UNIVERZITET U NOVOM SADU
PRIRODNO - MATEMATIČKI FAKULTET
DEPARTMAN ZA MATEMATIKU I INFORMATIKU

Ivana Nedeljković

Moduli i slobodni moduli

-master rad-

Mentor dr Petar Đapić

Novi Sad, 2021.

Sadržaj

Predgovor

Ovaj rad se bavi proučavanjem modula. Modul predstavlja uopštenje pojma vektorskog prostora, koje se sastoji u tome da se umesto polja F uzima komutativan prsten R sa jediničnim elementom. Specijalno, posmatraju se slobodni moduli.

U prvom poglavlju, Grupe, prsteni i vektorski prostori, nalaze se definicije, teoreme (bez dokaza) i primeri neophodni za razumevanje materijala koji će se obradjivati u nastavku rada.

U drugom poglavlju se obrađuju moduli. Pojam modula nad prstenom nastao je uopštavanjem dva pojma: Abelove grupe i vektorskog prostora. Definicija modula ponavlja definiciju vektorskog prostora s tom razlikom što skalari više nisu elementi polja vec nekog komutativnog prstena sa jedinicom. Vektorski prostori su specijalne vrste modula, tj. vektorski prostor je modul nad poljem. U radu se koristi da je prsten R komutativan i da ima jedinični element, pa nema potrebe da se pravi razlika između levih i desnih R-modula. Uvode se pojmovi i osobine analogne pojmovima i osobinama kod vektorskih prostora. Definišu se neki osnovni pojmovi, kao sto su linearna kombinacija, linearni omotač, linearna nezavisnost, generatrisa, baza i podmodul, kao i homomorfizmi modula. Sa druge strane, za razliku od vektorskih prostora, sistem elemenata R-modula može biti linearno zavisan i u slučaju kada nijedan od njih nije linearna kombinacija preostalih. U vezi sa tim, u radu se definiše pojam torzionog elementa, kao i torziono slobodnih elemenata i modula, i uvodi se pojam količničkog modula.

U trećem poglavlju se obrađuju moduli koji imaju bar jednu bazu, tj. slobodni moduli. Navodi se rang slobodnog modula. Za razliku od vektorskih prostora, u opštem slučaju, dati modul nad komutativnim domenom ne mora biti slobodan, a ako to i jeste to ne moraju biti i svi njegovi podmoduli. Iz tog razloga u radu se ograničava na konačno generisane slobodne module. Svaki takav modul ima konačnu bazu, a sve baze konačno generisanog slobodnog modula imaju isti broj elemenata. Ukoliko je R domen glavnih ideala, onda je i svaki podmodul slobodnog modula opet slobodan modul. A zatim se navodi veza izmedju torziono slobodnih i slobodnih modula.

Glava 1

Grupe, prsteni i vektorski prostori

1.1 Grupe

Definicija 1.1. Uređen par $(G, \cdot)$, gde je $\cdot : G \times G \to G$ binarna operacija, je polugrupa ako važi:

1) (zatvorenost) G je grupoid, tj. $(\forall x, y \in G)\ (x \cdot y \in G)$,

2) (asocijativnost) $(\forall x, y, z \in G)\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$.

Definicija 1.2. Uređen par $(G, \cdot)$, gde je $\cdot : G \times G \to G$ binarna operacija, zove se grupa ako važe sledeća svojstva:

1) (zatvorenost) $(G, \cdot)$ je grupoid,

2) (asocijativnost) $(\forall x, y, z \in G)\ ((x \cdot y) \cdot z = x \cdot (y \cdot z))$,

3) (neutralni element) $(\exists e \in G)\ (\forall x \in G)\ (e \cdot x = x \cdot e = x)$,

4) (inverzni element) $(\forall x \in G)\ (\exists! y \in G)\ (x \cdot y = y \cdot x = e)$. Inverzni element elementa x, ako postoji, je jedinstven, pa se inverzni element elementa x obeležava sa x^{-1}.

Ako je jasno o kojoj binarnoj operaciji je reč, umesto grupa $(G, \cdot)$ kaže se samo grupa G, ne pravi se distinkcija između algebarske strukture i njenog nosača (skupa na kojem je definisana), podrazumevajući da su u svakoj takvoj situaciji operacije jasne iz konteksta.

Grupa u kojoj važi komutativni zakon, $x \cdot y = y \cdot x$ za svako $x, y \in G$, naziva se komutativna ili Abelova grupa.

Teorema 1.1. *Neka je G grupa. Tada su tačne sledeće formule:*

1) $x \cdot a = y \cdot a \Rightarrow x = y$

2) $a \cdot x = a \cdot y \Rightarrow x = y$

3) $(a^{-1})^{-1} = a$

4) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Za elemente a i b grupe G kažemo da su konjugovani akko postoji element $g \in G$ tako da važi $b = g^{-1} \cdot a \cdot g$. Red elementa g grupe G je najmanji pozitivan prirodan broj n za koji važi $g^n = \underbrace{g \cdot g \cdot \cdot ... \cdot g}_{n} = e$. Ako je $g^n \neq e$ za svaki prirodan broj n, kažemo da je element g beskonačnog reda. Red grupe G je kardinalnost njenog domena, u oznaci $\mid G \mid$. Kažemo da je grupa G konačna ako je $\mid G \mid$ prirodan broj. U konačnim grupama, svi elementi su konačnog reda.

Definicija 1.3. Neka su $(H, \cdot_H)$ i $(G, \cdot)$ grupe. Tada je $(H, \cdot_H)$ podgrupa grupe $(G, \cdot)$ ako je $\emptyset \neq H \subseteq G$ i operacija $\cdot_H$ je restrikcija $\cdot$ i obeležava se sa $(H, \cdot_H) \prec (G, \cdot)$.

Teorema 1.2. *Neka je $(G, \cdot)$ grupa. Tada su sledeći uslovi ekvivalentni:*

1) $(H, \cdot_H) \prec (G, \cdot)$

2) $\emptyset \neq H \subseteq G$, $(\forall a, b \in H)$ *(* $a \cdot b \in H$ *i* $a^{-1} \in H$ *)*

3) $\emptyset \neq H \subseteq G$, $(\forall a, b \in H)$ *(* $a \cdot b^{-1} \in H$ *)*

Neka je $(G, \cdot)$ grupa, i neka je $(H, \cdot_H) \prec (G, \cdot)$. Dalje, neka je g proizvoljan element domena grupe $(G, \cdot)$. Definišemo skup $gH = \{gh | h \in H\}$, koji se naziva levi koset podgrupe $(H, \cdot_H)$. Analogno, definišemo i desni koset podgrupe $(H, \cdot_H)$, određen elementom g, $Hg = \{hg | h \in H\}$. Kardinalni broj skupa levih/desnih koseta podgrupe $(H, \cdot_H)$, u odnosu na grupu $(G, \cdot)$, predstavlja indeks podgrupe $(H, \cdot_H)$ i obeležava se sa $[G : H]$.

Teorema 1.3. *Neka je $(G, \cdot)$ grupa, i neka je $(H, \cdot_H) \prec (G, \cdot)$. Tada važi:*

$$|G| = |H| \cdot [G : H].$$

Definicija 1.4. Podgupa H je normalna podgrupa grupe G, u oznaci $H \lhd G$, akko $\forall x \in G$ važi $xH = Hx$.

Definišimo faktor grupu grupe G po podgupi H na sledeći način:

$$G/H = (\{gH | g \in G\}, \cdot),$$

gde je binarna operacija definisana sa $aH \cdot bH \overset{def}{=} abH$

Definicija 1.5. Neka su $(G, \cdot)$ i $(H, *)$ grupe. Preslikavanje $\varphi : G \to H$ je homomorfno preslikavanje grupe $(G, \cdot)$ u grupu $(H, *)$ ako važi:

$$(\forall a, b \in G)\varphi(a \cdot b) = \varphi(a) * \varphi(b).$$

Skup svih homomorfnih preslikavanja grupe G u grupu H obeležavamo sa $Hom(G, H)$. Lako možemo primetiti da je za ma koje dve grupe G i H, $Hom(G, H)$ neprazan skup, uvek postoji tzv. trivijalni homomorfizam koji sve elemente grupe G slika u jedinični element grupe H. Neka je $\varphi : G \to H$ homomorfno preslikavanje grupe G u grupu H. Definišemo:

$$Ker(\varphi) := \{g \in G | \varphi(g) = e_H\}.$$

Tada važi da je $(Ker(\varphi), \cdot)$ normalna podgrupa grupe G. Za skup $Ker(\varphi)$ se koristi naziv jezgro homomorfizma preslikavanja φ.
Izomorfizam grupe G na grupu H je homomorfno preslikavanje koje je ujedno i bijektivno. Ukoliko je grupa H baš grupa G, onda je u pitanju automorfizam

grupe G. Ako postoji izomorfizam izmedju grupa G i H to obeležavamo sa $G \cong H$. Skup svih izomorfnih preslikavanja grupe G u grupu H obeležavamo sa $Is(G, H)$.

Teorema 1.4. *Neka je $\varphi : G \to H$ epimorfizam, tj. surjektivni homomorfizam grupe G u grupu H. Tada je:*

$$G \cong H/Ker(\varphi).$$

Definicija 1.6. Neka je G grupa i $A \subseteq G$. Podgrupa generisana skupom A, u oznaci $\langle A \rangle$, je najmanja podgrupa grupe G čiji domen sadrži A.

1.2 Prsteni

Definicija 1.7. Ako je R neprazan skup, tada je uredjena trojka $(R, +, \cdot)$ prsten ako važi:

1) $(R, +)$ je Abelova grupa,

2) $(R, \cdot)$ je polugrupa,

3) $(\forall x, y, z \in R)$ $(x \cdot (y + z) = x \cdot y + x \cdot z$ i $(y + z) \cdot x = y \cdot x + z \cdot x)$.

Osobina 3) naziva se distributivni zakon. Abelova grupa je označena u aditvnoj notaciji, tj. operacija je označena sa $+$, neutralni element sa 0, inverzni za $x \in R$ sa $-x$ i $\underbrace{a + a + .. + a}_{n} = na$ za $\forall a \in R$. Odnosno, na se definiše rekurzivno za $\forall n \in \mathbf{N}$ i $\forall a \in R$ sa: $1a = a$; $(n + 1)a = na + a$. Kako je (R,+) grupa, to se ova definicija može proširiti na sve cele brojeve, odnosno $0a = 0$ i $(-n)a = n(-a)$ za $\forall n \in \mathbf{N}$.

Ako je jasno o kojim operacijama $+$ i $\cdot$ je reč umesto prsten $(R, +, \cdot)$ kaže se samo prsten R.

Definicija 1.8. Prsten $(R, +, \cdot)$ je

1) prsten sa jedinicom ako postoji neutralni element e multiplikativne operacije,

2) komutativan prsten ako je operacija $\cdot$ komutativna,

3) integralni domen ako je komutativan prsten sa jedinicom $e \neq 0$ u kome važi da je

$$a \cdot b = 0 \Rightarrow a = 0 \vee b = 0, \text{ tj. ne postoje delitelji nule,}$$

4) polje ako je $(R \setminus \{0\}, \cdot)$ komutativna grupa.

Teorema 1.5. *U prstenu $(R, +, \cdot)$ važi:*

1) $a \cdot 0 = 0 \cdot a = 0$,

2) $(-a)b = a(-b) = -(ab)$,

3) $(-a)(-b) = ab$,

za sve elemente a i b koji pripadaju prstenu $(R, +, \cdot)$.

Primer 1.1. Prsten celih brojeva - $\mathbf{Z} = (Z, +, \cdot)$ gde je Z skup celih brojeva, a + i $\cdot$ standardno sabiranje i množenje celih brojeva, komutativan je prsten sa jedinicom, bez delitelja nule.

Primer 1.2. Prsten ostataka po modulu $n(\geq 1)$ - $\mathbf{Z}_n = (\{0, ..., n-1\}, +_n, \cdot_n)$, komutativan je prsten, sa jedinicom ako je $n > 1$, a bez delitelja nule akko je n prost broj.

Primer 1.3. Prsten realnih kvadratnih matrica, odnosno prsten matrica nad prstenom $\mathbf{Re}$-$\mathbf{M_n}(\mathbf{Re}) = (M_n(\mathbf{Re}), +, \cdot)$, gde je $M_n(\mathbf{Re})$ skup svih realnih kvadratnih matrica formata $n \times n$, a + i $\cdot$ su standardne operacije sabiranja i množenja matrica. Ovaj prsten je sa jedinicom i to nekomutativan i sa delitejima nule ako je $n > 1$.

Primer 1.4. Neka je $C_{[0,1]}$ skup svih neprekidnih funkcija na zatvorenom intervalu [0,1]. Ako su na tom skupu definisane operacije + i $\cdot$ sa:

$$(f + g)(x) = f(x) + g(x), \ (f \cdot g)(x) = f(x) \cdot g(x),$$

tada je $\mathbf{C_{[0,1]}} = (C_{[0,1]}, +, \cdot)$ komutativan prsten sa jedinicom i sa deliteljima nule.

Definicija 1.9. Karakteristika prstena R, u oznaci $char(R)$, je najmanji pozitivan prirodan broj n takav da je $nr = 0$ za svaki element r prstena R, ukoliko takav postoji, inače je R beskonačne karakteristike (∞) ili karakteristike 0.

Teorema 1.6. *1) Ako je R konačne karakteristike, tada red svakog elementa Abelove grupe $(R, +)$ deli $char(R)$.*

2) Ako je R prsten sa jedinicom, onda je $char(R)$ red elementa 1 u Abelovoj grupi $(R, +)$.

3) Karakteristika integralnog domena je ili 0 ili prost broj.

Definicija 1.10. Neprazan podskup T nosača prstena R je nosač (domen) potprstena prstena R akko je $(T, +|_{T^2}, \cdot|_{T^2})$ prsten gde su $+|_{T^2}$ i $\cdot|_{T^2}$ restrikcije binarnih operacija prstena nad skupom T^2.

Teorema 1.7. *Neprazan podskup T domena R prstena $(R, +, \cdot)$ je domen potprstena akko važi: za svako $a, b \in T$ je (1) $a - b \in T$ i (2) $ab \in T$.*

Definicija 1.11. Potprsten $(I, +, \cdot)$ prstena R je levi (desni) ideal akko je zatvoren za množenje elementima iz R sleva (zdesna), tj. akko važi: za svako a iz I i svako r iz R je $ra \in I$ ($ar \in I$).
Potprsten je ideal akko je i levi i desni ideal.
Levi (desni) ideal je pravi akko je njegov nosač pravi podskup nosača prstena.
Pravi levi (desni) ideal je maksimalan levi (desni) ideal ako nije strogo sadržan ni u jednom drugom pravom levom (desnom) idealu. Analogno se definišu pravi ideal i maksimalan ideal.
Nula potprsten (ideal) i ceo prsten su trivijalni ideali.

Teorema 1.8. *Neprazan podskup I domena prstena R je nosač levog (desnog) ideala akko važi: za svako a i b iz I i svako r iz R je $a-b, ra \in I$ ($a-b, ar \in I$).*

Definicija 1.12. Levi (desni) ideal, odnosno ideal, generisan skupom X je najmanji u smislu inkluzije levi (desni) ideal, tj. ideal, čiji domen sadrži X. Ideali generisani jednoelementnim skupom su glavni ideali. Prsten čiji su svi ideali glavni zove se prsten glavnih ideala. Za glavni ideal generisan skupom $\{a\}$ kaže se da je generisan elementom a.

Teorema 1.9. *Neka je T potprsten prstena R. Ako na skupu koseta podgrupe $(T,+)$ grupe $(R,+)$ definišemo korespodenciju*

$$\odot : \{a+I|a \in R\} \times \{b+T|b \in R\} \to \{c+T|c \in R\}$$

sa: $\odot(a+T, b+T) = ab+T$, onda je ta korespodencija (binarna) algebarska operacija akko je T ideal.

Definicija 1.13. Ako je I ideal prstena R,tada je

$$R/I = \{a+I|a \in R\} = (R/I, \oplus, \odot),$$

gde je $\oplus$ sabiranje koseta, a $\odot$ algebarska operacija definisana u prethodnoj teoremi, prsten, tzv. faktor prsten prstena R po idealu I.

Homomorfizmi

Definicija 1.14. Neka su dati prsteni $(R,+,\cdot)$ i $(S,\oplus,\otimes)$. Preslikavanje $\varphi : R \to S$ je homomorfno preslikavanje prstena R u prsten S ako je ispunjeno za svako $a,b \in R$:

$$(a+b)\varphi = (a)\varphi \oplus (b)\varphi \text{ i } (a \cdot b)\varphi = (a)\varphi \otimes (b)\varphi, \forall a,b \in R$$

Ukoliko je φ injektivno (sirjektivno) preslikavanje govorimo o injektivnom (sirjektivnom) preslikavanju ili monomorfizmu, tj.utapanju (epimorfizmu). Ako je φ bijektivno preslikavanje, onda je to izomorfno preslikavanje prstena R na prsten S, a za prstene R i S kaže se da su izomorfni u oznaci $R \cong S$. Skup svih homomorfnih preslikavanaja prstena R u S obeležava se sa $Hom(R,S)$, a skup svih izomorfnih presliavanja prstena R u S obelêžava se sa $Is(R,S)$.

Homomorfno (izomorfno) preslikavanje prstena R u sebe se zove endomorfizam (automorfizam) prstena R.

Definicija 1.15. Neka je $\varphi : R \to S$ homomorfizam komutativnih prstena sa jedinicom. Jezgro homomorfizma f, u oznaci $Ker(f)$ definiše se sa:

$$Ker(f) := \{x \in R : f(x) = 0_S\}.$$

Teoreme o izomorfizmima prstena navodimo bez dokaza, koji se mogu naći u [3].

Teorema 1.10. *(Prva teorema o izomorfizmu) Neka je φ izomorfno preslikavanje prstena $\varphi : R \to S$. Tada je prsten S izomorfan prstenu $R/Ker(\varphi)$.*

Teorema 1.11. *(Druga teorema o izomorfizmu) Ako su A i B potprsteni prstena R, takvi da je A ideal potprstena generisanog skupom $A \cup B$, koji označavamo sa $\langle A \cup B \rangle_p$, tada je*

$$\langle A \cup B \rangle_p / A \cong B/(A \cap B).$$

Teorema 1.12. *(Treća teorema o izomorfizmu) Ako je I ideal prstena R sadržan u potprstenu S (prstena R), onda je S ideal prstena R akko je S/I ideal prstena R/I i ako je S ideal, važi:*

$$R/S \cong (R/I)/(S/I).$$

1.3 Vektorski prostori

Definicija 1.16. Neka je $(V, +)$ komutativna grupa, a $(F, +, \cdot)$ polje. V je vektorski prostor nad poljem F, ako je definisano preslikavanje $F \times V \to V$, pri čemu se slika para (α, a) obeležava sa αa, tako da za svako $\alpha, \beta \in F, a, b \in V$ važi:

1) $\alpha(a + b) = \alpha a + \alpha b$,

2) $(\alpha + \beta)a = \alpha a + \beta a$,

3) $(\alpha\beta)a = \alpha(\beta a)$,

4) $1a = a$,

gde je sa 1 označen neutralni element za množenje polja F.
Vektorski prostor V nad poljem F označava se i sa $V(F)$.
Elementi skupa V se nazivaju vektorima i obeležavaju malim slovima latinice $a, b, c, ...$, a elementi skupa F se nazivaju skalarima i označavaju malim grčkim slovima $\alpha, \beta, \gamma, ...$.

Primer 1.5. Neka je F polje i $F^n = \{(a_1, ..., a_n)|a_i \in F\}$ skup svih uređenih $n-$torki elemenata iz F. Ako se sabiranje elemenata iz F^n i množenje elemenata iz F^n elementima iz F definišu na sledeći način:

$$(a_1, ..., a_n) + (b_1, ..., b_n) = (a_1 + b_1, ..., a_n + b_n),$$
$$\alpha(a_1, ..., a_n) = (\alpha a_1, ..., \alpha a_n),\ \alpha \in F,$$

onda je F^n vektorski prostor nad F.
Neposredno iz osobina polja F sledi da je sabiranje asocijativna i komutativna operacija na F^n. Neutralni element za sabiranje je $(0, ..., 0)$, a suprotan element za $(a_1, ..., a_n)$ je $(-a_1, ..., -a_n)$, što znači da je $(F^n, +)$ komutativna grupa. Ostali aksiomi vektorskog prostora takodje slede iz odgovarajućih osobina polja F, pa je F^n vektorski prostor nad F.

Primer 1.6. Neka je F polje i $F^\infty = \{(a_1, a_2, ...)|a_i \in F\}$ skup svih beskonačnih nizova elemenata iz F. Ako se sabiranje elemenata iz F^∞ i množenje elemenata iz F^∞ elementima iz F definišu na sledeći način:

$$(a_1, a_2, ...) + (b_1, b_2, ...) = (a_1 + b_1, a_2 + b_2, ...),$$
$$\alpha(a_1, a_2, ...) = (\alpha a_1, \alpha a_2, ...),\ \alpha \in F,$$

onda je F^∞ vektorski prostor nad F. Dokaz je analogan dokazu u prethodnom primeru.

Primer 1.7. Neka je V skup svih geometrijskih vektora (orijentisanih duži) u prostoru vezanih za tačku, sa zajedničkom početnom tačkom O. V je vektorski prostor nad poljem realnih brojeva ako se na uobičajeni način definišu sabiranje vektora (po pravilu paralelograma) i množenje vektora realnim brojem.

Teoreme navodimo bez dokaza, koji se mogu naći u [5].

Teorema 1.13. *Neka je $V(F)$ vektorski prostor. Tada važi:*

1) Nula vektor je jedinstven.

2) Za svaki vektor suprotni vektor je jedinstven.

3) Važi zakon skraćivanja (kancelacije) za sabiranje vektora.

4) $(\forall \alpha \in F)\alpha 0_V = 0_V$.

5) $(\forall a \in V)0a = 0_V$.

6) $(\forall \alpha \in F)(\forall a \in V)(-\alpha)a = -(\alpha a) = \alpha(-a)$.

7) $(\forall \alpha \in F)(\forall a \in V)\alpha a = 0 \Leftrightarrow \alpha = 0 \vee a = 0_V$.

Definicija 1.17. Neka je V vektorski prostor nad poljem F. Podskup W skupa V je potprostor vektorskog prostora V, ako je W vektorski prostor nad poljem F u odnosu na restrikcije na W sabiranja vektora i množenja vektora skalarom.

Teorema 1.14. *Neprazan podskup W vektorskog prostora V nad poljem F je potprostor od V akko za svako $\alpha, \beta \in F, a, b \in W$*

$$\alpha a + \beta b \in W.$$

Definicija 1.18. U vektorskom prostoru $V(F)$, vektor v je linearna kombinacija vektora $a_1, ..., a_n$ ako postoje skalari $\alpha_1, ..., \alpha_n$ takvi da je

$$v = \alpha_1 a_1 + ... + \alpha_n a_n.$$

Definicija 1.19. Ako je S neprazan podskup vektorkog prostora $V(F)$, onda se skup svih linearnih kombinacija vektora iz S naziva linearni omotač (ili lineal) skupa S i označava sa $\mathcal{L}(S)$. Dakle,

$$\mathcal{L}(S) = \{\alpha_1 a_1 + ... + \alpha_n a_n | n \in \mathbf{N}, \alpha_i \in F, a_i \in S\}.$$

Definicija 1.20. Ako je S podskup (niz vektora) vektorskog prostora $V(F)$, onda kažemo da je potprostor $\mathcal{L}(S)$ generisan skupom (nizom) S, a elemente S nazivamo generatorima potprostora $\mathcal{L}(S)$.

U specijalnom slučaju, ako je $\mathcal{L}(S) = V$, onda kažemo da S generiše V, a elementi skupa S su generatori vektorskog prostora V.

Definicija 1.21. U vektorskom prostoru $V(F)$ niz vektora $(a_1, ..., a_n)$ je linearno zavisan, ako postoje skalari $\alpha_1, ..., \alpha_n$, od kojih je bar jedan različit od nule, takvi da je

$$\alpha_1 a_1 + ... + \alpha_n a_n = 0.$$

Niz vektora koji nije linearno zavisan je linearno nezavisan.

Iz prethodne definicije neposredno sledi:
-Poredak vektora u nizu ne utiče na njegovu linearnu zavisnost odnosno nezavisnost.
-Niz vektora koji sadrži nula-vektor je linearno zavisan.
-Niz vektora koji sadrži linearno zavisan podniz je linearno zavisan.
-Svaki podniz linearno nezavisnog niza vektora je linearno nezavisan.
-Ako su u nizu vektora bar dva vektora jednaka, onda je taj niz linearno zavisan.

Teorema 1.15. *U vektorskom prostoru $V(F)$ niz vektora $(a_1, ..., a_n), n \geq 2$, medju kojima nije nula-vektor, je linearno zavisan akko među vektorima $a_2, ..., a_n$ postoji vektor a_k koji je linearna kombinacija vektora $a_1, ..., a_{k-1}$.*

Definicija 1.22. Baza konačno generisanog vektorskog prostora je niz vektora koji je linearno nezavisan i koji generiše vektorski prostor.

Sledeće tri teoreme daju potrebne i dovoljne uslove da bi neki niz vektora bio baza vektorskog prostora, što znači da bi svaka od tih teorema mogla da posluži i kao definicija baze vektorskog prostora.

Teorema 1.16. *U vektorskom prostoru $V(F)$ niz vektora je baza akko je taj niz maksimalan linearno nezavisan niz.*

Teorema 1.17. *U vektorskom prostoru $V(F)$ niz vektora je baza akko je taj niz minimalan niz generatora.*

Teorema 1.18. *U vektorskom prostoru $V(F)$ niz vektora $(a_1, ..., a_n)$ je baza akko se svaki vektor $x \in V$ može na jedinstven način napisati u obliku*

$$x = \sum_1^n \alpha_i a_i,\ \alpha_1, ..., \alpha_n \in F.$$

Definicija 1.23. Broj vektora baze konačno generisanog nenula vektorskog prostora $V(F)$ naziva se dimenzija tog vektorskog prostora i označava sa $dimV$. Dimenzija nula-prostora je 0.

Definicija 1.24. Ako su W_1 i W_2 potprostori vektorskog prostora $V(F)$, onda je presek tih potprostora njihov skupovni presek, tj.

$$W_1 \cap W_2 = \{x | x \in W_1 \wedge x \in W_2\}.$$

Analogno se definiše presek proizvoljne familije potprostora.

Definicija 1.25. Neka su $W_1, ..., W_n$ potprostori vektorskog prostora $V(F)$. Suma potprostora $W_1, ..., W_n$ je sledeći skup vektora

$$W = W_1 + ... + W_n = \{w_1 + ... + w_n | w_1 \in W_1, ..., w_n \in W_n\}.$$

Suma prazne familije jednaka je trivijalnom potprostoru koji sadrži samo nula element.

Definicija 1.26. Neka su V_1 i V_2 vektorski prostori nad istim poljem F. Vektorski prostor V_1 je izomorfan vektorskom prostoru V_2 ako postoji bijekcija $f : V_1 \to V_2$ takva da je za svako $\alpha, \beta \in F, a, b \in V_1$

$$f(\alpha a + \beta b) = \alpha f(a) + \beta f(b).$$

Teorema 1.19. *Dva konačno dimenzionalna vektorska prostora nad istim poljem su izomorfna akko su iste dimenzije.*

Glava 2

Moduli : Osnovne osobine

2.1 Moduli

Neka je V vektorski prostor nad poljem F i neka je $\tau \in \mathcal{L}(V)$. Za svaki polinom $p(x) \in F[x]$, operator $p(\tau)$ je dobro definisan. Na primer, ako je $p(x) = 1 + 2x + x^4$, onda je

$$p(\tau) = i + 2\tau + \tau^4$$

gde je i operator identiteta i τ^4 je kompozicija $\tau \circ \tau \circ \tau \circ \tau$.
Pomoću operatora τ, možemo definisati proizvod polinoma $p(x) \in F[x]$ i vektora $v \in V$:

$$p(x)v = p(\tau)(v)$$

Ovaj proizvod zadovoljava uobičajena svojstva množenja skalarom za sve $r(x), s(x) \in F[x]$ i $u, v \in V$,

$$\begin{aligned} r(x)(u+v) &= r(x)u + r(x)v \\ (r(x)+s(x))u &= r(x)u + s(x)u \\ [r(x)s(x)]u &= r(x)[s(x)u] \\ 1u &= u \end{aligned}$$

Za $\tau \in \mathcal{L}(V)$, skup V se može posmatrati kao skup na kome postoji operacija sabiranja i operacija koja polinomu $F[x]$ i elementu iz V pridružuje neki element iz V. Kao i kod vektorskog prostora, ali V nije vektorski prostor nad $F[x]$ zato što $F[x]$ nije polje, pa iz tog razloga ima smisla uvesti novi pojam modul.

Definicija 2.1. Neka je R komutativni prsten sa jedinicom. R-modul M je Abelova grupa $(M,+)$ sa preslikavanjem $\cdot\ : R \times M \to M$ za koje važe aksiome:

1) $\alpha(u+v) = \alpha u + \alpha v$;

2) $(\alpha+\beta)u = \alpha u + \beta u$;

3) $(\alpha\beta)u = \alpha(\beta u)$;

4) $1u = u$;

za sve $\alpha, \beta \in R$ i $u, v \in M$.

Vektorski prostori su samo specijalne vrste modula. Vektorski prostor je modul nad poljem.

Ako je jasno o kojim operacijama $+$ i $\cdot$ je reč, umesto modul $(M,+,\cdot)$ kaže se samo modul ili R-modul M, kao i da je sam skup M jedan R-modul u odnosu na te operacije.

U apstraktnoj formi, operacije modula M nad prstenom R obično se označavaju sa $+$ i $\cdot$ (tim redom). Prvu od njih zovemo sabiranjem, drugu množenjem skalarima, a elemente samog prstena R, skalarima u tom modulu. U vezi sa tim govori se o nuli $0_M = 0$, zatim o opozitu $-u$ od u, kao i operaciji oduzimanja $(u,v) \to u - v$ u tom modulu, misleći pri tom na odgovarajuće pojmove njegove aditivne grupe $(V,+)$.

Teorema 2.1. *Ako je M bilo koji modul nad prstenom R, za proizvoljne skalare $\alpha, \alpha_i \in R$ i svako $u, u_i \in M$ važi:*

1) $0u = 0_M, \alpha 0_M = 0_M$,

2) $\alpha(-u) = (-\alpha)u = -\alpha u$,

3) $\alpha(u_1 + ... + u_n) = \alpha u_1 + ... + \alpha u_n$, *4)* $(\alpha_1 + ... + \alpha_n)u = \alpha_1 u + ... + \alpha_n u.$

Dokaz. Ako je $a = 0u$, iz $0 + 0 = 0$ iz uslova definicije modula, $(\alpha + \beta)u = \alpha u + \beta u$, sledi da mora biti i $0u + 0u = 0u$, to jest $a + a = a$, a time i $a = 0_M$. I slično se pokazuje da je za $\alpha 0_M = 0_M$. Dalje, kako je $\alpha u + \alpha(-u) = \alpha(u + (-u)) = \alpha 0_M$, na osnovu druge od relacija od jednakosti u 1) sledi da je $\alpha(-u)$ jedno rešenje jednačine $\alpha u + x = 0_M$, pa mora biti $\alpha(-u) = -\alpha u$. Relacije 3) i 4) su neposredne posledice uslova iz definicije modula. □

Primer 2.1. 1) Za svaki komutativan prsten R i svaki prirodan broj n, skup R^n je R-modul u odnosu na operacije:

$$(a_1,.....a_n)+(b_1,.....b_n)=(a_1+b_1,.....a_n+b_n)$$
$$\text{i}$$
$$\mathrm{r}(a_1,.....a_n)=(\mathrm{r}a_1,....\mathrm{r}a_n)$$

za a_i,b_i, $r \in R$.

2) Bilo koji komutativni prsten R sa jedinicom je modul nad samim sobom, odnosno, R je R-modul. U ovom slučaju, množenje skalarom je samo množenje elemenata R. Ove osobine prstena ukazuju da su osobine R-modula zadovoljene.

3) Ako je R prsten, skup $M_{mn}(R)$ svih matrica veličine $m \times n$ je R-modul, podrazumevajući operacije sabiranja matrica i skalarnog množenja.

4) Svaka Abelova grupa $(G, +)$ je $\mathbb{Z}$-modul.

5) Svaki komutativan prsten R je modul nad bilo kojim njegovim potprstenom R.

6) Ideal I prstena R je modul nad prstenom R.

2.2 Podmoduli i homomorfizmi

Definicija 2.2. Za modul S kaže se da je podmodul R-modula M, ako su njegove operacije restrikcije odgovarajućih operacija samog modula M. To posebno znači da je S podskup od M i da ovi moduli imaju isti prsten skalara kao i da za svako $m, n \in M$ važi:

1) $m, n \in S \Rightarrow m + n \in S$,

2) $\alpha \in R, m \in S \Rightarrow \alpha \cdot m \in S$.

Piše se $S \leq M$, da bi naglasili da je S podmodul od M.
I obratno, kako je $-1u = -u$, svaki neprazan podskup S modula M koji zadovoljava prethodne uslove 1) i 2) jeste skup-nosač tačno jednog od njegovih podmodula.

Teorema 2.2. *Neprazan podskup S od R-modula je podmodul ako i samo ako za svako $\alpha, \beta \in R, m, n \in S$ važi*

$$\alpha m + \beta n \in S$$

Dokaz. Ako je S podmodul R-modula onda važe osobine:

1) $m, n \in S \Rightarrow m + n \in S$

2) $\alpha \in R, m \in S \Rightarrow \alpha \cdot m \in S$.

Iz osobina 1) i 2) sledi $\alpha, \beta \in R$, $m, n \in S \Rightarrow \alpha m + \beta n \in S$.

Obrnuto, pretpostavimo da važi $\alpha, \beta \in R, m, n \in S \Rightarrow \alpha m + \beta n \in S$. Ako se uzme da je $\alpha = \beta = 1$ dobija se uslov 1), a ako se uzme da je $\beta = 0$ dobija se uslov 2), iz toga sledi da je S podmodul.

□

Definicija 2.3. Za neko preslikavanje $f : M \rightarrow N$ kaže se da je homomorfizam modula M u modul N nad istim prstenom skalara R, ako je saglasno sa parovima njihovih odgovarajućih operacija, to jeste ako za svako $u, v \in M$ i svako $\alpha \in R$ važi:

1) $f(u + v) = f(u) + f(v)$,

2) $f(\alpha \cdot u) = \alpha \cdot f(u)$.

Skup svih homomorfizama označava se sa $Hom(M, N)$. Ukoliko je $M = N$ uvodi se oznaka $End(M) = Hom(M, M)$, elementi skupa $End(M)$ zovu se endomorfizmi modula M.

Uslovi 1) i 2) iz prethodne definicije, zajedno su ekvivalentni sa uslovom

$$f(\alpha u + \beta v) = \alpha \cdot f(u) + \beta \cdot f(v)$$

za svako $u, v \in M$ i svako $\alpha, \beta \in R$.
Naime, na osnovu uslova 1) i 2) dobija se

$$f(\alpha u + \beta v) = f(\alpha u) + f(\beta v) = \alpha \cdot f(u) + \beta \cdot f(v)$$

za svako $u, v \in M$ i svako $\alpha, \beta \in R$.

Jezgro homomorfizma i slika homomorfizma se definišu na sledeći način: $Kerf := \{u \in M | f(u) = 0\}$ i $Imf := \{f(u) \in N | u \in M\}$.

Za jezgro homomorfizma $Kerf$ važi $Kerf \subset M$ i da je podmodul R-modula M, takođe za sliku homorfizma Imf važi da je $Imf \subset N$ i da je podmodul.

Bijektivni homomorfizmi se nazivaju izomorfizmima, injektivni se nazivaju monomorfizmima, a sirjektivni epimorfizmima.

Za neki R-modul N kaže se da je izomorfan R-modulu M i piše $M \cong N$, ako postoji bar jedan izomorfizam $f : M \to N$.

2.3 Suma i presek podmodula

Definicija 2.4. Neka su $S_1, ..., S_n$ podmoduli R-modula M. Suma podmodula $S_1, ..., S_n$ je skup $S = S_1 + ... + S_n = \{x_1 + ... + x_n | \, x_1 \in S_1, ..., x_n \in S_n\}$.

Teorema 2.3. *Neka su $S_1, ..., S_n$ podmoduli R-modula M. Suma tih podmodula $S = S_1 + ... + S_n$ je podmodul R-modula M. To je najmanji podmodul R-modula M koji sadrži sve podmodule $S_1, ..., S_n$.*

Dokaz. Neka $x, y \in M, \quad \alpha, \beta \in R$.
Tada je $x = a_1 + ... + a_n, \ \ y = b_1 + ... + b_n, \ \ a_i, b_i \in S_i, \ \ i = 1, ..., n$, pa je $\alpha x + \beta y = (\alpha a_1 + \beta b_1) + ... + (\alpha a_n + \beta b_n)$.
Kako su $S_1, ..., S_n$ podmoduli, sledi da
$\alpha a_1 + \beta b_1 \in S_1, ..., \alpha a_n + \beta b_n \in S_n$,
pa $\alpha x + \beta y \in S$, tj. S je podmodul R-modula M.
S sadrži sve podmodule $S_j, j = 1, .., n$, jer za svako $j \in I$ i za svako $x \in S_j$ imamo familiju $\langle x_i \rangle, i = 1, .., n$, za koju je $x_i = 0_M \in S_i$ $(i = 1, .., n, \ i \neq j)$, $x_j = x \in S_j$, pa je $x = \sum\limits_i x_i$. Svaki podmodul S' modula M koji sadrži sve podmodule $S_i, \ i = 1, .., n$, sadrži očigledno i podmodul S, pa je S najmanji podmodul modula M koji sadrži sve podmodule $S_i, \ i = 1, ..., n$. □

Definicija 2.5. Skup $T = \bigcap\limits_{i \in I} S_i$ zove se presek familije $\langle S_i \rangle_{i \in I}$ podmodula R-modula M. Ako je I konačan skup, na primer, $I = \{1, ..., n\}$, tada se piše $S_1 \cap S_2 \cap ... \cap S_n$ umesto $\bigcap\limits_{i \in I} S_i$.

Teorema 2.4. *Neka je $(S_i)_{i \in I}$ familija podmodula R-modula M. Tada je presek $T = \bigcap\limits_{i \in I} S_i$ te familije podmodula opet podmodul R-modula M. To je najveći podmodul sadržan u svakom od podmodula $S_i, (i \in I)$.*

Dokaz. Ako je familija $(S_i)_{i \in I}$ prazna, tada je $S = M, T = \{0_M\}$ i tvrdnja tačna. Neka zato familija $(S_i)_{i \in I}$ nije prazna.
Sigurno je $S \neq \emptyset$, jer $0_M \in S_i$ dakle $0_M \in S$. Osim toga

$$x, y \in T \Rightarrow x, y \in S_i(i \in I) \Rightarrow x + y \in S_i(i \in I) \Rightarrow x + y \in T.$$

$$\alpha \in R, x \in T \Rightarrow \alpha \in R, \ \ x \in S_i(i \in I) \Rightarrow \alpha x \in S_i(i \in I) \Rightarrow \alpha x \in T.$$

Prema tome, T je podmodul R-modula modula M.
Očigledno je T najveći podmodul modula M sadržan u svakom od podmodula $S_i, \ (i \in I)$. □

2.4 Direktna suma

Prema samoj definiciji sume $\sum\limits_{i \in I} S_i$ podmodula $S_i(i \in I)$ nekog R-modula M, svako x iz te sume jednako je sumi bar jedne familije $\langle x_i \rangle_{i \in I}$ za koju je $x_i \in S_i(i \in I)$, za neki konačan skup $I = \{1, ..., n\}$.

Definicija 2.6. Za sumu $\sum\limits_{i\in I} S_i$ podmodula $S_i (i \in I)$ R-modula M kaže se da je direktna ako je svako x iz te sume jednako sumi tačno jedne familije $\langle x_i\rangle_{i\in I}, x_i \in S_i (i \in I)$, za neki konačan skup $I = \{1, ..., n\}$.
Direktnu sumu obeležavamo i sa $S_1 \oplus S_2 \oplus ... \oplus S_n$ ako je $I = \{1, ..., n\}$.

U definiciji direktne sume zahteva se jedinstvenost prikaza svakog elementa x iz te sume u obliku sume familije $\langle x_i\rangle_{i\in I}, x_i \in S_i (i \in I)$. Zanimljivo je da se taj zahtev može prividno ublažiti, jer važi:

Teorema 2.5. *Neka je $I = \{1, ..., n\}$. Suma $\sum\limits_{i\in I} S_i$ podmodula je direktna, akko se bar jedan element iz te sume može napisati kao suma tačno jedne familije $\langle x_i\rangle_{i\in I}, x_i \in S_i, i \in I$.*

Dokaz. Očigledno je dovoljno pokazati da je suma $\sum\limits_{i\in I} S_i$ podmodula direktna ukoliko bar jedan njen element x ispunjava uslov jednoznačnosti prikaza $x = \sum\limits_{i\in I} x_i, x_i \in S_i, (i \in I)$. Pretpostavimo da je y bilo koji element sume $\sum\limits_{i\in I} S_i$, a

$$y = \sum_{i\in I} y_i = \sum_{i\in I} z_i; \;\; y_i, z_i \in S_i (i \in I).$$

Tada je

$$x = x + y + (-y) = \sum_{i\in I} (x_i + y_i - z_i), \;\; x_i + y_i - z_i \in S_i (i \in I)$$

Pa zbog jedinstvenosti prikaza vektora x mora biti

$$x_i + y_i - z_i = x_i (i \in I), \text{ tj. } y_i = z_i (i \in I).$$

□

Direktna suma $\sum\limits_{i\in I} S_i$ se može okarakterisati i na sledeći način:

Teorema 2.6. *Da bi suma $\sum\limits_{i\in I} S_i$ bila direktna potrebno je i dovoljno da za svako $j \in I$ važi*

$$S_j \cap (\sum_{i\in I\setminus\{j\}} S_i) = \{0_M\}.$$

Dokaz. Neka je posmatrana suma podmodula direktna. Tada za svako $j \in I$ i svako $x \in S_j \cap (\sum\limits_{i\in I\setminus\{j\}} S_i)$ važi

$$x = \sum_{i \in I} x_i, \ \ x_i = 0_M (i \neq j), \ \ x_j = x,$$

jer je $x \in S_j$, odnosno

$$x = \sum_{i \in I} x_i^{'}, \ \ x_i^{'} \in S_i (i \neq j), \ \ x_j^{'} = 0_M,$$

jer $x \in \sum\limits_{i \in I \setminus \{j\}} S_i$.
Prikaz elementa x je jedinstven, tj. familije $\langle x_i \rangle_{i \in I}, \langle x_i^{'} \rangle_{i \in I}$ su iste, pa je specijalno, $x = x_j = x_j^{'} = 0_M$.
Prema tome, važi $S_j \cap (\sum\limits_{i \in I \setminus \{j\}} S_i) = \{0_M\}$.

Obrnuto, neka je ovaj uslov ispunjen za svako $j \in I$ i neka je x proizvoljan element sume $\sum\limits_{i \in I} S_i$. Ako je

$$x = \sum_{i \in I} x_i = \sum_{i \in I} x_i^{'}, \quad \ x_i, x_i^{'} \in S_i (i \in I),$$

tada važi

$$\sum_{i \in I} (x_i - x_i^{'}) = x - x = 0_M, \text{ tj.}$$

$$S_j \ni x_j - x_j^{'} = \sum_{i \in I \setminus \{j\}} (x_i^{'} - x_j) \in \sum_{i \in I \setminus \{j\}} S_i,$$

pa prema tome, za svako $j \in I$

$$x_j - x_j^{'} = 0_M, \text{ tj. } x_j = x_j^{'}.$$

To znači da je suma direktna. $\square$

2.5 Komplement podmodula

Suma $S + T$ dva podmodula S i T R-modula M sastoji se od svih elemenata iz M koji imaju oblik $x + y$ $(x \in S, y \in T)$. Prema teoremi 3.5. ta suma je direktna akko je $S \cap T = \{0_M\}$. Ukoliko je još $S + T = M$, onda se svako $x \in M$ može na jedinstven način napisati u obliku

$$x = x_1 + x_2 \ \ (x_1 \in S, x_2 \in T).$$

Definicija 2.7. Neka je S podmodul R-modula M. Za podmodul T R-modula M kaže se da je komplement podmodula S, ako je suma $S+T$ direktna i daje čitav modul M, tj. ako važi

$$S \oplus T = M.$$

Prema samoj definiciji, komplement modula S ne zavisi samo od S već i od modula M. Osim toga, komplement T podmodula S, ako uopšte postoji, nije obavezno jedinstven (što možemo videti u sledećem primeru).

Primer 2.2. U $\mathbb{Z}$-modulu podmodul $2\mathbb{Z}$ nema komplement, zato što svaki podmodul ako sadrži x onda će sadržati i $2x$ pa im presek ne može biti trivijalan.

Primer 2.3. Neka je M modul radijus vektora, trodimenzionalnih vektora u R^3, koji izlaze iz tačke O. Ako je S_1 podmodul radijus vektora svih tačaka prave p_1 koja prolazi kroz O, a S_2 podmodul radijus vektora ravni π kroz O koja ne sadrži pravu p_1. Tada je S_1+S_2 direktna suma i važi $S_1+S_2=M$, pa je podmodul S_2 komplement podmodula S_1. Sa druge strane, ako je $S_2{}'$ podmodul radijus vektora ravni π' kroz O koja se ne poklapa sa ravni π i ne sadrži pravu p_1, tada je $S_1+S_2{}'$ direktna suma i važi $S_1+S_2{}'=M$. Što znači da je i podmodul $S_2{}'$ komplement podmodula S_1.

Teorema 2.7. *Neka je S podmodul R-modula M. Ako je T komplement modula S, tada je T maksimalni element skupa $\mathcal{J}$ svih podmodula T koji imaju osobinu $S \cap T = \{0_M\}$.*

Dokaz. Ako je T komplement podmodula S, tada je sigurno $T \in \mathcal{J}$. Osim toga za svako $T' \in \mathcal{J}$ sa osobinom $T \subseteq T'$ važi

$$T' = T' \cap M = T' \cap (S+T).$$

Pokazaćemo da važi $T' \cap (S+T) = (T' \cap S) + T$. Pošto je $S+T=M$ onda se svako $x \in M$ može na jedinstven način napisati u obliku $x = x_1 + x_2$ $(x_1 \in S, x_2 \in T)$.

$$\begin{aligned} x \in T' \cap (S+T) &\Leftrightarrow x \in T' \wedge x \in (S+T) \\ &\Leftrightarrow (x_1+x_2) \in T' \wedge (x_1+x_2) \in (S+T) \\ &\Leftrightarrow \underbrace{(x_1 \in T' \wedge x_2 \in T')}_{T \subset T' \ i\ T' \ je\ podmodul} \wedge (x_1 \in S \wedge x_2 \in T) \\ &\Leftrightarrow (x_1 \in T' \wedge x_1 \in S) \wedge (x_2 \in T \wedge x_2 \in T') \end{aligned}$$

$$\begin{aligned}
&\Leftrightarrow x_1 \in (T' \cap S) \wedge x_2 \in (T \cap T') \\
&\overset{T \subseteq T'}{\Leftrightarrow} x_1 \in (T' \cap S) \wedge x_2 \in T \\
&\Leftrightarrow (x_1 + x_2) \in (T' \cap S) + T \\
&\Leftrightarrow x \in (T' \cap S) + T.
\end{aligned}$$

Pa važi da je

$$T' = T' \cap M = T' \cap (S + T) = (T' \cap S) + T = \{0_M\} + T = T,$$

što znači da je T maksimalni element skupa $\mathcal{J}$. □

Ukoliko je R polje, tj. M vektorski prostor, važi i obrnuta tvrdnja teoreme: svaki maksimalni element skupa $\mathcal{J}$ je i komplement potprostora S. Da za R-modul ne važi obrnuta tvrdnja teoreme pokazuje sledeći primer:

Primer 2.4. Neka je dat $\mathbb{Z}$-modul $\mathbb{Z}_4$. Za podmodul $S = \{0, 2\}$ modula $\mathbb{Z}_4$, jedini podmodul T modula $\mathbb{Z}_4$ koji ima osobinu $S \cap T = \{0\}$ je podmodul $T = \{0\}$, a on ne može biti komplement.

2.6 Linearna nezavisnost

Neka je M R-modul, $\langle \alpha^i \rangle_{i \in I}$ familija skalara, a $\langle x_i \rangle_{i \in I}$ familija elemenata iz M. Ako su članovi prve familije, osim eventualno konačno mnogo njih, jednaki 0_R tada to isto važi i za familiju $\langle \alpha^i x_i \rangle_{i \in I}$ (sa 0_M umesto 0_R). U sledećoj definiciji uvodi se pojam linearne kombinacije familije elemenata modula.

Definicija 2.8. Suma $\sum\limits_{i \in I} \alpha^i x_i$ zove se linearna kombinacija familije $\langle x_i \rangle_{i \in I}$. Skalari $\alpha^i (i \in I)$ zovu se koeficijenti te linearne kombinacije. Među ovim koeficijentima je samo konačno mnogo različitih od 0_R. Ako su svi koeficijenti linearne kombinacije jednaki 0_R, onda kaže se da je ta linearna kombinacija trivijalna

Prema samoj definiciji, svaka linearna kombinacija familije elemenata R-modula M je odredjeni element iz M. Trivijalna linearna kombinacija je jednaka 0_M. U aditivnoj Abelovoj grupi definisana je i suma prazne familije, ta suma je jednaka nula elementu te grupe. Pa postoji i linearna kombinacija prazne familije svakog R-modula. Kako ona, zapravo, nema koeficijenata, i ta kombinacija smatra se trivijalnom. To je jedina linearna kombinacija prazne familije. Svaka neprazna, pored trivijalne, ima bar još jednu (netrivijalnu) linearnu kombinaciju.

Za svaku familiju $\langle x_i \rangle_{i \in I}$ elemenata R- modula M trivijalna linearna kombinacija te familije daje 0_M. Za neke familije se može dogoditi da i neka njihova netrivijalna linearna kombinacija bude 0_M.

Definicija 2.9. Familija $\langle x_i \rangle_{i \in I}$ elemenata R- modula M je linearno nezavisna ako se 0_M može dobiti samo kao trivijalna linearna kombinacija te familije. U suprotnom slučaju, kaže se da je ta familija linearno zavisna.

Prema samoj definiciji, prazna familija je linearno nezavisna, jer ona i nema drugih linearnih kombinacija osim trivijalne. Ako je neprazna familija $\langle x_i \rangle_{i \in I}$ linearno nezavisna, tada za svaku familiju skalara $\langle \alpha^i \rangle_{i \in I}$ važi

$$\sum_{i \in I} \alpha^i x_i = 0_M \Rightarrow \alpha_i = 0 \ \ (i \in I),$$

dok u slučaju kada je neprazna familija $\langle x_i \rangle_{i \in I}$ linearno zavisna

$$(\exists j \in I) \alpha^j \neq 0, \ \sum_{i \in I} \alpha^i x_i = 0_M.$$

Teorema 2.8. *Ako je bar jedan član x_j familije $\langle x_i \rangle_{i \in I}$ elemenata R-modula M linearna kombinacija $\langle x_i \rangle_{i \in I \setminus \{j\}}$ preostalih članova, tada je data familija linearno zavisna.*

Dokaz. Ako je bar jedan član x_j familije $\langle x_i \rangle_{i \in I}$ linearna kombinacija preostalih članova, tj.

$$x_j = \sum_{i \in I \setminus \{j\}} \alpha^i x_i,$$

tada je

$$\sum_{i \in I} \alpha^i x_i = 0_M \text{ za } \alpha^j = -1 \neq 0,$$

pa familija je $\langle x_i \rangle_{i \in I}$ linearno zavisna. □

U slučaju da je $R = K$, tj. M vektorski prostor, važi i obrnuta tvrdnja ove teoreme: ako je familija $\langle x_i \rangle_{i \in I}$ linearno zavisna, tada je bar jedan član te familije linearna kombinacija familije preostalih članova. Da za R-modul ne važi obrnuta tvrdnja teoreme pokazuje sledeći primer:

Primer 2.5. U $\mathbb{Z}$-modulu $\mathbb{Z}$ važi da je $(-3) \cdot 2 + 2 \cdot 3 = 0$, a 2 ne možemo izraziti preko 3, a ni obrnuto.

Nijedan član linearno nezavisne familije $\langle x_i \rangle_{i \in I}$ elemenata R-modula M ne sme biti 0_M. Osim toga nikoja dva člana x_i, x_j, $(i \neq j)$ ne mogu biti jednaki. Drugim rečima, u slučaju linearno nezavisne familije $\langle x_i \rangle_{i \in I}$ skup $A = \{x_i | i\}$ ne sadrži 0_M, a preslikavanje

$$f : I \to A,\ \ f(i) = x_i\ \ (i \in I)$$

je bijektivno.
Za svaki skup A elemenata R-modula M imamo bijektivno preslikavanje $id_A : A \to A$, dakle familiju $\langle a \rangle_{a \in A}$ u kojoj je ulogu skupa indeksa I preuzeo skup A članova familije. Kako je za ovu familiju $x_a = a$, umesto $\sum\limits_{a \in A} \alpha^a x_a$ piše se $\sum\limits_{a \in A} \alpha^a a$.
Na osnovu toga, pojam linearne kombinacije, a time i linearne (ne)zavisnosti može se definisati za svaki podskup A R-modula M.

Definicija 2.10. Neka je A podskup R-modula M. Pod linearnom kombinacijom skupa A podrazumeva se linearna kombinacija $\langle a \rangle_{a \in A}$. Za skup A kaže se da je linearno (ne)zavisan, ako je familija $\langle a \rangle_{a \in A}$ linearno (ne)zavisna. Ako je skup A prazan, tada je i familija $\langle a \rangle_{a \in A}$ prazna, pa je svaki prazan podskup A R-modula M linearno nezavisan.

Neka je zadana familija $\langle x_i \rangle_{i \in I}$. Skup $[\langle x_i \rangle_{i \in I}]$ svih linearnih kombinacija te familije je podmodul modula M. To je najmanji podmodul modula M koji sadrži sve članove ove familije.

Definicija 2.11. Za podmodul $[\langle x_i \rangle_{i \in I}]$ R-modula M sastavljen od svih linearnih kombinacija familije $\langle x_i \rangle_{i \in I}$, kaže se da je generisan tom familijom ili da mu je ta familija generator.
Za module koji imaju bar jedan konačan generator kaže se da su konačnog tipa.

Definicija 2.12. Linearno nezavisan generator R-modula M zove se baza modula M.
R-modul M koji ima bazu zove se slobodan modul.

Može se dokazati da postoje moduli koji nisu slobodni, kao na primer, svaki od $\mathbb{Z}$-modula $M = \mathbb{Z}_k$, ($\forall k \in \mathbb{N}$, skup $\mathbb{Z}_k = \{0, 1, ..., k-1\}$ je komutativna grupa u odnosu na sabiranje $+_k$ po modulu k), nije slobodan. Važi da je $ku = 0, \forall u \in M$, pa modul M nema linearno nezavisan generator..

Primer 2.6. Neka je R bilo koji komutativan prsten. Za svaki prirodan broj n odgovarajući R-modul R^n ima bazu sa n elemenata. Ako je, na primer,

$$\begin{array}{c} x_1 = (1, 0, 0, ..., 0, 0) \\ x_2 = (0, 1, 0, ..., 0, 0) \\ . \\ . \\ . \\ x_n = (0, 0, 0, ..., 0, 1), \end{array}$$

odredjujući prvo svaku od n-torki $\alpha^i x_i$, a zatim i njihovu sumu, odmah sledi da za proizvoljne α_i-ove iz R važi

$$\alpha^1 x_1 + \alpha^2 x_2 + ... + \alpha^n x_n = (\alpha_1, \alpha_2, ..., \alpha_n).$$

Pri tom je $\alpha^1 x_1 + \alpha^2 x_2 + ... + \alpha^n x_n = 0_M$, to jeste $(\alpha_1, \alpha_2, ..., \alpha_n) = (0, ..., 0)$, akko je $\alpha_i = 0$ za svako i, pa je $[\langle x_i \rangle_{i \in I}]$ i generator i linearno nezavisan u ^{n}.

2.7 Količnički modul

Ako je S podmodul R-modula M, tada je S (normalna) podgrupa grupe $(M, +)$, pa postoji relacija ϱ zadana na sledeći način:

$$x \varrho y \Leftrightarrow -x + y \in S$$

za svako $x, y \in M$. Ta relacija je saglasna sa sabiranjem u M, pa postoji faktorska grupa $(M/S, +)$, pri čemu je u faktorskom skupu M/S svih klasa ekvivalencije $x + S$, $(x \in M)$ u odnosu na relaciju ϱ sabiranje definisano pomoću predstavnika, tj.

$$(x + S) + (y + S) = (x + y) + S$$

za svako $x, y \in M$.
Relacija ϱ je saglasna i sa množenjem skalarima, pa u faktorskom skupu M/S i množenje skalarima se može definisati preko predstavnika, tj.

$$\alpha \cdot (x + S) = \alpha \cdot x + S$$

za svako $\alpha \in R$ i svako $x \in M$.
Na taj način faktorski skup dobija strukturu R-modula. Osim toga, pirodno preslikavanje

$$f_\varrho : M \to M/S, \;\; f_\varrho(x) = x + S (x \in M)$$

predstavlja ne samo epimorfizam aditivnih grupa nego i modula.

Definicija 2.13. Neka je S podmodul R-modula M, ϱ relacija ekvivalencije u M zadana $x\varrho y \Leftrightarrow -x + y \in S$. Tada se modul M/S u kome su operacije modula definisane pomoću predstavnika zove količnički modul ili faktorski modul modula M po podmodulu S. Prirodno preslikavanje $f_\varrho : M \to M/S$, $f_\varrho(x) = x + S (x \in M)$, koje predstavlja epimorfizam modula, zove se i prirodni epimorfizam.

Ako je S podmodul R-modula M, tada za prirodni epimorfizam

$$f : M \to M/S$$

i svaki podmodul T modula M imamo homomorfizam modula

$$f_T : T \to M/S, \;\; f_T(y) = f(y)(y \in T).$$

2.8 Teoreme o izomorfizmima modula

Teoreme o izomorfizmima modula navodimo bez dokaza, koji se mogu naći u [6].

Teorema 2.9. *(Prva teorema o izomorfizmu modula) Neka su M, N R-moduli i neka je $f : M \to N$ homomorfizam R-modula. Tada važi*

$$M/Ker(f) \cong Im(f)$$

Teorema 2.10. *(Druga teorema o izomorfizmu modula) Neka je M R-modul i neka su N i P njegovi podmoduli. Tada postoji izomorfizam R-modula*

$$(N + P)/P \cong N/(N \cap P).$$

Teorema 2.11. *(Treća teorema o izomorfizmu modula) Neka je M R-modul i neka su N i P njegovi podmoduli takvi da je $P \subseteq N$. Tada je*

$$(M/N) \cong (M/P)/(N/P).$$

2.9 Torzioni elementi

Za razliku od vektorskih prostora, sistem elemenata R-modula može biti linearno zavisan i u slučaju kada nijedan od njih nije linearna kombinacija preostalih. Štaviše, u njemu ne mora da važi ni

$$\alpha x = 0_M \Rightarrow \alpha = 0_R \vee x = 0_M.$$

U vezi sa tim, definiše se pojam torzionog elementa:

Definicija 2.14. Neka je M R-modul, i neka $x \in M$. Ako postoji $\alpha \in R$ tako da važi $\alpha x = 0_M$, $\alpha \neq 0_R$, tada se kaže da je x torzioni element modula M. Ako je svako $x \in M$ torzioni element modula M, tada se kaže da je M torzioni modul.
Ukoliko x nije torzioni element, tada se kaže da je x element bez torzije ili torziono slobodan. Ukoliko je svako $x \in X$, $x \neq 0_M$, element bez torzije, tada se kaže da je M modul bez torzije ili torziono slobodan. Ako posmatramo R kao R-modul, tada za svako $x \in X$ imamo epimorfizam modula $R \to Rx$, $\alpha \to \alpha x, \alpha \in R$. Jezgro ovog epimorfizma zove se torzioni ideal i označava se sa $Tor(x)$. Dakle,

$$Tor(x) = \{\alpha \in R : \alpha x = 0_M\}.$$

Ako je modul M generisan torzionim elementima $x_1, ..., x_n$, onda je M torzioni modul jer za $\alpha_i \in Tor(x_i)$, $\alpha \neq 0$ $(i = 1, ..., n)$ možemo uzeti i $\alpha = \alpha_1 ... \alpha_n \neq 0$ i $\alpha x = 0_M$ $(x \in M)$.

Teorema 2.12. *1)Neka je R komutativan prsten se jedinicom i bez delitelja nule i neka je M R-modul. Skup T svih torzionih elemenata $x \in M$ čini podmodul modula M.*

2) Količnički modul M/T je modul bez torzije.

Dokaz. 1) T je podmodul modula M. Naime, $T \neq \emptyset$, jer $0_M \in T$, a osim toga

$$x, y \in T \Rightarrow x + y \in T; \ \lambda \in R, \ x \in T \Rightarrow \lambda x \in T,$$

jer ako je

$$\alpha x = 0_M, \ \alpha \neq 0_M; \ \beta y = 0_M, \ \beta \neq 0,$$

tada

$$(\alpha\beta)(x+y) = \beta(\alpha x) + \alpha(\beta y) = 0_M, \ \ \alpha\beta \neq 0,$$

odnosno

$$\alpha(\lambda x) = \lambda(\alpha x) = 0_M, \ \ \alpha \neq 0.$$

2) M/T je modul bez torzije.
Ako za $x+T \in M/T$ postoji $\alpha \in R$, tako da važi $\alpha(x+T) = 0_M + T, \ \ \alpha \neq 0$, tada

$$\alpha x \in T, \alpha \neq 0,$$

pa postoji $\beta \in R$ tako da važi

$$(\alpha\beta)x = \beta(\alpha x) = 0_M, \ \ (\alpha\beta) \neq 0,$$

što žnači da je

$$x \in T, \text{ tj. } x + T = 0_M + T.$$

$\square$

Definicija 2.15. Neka je M R-modul. Tada se podmodul T modula M sastavljen od svih torzionih elemenata modula M zove torzioni podmodul modula M.

Glava 3

Slobodni moduli

3.1 Slobodni moduli

Za podmodul U R-modula M kažemo da je cikličan, ako ima jednočlan generator, to jeste bar jedan element u za koji je

$$U = Ru = \{au : a \in R\}.$$

Definicija 3.1. Za fiksirano u, sa $\phi : a \to au$ definisan je i jedan homomorfizam R-modula R u R-modul M, čija je slika $Im\phi = Ru$. Samo njegovo jezgro $Ker\ \phi$ označavamo sa

$$Ann(u) = \{a \in R : au = 0\}$$

i zovemo anulatorom uočenog elementa u. On je i jedan ideal prstena R, pa prema prvoj teoremi o izomorfizmima, u klasi R-modula važi i

$$Ru \cong R/Ann(u).$$

Otuda je $Ru \cong R$ akko je $Ann(u) = 0$. To znači da je uočeni element u torziono slobodan, a time i linearno nezavisan u R-modulu M.

Za R-modul M kaže se da je konačnog tipa ili konačno generisan, ako ima jedan konačan generator, na primer $e = [e_1, ..., e_n]$. Time je on i suma

$$M = Re_1 + ... + Re_n$$

konačno mnogo cikličnih podmodula Re_i, jer se svaki njegov element $u \in M$ može predstaviti u obliku $u = \alpha_1 e_1 + ... + \alpha_n e_n$ za neke α_i-ove iz prstena R. U opštem slučaju, ta suma ne mora biti i direktna, tj. tu ne mora biti i

$$M = Re_1 \oplus ... \oplus Re_n$$

To važi akko su su uočeni e_i-ovi i linearno nezavisni u modulu M. Štaviše, tada je $Re_i \cong R$, a time i

$$M \cong R \times R \times ... \times R = R^n.$$

Kao što je već rečeno, za R-modul M kažemo da je slobodan, ako ima bar jednu bazu, to jeste jedan linearno nezavisan generator.

3.2 Rang slobodnog modula

Teorema 3.1. *Neka je R komutativan prsten se jedinicom i bez delitelja nule i neka je M R-modul. Ako M ima bazu $\{e_1, ..., e_n\}$, onda svaki linearno nezavisni podskup modula M ima najvise n elemenata. Specijalno, svake dve baze toga modula imaju isti broj elemenata.*

Dokaz. Neka je $\{x_1, ..., x_m\}$ bilo koji linearno nezavisni podskup modula M. Indukcijom u odnosu na n dokazuje se da je $m \leqslant n$. Za $n = 0$ to je jasno, jer tada je $M = \{0_M\}$, pa je samo prazan podskup modula M linearno nezavisan.
Neka je $n > 0$. Pretpostavimo da je tvrdnja tačna za $n - 1$.
Treba pokazati da je tvrdnja tačna i za n.
Razmotrimo prvo slučaj $n = 1$.
Ako je $n = 1$, tada su svaka dva elementa $a, b \in M$ linearno zavisna, pa ne postoji linearno nezavisan podskup modula M koji bi mogao imati više nego jedan element. Ako je jedan od elemenata a, b jednak 0_M, to je jasno. Inače je $a = \alpha e_1,\ \ b = \beta e_1\ \ (\alpha \neq 0, \beta \neq 0)$, pa se iz $\beta a - \alpha b = 0_M$ vidi da su elementi a i b linearno zavisni.
Neka je sada $n > 1$. Tada je $M = Re_1 + ... + Re_n$. Podmodul

$$M' = Re_2 + ... + Re_n$$

modula M ima bazu od $n - 1$ elemenata, pa je za njega tačna tvrdnja koju treba dokazati za M. Isto tako faktorski modul

$$M/M' = R \cdot (e_1 + M')$$

ima bazu od jednog elementa, pa je i za njega tačna ova tvrdnja. Ako svako x_i pripada podmodulu M', onda znači, mora biti $m \leqslant n - 1$, dakle sigurno je $m \leqslant n$.

Neka, na primer, $x_1 \notin M^{'}$. Tada $x_1 + M^{'} \neq 0_M + M^{'}$. Osim toga, za svako $i = 2, ..., m$, elementi $x_1 + M^{'}$, $x_i + M^{'}$ modula $M/M^{'}$ su linearno zavisni (na osnovu slučaja $n = 1$), tj. postoje $\alpha_i, \beta_i \in R$, od kojih je bar jedan različit od 0, takvi da je

$$\alpha_i \cdot (x_1 + M^{'}) + \beta_i(x_i + M^{'}) = 0_M + M^{'}, \text{ tj. } \alpha_i x_1 + \beta_i x_i = y_i \in M^{'}.$$

Zapravo je $\beta_i \neq 0$ $(i = 2, 3, ..., m)$. Inače bi za bar jedno i važilo $\alpha_i x_1 \in M^{'}, \alpha_i \neq 0$. To je nemoguće, jer je

$$x_1 + M^{'} = \alpha(e_1 + M^{'}), \text{ tj. } x_1 - \alpha e_1 = y_1 \in M^{'}, \ (\alpha \neq 0)$$

pa bi važilo

$$\alpha_i \alpha e_1 = \alpha_i x_1 - \alpha_i y_1 \in M^{'},$$

a to je u suprotnosti sa linearnom nezavisnosti elemenata $e_1, ..., e_n$ budući da je $\alpha \neq 0, \alpha_i \neq 0$, dakle $\alpha_i \alpha \neq 0$.
Kada bi bilo $m > n$, onda bi bilo $m - 1 > n - 1$, pa bi elementi $y_2, ..., y_m$ modula $M^{'}$ bili linearno zavisni. Postojali bi elementi $\gamma_i \in R, (i = 2, ..., m)$, od kojih je bar jedan različit od 0, takvi da važi

$$\gamma_2 y_2 + ... + \gamma_m y_m = 0_M,$$

tj.

$$(\alpha_2\gamma_2 + ... + \alpha_m\gamma_m)x_1 + \beta_2\gamma_2 x_2 + ... + \beta_m\gamma_m x_m = 0_M.$$

Ovo je nemoguće, jer je bar jedno γ_i i svako β_i različito od 0, a elementi $x_1, x_2, ..., x_m$ su linerno nezavisni.
Dakle, mora važiti $m \leqslant n$.
Specijalno je svaka druga baza modula M konačna, jer bi se inače u takvoj bazi moglo naći $n + 1$ linearno nezavisnih elemenata.
Ako je $f_1, ..., f_m$ bilo koja druga baza modula M, tada mora biti $m \leqslant n$. Ako zamenimo uloge ovim bazama dobijamo $n \leqslant m$. Dakle, $m = n$ i time je teorema dokazana. $\square$

Definicija 3.2. Ako R-modul M ima konačnu bazu, onda se kaže da modul M ima konačan rang. U tom slučaju broj elemenata bilo koje baze modula M zove se rang modula M.

Slobodan R-modul M je ranga n akko je izomorfan modulu R^n. Posebno, ako je $m \neq n$, moduli R^n i R^m nisu izomorfni.

Teorema 3.2. *Za svaku bazu $\{e_1, ..., e_n\}$ R-modula F ranga n i bilo koje elemente $c_1, ..., c_n$ R-modula M postoji i tačno jedan homomorfizam $\pi : F \to M$, takav da je $\pi(e_i) = c_i$, za svako i. Posebno, svaki R-modul M konačnog tipa je homomorfna slika bar jednog slobodnog R-modula F, a time je $M \cong F/U$ za neki podmodul U modula F.*

Dokaz. Pretpostavimo da postoji homomorfizam $\pi^{'} : F \to M$, takav da je $\pi^{'}(e_i) = c_i$, za svako i. Tada važi da je $\pi^{'}(e_i) = c_i = \pi(e_i)$. Neka je $x \in F$. Tada postoje α_i, $i = 1, ..., n$, tako da je $x = \sum_{n=1}^{n} \alpha_i e_i$, pa važi

$$\begin{aligned} \pi(x) = \pi(\sum_{n=1}^{n} \alpha_i e_i) &\overset{\pi je\ homom.}{=} \sum_{n=1}^{n} \alpha_i \pi(e_i) = \sum_{n=1}^{n} \alpha_i \pi^{'}(e_i) \\ &\overset{\pi^{'} je\ homom.}{=} \pi^{'}(\sum_{n=1}^{n} \alpha_i e_i) = \\ &= \pi^{'}(x). \end{aligned}$$

Prema tome $\pi = \pi^{'}$, tj. π je jedinstveni homomorfizam sa navedenom osobinom. □

3.3 Slobodni moduli nad prstenom glavnih ideala

Za razliku od vektorskih prostora, dati R-modul ne mora biti slobodan, a ako jeste slobodan, to ne moraju biti i svi njegovi podmoduli.

Šta više ako ovo poslednje važi za sve slobodne module nad R, onda R mora biti prsten glavnih ideala. Kako je $ac - ca = 0$, u samom R-modulu R su svaka dva elementa linearno zavisna. Otuda i baza bilo kog njegovog podmodula, tj. ideala U prstena R mora biti jednočlana, pa je tako i $U = aR$ za neko a iz R. Zato se ograničava na slobodne module konačnog tipa nad bilo kojim prstenom glavnih ideala.

Teorema 3.3. *Svaki podmodul U, slobodnog modula M ranga n nad prstenom glavnih ideala R, je takodje slobodan i ranga ne većeg od n.*

Dokaz. Neka je $\{e_1, ..., e_n\}$ baza modula M. Dokaz ćemo provesti indukcijom u odnosu na n.

Ako je $n = 0$, tada je $M = \{0_M\}$, pa je i $U = \{0_M\}$, dakle rang U=0.
Pretpostavimo da je tvrdnja tačna za $n-1$ i dokažimo da važi za n.
Treba pokazati da su tvrdnje tačne i za $n = 1$.
U slučaju $n = 1$ preslikavanje $\alpha \to \alpha e_1 (\alpha \in R)$ predstavlja izomorfizam modula R^1 na modul M. Inverzna slika od U je podmodul J R-modula R, odnosno ideal prstena R. Pa izmedju ideala J i prstena R i podmodula modula M postoji korespodencija: $J \to U = Je_1$.
Svaki ideal J prstena glavnih ideala R ima oblik $J = R\alpha$, za neko $\alpha \in R$, pa je svaki podmodul U modula M oblika $U = R \cdot \alpha e_1$, dakle ranga 0 (za $\alpha = 0$) ili 1 (za $\alpha \neq 0$).
Neka je sada $n > 0$.
Podmodul $M' = Re_2 \oplus ... \oplus Re_n$ modula M je slobodan modul ranga $n-1$.
Zato je po pretpostavci indukcije za svaki podmodul U modula M, podmodul $U \cap M'$ modula M' slobodan i ima rang $(U \cap M') \leqslant n-1$.
Sa druge strane, modul $M/M' \cong Re_1$ je slobodan ranga 1.
Postoji prirodni epimorfizam

$$M \to M/M'$$

i njegova restrikcija

$$\phi : U \to M/M'.$$

Podmodul $Im(\phi)$ modula M/M' je slobodan modul ranga $\leqslant 1$. Sa druge strane, $Ker(\phi) = U \cap M'$ je slobodan modul ranga $\leqslant n-1$.
Ako dokažemo da postoji podmodul U' modula U tako da važi $U = U' \oplus Ker(\phi)$, U će biti i slobodan i

$$rang\ \ U \leqslant 1 + (n-1) = n.$$

Egzistencija U' sa tom osobinom sledi iz sledeće leme.

Lema : Neka je U modul nad prstenom R, a F slobodni R modul. Tada za svaki epimorfizam $\phi : U \to F$ postoji podmodul U' modula U takav da važi $U = U' \oplus Ker(\phi)$.

Dokaz : Neka je $(f_i)_{i \in I}$ baza slobodnog modula F. Tada postoje elementi

$$u_i \in U,\ \ f_i = \phi(u_i) \quad (i \in I).$$

Za tako odabrane elemente $u_i \in U$ prema teoremi 4.2. postoji homomorfizam

$$\psi : F \to U,\ \ \psi(f_i) = u_i \quad (i \in I).$$

Kako je

$$(\phi \circ \psi)(f_i) = \phi(\psi f_i) = \phi(u_i) = f_i \quad (i \in I),$$

važi $\phi \circ \psi = id_F$. Ako je $U^{'}$ podmodul $Im(\psi)$ modula U, dokazaćemo da je $U = U^{'} \oplus Ker(\phi)$, a $U^{'} \cong F$. Zaista,

$$\phi(U^{'}) = (\phi \circ \psi)(F) = id_F(F) = F = Im(\phi).$$

Prema tome, za svako $u \in U$ postoji $u^{'} \in U^{'}$ sa $\phi(u) = \phi(u^{'})$, tj.

$$u - u^{'} = u^{''} \in Ker(\phi), \text{ dakle } u = u^{'} + u^{''} \ \ (u^{'} \in U^{'}, \ u^{''} \in Ker(\phi)).$$

Ako dokažemo da je $U^{'} \cap Ker(\phi) = \{0_U\}$, tada je $\phi : U^{'} \rightarrow F$ izomorfizam, a $U = U^{'} \oplus Ker(\phi)$.
Neka je $u \in U^{'} \cap Ker(\phi)$. Tada je $\phi(u) = 0_F$, jer $u \in Ker(\phi)$. Sa druge strane, $u = \psi(v)$ za neko $v \in F$, jer je $U^{'} = Im(\psi)$, a $u \in U^{'}$. Zato je $v = id_F(v) = (\phi \circ \psi)(v) = \phi(\psi v) = \phi(u) = 0_F$, dakle $u = \psi(v) = 0_U$.
Time je lema dokazana. □

Prema tome, ako modul M nad prstenom glavnih ideala R ima bazu e dužine n, tada i svaki njegov podmodul U ima bazu f izvesne dužine $m \leqslant n$. Uz to i za $U \neq M$ može biti $m = n$. To posebno znači da baza f podmodula U ne mora biti i deo neke baze samog modula M. Ipak, u vezi sa tim važi:

Teoreme 4.4. i 4.5. navodimo bez dokaza, koji se mogu naći u [7].

Teorema 3.4. *Za svaki pravi podmodul U slobodnog modula M ranga n nad prstenom glavnih ideala R postoji sistem $\{\alpha_1, ..., \alpha_k\}$ elemenata iz R, medju kojima svaki deli onaj naredni, i za koji modul M ima bar jednu bazu $e = \{e_1, ..., e_n\}$ takvu da je i*

$$f = \{\alpha_1 e_1, ..., \alpha_k e_k\}$$

jedna baza uočenog modula U.

Neka je M bilo koji konačno generisan modul nad prstenom glavnih ideala R. Ako je generisan sa n elemenata, on je izomorfan i količničkom modulu F/U bar jednog slobodnog R-modula F ranga n po njegovom podmodulu U.

Teorema 3.5. *Neka je R prsten glavnih ideala, svaki R-modul M konačnog tipa je izomorfan direktnoj sumi cikličnih modula, tj. $R/a_iR, \ 1 \leq i \leq n$*

$$M \cong R/a_1R \oplus ... \oplus R/a_nR.$$

gde za elemente $a_1, ..., a_n \in R$ važi $a_i | a_{i+1}$ za svako i.

3.4 Torziono slobodni i slobodni moduli

Neka je skup τM skup svih torzionih elemenata modula M, i on je jedan njegov podmodul. Naime, ako je $u, v \in \tau M$, a time i $au = cv = 0$ za neke ne-nula elemente a i c iz integralnog domena R, biće $ac \neq 0$, pa iz $ac(u - v) = 0$ sledi da je i $u - v \in \tau M$.

Tako odredeđen podmodul $T = \tau M$ R-modula M, kao što je već rečeno, zovemo torzionim podmodulom. To posebno znači da je taj modul i torziono slobodan akko je $\tau M = 0$. Pri tom važi i:

Teorema 3.6. *Ako je konačno generisan R-modul M nad prstenom glavnih ideala R torziono slobodan, tada je R-modul M slobodan.*

Dokaz. Na osnovu Teoreme 4.5. modul M je izomorfan direktnoj sumi cikličnih modula $R/a_1R \oplus ... \oplus R/a_nR$. Bez umanjenja opštosti može se pretpostaviti da su svi elementi $a_1, ..., a_n$ neinvertibilni, tj. za svako i, $1 \leq i \leq n$, $a_iR \neq R$. U suprotnom odgovarajuće elemente možemo izbrisati iz sume. Kako važi da je $a_1R \neq R$ postoji nenula element $x_1 \in R/a_1R$ pa x_1 možemo zapisati kao $x_1 = b + a_1R$ i $x_1 \notin a_1R$. Ako pretpostavimo da je $a_1 \neq 0$ onda postoji i nenula element $a \in a_1R$ i a možemo zapisati kao $a = a_1c, c \in R$, a iz toga sledi da je $ax_1 = a(b + a_1R) = ab + aa_1R = a_1cb + aa_1R = a_1(cb + aR) \subseteq a_1R$, a iz toga sledi da je ax_1 nula element u R/a_1R. Iz toga sledi, da za element $x = (x_1, 0, ..., 0) \in R/a_1R \oplus ... \oplus R/a_n$ važi $ax = 0$ i $a \neq 0$ i $x \neq 0$, odnosno x je torzioni element, što je u suprotnosti da je R-modul M torziono slobodan. Prema tome, $a_1 = 0$. Slično se pokazuje da važi $a_1 = a_2 = ... = a_n = 0$. Odnosno R-modul M je izomorfan slobodnom modulu R^n, pa je i sam slobodan. $\square$

Literatura

[1] Roman S., *Advanced Linear Algebra*, Third Edition, Springer , (2008)

[2] Perić V., *Algebra 1.dio –prsteni i moduli, linearna algebra* Svjetlost, Sarajevo

[3] Grulović M., *Predavanja iz Algebre 4*, Departman za matematiku i informatiku PMF Novi Sad, 2017. https://www.researchgate.net/publication/321151760_Predavanja_iz_Algebre_4

[4] Kalajdžić G, *Algebra*, Matematički fakultet, Beograd (2011)

[5] Stojaković Z., Bošnjak I., *Elementi linearne algebre*, Novi Sad (2010)

[6] Kraljević H., https://web.math.pmf.unizg.hr/~hrk/nastava/2006-07/algebra_Osijek_2006_7.pdf?fbclid=IwAR3f57fEBCGqmGNhfVTXqS0h68q2wdO-BxsQHTCYvA0Ctd7T9M16j5y-fh4, Osijek (2007)

[7] Jovović I. https://nardus.mpn.gov.rs/bitstream/handle/123456789/2841/Disertacija.pdf?sequence=4&isAllowed=y, Beograd (2013)

Biografija

Ivana Nedeljković je rođena 13.06.1993. u Ljuboviji, Republika Srbija. Osnovnu školu "Vuk Karadžić" završila je 2008. godine kao nosilac Vukove diplome. Iste godine upisala je gimnaziju "Vuk Karadžić" u Ljuboviji. Po završetku gimnazije 2012. godine upisala je Prirodno-matematički fakultet u Novom Sadu, smer Profesor matematike. U septembru 2017. godine je završila osnovne studije. U oktobru 2017. godine upisala master studije na Prirodno-matematičkom fakultetu u Novom Sadu, smer Profesor matematike, i počela da radi kao nastavnik matematike.

Ivana Nedeljković

Novi Sad, 2021.

UNIVERZITET U NOVOM SADU
PRIRODNO - MATEMATIČKI FAKULTET
KLJUČNA DOKUMENTACIJSKA INFORMACIJA

Redni broj:
RBR

Identifikacioni broj:
IBR

Tip dokumentacije: Monografska dokumentacija
TD

Tip zapisa: Tekstualni štampani materijal
TZ

Vrsta rada:Master rad
VR

Autor:Ivana Nedeljković
AU

Mentor:dr Petar Đapić, vanredni profesor
ME

Naslov rada:Naslov rada: Moduli i slobodni moduli
NR

Jezik publikacije: srpski (latinica)
JP

Jezik izvoda: srpski
JI

Zemlja publikovanja: Republika Srbija
ZP

Uže geografsko područje: Vojvodina
UGP

Godina: 2021
GO

Izdavač: Autorski reprint
IZ

Mesto i adresa: Novi Sad, Trg D. Obradovića 4
MA

Fizički opis rada: (5, 49, 4, 0, 0, 0, 0)
FO:

Naučna oblast: Matematika
NO

Naučna disciplina: Algebra
ND

Ključne reči:
PO

Čuva se: U biblioteci Departmana za matematiku i informatiku, Prirodno-matematički fakultet, Univerzitet u Novom Sadu
ČU

Važna napomena:
VN

Izvod: U ovom master radu bavili smo se proučavanjem modula. Modul predstavlja uopštenje pojma vektorskog prostora, koje se sastoji u tome da umesto polja F uzima komutativan prsten R sa jediničnim elementom. Speci-

jalno, posmatraju se slobodni moduli **IZ**

Datum prihvatanja teme od strane NN veća: 09.09.2021.
DP

Datum odbrane:
DO

Članovi komisije:
ČK

Predsednik: Dr Boris Šobot, vanredni profesor, Prirodno-matematički fakultet, Univerzitet u Novom Sadu
Mentor: dr Petar Đapić, vanredni profesor, Prirodno-matematički fakultet, Univerzitet u Novom Sadu, mentor
Član: dr Boriša Kuzeljević, docent, Prirodno-matematički fakultet, Univerzitet u Novom Sadu

UNIVERSITY OF NOVI SAD
FACULTY OF SCIENCES
KEY WORDS DOCUMENTATION

Accession number:
ANO

Identification number:
INO

Document type: Monograph type
DT

Type of record: Printed text
TR

Contents Code:
CC

Author:Ivana Nedeljković
AU

Mentor: Petar Đapić, Ph.D.
MN

Title:
TI

Language of text: Serbian (Latin)
LT

Language of abstract: s / en
LA

Country of publication: Republic of Serbia
CP

Locality of publication: Vojvodina
LP

Publication year: 2021.
PY

Publisher: Author's reprint
PU

Publication place: Novi Sad, Trg D. Obradovića 4
PP

Physical description: (5/49/4/0/0/0/0)(chapters/ pages/ quotations/ tables/ pictures/ graphics/ enclosures)
PD

Scientific field: Mathematics
SF

Scientific discipline: Algebra
SD

Subject/Key words:
SKW

Holding data: The Library of the Department of Mathematics and Informatics, Faculty of Science and Mathematics, University of Novi Sad
HD

Note:
N

Abstract: In this master thesis we dealt with the study of modules. The module represents a generalization the notion of vector space, which consists in the fact that instead of the field F takes a commutative ring R with a unit

element. Especially, free modules are observed
AB
Few words about this thesis.

Accepted by the Scientific Board on:
ASB

Defended:
DE

Thesis defend board:
DB

President: Boris Šobot, Ph.D, Associate professor, Faculty of Science, University of Novi Sad
Mentor: Petar Đapić, Ph.D, Associate professor, Faculty of Science, University of Novi Sad
Member: Boriša Kuzeljević, Ph.D, Assistant professor, Faculty of Science, University of Novi Sad