je K podkolobar kolobarja R, lahko R obravnavamo kot K-bimodul ($kr \in R, rk \in R$).

Vsak neničelni levi K-modul ima vsaj dva podmodula, to sta M in ničelni podmodul 0.

Definicija 2.7 *Neničelni levi K-modul M, ki ima samo 0 in M kot svoja podmodula imenujemo* enostavni modul. Minimalni podmodul *modula M je enostaven podmodul modula M. Ustrezen podmodul modula M je* maksimalni podmodul *modula M, če je katerikoli N' podmnožica M, tako da če je $N \subseteq N' \subseteq M$, je $N = N'$ ali $N' = M$.*

Iz definicije sledi, da je L minimalni levi ideal kolobarja K natanko tedaj, ko je L enostaven levi K-modul.

Definicija 2.8 *Naj bo N podmodul K-modula modula M in recimo, da je S podmnožica od N. Če vsak element $x \in N$ lahko zapišemo kot*

$$x = a_1x_1 + a_2x_2 + \cdots + a_nx_n,$$

kjer je $x_i \in S$ in $a_i \in K$ za vse $i = 1, 2, ...n$, potem rečemo, da je S množica generatorjev *od N oziroma, da je N* generiran *z S. Če je N generiran z S, zapišemo $N = \sum_S Kx$ in ko je S končna množica, pravimo da je N končno generiran.*

Vsak levi K-modul modula M ima vsaj eno množico generatorjev, namreč množico M.

Če je N podmodul modula M, lahko definiramo *kvocientni modul M/N.* Njegovi elementi so odseki $m + N, m \in M$, operaciji seštevanja in modulskega množenja definiramo takole

$$(m + N) + (m' + N) = (m + m') + N$$
$$x(m + N) = xm + N$$

za vse $m, m' \in M$ in vsak $x \in K$.

V nadaljevanju bomo uporabljali leve K-module, zato bomo pridevnik levi izpuščali. Podmnožica N modula M je *podmodul* modula M, če je za isti operaciji

N tudi sama modul. Če sta M in M' K-modula, potem preslikavo $\varphi : M \to M'$ imenujemo (*modulski*) *homomorfizem*, če velja

$$\begin{aligned} \varphi(m+n) &= \varphi(m) + \varphi(n) \quad \text{za vse } m, n \in M, \\ \varphi(xm) &= x\varphi(m) \quad \text{za vsak } x \in K \text{ in vsak } m \in M. \end{aligned}$$

Če imamo podan modulski homomorfizem $\varphi : M \to N$, je jedro φ množica:

$$\ker \varphi = \{m \in M | \varphi(m) = 0\}$$

in slika od φ je množica:

$$\operatorname{im} \varphi = \{n \in N | \exists m \in M, \varphi(m) = n\}.$$

Z $\hom_K(M, M')$ označimo množico vseh modulskih homomorfizmov, ki slikajo iz M v M'. Množico $\hom_K(M, M')$ opremimo s seštevanjem in množenjem z elementi iz K

$$\begin{aligned} (f+g)(m) &= f(m) + g(m) \quad \text{za vse } f, g \in \hom_K(M, M'), \\ (xf)(m) &= xf(m) \quad \text{za vsak } f \in \hom_K(M, M') \text{ in vsak } x \in K \end{aligned}$$

in tako postane K-modul.

Trditev 2.9 *Če je M K-modul, potem je $\hom_K(K, M) \cong M$ kot K-modul.*

Dokaz. Naj bo $\varphi : \hom_K(K, M) \to M$, tako da je $\varphi(f) = f(1)$. Potem je $\varphi(f+g) = (f+g)(1) = f(1)+g(1) = \varphi(f)+\varphi(g)$ in $\varphi(af) = (af)(1) = f(a) = af(1) = a\varphi(f)$, torej je φ modulski homomorfizem. Če je $f \in \ker \varphi$, potem $0 = \varphi(f) = f(1)$ očitno implicira da je $f = 0$, torej je φ injektiven. Če je $x \in M$, potem je $f_x : K \to M$ definiran z $f_x(a) = ax$ homomorfizem in $\varphi(f_x) = x$. Torej je φ tudi surjektiven. □

Izrek 2.10 (Osnovni izrek o izomorfizmih) *Naj bosta M in M' K-modula in $\varphi : M \to M'$ K-homomorfizem. Potem je*

$$\ker \varphi = \{m \in M | \varphi(m) = 0\}$$

K-podmodul modula M in

$$\operatorname{im} \varphi = \{\varphi(m) | m \in M\}$$

je K-podmodul modula M' in obstaja K-izomorfizem $\Phi : M/\ker \varphi \to \operatorname{im} \varphi$, tako da je $\Phi(m + \ker \varphi) = \varphi(m)$ za vse $m \in M$.

Opomba. Podoben izrek velja za vektorske prostore: če sta U in V vektorska prostora in je $f : V \to V$ linearna preslikava, potem sta jedro in slika od f podprostora V in W in kvocientni prostor $V/\ker f$ je izomorfen $\operatorname{im} f$. Izreku rečemo tudi "Osnovni izrek linearnih preslikav". Ker sta vektorska prostora izomorfna natanko tedaj, ko imata enako dimenzijo in ker ni težko pokazati da je $\dim(V/U) = \dim V - \dim U$, se trditev glasi $\dim V = \dim(\ker f) + \dim(\operatorname{im} f)$.

Dokaz. Najprej pokažimo, da je jedro K-podmodul modula M. Ker je φ linearen, je $\varphi(0_M) = 0_{M'}$ in tako je $0_M \in \ker \varphi$. Če sta $m_1, m_2 \in \ker \varphi$, potem je $\varphi(m_1+m_2) = \varphi(m_1) + \varphi(m_2) = 0 + 0 = 0$, torej je $m_1 + m_2 \in \ker \varphi$ in sledi, da je φ zaprt za seštevanje. Če je $m \in \ker \varphi$ in $x \in K$, potem je $\varphi(xm) = x\varphi(m) = x0 = 0$ in sledi, da je $\ker \varphi$ zaprt za množenje. Zdaj še dokažimo, da je $\operatorname{im} \varphi$ podmodul M'. Če sta $n_1, n_2 \in \operatorname{im} \varphi$, potem je $n_1 = \varphi(m_1)$ in $n_2 = \varphi(m_2)$ za nekatere $m_i \in M$ in ker je $n_1 + n_2 = \varphi(m_1) + \varphi(m_2) = \varphi(m_1 + m_2)$ sledi, da je $\operatorname{im} \varphi$ zaprta za seštevanje. Podobno za zaprtost za množenje, če je $n = \varphi(m) \in \operatorname{im} \varphi$, potem imamo za vse $x \in K$, $xn = \varphi(xm) \in \operatorname{im} \varphi$ in za vse $\psi \in K$ imamo $\psi n = \psi\varphi(m) = \varphi(\psi m) \in \operatorname{im} \varphi$. Torej je $\operatorname{im} \varphi$ podmodul M'.

Ker je $\ker \varphi$ podmodul M, kvocientni modul $M/\ker \varphi$ obstaja. Moramo pokazati, da je preslikava $\Phi : M/\ker \varphi \to \operatorname{im} \varphi$ dobro definirana, tako da je $\Phi(m + \ker \varphi) = \varphi(m)$ za vse $m \in M$. Zagotovo drži, da je $\varphi(m) \in \operatorname{im} \varphi$ za vse m, torej moramo samo pokazati, da če sta $m_1, m_2 \in M$, kjer je $m_1 + \ker \varphi = m_2 + \ker \varphi$, potem je $\varphi(m_1) = \varphi(m_2)$. Ampak to je očitno: če je $m_1 + \ker \varphi = m_2 + \ker \varphi$ potem je $m_1 - m_2 \in \ker \varphi$, torej $\varphi(m_1 - m_2) = 0$ in $\varphi(m_1) = \varphi(m_2)$.

Zdaj, ko smo videli, da je preslikava Φ dobro definirana, nam ostane še samo, da pokažemo da je bijektivna in zaprta za seštevanje in množenje. Naj bosta $m, n \in M$ in $x \in K$, potem je:

$$\begin{aligned}
\Phi((m + \ker \varphi) + (n + \ker \varphi)) &= \Phi((m + n) + \ker \varphi) \\
&= \varphi(m + n) = \varphi(m) + \varphi(n) \\
&= \Phi(m + \ker \varphi) + \Phi(n + \ker \varphi)
\end{aligned}$$

in

$$\begin{aligned}
\Phi(x(m + \ker \varphi)) &= \Phi(xm + \ker \varphi) \\
&= \varphi(xm) = x\varphi(m) \\
&= x\Phi(m + \ker \varphi)
\end{aligned}$$

podobno za $\psi \in K$:

$$\Phi(\psi(m + \ker\varphi)) = \Phi(\psi m + \ker\varphi) = \varphi(\psi m) = \psi\Phi(m + \ker\varphi)$$

Surjektivnost Φ je očitna: po definiciji, je vsak element iz $\operatorname{im}\varphi$ oblike $\varphi(m) = \Phi(m+\ker\varphi)$ za nekatere $m \in M$. Inkjektivnost: če je $\Phi(m_1+\ker\varphi) = \Phi(m_2+\ker\varphi)$, potem je $\varphi(m_1) = \varphi(m_2)$, torej je $\varphi(m_1 - m_2) = 0$ in sledi, da je $m_1 - m_2 \in \ker\varphi$ in zato je $m_1 + \ker\varphi = m_2 + \ker\varphi$. □

Izrek 2.11 (Drugi izrek o izomorfizmih) *Če sta M_1 in M_2 podmodula K-modula modula M, tako da je $M_1 \subseteq M_2$, potem je M_2/M_1 podmodul M/M_1 in*

$$(M/M_1)/(M_2/M_1) \cong M/M_2.$$

Dokaz. Enolično pokažemo, da je M_2/M_1 podmodul M/M_1. Dalje, preslikava $\varphi : M/M_1 \to M/M_2$ podana z $\varphi(m_1+M_1) = m_1+M_2$ je dobro definirana. Zagotovo drži, da če je $m_1+M_1 = m_2+M_2$, potem je $m_1-m_2 \in M_1 \subseteq M_2$, torej $\varphi(m_1+M_1) = m_1+M_2 = m_2+M_2 = \varphi(m_2+M_2)$. Dalje, z lahkoto pokažemo, da je φ epimorfizem z jedrom M_2/M_1, torej rezultat sledi iz osnovnega izreka o homomorfizmih. □

Izrek 2.12 (Tretji izrek o izomorfizmih) *Če sta M_1 in M_2 podmodula K-modula modula M, potem je*

$$M_1/(M_1 \cap M_2) \cong (M_1 + M_2)/M_2.$$

Dokaz. Epimorfizem $\varphi : M_1 \to (M_1 + M_2)/M_2$ definiran z $\varphi(m) = m + M_2$ ima jedro $M_1 \cap M_2$. Drugi izrek o izomorfizmih nam da željen rezultat. □

Poglavje 3

Verižni pogoji, eksaktna zaporedja in kompozicijske vrste

3.1 Verižni pogoji

V tem poglavju bomo povzeli osnovna dejstva o naraščajočih in padajočih verigah za module in kolobarje.

Definicija 3.1 *Modul A zadošča* pogoju naraščajočih verig na podmodulih, *če za vsako naraščajočo verigo $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$ podmodulov modula A, obstaja naravno število n, da je $A_i = A_n$ za vsak $i \geq n$. Verigi iz definicije pravimo, da je stacionarna veriga, tak modul se imenuje* noetherski.

Definicija 3.2 *Modul B zadošča* pogoju padajočih verig na podmodulih, *če za vsako padajočo verigo $B_1 \supseteq B_2 \supseteq B_3 \supseteq \cdots$ podmodulov modula B, obstaja naravno število m, da je $B_i = B_m$ za vsak $i \geq m$. Verigi iz definicije pravimo, da je stacionarna veriga, tak modul se imenuje* artinski.

Zgled: Naj bo $\mathbb{Z}$ kolobar celih števil. Potem $\mathbb{Z}$ kot $\mathbb{Z}$-modul, zadošča pogoju padajočih verig na podmodulih, vendar ne zadošča pogoju naraščajočih verig na podmodulih. Namreč vidimo, da $2\mathbb{Z}$ vsebuje $4\mathbb{Z}$, potem vsebuje $8\mathbb{Z}, ...$torej dobimo $2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z} \supset \cdots$ neskončno padajočo verigo, ki ni stacionarna. Zdaj pokažimo, da je $\mathbb{Z}$-modul $\mathbb{Z}$ noetherski modul. Namreč iz vsebovanosti $n_1\mathbb{Z} \subseteq n_2\mathbb{Z} \subseteq n_3\mathbb{Z} \subseteq \cdots$, sledi $n_1 = k_1 n_2$, $n_2 = k_2 n_3$, ... To pomeni, $n_1 \geq n_2 \geq n_3 \ldots$. Ker je množica naravnih števil dobro urejena, obstaja n_i, da je $n_k = n_i$ za vsak $k \geq i$. Zato je dana veriga stacionarna.

Če privzamemo, da je kolobar K levi K-modul, potem lahko rečemo, da so njegovi podmoduli K natanko levi ideali kolobarja K. Posledično, v tem primeru običajno rečemo, pogojna veriga na levih in desnih idealih namesto podmodulih.

Definicija 3.3 *Kolobar K je* levi (desni) noetherski kolobar*, če K ustreza pogoju naraščajočih verig na levih (desnih) idealih. K je noetherski kolobar, če je K hkrati levi in desni noetherski kolobar.*

Definicija 3.4 *Kolobar K je* levi (desni) artinski kolobar*, če K ustreza pogoju padajočih verig na levih (desnih) idealih. K je artinski kolobar, če je K hkrati levi in desni artinski kolobar.*

Z drugimi besedami, kolobar K je (levi ali desni) noetherski kolobar, če je (levi ali desni) noetherski K-modul, podobno velja za artinske. Posledično, vse kasnejše definicije in rezultati glede modulov, ki zadoščajo pogoju naraščajočih ali padajočih verig na podmodulih se nanašajo tudi na *noetherske ali artinske kolobarje.*

Zgled. Obseg D je noetherski in artinski kolobar, namreč edina leva oz. desna ideala obsega D sta D in 0. Vsak glavni komutativen kolobar je noetherski; posebni primeri takih kolobarjev so $\mathbb{Z}$, $\mathbb{Z}_n$, $F[X]$, kjer je F polje.

Zgled. Kolobar $M_n(D)$ vseh $n \times n$ matrik nad obsegom D je tako noetherski kot artinski kolobar. To bomo dokazali v nadaljevanju.

Opomba: Desni noetherski (artinski) kolobar ni nujno levi noetherski (artinski) kolobar. To dokazujeta naslednja zgleda.

Predno omenimo zgleda vpeljimo pojem trikotnega kolobarja. Naj bosta R in S kolobarja in naj bo M (R,S)-bimodul (to pomeni, da je M levi R-modul in desni S-modul, ter velja $(rm)\,s = r\,(ms)$ za vse $r \in R, s \in S, m \in M$). Nadalje vpeljemo množico formalnih 2×2 zgornje trikotnih matrik

$$K = \begin{pmatrix} R & M \\ & S \end{pmatrix} \left\{ \begin{pmatrix} r & m \\ 0 & s \end{pmatrix}; r \in R, s \in S, m \in M \right\}.$$

Ko množico A opremimo s seštevanjem in množenjem na podoben način, kot to naredimo pri matrikah:

$$\begin{pmatrix} r & m \\ 0 & s \end{pmatrix} + \begin{pmatrix} r' & m' \\ 0 & s' \end{pmatrix} = \begin{pmatrix} r + r' & m + m' \\ 0 & s + s' \end{pmatrix},$$
$$\begin{pmatrix} r & m \\ 0 & s \end{pmatrix} \begin{pmatrix} r' & m' \\ 0 & s' \end{pmatrix} = \begin{pmatrix} rr' & rm' + ms' \\ 0 & ss' \end{pmatrix},$$

dobimo kolobar. Tak kolobar K se imenuje trikotni kolobar, in ima zanimive lastnosti. V literaturi se ga zelo pogosto uporablja za konstruiranje protiprimerov.

Zgled. Naj bo

$$K = \begin{pmatrix} \mathbb{Z} & \mathbb{Q} \\ & \mathbb{Q} \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}; a \in \mathbb{Z} \text{ in } b, c \in \mathbb{Q} \right\}$$

trikotni kolobar. Kolobar K je desni noetherski kolobar, ki pa ni levi noetherski kolobar.

Ugotovimo, da sta sta oba kolobarja $\mathbb{Z}$ in $\mathbb{Q}$ noetherska kolobarja. Kolobar $\mathbb{Q}$ ni noetherski, ko nanj gledamo kot na levi $\mathbb{Z}$-modul. Zgled neskončne naraščajoče verige $\mathbb{Z}$-modulov je

$$\frac{1}{2}\mathbb{Z} \subset \frac{1}{4}\mathbb{Z} \subset \frac{1}{8}\mathbb{Z} \subset \cdots .$$

Zato, če se $I_1 \subset I_2 \subset I_3 \dots$ neskončna naraščajoča veriga $\mathbb{Z}$-modulov od $\mathbb{Q}$, potem je

$$\begin{pmatrix} 0 & I_1 \\ 0 & 0 \end{pmatrix} \subset \begin{pmatrix} 0 & I_2 \\ 0 & 0 \end{pmatrix} \subset \begin{pmatrix} 0 & I_3 \\ 0 & 0 \end{pmatrix} \subset \dots$$

neskončna naraščajoča veriga levih idealov kolobarja K. Torej kolobar K ni levi noetherski.

Po drugi strani, pa pokažemo, da je K desni noetherski. Ker je K kolobar z identiteto zadošča pokazati da so vsi desni ideali kolobarja K končno generirani (glej trditev 3.6). Naj bo I desni ideal kolobarja K. Pokazati moramo, da je I končno generiran, kar pa pokažemo z dvema primeroma:

1. primer: V prvem primeru predpostavimo, da vsaka matrika ideala I vsebuje ničlo v zgornjem levem stolpcu. Potem je vsak element ideala I oblike

$$\begin{pmatrix} 0 & y \\ 0 & z \end{pmatrix} \quad \text{za } y, z \in \mathbb{Q}.$$

Ne pozabimo, da za poljuben $c \in \mathbb{Q}$ in poljuben

$$\begin{pmatrix} 0 & y \\ 0 & z \end{pmatrix} \in I \quad \text{imamo} \quad \begin{pmatrix} 0 & cy \\ 0 & cz \end{pmatrix} \in I,$$

saj je

$$\begin{pmatrix} 0 & y \\ 0 & z \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & cy \\ 0 & cz \end{pmatrix}$$

in I je desni ideal kolobarja K. Torej I zgleda kot racionalen vektorski prostor. Dejansko upoštevajmo, da je

$$V = \left\{ (y, z) \in \mathbb{Q}^2; \begin{pmatrix} 0 & y \\ 0 & z \end{pmatrix} \in I \right\}$$

podprostor dvo-dimenzionalnega vektorskega prostora $\mathbb{Q}^2$. Torej v V obstajata dva (ne nujno linearno neodvisna) vektorja (y_1, z_1) in (y_2, z_2), ki razpenjata V. Poljuben element

$$\begin{pmatrix} 0 & y \\ 0 & z \end{pmatrix} \in I$$

ustreza vektorju $(y, z) \in V$ in $(y, z) = (c_1 y_1 + c_2 y_2, c_1 z_1 + c_2 z_2)$ za določena $c_1, c_2 \in \mathbb{Q}$. Tako je

$$\begin{pmatrix} 0 & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} 0 & c_1 y_1 + c_2 y_2 \\ 0 & c_1 z_1 + c_2 z_2 \end{pmatrix} = \begin{pmatrix} 0 & y_1 \\ 0 & z_1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & c_1 \end{pmatrix} + \begin{pmatrix} 0 & y_2 \\ 0 & z_2 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & c_2 \end{pmatrix}$$

in sledi, da je ideal I končno generiran z množico

$$\left\{ \begin{pmatrix} 0 & y_1 \\ 0 & z_1 \end{pmatrix}, \begin{pmatrix} 0 & y_2 \\ 0 & z_2 \end{pmatrix} \right\}$$

kot desni ideal kolobarja K.

2. primer: Recimo, da obstaja matrika ideala I z neničelnim levim zgornjim delom. Potem obstaja še naravno število n v zgornjem levem stolpcu matrike ideala I. Sledi, da je vsak element ideala I lahko oblike:

$$\begin{pmatrix} kn & y \\ 0 & z \end{pmatrix} \quad \text{za } k \in \mathbb{Z}, y, z \in \mathbb{Q}$$

Ker je I desni ideal kolobarja K, in ker je

$$\begin{pmatrix} n & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix},$$

sledi da

$$\begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}$$

leži v idealu I. Zdaj primer razdelimo v dva podprimera:

a. Recimo, da ima vsaka matrika ideala I ničelni spodnji desni stolpec. Potem je poljuben element ideala I oblike:

$$\begin{pmatrix} kn & y \\ 0 & 0 \end{pmatrix} \quad \text{za } k \in \mathbb{Z}, y \in \mathbb{Q}.$$

Opomnimo, da je

$$\begin{pmatrix} kn & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} k & \frac{y}{n} \\ 0 & 0 \end{pmatrix}.$$

Torej element

$$\begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}$$

generira I kot desni ideal kolobarja K.

b. Recimo, da obstaja matrika ideala I z neničelnim spodnjim desnim stolpcem. To pomeni, da imamo v idealu I matriko oblike:

$$\begin{pmatrix} mn & y_1 \\ 0 & z_1 \end{pmatrix} \quad \text{za določene } m \in \mathbb{Z}, y_1, z_1 \in \mathbb{Q}, z \neq 0.$$

Ker je $\begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} \in I$, sledi da je $\begin{pmatrix} n & y_1 \\ 0 & z_1 \end{pmatrix} \in I$. Naj bo $\begin{pmatrix} kn & y \\ 0 & z \end{pmatrix}$ poljuben element ideala I. Ker je

$$\begin{pmatrix} kn & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} n & y_1 \\ 0 & z_1 \end{pmatrix} \begin{pmatrix} k & \frac{1}{n}\left(y - \frac{y_1 z}{z_1}\right) \\ 0 & \frac{z}{z_1} \end{pmatrix},$$

sledi da $\begin{pmatrix} n & y_1 \\ 0 & z_1 \end{pmatrix}$ generira I kot desni ideal kolobarja K.

V vseh primerih je ideal I končno generiran.

Zgled. Trikotni kolobar

$$K = \begin{pmatrix} \mathbb{Q} & \mathbb{R} \\ & \mathbb{R} \end{pmatrix} = \left\{ \begin{pmatrix} d & r \\ 0 & s \end{pmatrix}; d \in \mathbb{Q} \text{ in } r, s \in \mathbb{R} \right\}$$

je desni artinski, ki pa ni levi artinski kolobar.

Podobno rešimo kot v prejšnjem zgledu. $\mathbb{R}$ kot levi $\mathbb{Q}$ vektorski prostor ni levi artinski. Ta vektorski prostor je neskončno dimenzionalen zato imamo neskončno padajočo verigo vektorskih podprostorov v $\mathbb{R}$. Za vsak $V \subseteq \mathbb{R}$, ki je vektorski prostor nad $\mathbb{Q}$, velja da je

$$\begin{pmatrix} 0 & V \\ 0 & 0 \end{pmatrix} = \left\{ \begin{pmatrix} 0 & v \\ 0 & 0 \end{pmatrix}; v \in V \right\}$$

levi ideal kolobarja K. Zato neskončna padajoča veriga vektorskih podprostorov v $\mathbb{R}$ porodi padajočo verigo levih idealov kolobarja K, ki ni stacionarna.

Zdaj pokažemo, da je kolobar K desni artinski. Ločimo tri primere.

1. primer: Recimo da ideal I vsebuje matriko z neničelnimi elementi po diagonalah, potem je ideal celoten kolobar. Dobimo identiteto.

2. primer: Recimo, da imajo vse matrike ideala I ničelni zgornji levi stolpec. V tem primeru preverimo, da je ideal dvo-dimenzionalen vektorski prostor nad $\mathbb{R}$. Potem je generiran z vsaj dvema elementoma. Ideali, ki so vsebovani v tem vektorskem prostoru nad $\mathbb{R}$ so sami vektorski prostor. Padajoča veriga idealov se zaključi, saj so vektorski prostori z enako dimenzijo enaki.

3. primer: Recimo, da imajo vse matrike ideala I ničle po diagonali. Potem je I eno-dimenzionalen vektorski prostor nad $\mathbb{R}$. Podobno kot v primeru b., se padajoča veriga idealov I zaključi.

Naj bo $(C, \leq)$ delno urejena množica. Spomnimo se definicije minimalnega elementa delno urejene množice C. Element $b \in C$ je minimalni element, če za vsak $c \in C$, ki je primerljiv z b velja $b \leq c$. Opomnimo, da $b \leq c$ ne velja nujno za vse $c \in C$. Nadalje, C lahko vsebuje veliko minimalnih elementov ali pa nobenega. Podobno je definiran tudi maksimalni element.

Definicija 3.5 *Modul A izpolnjuje* maksimalni pogoj na podmodulih*, če vsaka neprazna množica podmodulov modula A vsebuje maksimalni element. Podobno modul A izpolnjuje* minimalni pogoj na podmodulih*, če vsaka neprazna množica podmodulov modula A vsebuje minimalni element.*

Trditev 3.6 *Naj bo K kolobar z identiteto in naj vsebuje levi K-modul M, potem so naslednji trije pogoji K-podmodula modula M ekvivalentni:*

1. *(pogoj naraščajočih verig) vsaka strogo naraščajoča veriga podmodula M: $M_1 \subsetneqq M_2 \subsetneqq \ldots$ se zaključi po končnem številu korakov;*

2. *(maksimalni pogoj) vsaka neprazna množica K-podmodulov M ima maksimalni element (glede na inkluzijo);*

3. *(osnovni pogoj za končnost) vsak K-podmodul modula M je končno generiran.*

Dokaz. Da vidimo da 1. implicira 2., naj bo S neprazna množica K-podmodulov modula M. Vzamemo M_1 iz S. Če M_1 ni maksimalni, izberemo M_2 iz S, ki vsebuje M_1. Če M_2 ni maksimalni, izberemo M_3 iz S, ki vsebuje M_2. Postopek nadaljujemo, dokler ne pridemo do maksimalnega elementa(zaradi 1.).

Zdaj poglejmo, da 2. implicira 3. Naj bo N K-podmodul modula M in naj bo S množica vseh končno generiranih K-podmodulov od N. Ta množica je neprazna, saj vsebuje 0. Po 2. ima S maksimalni element, recimo N'. Če je x v N ampak ne v N', potem je $N' + Kx$ končno generiran K-podmodul od N, ki vsebuje N'. To pa je protislovje. Torej $N' = N$ in je zato N končno generiran.

Poglejmo še, ko 3. implicira 1. Naj bo dana $M_1 \subsetneqq M_2 \subsetneqq \ldots$ in naj bo $N = \bigcup_{n=1}^{\infty} M_n$. Po 3. je N končno generiran. Ker je M_n naraščajoče z n, lahko najdemo nekatere M_{n_0}, ki vsebujejo vse generatorje. Potem se zaporedje ne konča prej, kot pri M_{n_0}. $\square$

Naj bodo A, B, C moduli in naj bosta $f : A \to B, g : B \to C$ modulska homomorfizma. V nadaljevanju bomo takšen par homomorfizmov f in g krajše označili z

$$A \xrightarrow{f} B \xrightarrow{g} C.$$

Podobno bomo za zaporedje modulov $A_1, ..., A_{i-1}, A_i, A_{i+1}, ...$ in modulskih homomorfizmov $f_i : A_{i-1} \to A_i$ uporabljali oznako

$$\cdots \xrightarrow{f_{i-1}} A_{i-1} \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \to \cdots$$

Definicija 3.7 *Par modulskih homomorfizmov* $A \xrightarrow{f} B \xrightarrow{g} C$ *je* eksaktno, *če je* $\operatorname{im} f = \ker g$. *Zaporedje modulskih homomorfizmov* $\xrightarrow{f_{i-1}} A_{i-1} \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \to \cdots$ *je eksaktno, če je* $\operatorname{im} f_i = \ker f_{i+1}$ *za vsak* i.

Definicija 3.8 *Eksaktnemu zaporedju* $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ *pravimo* kratko eksaktno zaporedje

Pojasnimo, da je $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ kratko eksaktno zaporedje natanko tedaj, ko je f injektiven homomorfizem ($\ker f = 0$), g surjektiven homomorfizem ($\operatorname{im} g = C$) in velja $\operatorname{im} f = \ker g$.

Izrek 3.9 *Modul A zadošča pogoju padajočih (naraščajočih) verig na podmodulih natanko tedaj, ko A zadošča minimalnemu (maksimalnemu) pogoju na podmodulih.*

Dokaz. Predpostavimo, da modul A zadošča minimalnemu pogoju na podmodulih in da je $A_1 \supseteq A_2 \supseteq \cdots$ poljubna veriga podmodulov modula A. Potem ima množica $\{A_i | i \geq 1\}$ minimalni element, recimo A_n. Posledično, za vsak $i \geq n$ po predpostavki velja $A_n \supseteq A_i$ in po minimalnosti $A_i \subseteq A_n$, od koder sledi $A_i = A_n$ za vsak $i \geq n$. Zato modul A zadošča pogoju padajočih verig.

Obratno, predvidevamo, da modul A zadošča pogoju padajočih verig in naj bo S neprazna podmnožica podmodulov modula A. Potem obstaja $B_0 \in S$. Če S ne vsebuje minimalnega elementa, potem za vsak podmodul B iz S obstaja vsaj en podmodul B' iz S, da je $B \supsetneqq B'$. Za vsak B iz S, izberemo B' po aksiomu izbire. Ta izbira potem definira funkcijo $f : \mathbb{N} \to S$ s predpisom $B \longmapsto B'$. Obstaja torej taka funkcija $\varphi : \mathbb{N} \to \mathbb{N}$, da je

$$\varphi(0) = B_0 \quad \text{in} \quad \varphi(n+1) = f(\varphi(n)) = \varphi(n)'.$$

Torej, če je $\varphi(n) = B_n \in S$, potem obstaja množica $B_0, B_1, ...$ tako da je $B_0 \supsetneqq B_1 \supsetneqq B_2 \supsetneqq \ldots$ To je v protislovju s pogojem padajočih verig. Zato mora S imeti minimalni element in modul A zadošča minimalnemu pogoju. Dokaz za pogoj naraščajočih verig in maksimalni pogoj je analogen. $\square$

Za dokaz naslednjega izreka bomo potrebovali lemo:

Lema 3.10 (The short five lemma) *Naj bo dan komutativen diagram*

$$\begin{array}{ccccccccc} 0 & \to & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \to & 0 \\ & & \downarrow\alpha & & \downarrow\beta & & \downarrow\gamma & & \\ 0 & \to & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \to & 0 \end{array}$$

pri čemer je vsaka vrstica kratko eksaktno zaporedje. Potem velja:

1. *če sta α in γ injektivna, potem je β injektiven;*
2. *če sta α in γ surjektivna, potem je β surjektiven;*
3. *če sta α in γ izomorfna, potem je β izomorfen.*

Dokaz. 1. Naj bo $b \in B$ in recimo da je $\beta(b) = 0$. Moramo pokazati, da je $b = 0$. Po komutativnosti imamo

$$\gamma g(b) = g'\beta(b) = g'(0) = 0$$

To implicira $g(b) = 0$, saj je γ monomorfizem. Po eksaktnosti v zgornji vrstici pri B, imamo $b \in \ker g = \operatorname{im} f$, saj je $b = f(a), a \in A$. Po komutativnosti je

$$f'\alpha(a) = \beta f(a) = \beta(b) = 0$$

Po eksaktnosti v spodnji vrstici pri A', je f' monomorfizem, torej je $\alpha(a) = 0$. Ampak α je monomorfizem, zato je $a = 0$ in $b = f(a) = f(0) = 0$. Torej je β monomorfizem.

2. Naj bo $b' \in B'$, potem je $g'(b') \in C'$. Ker je γ epimorfizem je $g'(b') = \gamma(c)$ za nekatere $c \in C$. Po eksaktnosti v zgornji vrstici pri C, je g epimorfizem in je zato $c = g(b)$ za nekatere $b \in B$. Po komutativnosti je

$$g'\beta(b) = \gamma g(b) = \gamma(c) = g'(b')$$

Torej je $g'[\beta(b) - b'] = 0$ in $\beta(b) - b' \in \ker g' = \operatorname{im} f'$ po eksaktnosti, recimo $f'(a') = \beta(b) - b', a' \in A'$. Ker je α epimorfizem, je $a' = \alpha(a)$ za nekatere $a \in A$. Obravnavajmo $b - f(a) \in B$:

$$\beta[b - f(a)] = \beta(b) - \beta f(a)$$

Po komutativnosti je $\beta f(a) = f'\alpha(a) = f'(a') = \beta(b) - b'$, zato je

$$\beta[b - f(a)] = \beta(b) - \beta f(a) = \beta(b) - (\beta(b) - b') = b'$$

in β je epimorfizem.

3. je direktna posledica 1. in 2. $\square$

Izrek 3.11 *Naj bo $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ kratko eksaktno zaporedje modulov. Potem modul B zadošča pogoju naraščajočih (oz. padajočih) verig na podmodulih natanko tedaj, ko modula A in C zadoščata pogoju naraščajočih (oz.padajočih) verig.*

Dokaz. Če modul B zadošča pogoju naraščajočih verig, potem tudi podmodul $f(A)$ zadošča pogoju naraščajočih verig. Zaradi eksaktnosti je modul A izomorfen modulu $f(A)$, zato modul A zadošča pogoju naraščajočih verig. Če je $C_1 \subseteq C_2 \subseteq \ldots$ veriga podmodulov C, potem je tudi $g^{-1}(C_1) \subseteq g^{-1}(C_2) \subseteq \ldots$ veriga podmodulov modula B. Potem obstaja tak n, tako da je $g^{-1}(C_i) = g^{-1}(C_n)$ za vse $i \geq n$. Ker je zaradi eksaktnosti g izomorfen, sledi da je $C_i = C_n$ za vse $i \geq n$. Potem modul C zadošča pogoju naraščajočih verig.

Predpostavimo, da A in C zadoščata pogoju naraščajočih verig in je $B_1 \subseteq B_2 \subseteq \ldots$veriga podmodulov B. Za vsak i je

$$A_i = f^{-1}(f(A) \cap B_i) \quad \text{in} \quad C_i = g(B_i).$$

Označimo naslednji zožitvi $f_i = f|A_i$ in $g_i = g|B_i$. Preverimo, da je za vsak i naslednje zaporedje eksaktno

$$0 \to A_i \xrightarrow{f_i} B_i \xrightarrow{g_i} C_i \to 0.$$

Preverimo, da je $A_1 \subseteq A_2 \subseteq \ldots$ in $C_1 \subseteq C_2 \subseteq \ldots$ Po predpostavki, obstaja naravno število n, tako da je $A_i = A_n$ in $C_i = C_n$ za vse $i \geq n$. Za vsak $i \geq n$ je spodnji diagram z eksaktnimi vrsticami komutativen:

$$\begin{array}{ccccccccc}
0 & \to & A_n & \xrightarrow{f_n} & B_n & \xrightarrow{g_n} & C_n & \to & 0 \\
 & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\
0 & \to & A_i & \xrightarrow{f_i} & B_i & \xrightarrow{g_i} & C_i & \to & 0
\end{array}$$

pri tem sta α in γ identični preslikavi in β je inkluzija oziroma vložitev. Prejšnja lema implicira, da je B_i identična preslikava, zato B zadošča pogoju naraščajočih verig. Dokaz za padajoč verižni pogoj je analogen. $\square$

Posledica 3.12 *Če je A podmodul modula B, potem modul B zadošča pogoju naraščajočih (oz. padajočih) verig natanko tedaj, ko podmodula A in $B|A$ zadoščata pogoju naraščajočih (oz. padajočih) verig.*

Dokaz. Naj bo $f : A \to B$ vložitev in $g : B \to B|A$ naravni homomorfizem. Tedaj velja, da je f injektiven, g surjektiven in velja $\operatorname{im} f = \ker g$. Zato je zaporedje $0 \to A \xrightarrow{f} B \xrightarrow{g} B|A \to 0$ eksaktno zaporedje in željeni rezultat sledi neposredno iz izreka 3.11. $\square$

Posledica 3.13 *Če so $A_1, \ldots A_n$ moduli, potem njihova direktna vsota $A_1 \oplus A_2 \oplus \ldots \oplus A_n$ zadošča pogoju naraščajočih (oz. padajočih) verig natanko tedaj, ko vsak podmodul A_i zadošča pogoju naraščajočih (oz. padajočih) verig.*

Dokaz. Za dokaz posledice uporabimo matematično indukcijo. Zato zadošča, da dokažemo posledico v primeru $n = 2$. Naj bo $\pi_1 : A_1 \to A_1 \oplus A_2$ injektivni homomorfizem definiran z $\pi_1 (a_1) = (a_1, 0)$ za vsak $a_1 \in A_1$. Podobno naj bo $\pi_2 : A_1 \oplus A_2 \to A_2$ projekcija definirana z $\pi_2 (a_1, a_2) = a_2$ za vsak $(a_1, a_2) \in A_1 \oplus A_2$. Potem velja $\operatorname{im} \pi_1 = \ker \pi_2$. Zato je zaporedje

$$0 \to A_1 \xrightarrow{\pi_1} A_1 \oplus A_2 \xrightarrow{\pi_2} A_2 \to 0$$

eksaktno in z uporabo izreka 3.11 sledi željeni rezultat. $\square$

Posledica 3.14 *Vsak enotski modul A nad enotskim kolobarjem K je homomorfna slika prostih K-modulov F. Če je A končno generiran, potem lahko F izberemo kot končno generiranega.*

Dokaz. Naj bo X množica generatorjev iz A v F in naj bo prost K-modul množice X. Potem inkluzija preslikav $X \to A$ povzroči K-modulski homomorfizem $\bar{f} : F \to A$, tako da je $X \subset \operatorname{im} f$. Ker je X množica generatorjev A, imamo $\operatorname{im} \bar{f} = A$. $\square$

Izrek 3.15 *Če je K levi noetherski (oz. artinski) kolobar z enoto, potem vsak končno generiran enotski levi K-modul A zadošča pogoju naraščajočih (oz. padajočih) verig.*

Dokaz. Če je modul A končno generiran, potem po prejšnji posledici obstaja prosti K-modul F s končno bazo in epimorfizmom $\pi : F \to A$. Ker je modul F direktna vsota končnega števila kopij K, je F levi noetherski (oz. artinski) po posledici 3.13. Zato je $A \cong F| \ker \pi$ noetherski (oz.artinski) modul po posledici 3.12.

Tukaj gre za karakterizacijo naraščajočega verižnega pogoja, ki ni analogna pogoju padajočih verig. $\square$

Izrek 3.16 *Modul A zadošča pogoju naraščajočih verig na podmodulih natanko tedaj, ko je vsak podmodul B modula A končno generiran.*

Dokaz. Naj bo B podmodul modula A. Naj bo S množica vseh končno generiranih podmodulov modula B. Ker je S neprazna množica ($0 \in S$), vsebuje maksimalni element C. Modul C je po izreku končno generiran z elementi $c_1, c_2, \ldots c_n$. Za vsak $b \in B$ naj bo D_b podmodul modula B generiran z elementi $b, c_1, c_2, \ldots c_n$. Potem je $D_b \in S$ in $C \subset D_b$. Ker je C maksimalni, je $D_b = C$ za vsak $b \in B$, kjer je $b \in D_b = C$ za vsak $b \in B$ in $B \subset C$. Ker velja $C \subset B, B = C$, je torej B končno generiran.

Obratno predpostavimo, da imamo podano verigo podmodulov $A_1 \subseteq A_2 \subseteq A_3 \subseteq \ldots$. Potem ni težko preveriti, da je $\bigcup_{i \geq 1} A_i$ tudi podmodul modula A in je zato končno generiran z elementi $a_1, ..., a_k$. Ker je vsak a_i element nekega A_i, potem obstaja tak indeks n, tako da je $a_i \in A_i$, za $i = 1, 2, ..., k$. Posledično je $\bigcup A_i \subset A_n$, torej $A_i = A_n$ za $i \geq n$. □

Izrek 3.17 *Če je K komutativen noetherski kolobar z enoto, potem je tudi kolobar polinomov $K[x_1, \ldots, x_n]$ noetherski kolobar.*

Dokaz. Zadostuje pokazati, da je kolobar polinomov $K[x]$ noetherski kolobar (ker lahko potem uporabimo matematično indukcijo). Po izreku 3.16 moremo samo pokazati, da je vsak ideal J v $K[x]$ končno generiran. Za vsak $n \geq 0$, naj bo I_n množica vseh $r \in K$, tako da je $r = 0$ ali pa je r vodilni koeficient $f \in J$ stopnje n. Preverimo, da je vsak I_n ideal v K. Če je r neničelni element I_n in je $f \in J$ polinom stopnje $n+1$, je $I_0 \subset I_1 \subset I_2 \subset \ldots$. Če je K noetherski kolobar, obstaja tako naravno število t, da je $I_n = I_t$ za vse $n \geq t$, nadalje vsak ideal $I_n (n \geq 0)$ je končno generiran z naprimer $I_n = (r_{n1}, r_{n2}, \ldots, r_{n_i n})$. Za vsak r_{nj} kjer je $0 \leq n \leq t$ in $1 \leq j \leq n$, naj bo $f_{nj} \in J$ polinom stopnje n z vodilnim koeficientom r_{nj}. Opazimo, da je $fo_i = ro_j \in K \subset K[x]$. Pokažimo, da je ideal J iz $K[x]$ generiran po končni množici polinomov $X = \{f_{nj} \mid 0 \leq n \leq t; 1 \leq j \leq i_n\}$. Očitno je $(x) \subset J$. Obratno, polinomi stopnje P in J so natančni elementi I_0 zato so vsebovani v (x). Nadaljujemo po induktivni predpostavki, da (x) vsebuje vse polinome iz J stopnje manjše od k in naj ima $g \in J$ stopnjo k in vodilni koeficient $r \neq 0$.

Če je $k \leq t$, potem je $r \in I_k$ zato je $r = s_1 r_{k1} + s_2 r_{k2} + \ldots + s_{ik} r_{kik}$ za nekatere $s_j \in K$. Potem ima polinom $\sum_{j=1}^{i_k} s_j f_{kj} \in (x)$ vodilni koeficient r in stopnjo k, zato ima $g - \sum_j s_j f_{kj}$ stopnjo kvečjemu $k-1$. Po indukcijski predpostavki je $g - \sum_j s_j f_{kj} \in (x)$, zato je $g \in (x)$.

Če je $k \geq t$, potem je $r \in I_k = I_t$ in $r = \sum_{j=1}^{i_t} s_j r_{tj} (s_j \in K)$. Nadalje $\sum_{j=1}^{i_t} s_j x^{k-t} f_{tj} \in (x)$ ima vodilni koeficient r in stopnjo k. Torej ima $g - \sum_j s_j x^{k-t} f_{tj}$ stopnjo največ $k-1$ in leži v (x) po indukcijski predpostavki. Posledično, $g \in (x)$ in indukcija je končana. Zato je $J = (x)$. $\square$

3.2 Kompozicijske vrste

V abstraktni algebri, kompozicijska vrsta omogoča način, kako pretrgati algebraično strukturo, kot so grupe ali modul na enostavne dele. *Normalna vrsta* modula A je veriga podmodulov $A = A_0 \supseteq A_1 \supseteq A_2 \supseteq \ldots \supseteq A_n$. *Faktorji* te vrste so kvocientni moduli $A_i | A_{i+1}$ $(i = 0, 1, \ldots, n-1)$. *Dolžina* te vrste je število pravih inkluzij, to je število netrivialnih faktorjev. *Nadaljevanje* normalnih vrst $A_0 \supseteq A_1 \supseteq A_2 \supseteq \ldots \supseteq A_n$ je normalna vrsta pridobljena z vstavljanjem končnega števila dodatnih podmodulov med že podanimi.

Pravo nadaljevanje normalne vrste je tisto, ki ima dolžino večjo od originalnih vrst. Dve normalni vrsti sta *ekvivalentni*, če obstaja bijektivna preslikava med netrivialnimi faktorji, tako da so ustrezni faktorji izomorfni moduli. Torej imajo ekvivalentne vrste nujno isto dolžino.

Definicija 3.18 Kompozicijska vrsta *modula A je normalna vrsta $A = A_0 \supseteq A_1 \supseteq A_2 \supseteq \ldots \supseteq A_n = 0$, tako da je vsak faktor $A_k | A_{k+1}$ $(k = 0, 1, \ldots n-1)$ neničelni modul brez pravih podmodulov.*

Če je K kolobar z enoto, potem je neničeln enotski modul brez pravih podmodulov enostaven. V tem primeru je kompozicijska vrsta normalna vrsta $A = A_0 \supseteq A_1 \supseteq A_2 \supseteq \ldots \supseteq A_n = 0$ z enostavnimi faktorji.

Izrek 3.19 *Neničelni modul A ima kompozicijsko vrsto natanko tedaj, ko A zadošča pogoju naraščajočih in padajočih verig.*

Dokaz. Predpostavimo, da ima modul A kompozicijsko vrsto S dolžine n. Če kateri od pogojev verig ne drži, lahko najdemo podmodule

$$A = A_0 \supsetneqq A_1 \supsetneqq A_2 \supsetneqq \ldots \supsetneqq A_n \supsetneqq A_{n+1},$$

ki tvorijo normalno vrsto T dolžine $n+1$. Obstajata ekvivalentni nadaljevanji S in T, kar pa je protislovje, saj imajo ekvivalentne vrste enako dolžino. Vsako nadaljevanje kompozicijske vrste S ima dolžino n, vendar vsako nadaljevanje vrste T je dolžine vsaj $n+1$. Torej A zadošča obema verižnima pogojema.

Obratno, če je B neničelni podmodul modula A, potem naj bo $S(B)$ množica vseh podmodulov C modula B, tako da je $C \neq B$. Torej, če je modul B brez pravih podmodulov potem je $S(B) = \{0\}$. Definiramo tudi $S(0) = \{0\}$. Za vsak modul B obstaja maksimalni element B' od $S(B)$ po izreku 3.9. Naj bo S množica vseh podmodulov A in definirajmo preslikavo $f : S \to S$ pri $f(B) = B'$. Obstaja funkcija $\varphi : N \to S$, tako da je

$$\varphi(0) = A \quad \text{in} \quad \varphi(n+1) = f(\varphi(n)) = \varphi(n)'.$$

Če je $A_i = \varphi(i)$, potem je $A \supseteq A_1 \supseteq A_2 \supseteq \ldots$padajoča veriga po konstrukciji, od koder je za nek n, $A_i = A_n$ za vse $i \geq n$. Ker je $A_{n+1} = A_n' = f(A_n)$, po definiciji f je $A_{n+1} = A_n$ samo, če je $A_n = 0 = A_{n+1}$. Naj bo m najmanjše naravno število, tako da je $A_m = 0$. Potem je $m \leq n$ in $A_k \neq 0$ za vse $k < m$. Nadalje, za vsak $k < m$, je A_{k+1} maksimalni podmodul od A_k, tako da je $A_k \supsetneqq A_{k+1}$. Posledično je vsak $A_k | A_{k+1}$ neničelni in je brez pravih podmodulov. Torej je $A \supseteq A_1 \supseteq \ldots \supseteq A_m = 0$ kompozicijska vrsta za A. $\square$

Posledica 3.20 *Če je D obseg, potem je kolobar $M_n(D)$ vseh $n \times n$ matrik artinski in noetherski kolobar.*

Dokaz. Po definiciji noetherskega kolobarja in po prejšnjem izreku zadostuje pokazati, da ima $K = M_n(D)$ kompozicijsko vrsto levih in desnih K-modulov. Naj bodo e_{ij} standardne matrične enote in $1 = e_{11} + e_{22} + ... + e_{nn}$. Potem lahko zapišemo

$$\begin{aligned} K = K1 &= K(e_{11} + e_{22} + ... + e_{nn}.) \\ &= Ke_{11} + Ke_{22} + ... + Ke_{nn}. \end{aligned}$$

Pri tem je $Ke_{ii} = \{Ae_{ii} | A \in K\}$ levi ideal (podmodul) K, ki vsebuje vse matrike v K z kvečjemu neničelnim i-tim stolpcem. Velja, da je Ke_{ii} minimalni neničelni levi ideal (nima ustreznih podmodulov). Nadalje definiramo $M_0 = 0$ in $M_i = Ke_{11} + Ke_{22} + ... + Ke_{ii}$ za $i = 1, 2, ..., n$. Za $i \geq 1$ velja, da je $M_i | M_{i-1} \cong Ke_{ii}$, od koder je $K = M_n \supseteq M_{n-1} \supseteq \ldots \supseteq M_1 \supseteq M_0 = 0$ kompozicijska vrsta levih K-modulov. Podoben argument z desnimi ideali, $e_{ii}K = \{e_i A | A \in K\}$ pokaže, da ima K kompozicijsko vrsto iz desnih K-modulov. $\square$

Poglavje 4

Jordan - Hölderjev izrek

Jordan - Hölderjev izrek je klasični in temeljni rezultat v teoriji grup in modulov. Za dokaz Jordan - Hölderjeva izreka imamo dva pristopa.

4.1 Prvi pristop

Začnemo z idejo o dimenzijah vektorskih prostorov. Lastnosti dimenzij v vektorskem prostoru:

1. Če je $V = \{0\}$, potem je $\dim V = 0$.
2. Če je W pravi podprostor vektorskega prostora V, potem je $\dim W < \dim V$.
3. Če je $V \neq \{0\}$, potem V vsebuje eno-dimenzionalen podprostor.
4. Velja $\dim (U \oplus W) = \dim U + \dim W$.
5. Če je $\{W_i | i \in I\}$ veriga podprostorov vektorskega prostora V, potem je
$$\dim \bigcup_{i \in I} W_i = \sup_{i \in I}\{\dim W_i\}.$$

Lastnosti od 1. do 4. nam bodo služile kot model za definiranje pojma dolžina pri nekaterih modulih. Moduli, ki bodo imeli dolžino, bodo analogni končno-dimenzionalnim vektorskim prostorom in bodo zato imeli podobne lastnosti.

Definicija 4.1 *Dolžina levega K-modula M je število $d(M)$, ki zadošča:*

1. Če je $M = \{0\}$, potem je $d(M) = 0$.
2. Če obstaja $d(M)$ in je N pravi podmodul modula M in je $d(M)$ končno število, potem je $d(N) < d(M)$.

3. Za neničelni modul M velja $d(M) = 1$ natanko tedaj, ko modul M ne vsebuje pravih netrivialnih podmodulov (M je enostaven modul).

4. Če je N podmodul M, potem je $d(M)$ določena natanko tedaj, ko sta določeni $d(N)$ in $d(M/N)$ in v tem primeru velja $d(M) = d(N) + d(M/N)$.

Opomniti je treba, da sta točki 3. in 4. iz definicije dolžine modula drugačni kot lastnosti 3. in 4. pri vektorskih prostorih. Vsak vektorski prostor vsebuje enostaven (eno-dimenzionalen) podprostor, ampak veliko modulov ne vsebuje enostavnih podmodulov in podprostor vektorskega prostora je vedno direktna vsota, medtem ko podmodul modula ni nujno direktna vsota.

V nadaljevanju nas bodo zanimali le moduli s končno dolžino s vprašanjem, če lahko definiramo dolžino na tak način, da imajo nekateri moduli neskončno dolžino. Podana definicja, nam omogoča dokazati, da je veliko podobnih lastnosti med končno-dimenzionalnimi vektorskimi prostori z moduli s končno dolžino.

Izrek 4.2 *Naj bo M levi K-modul s končno dolžino in naj bo φ endomorfizem modula M. Potem so naslednje trditve ekvivalentne:*

1. *φ je izomorfizem;*

2. *φ je monomorfizem;*

3. *φ je surjektiven;*

4. *Obstaja endomorfizem ψ modula M, da je $\psi\varphi = 1_M$;*

5. *Obstaja endomorfizem ψ modula M, da je $\varphi\psi = 1_M$.*

Dokaz. Dokazali bomo le ekvivalentnost trditev 2. in 3. Naj bo φ monomorfizem iz M na M. Potem je $\varphi(M) \approx M$, zato je $d_\varphi(M) = d(M)$. Ampak, ker je $\varphi(M) \subseteq M$, sledi iz 2. točke definicje , da je $\varphi(M) = M$. Torej je φ surjektiven.

Obratno, recimo, da je φ surjektiven. Potem je $\varphi(M) = M$, tako da je $d_\varphi(M) = d(M)$. Ampak po 4. točki definicije je $d(M) = d_\varphi(M) + d(\ker\varphi)$. Zato je $d(\ker f) = 0$(ker so vse dolžine končne), kar implicira, da je $\ker f = 0$ (drugače pridemo v protislovje z 2. točko definicije). Torej φ je monomorfizem. $\square$

Izrek 4.3 *Levi K-modul M ima končno dolžino ℓ natanko tedaj, ko obstaja taka veriga podmodulov*

$$0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_{\ell-1} \subsetneq M_\ell = M, \tag{4.1}$$

da je vsak M_i maksimalni podmodul modula M_{i+1}.

Dokaz. Predpostavimo, da za levi K-modul M obstaja veriga podmodulov (4.1). Dokažimo, da ima potem levi K-modul M končno dolžino ℓ. Če je M_i maksimalni podmodul M_{i+1}, potem je kvocientni modul M_{i+1}/M_i enostaven modul in je po definiciji njegova dolžina $d(M_{i+1}/M_i) = 1$. Zato, po 4. točki definicije sledi, da če je $d(M_i)$ končna, je tudi $d(M_{i+1})$ končna in določena kot $d(M_{i+1}) = d(M_i) + 1$. To nam omogoča, da začnemu na koncu verige in induktivno pridemo do začetka verige, tako da pokažemo da je dolžina M_i enaka i za vsak i. Zato je $d(M) = \ell$.

Obratno, predpostavimo, da ima levi K-modul M dolžino ℓ. Če je $M \neq 0$, potem je $0 \subsetneq M$ in po 2. točki definicije, če je $d(M)$ določena, potem je $d(M) > 0$. Če je zdaj $d(M) = 1$, potem mora M biti enostaven modul, drugače ima M prava netrivialna podmodula N in $0 < d(N) < d(M)$, kar pa je protislovje. To nam pokaže, da izrek velja za module dolžine 1.

Zdaj induktivno predpostavimo, da je določen $\ell > 1$. Kadarkoli je dolžina modula določena in je manjša od ℓ, potem obstaja veriga (4.1) predpisanih tipov. Predpostavimo, da je $d(M)$ določena in $d(M) = \ell$.

Ker je $\ell > 1, M \neq 0$ in M ni enostaven. Zato ima M pravi netrivialen podmodul N. Po 2. točki definicije je $d(N) < \ell$. Recimo, da je $d(N) = r$. Potem je po 4. točki definicije $0 \neq d(M/N) = \ell - r < \ell$, zato lahko uporabimo induktivno predpostavko za M in M/N, da dobimo verigi

$$0 \subsetneq N_1 \subsetneq \ldots \subsetneq N_{r-1} \subsetneq N_r = N \quad \text{in}$$

$$0 = N/N \subsetneq M_{\ell-r+1}/N \subsetneq \ldots \subsetneq M_{\ell-1}/N \subsetneq M_\ell/N = M/N$$

V drugi verigi smo uporabili dejstvo, da je vsak podmodul M/N oblike X/N, kjer je X podmodul modula M, ki vsebuje N. Izbrali smo tudi, da v drugi verigi oštevilčimo z indeksom $\ell - r + 1$. Ker je dolžina verige $\ell - r$, aritmetično pokaže, da bo končen indeks ℓ. Če združimo ti dve verigi skupaj, vidimo, da bo za modul M z dolžino $d(M) = \ell$ ustrezna veriga podmodulov enaka:

$$0 \subsetneq N_1 \subsetneq \ldots \subsetneq N_{r-1} \subsetneq N = M_{\ell-r} \subsetneq M_{\ell-r+1} \subsetneq \ldots \subsetneq M_{\ell-1} \subsetneq M.$$

S tem je izrek dokazan. □

Ta izrek nam pokaže, da nas izbrane definicije za dolžino prislijo, da definiramo $d(M)$ v končnem primeru kot dolžino maksimalne verige podmodulov modula M. Možno bi bilo, da ima modul nad nekim kolobarjem dve maksimalni verigi podmodulov z različnima dolžinama. Če se to zgodi, potem dolžine seveda ne moremo definirati na ta način. Vendar nam Jordan-Hölderjev izrek zagotovi, da se nam kaj takšnega ne more zgoditi.

Izrek 4.4 (Jordan - Hölderjev izrek) *Naj bo M levi K-modul in naj obstaja veriga podmodulov $0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_\ell = M$, kjer je vsak M_i/M_{i-1} enostaven K-modul. Potem bo katerakoli veriga te vrste imela enako dolžino ℓ in enako množico kvocientnih modulov M_i/M_{i-1}, čeprav ne nujno v istem vrstnem redu.*

Dokaz. Vzemimo dve verigi podmodulov modula M :

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_\ell = M,$$
$$0 \subsetneq N_1 \subsetneq N_2 \subsetneq \ldots \subsetneq N_k = M,$$

kjer so kvocienti sami enostavni moduli. Moramo dokazati, da je nujno $k = \ell$ in da sta družini enostavnih kvocientov M_i/M_{i-1} in N_i/N_{i-1} enaki. Induktivno predpostavimo, da izrek drži za vse module, za katere obstaja veriga dolžine manjše od ℓ.

Primer 1. Če je $M_i = N_j$ za nekatere i, j, tako da je $0 \neq M_i = N_j \neq M$, potem indukcijska predpostavka uporabljena pri M_i, pokaže da je $i = j$. Nadalje je indukcijska predpostavka lahko uporabljena pri kvocientu $M/M_i = M/N_i$, da velja $k - i = \ell - i$. To je zaradi nadaljnega standardnega dejstva: če je R podmodul K-modula M potem so podmoduli od M/R natančno tisti, oblike X/R, kjer je $R \subseteq X \subseteq M$ in različni podmoduli X donašajo različne podmodule M/R.

Primer 2. Če prejšnji primer ni uporaben, predpostavimo da obstajata N_i in M_j tako da je $0 \neq N_i \subseteq M_j \neq M$. Sledi da je $N_1 \subseteq M_{\ell-1}$. Če je možno, vstavimo dodatne module L_i med $N_1 \subseteq M_{\ell-1}$. Po indukcijski predpostavki uporabljeni pri $M_{\ell-1}$, to ne more iti do neskončnosti in čez čas dobimo vrsto:

$$0 \subsetneq N_1 \subsetneq L_2 \subsetneq \ldots \subsetneq L_s \subsetneq M_{\ell-1}$$

kjer so vsi kvocientni moduli enostavni. Po indukcijski predpostavki (uporabljene pri $M_{\ell-1}$), mora veriga imeti dolžino $\ell - 1$ (tako da je $s = \ell - 2$) in dobimo enake kvocientne module za dve verigi. Zdaj lahko uporabimo *Primer 1.* za naslednji verigi

$$0 \subsetneq N_1 \subsetneq L_2 \subsetneq \ldots \subsetneq L_{\ell-2} \subsetneq M_{\ell-1} \subsetneq M$$
$$0 \subsetneq N_1 \subsetneq N_2 \subsetneq \ldots \subsetneq N_{k-2} \subsetneq N_{k-1} \subsetneq M$$

(glede na to, da imata skupen modul N_1) da vidimo $k = \ell$ in da izrek podpira ta primer.

Primer 3. Edini primer, ki je še ostal za obravnavo, je $N_1 \subsetneq M_{\ell-1}$. Upoštevajmo, da je s predpostavko o verigah N_1 enostaven modul. Ampak $N_1 \cap M_{\ell-1} \subseteq N_1$, tako da če je $N_1 \nsubseteq M_{\ell-1}$ sledi $N_1 \cap M_{\ell-1} = 0$. Opazimo tudi, da če je $N_1 \nsubseteq M_{\ell-1}$ potem je $M_{\ell-1} \subsetneq N_1 + M_{\ell-1}$. Ampak $M_{\ell-1}$ je po predpostavki maksimalni pravi podmodul modula M. Zato je $N_1 + M_{\ell-1} = M$ in ker smo že opazili, da je $N_1 \cap M_{\ell-1} = 0$, sledi $M = N_1 \oplus M_{\ell-1}$. Zato je $M/N_1 \approx M_{\ell-1}$. Zdaj je strogo padajoča veriga

$$0 = N_1/N_1 \subsetneq N_2/N_1 \subsetneq \ldots \subsetneq N_k/N_1 = N/N_1$$

podmodulov N/N_1 dolžine $k-1$ in izomorfizem preslikav $M/N_1 \approx M_{\ell-1}$ k strogo naraščajoči verigi podmodulov $M_{\ell-1}$. Po indukcijski predpostavki, morata ti dve verigi biti enake dolžine: $k-1 = \ell - 1$. Dalje, v vsakem primeru so kvocientni moduli izomorfni (ampak ne nujno v enakem vrstnem redu). $\square$

4.2 Drugi pristop

Končna vrsta enotskega levega K-modula M, je končna padajoča veriga $M = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_n = 0$ K-podmodulov. Modulom M_i/M_{i+1} za $0 \leq i \leq n-1$ pravimo zaporedni kvocienti vrste. Končni vrsti pravimo kompozicijska vrsta, če so vsi zaporedni kvocienti enostavni K-moduli.

Naj bosta

$$M = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_m = 0$$

in

$$M = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_n = 0$$

dve končni vrsti modula M. Pravimo, da je druga vrsta nadaljevanje prve, če je funkcija $f : \{0, ..., m\} \mapsto \{0, ..., n\}$ z $M_i = N_{f(i)}$ za $0 \leq i \leq m$. Dve končni vrsti modula M sta ekvivalentni, če je $m = n$ in, če lahko zaporedje kvocientov $M_0/M_1, M_1/M_2, ..., M_{m-1}/M_m$ razvrstimo tako, da so izomorfni N_0/N_1, N_1/N_2, ..., N_{m-1}/N_m.

Lema 4.5 (Zassenhaus) *Naj bodo M_1, M_2, M_1' in M_2' podmoduli levega K-modula M in naj bo $M_1' \subseteq M_1$ in $M_2' \subseteq M_2$. Potem velja*

$$((M_1 \cap M_2) + M_1')/((M_1 \cap M_2') + M_1') \cong ((M_1 \cap M_2) + M_2)/((M_1' \cap M_2) + M_2')$$

Dokaz. Po drugem izreku o izomorfizmih, izrek 2.11, lahko zapišemo

$$\begin{aligned}
&(M_1 \cap M_2)/(((M_1 \cap M_2') + M_1') \cap (M_1 \cap M_2)) \\
&\cong ((M_1 \cap M_2) + (M_1 \cap M_2') + M_1')/((M_1 \cap M_2') + M_1') \\
&= ((M_1 \cap M_2) + M_1')/((M_1 \cap M_2') + M_1'
\end{aligned}$$

Ker imamo

$$
\begin{aligned}
((M_1 \cap M_2') + M_1') \cap (M_1 \cap M_2) &= ((M_1 \cap M_2') + M_1') \cap M_2 \\
&= (M_1 \cap M_2') + (M_1' + M_2)
\end{aligned}
$$

lahko zgornji zapis zapišemo kot

$$
(M_1 \cap M_2)/((M_1 \cap M_2') + (M_1' \cap M_2)) \cong ((M_1 \cap M_2) + M_1')/((M_1 \cap M_2') + M_1')
$$

in leva stran tega izomorfizma je simetrična. □

Izrek 4.6 (Schreier) *Poljubni dve končni vrsti modula M imata ekvivalentno nadaljevanje.*

Dokaz. Naj bosta vrsti končni

$$
M = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_m = 0
$$

in

$$
M = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_n = 0
$$

in definirajmo

$$
M_{ij} = (M_i \cap N_j) + M_{i+1} \quad \text{za } 0 \leq i \leq m-1 \text{ in } 0 \leq j \leq n,
$$

$$
N_{ji} = (M_i \cap N_j) + N_{j+1} \quad \text{za } 0 \leq i \leq m \text{ in } 0 \leq j \leq n-1.
$$

Potem je

$$
\begin{aligned}
M = M_{00} &\supseteq M_{01} \supseteq \ldots \supseteq M_{0n} \\
&\supseteq M_{10} \supseteq M_{11} \supseteq \ldots \supseteq M_{1n} \supseteq \ldots \supseteq M_{m-1.n} = 0
\end{aligned}
$$

in

$$
\begin{aligned}
M = N_{00} &\supseteq N_{01} \supseteq \ldots \supseteq N_{0m} \\
&\supseteq N_{10} \supseteq N_{11} \supseteq \ldots \supseteq N_{1m} \supseteq \ldots \supseteq N_{n-1,m} = 0
\end{aligned}
$$

so nadaljevanja danih vrst. Vsebovanosti $M_{in} \supseteq M_{i+1,0}$ in $N_{jm} \supseteq N_{j+1,0}$ sta ekvivalentni in edini neničelni kvocienti so zato oblike $M_{ij}/M_{i,j+1}$ in $N_{ji}/N_{j,i+1}$. Za te imamo

$$
\begin{aligned}
M_{ij}/M_{i,j+1} &= ((M_i \cap N_j) + M_{i+1})/((M_i \cap N_{j+1}) + M_{i+1} \\
&\cong ((M_i \cap N_j) + N_{j+1})/((M_{i+1} \cap N_j) + N_{j+1} \\
&= N_{ji}/N_{j,i+1}
\end{aligned}
$$

in zato sta zgornji nadaljevanji ekvivalentni. $\square$

Naj bo M modul, ki zadošča pogoju naraščajočih in padajočih verig. Z drugimi besedami, vsako naraščajoče zaporedje podmodulov

$$M_1 \subset M_2 \subset \dots$$

in vsako padajoče zaporedje

$$M_1 \supset M_2 \supset \dots$$

je končno. Potem vidimo (glej izrek 3.19), da obstaja končno zaporedje

$$M = M_0 \supset M_1 \supset \dots \supset M_k = 0$$

tako da je vsak M_i/M_{i+1} enostaven modul. Takemu zaporedju pravimo tudi *Jordan - Hölderjeva vrsta*. Dve Jordan-Hölderjevi vrsti

$$M = M_0 \supset M_1 \supset \dots \supset M_k = 0$$

in

$$M = N_0 \supset N_1 \supset \dots \supset N_l = 0$$

sta ekvivalentni, če je $k = l$ in obstaja permutacija s, da velja $M_i/M_{i+1} \cong N_{s(i)}/N_{s(i+1)}$.

Izrek 4.7 (Jordan - Hölderjev izrek) *Če je M levi K-modul s kompozicijsko vrsto, potem*

1. *se poljubna končna vrsta modula M, kjer so vsi kvocienti neničelni, lahko nadaljuje do kompozicijske vrste in*

2. *sta poljubni dve kompozicijski vrsti ekvivalentni.*

Dokaz. Uporabimo Schreierjev izrek za dano končno vrsto in z znano kompozicijsko vrsto. Ko se znebimo pogojev iz vsakega nadaljevanja (tistih, ki vodijo k 0 kot zaporedni kvocienti), pridemo do nadaljevanja naše dane končne vrste, ki je ekvivalentna naši znani kompozicijski vrsti. Zato je to nadaljevanje kompozicijska vrsta. S tem smo dokazali 1. Če specializiramo ta argument za primer, ko je končna vrsta kompozicijska vrsta, smo dokazali 2. $\square$

Jordan - Hölderjev izrek nam implicira, da so kompozicijski faktorji za dano kompozicijski vrsto odvisni le od modula M in ne od dane kompozicijske vrste. Še več, če sta $M' \supseteq M''$ K-podmodula modula M s kompozicijsko vrsto, tako da je M'/M'' enostaven, potem je M'/M'' kompozicijski faktor modula M. Do te ugotovitve pridemo, ko se znebimo pogojev za končno vrsto $M \supseteq M' \supseteq M'' \supseteq 0$ in dodamo Jordan-Hölderjev izrek.

Literatura

[1] T. W. Hungerford, *Algebra*, Springer-Verlag, 1989.

[2] N. Jacobson, *Basic Algebra II*, W. H. Freeman & Company, 1989.

[3] L. Rowen, *Ring Theory*, Academic Press, Inc, 1988.

[4] A. W. Knapp, *Basic Algebra,* Birkhäuser, 2006