Moduli nad domenama glavnih ideala

Hrvoj, Dora

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Dora Hrvoj

MODULI NAD DOMENAMA GLAVNIH IDEALA

Diplomski rad

Voditelj rada:
Prof. dr. sc. Ozren Perše

Zagreb, veljača, 2020.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

U ovom radu bavit ćemo se algebarskim strukturama u modernoj algebri. Strukture koje će nama biti najvažnije su grupe, prsteni i moduli. Osim definiranja navedenih algebarskih struktura, proučavat ćemo i neka njihova svojstva te preslikavanja.

Poseban naglasak stavljamo na module, točnije R-module gdje je R komutativan prsten. Formalno, oni generaliziraju vektorski prostor tako da je skalarima dopušteno da budu iz prstena umjesto iz polja, možemo ih shvatiti kao generalizaciju vektorskih prostora nad poljem. U drugom dijelu rada bazirat ćemo se na slučaj kada je R domena glavnih ideala te će se tvrdnje iz prvog poglavlja generalizirati na module kao i njihovi dokazi.

U prvom poglavlju pod nazivom Grupe, prsteni i moduli uvodimo osnovne pojmove koji su nam potrebni u daljnjem dijelu rada. Nakon definicija i osnovnih teorema iz teorije grupa prelazimo na konačne Abelove grupe. Zatim predstavljamo prstene i baziramo se na komutativne prstenove. Definiramo integralnu domenu i glavne ideale pomoću kojih dolazimo do domene glavnih ideala. Osim osnovnih definicija iz teorije modula, obrađujemo i module koji imaju bazu, to jest slobodne module.

Drugi dio rada posvećen je modulima. Naglasak je stavljen na konačno generirane module čiji rezultati proizlaze iz generaliziranih tvrdnji o Abelovim grupama. Strukturne teoreme za konačne Abelove grupe ćemo generalizirati na module nad domenama glavnih ideala. Vidjet ćemo da se ne generaliziraju samo teoremi već i dokazi.

Poglavlje 1

Grupe, prsteni i moduli

1.1 Grupe

U ovom poglavlju navodimo osnovne rezultate o grupama. Tvrdnje navodimo bez dokaza jer smatramo da su poznati čitatelju.

Definicija 1. Neprazan skup $G = (G, \cdot)$, gdje je $\cdot : G \times G \to G$ binarna operacija, zove se **grupa** ako vrijede sljedeća svojstva:

i) (asocijativnost) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, za svaki $x, y, z \in G$

ii) (neutralni element) $(\exists e \in G)$ tako da $e \cdot x = x \cdot e = x$, za svaki $x \in G$

iii) (inverzni element) $(\forall x \in G)\ (\exists!\ x^{-1} \in G)\ x \cdot x^{-1} = x^{-1} \cdot x = e$

Ako G zadovoljava uvjet komutativnosti $x \cdot y = y \cdot x$, za svaki $x, y \in G$, onda je G **komutativna** ili **Abelova grupa**. Inače je G **nekomutativna** (ne-Abelova) **grupa**.

Definicija 2. Podskup H grupe G je **podgrupa** ako:

i) $1 \in H$

ii) ako je $x, y \in H$, tada je $xy \in H$

iii) ako je $x \in H$, tada je $x^{-1} \in H$

Ako je H podgrupa od G, onda pišemo $H \leq G$, ako je **prava podgrupa**, to jest $H \neq G$, tada pišemo $H < G$.

Definicija 3. Neka je G grupa i neka je $a \in G$, ako je $a^k = 1$ za neki $k \geq 1$, onda najmanji takav eksponenet k zovemo **red elementa** a, ako takav k ne postoji onda kažemo da ima **beskonačan red**.

Definicija 4. Ako je G grupa, definirajmo njezin **red** kao

$$|G| := \text{card(G)},$$

to jest red grupe je kardinalni broj skupa G. Kažemo da je grupa G **konačna grupa** ako je $|G| < \infty$, inače je G **beskonačna grupa**.

Definicija 5. Neka su G i H dvije grupe. Preslikavanje $f : G \to H$ je **homomorfizam grupa** ako "čuva strukturu", to jest ako vrijedi

$$f(xy) = f(x)f(y) \quad \forall x, y \in G.$$

Uvodimo oznaku

$$\text{Hom}(G, H) := \text{skup svih homomorfizama iz } G \text{ u } H.$$

Nadalje, homomorfizam f koji je još i injekcija naziva se **monomorfizam**, f koji je i surjekcija zovemo **epimorfizam**, a homomorfizam koji je u mono- i epi-, to jest bijektivan homomorfizam, zovemo **izomorfizam**. Za dvije grupe G i H reći ćemo da su **izomorfne** ako postoji neki izomorfizam f među njima. Tu činjenicu označavamo s

$$G \cong H.$$

Za proizvoljan homomorfizam $f : G \mapsto H$ definiramo njegovu **jezgru**

$$\text{Ker} f := \{x \in G | f(x) = e_H\}$$

i njegovu **sliku**

$$\text{Im} f := \{f(x) | x \in G\}$$

Definicija 6. Za proizvoljan podskup S neke grupe G definirajmo

$$\langle S \rangle := \bigcap_{\substack{H \leq G \\ S \subseteq H}} H.$$

To je podgrupa od G koju zovemo **grupa generirana** sa S. Kažemo da je G **konačno generirana** grupa ako postoji konačan podskup $S = \{x_1, ..., x_n\}$ takav da je $G = \langle S \rangle$, u tom slučaju pišemo i $G = \langle x_1, ..., x_n \rangle$. Grupa G je **ciklička** ako se može generirati jednim elementom, to jest, ako postoji neki $g \in G$ takav da je $G = \langle g \rangle$, svaki takav g zovemo **generator** cikličke grupe G.

Jasno je da je svaka ciklička grupa nužno komutativna.

Sada uvodimo pojam klase grupe po nekoj njezinoj podgrupi. Neka je G neka grupa i $H \leq G$ neka podgrupa. Definirajmo jednu relaciju na G ovako:

$$\forall x, y \in G, \quad x \sim y \quad \Longleftrightarrow \quad xH = yH \quad \Leftrightarrow \quad x^{-1}y \in H.$$

Pritom xH nazivamo lijeve klase od G po H i definiramo G/H s

$$G/H = \{xH : x \in G\}.$$

Teorem 1.1.1. *(Lagrange) Ako je H podgrupa konačne grupe G, onda red podgrupe H dijeli red od G, to jest $|H| \mid |G|$.*

Definicija 7. Podgrupa $N \leq G$ grupe G je **normalna podgrupa** ako vrijedi uvjet

$$xNx^{-1} = N, \quad \forall x \in G$$

Činjenicu da je podgrupa N normalna u G označavamo s

$$N \trianglelefteq G.$$

Teorem 1.1.2. *Neka je G proizvoljna grupa i N neka njezina normalna podgrupa. Tada kvocijentni skup G/N s operacijom*

$$G/N \times G/N \to G/N, \quad (xN, yN) \mapsto xyN,$$

*ima strukturu grupe, sada se G/N zove **kvocijentna grupa** od G po N. Nadalje, preslikavanje*

$$\pi = \pi_N : G \to G/N, \quad x \mapsto xN,$$

*je epimorfizam grupa s jezgrom $Ker\pi = N$,π zovemo **kanonski epimorfizam** ili **kanonska surjekcija**.*

Teorem 1.1.3. *(Prvi teorem o izomorfizmu) Neka je $f : G \to H$ proizvoljan homomorfizam grupa. Tada je $Ker\, f \trianglelefteq G$, $Im f \leq H$ i preslikavanje*

$$\bar{f} : G/Ker f \to Im f, \quad \bar{f}(gKer f) := f(g)$$

je (dobro definiran) izomorfizam grupa, to jest vrijedi

$$G/Ker f \cong Im f.$$

Teorem 1.1.4. *(Drugi teorem o izomorfizmu) Neka je G grupa, $A \leq G$ neka podgrupa i $N \trianglelefteq G$ neka normalna podgrupa. Tada je*

$$A/A \cap N \cong AN/N.$$

Teorem 1.1.5. *(Treći teorem o izomorfizmu) Neka je G grupa i neka su $M, N \trianglelefteq G$ dvije normalne podgrupe takve da je $N \leq M$. Tada je*

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

Definicija 8. Kartezijev produkt

$$\prod_{i \in I} G_i := \{f : I \to \bigcup_{i \in I} G_i \mid f(i) \in G_i\}$$

uz operaciju "množenja po komponentama"

$$(f \cdot g)\,(i) := f(i) \cdot g(i),$$

zove se **direktan produkt grupa** $\{G_i\}_I$.
Podgrupa

$$\bigoplus_{i \in I} G_i := \{f \in \prod_{i \in I} G_i \mid f(i) \neq e_i \text{ za konačno mnogo } i \in I\}$$

direktnog produkta $\prod_I G_i$, zove se **direktna suma grupa** $\{G_i\}_I$.

Konačne Abelove grupe

U ovom odjeljku navodimo osnovne rezultate o konačnim Abelovim grupama. Te ćemo rezultate u poglavlju 2. poopćiti na module nad domenama glavnih ideala. U tom poglavlju će biti prezentirani i dokazi tvrdnji.

Definicija 9. Neka je $F = \langle x_1, ..., x_n \rangle$ Abelova grupa. Ako je

$$F = \langle x_1 \rangle \oplus \cdots \oplus \langle x_n \rangle,$$

gdje je svaki $\langle x_i \rangle \cong \mathbb{Z}$, onda F zovemo **slobodna Abelova grupa** s **bazom** $x_1, ...x_n$. Generalnije, svaku grupu izomorfnu s F zovemo slobodnom Abelovom grupom.

Na primjer, $\mathbb{Z}^m = \mathbb{Z} \times \cdots \times \mathbb{Z}$ je grupa svi m-torki cijelih brojeva $(n_1, ..., n_m)$ i ona je slobodna Abelova grupa.

Definicija 10. Ako je F slobodna Abelova grupa s bazom $x_1, ..., x_n$, onda n zovemo **rang** od F i pišemo $rang(F) = n$.

Sjetimo se da je p-grupa zapravo konačna grupa G reda p^k za neki $k \geq 0$. Kada radimo u okruženju Abelovih grupa, p-grupe zovemo p-primarne grupe.

Definicija 11. Kažemo da je Abelova grupa G **p-primarna** ako je p prost broj i ako za svaki $a \in G$ postoji $n \geq 1$ tako da vrijedi $p^n a = 0$.

Ako je G Abelova grupa, onda je njezina p-**primarna komponenta**

$$G_p = \{a \in G : p^n a = 0 \text{ za neki } n \geq 1\}$$

Lako je vidjeti da je za svaki prost broj p, grupa G_P podgrupa grupe G što ne vrijedi ako grupa nije Abelova.

Teorem 1.1.6. *(Primarna dekompozicija)*

i) Svaka konačna Abelova grupa je direktna suma p-primarnih komponenata:

$$G = G_{P_1} \oplus \cdots \oplus G_{P_n}.$$

ii) Dvije konačne Abelove grupe G i G' su izomorfne ako i samo ako vrijedi $G_P \cong G'_P$ za svaki prost broj p.

Teorem 1.1.7. *(Teorem o bazi) Svaka konačna Abelova grupa G je direktna suma cikličkih grupa, čiji su redovi potencije prostih brojeva.*

Definicija 12. Ako je p prost broj i G konačna p-primarna Abelova grupa, onda

$$d(G) = \dim(G/pG).$$

Generalnije,

$$d(pG) = \dim(p^n G/p^{n+1}G).$$

Definicija 13. Neka je G konačna p-primarna Abelova grupa gdje je p prost broj. Za svaki $n \geq 0$ definiramo

$$U_P(n, G) = d(p^n G) - d(p^{n+1}G).$$

Teorem 1.1.8. *Ako je p prost, onda svake dvije dekompozicije konačnih p-primarnih Abelovih grupe G u direktnu sumu cikličkih grupa imaju isti broj cikličkih sumanada svakog tipa. Preciznije, za svaki $n \geq 0$ broj cikličkih sumanada koji imaju red p^{n+1} je $U_P(n, G)$.*

Korolar 1.1.9. *Ako su G i G' konačne p-primarne Abelove grupe, onda je $G \cong G'$ ako i samo ako $U_p(n, G) = U_P(n, G')$ za svaki $n \geq 0$.*

Definicija 14. Ako je G p-primarna Abelova grupa, onda su njezini **elementarni divizori** brojevi u nizu koji imaju $U_P(0,G)$ brojeva p, $U_P(1,G)$ brojeva p^2, ..., $U_P(t-1,G)$ brojeva p^t gdje je p^t najveći red cikličkog sumanda od G.

Ako je G konačna Abelova grupa, onda su njezini elementarni divizori zapravo elementarni divizori svih njezinih primarnih komponenti.

Teorem 1.1.10. *(Fundamentalni teorem za konačne Abelove grupe) Dvije konačne Abelove grupe G i G' su izomorfne ako i samo ako imaju iste elementarne divizore, to jest ako svake dvije dekompozicije od G i G' u direktnu sumu primarnih cikličkih grupa imaju isti broj sumanada svakog tipa.*

Propozicija 1.1.11. *Svaka konačna Abelova grupa G je direktna suma cikličkih grupa*

$$G = S(c_1) \oplus S(c_2) \oplus ... \oplus S(c_t).$$

gdje je $t \geq 1$, $S(c_i)$ je ciklička grupa reda c_i i

$$c_1 \mid c_2 \mid \cdots \mid c_t.$$

Definicija 15. Ako je G Abelova grupa, onda je njen **eksponent** najmanji pozitivni broj m za koji vrijedi $mG = \{0\}$.

Korolar 1.1.12. *Ako je G konačna Abelova grupa i $G = S(c_1) \oplus S(c_2) \oplus ... \oplus S(c_t)$, $S(c_i)$ je ciklička grupa reda c_i i vrijedi $c_1 \mid c_2 \mid \cdots \mid c_t$, onda je c_t eksponent od G.*

Definicija 16. Ako je G konačna Abelova grupa i ako

$$G = S(c_1) \oplus S(c_2) \oplus \cdots \oplus S(c_t),$$

gdje je $t \geq 1$, $S(c_j)$ ciklička grupa reda $c_j > 1$ i

$$c_1 \mid c_2 \mid \cdots \mid c_t,$$

onda se $c_1, c_2, ...c_t$ zovu **invarijantni faktori** od G.

Korolar 1.1.13. *Ako je G konačna Abelova grupa s invarijantnim faktorima $c_1, ..., c_t$ i elementarnim divizorima $\{p_i^{e_{ij}}\}$, onda vrijedi*

$$|G| = \prod_{j=1}^{t} c_j = \prod_{ij} p_i^{e_{ij}}$$

i njen eksponent je c_t.

Teorem 1.1.14. ***(Invarijantni faktori)*** *Dvije konačne Abelove grupe su izomorfne ako i samo ako imaju iste invarijantne faktore.*

1.2 Prsteni

U ovom poglavlju ponavljamo osnovne rezultate o prstenovima. Poseban naglasak stavljamo na komutativne prstene i posebno domene glavnih ideala, koje imaju važnu ulogu u radu.

Definicija 17. Prsten je uređena trojka $(R, +, \cdot)$ takva da vrijedi:

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

ii) (asocijativnost) $a(bc) = (ab)c$, za svaki $a, b, c \in R$

iii) Postoji jedinični element $1 \in R$ tako da $1a = a1 = a$ za svaki $a \in R$

iv) (distributivnost) $a(b + c) = ab + ac$, za svaki $a, b, c \in R$

Ako vrijedi i

$$ab = ba, \quad \forall a, b \in R$$

onda kažemo da je to **komutativan prsten**.

Definicija 18. Podskup S komutativnog prstena R je **potprsten** od R ako vrijedi

i) $1 \in R$

ii) Ako su $a, b \in S$, onda je $a - b \in S$

iii) Ako su $a, b \in S$, onda je $a \in S$.

Činjenicu da je S potprsten od R označavamo analogno kao i kod grupa s

$$S \leq R.$$

Teorem 1.2.1. *Ako je R integralna domena, onda postoji polje F koje sadrži R kao potprsten. Nadalje, F može biti izabran tako da za svaki $f \in F$ postoje $a, b \in R$ s $b \neq 0$ i $f = ab^{-1}$.*

Definicija 19. Polje F konstruiranog iz R uz pomoć prethodnog teorema zovemo **polje razlomaka** od R, oznaka $\mathrm{Frac}(R)$.

Definicija 20. Neka je R prsten. Ako postoje $a, b \in R$ takvi da $a \neq 0$, $b \neq 0$, $ab = 0$, onda se a i b zovu **djelitelji nule**. Prsten R nazivamo **integralna domena** ako je R komutativan prsten i ako nema djelitelja nule.

Element $\omega \in R$, gdje je R prsten, je **invertibilan** ako postoji $\omega' \in R$ takav da je

$$\omega\omega' = \omega'\omega = 1.$$

Oznaka

$$R^x := \text{grupa invertibilnih elemenata u } R.$$

Definicija 21. Prsten R je **tijelo** ili prsten s dijeljenjem ako je svaki ne-nul element u R invertibilan, to jest ukoliko je

$$R^x = R\backslash\{0\}.$$

Komutativno tijelo zove se **polje**.

Definicija 22. Neka su R i S dva prstena. Preslikavanje $f : R \to S$ je **homomorfizam prstena** ukoliko je aditivno i multiplikativno, to jest ako vrijedi

$$f(x+y) = f(x) + f(y) \quad \text{i} \quad f(xy) = f(x)f(y), \quad \forall x, y \in R$$

te ako je

$$f(1_R) = 1_S.$$

S $\mathrm{Hom}(R, S)$ označavamo skup svih homomorfizama iz R u S. Homomorfizam f koji je još i injekcija naziva se **monomorfizam**, f koji je i surjekcija zovemo **epimorfizam**, a homomorfizam koji je i mono- i epi-, to jest bijektivan homomorfizam, zovemo **izomorfizam**. Za dva prstena R i S reći ćemo da su **izomorfni** ako postoji neki izomorfizam f među njima, tu činjenicu označavamo s

$$R \cong S.$$

Definicija 23. Ako su $(R_\lambda, \lambda \in \Lambda)$ prsteni, definiramo

$$\prod_{\lambda\in\Lambda} R_\lambda := \{f : \Lambda \to \bigcup_{\Lambda} R_\lambda \mid f(\lambda) \in R_\lambda\}$$

s zbrajanjem i množenjem "po komponentama"

$$(f+g)(\lambda) := f(\lambda) + g(\lambda) \quad \text{i} \quad (f \cdot g)(\lambda) := f(\lambda) \cdot g(\lambda).$$

Tako je dobiven prsten $(\prod_{\lambda\in\Lambda} R_\lambda, +, \cdot)$, koji se zove **direktan produkt prstena** $(R_\lambda)_\Lambda$. Potprsten

$$\bigoplus_{\lambda\in\Lambda} R_\lambda := \{f \in \prod_{\lambda\in\Lambda} R_\lambda \mid f(\lambda) \neq 0_\lambda \text{ za konačno mnogo } \lambda \in \Lambda\},$$

direktnog produkta $\prod_{\lambda\in\Lambda} R_\lambda$ zovemo **direktna suma prstena** $(R_\lambda)_\Lambda$, dakle ovdje je s 0_λ označen neutral za zbrajanje u grupi $(R_\lambda, +)$.

Definicija 24. Neka je R prsten i neka je I potprsten od R. Tada je I **lijevi ideal** ako za svaki $a \in I$ i $r \in R$ vrijedi $ra \in I$, dok je **desni ideal** ako vrijedi $ar \in I$. Kažemo da je I **ideal** ako je i lijevi i desni ideal.

Činjenicu da je I ideal u prstenu R označavamo s

$$I \trianglelefteq R.$$

Uvijek postoje dva trivijalna ideala: $\{0\}$ i sam R. Za netrivijalni ideal kažemo da je **pravi ideal**.

Definicija 25. Za prsten R kažemo da je **prsten glavnih ideala** (PGI) ukoliko je svaki ideal u R glavni. Ako je R još i integralna domena, onda za njega kažemo da je **domena glavnih ideala** (DGI).

Primjer 1.2.2. *Neka je R komutativan prsten. Ako su $b_1, b_2, ...b_n \in R$, tada je skup svih linearnih kombinacija:*

$$I = \{r_1b_1 + r_2b_2 + ... + r_nb_n \mid r_i \in R \text{ za sve } i\}$$

ideal u R. U tom slučaju pišemo $I = (b_1, b_2, ..., b_n)$, a I zovemo ideal generiran s $b_1, b_2, ..., b_n$. Ako je $n = 1$, tada je:

$$I = (b) = \{rb \mid r \in R\}$$

ideal u R, (b) sadrži sve višekratnike od b i zove se glavni ideal generiran s b.

Definicija 26. Neka je R prsten i $I \trianglelefteq R$ neki ideal. Skup $S \subseteq R$ je **skup generatora** od I ako je

$$I = \langle S \rangle = (S) := \bigcap_{\substack{J \trianglelefteq R \\ S \subseteq J}} J,$$

to jest I je najmanji ideal u R koji sadrži skup S. Ideal I je konačno generiran ako postoji konačan podskup $S \subseteq R$ takav da $I = \langle S \rangle$. Ideal I je **glavni ideal** ako postoji neki element $r \in R$ takav da je $I = \langle r \rangle$.

Teorem 1.2.3. *Neka je R prsten i $I \trianglelefteq R$ bilo koji ideal. Ako na kvocijentnoj, aditivnoj grupi R/I definiramo množenje iz $R/I \times R/I$ u R/I s*

$$(x + I)(y + i) := xy + I, \quad x, y \in R,$$

*onda R/I ima strukturu prstena te se zove **kvocijentni prsten** od R po I. Nadalje, preslikavanje*

$$\pi = \pi_I : R \to R/I, \quad x \mapsto x + I$$

*je epimorfizam prstena i zove se **kanonski epimorfizam** ili **kanonska surjekcija**.*

Teorem 1.2.4. *(Prvi teorem o izomorfizmu) Neka je $f : R \to S$ proizvoljan homomorfizam prstena. Tada je $Ker\ f \trianglelefteq R$ ideal, $Im\ f \leq S$ je potprsten, a preslikavanje*

$$\bar{f} : R/Ker\ f \to Im\ f, \qquad \bar{f}(r + Ker\ f) := f(r)$$

je (dobro definiran) izomorfizam prstena, to jest vrijedi

$$R/Ker\ f \cong Im\ f.$$

Teorem 1.2.5. *(Drugi teorem o izomorfizmu) Neka je R prsten, $S \leq R$ neki potprsten i $I \trianglelefteq R$ neki ideal. Tada je $S + I \leq R$ potprsten i $S \cap I \trianglelefteq S$ ideal. Nadalje, vrijedi*

$$S/(S \cap I) \cong (S + I)/I.$$

Teorem 1.2.6. *(Treći teorem o izomorfizmu) Neka je R prsten te neka su $I, J \trianglelefteq R$ ideali takvi da je $I \subseteq J$. Tada je $J/I \trianglelefteq R/I$ ideal i vrijedi*

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

Komutativni prsteni

Definicija 27. Neka su a i b elementi iz komutativnog prstena R. Tada a **dijeli** b u R ako postoji element $c \in R$ tako da vrijedi $b = ca$. Oznaka $a \mid b$.

Definicija 28. Elementi a i b u prstenu R su **asocirani** ako postoji invertibilni element $u \in R$ tako da $b = ua$.

Definicija 29. Element integralne domene je **ireducibilan** ako nije nula niti invertibilan i ako ne može biti prikazan kao produkt dva neinvertibilna elementa.

Definicija 30. Ideal I u komutativnom prstenu R je **prost ideal** ako je pravi ideal, to jest $I \neq R$ te ako $ab \in I$ povlači $a \in I$ ili $b \in I$.

Definicija 31. Element p za kojeg je (p) ne-nul prost ideal se često naziva **prost element**. Takvi elementi imaju svojstvo da $p \mid ab$ povlači $p \mid a$ ili $p \mid b$.

Definicija 32. Integralna domena R je **domena jedinstvene faktorizacije** ako:

i) Svaki $r \in R$ koji je različit od nule i nije invertibilan, je produkt ireducibilnih elementa.

ii) Ako je $up_1 \cdots p_m = vq_1 \cdots q_n$ gdje su u i v invertibilni elementi, a svi p_i i q_i ireducibilni, onda je $m = n$ i postoji permutacija $\sigma \in S_n$ za koju su p_i i $q_{\sigma(i)}$ asocirani za svaki i.

Korolar 1.2.7. *Ako je R domena glavnih ideala i $p \in R$ je ireducibilan, onda je (p) prost ideal.*

Propozicija 1.2.8. *Neka je R integralna domena u kojoj je svaki $r \in R$ različit od nule i nije invertibilan element, produkt ireducibilnih (elemenata). Nadalje, R je domena jedinstvene faktorizacije ako i samo ako je p prost ideal u R za svaki ireducibilni element $p \in R$.*

Teorem 1.2.9. *Ako je R domena glavnih ideala onda je R domena jedinstvene faktorizacije.*

Definicija 33. Ideal I u komutativnom prstenu R je **maksimalan ideal** ako je pravi ideal te ne postoji ideal J za kojeg vrijedi $I \subsetneq J \subsetneq R$.

Definicija 34. Neka je R komutativni prsten. Označimo s $R[X]$ skup svih funkcija f : $\mathbb{Z}^+ \to R$ takvih da je $f(n) = 0$ za sve osim za konačno mnogo nenegativnih brojeva n. Strukturu na skupu $R[X]$ zajedno s operacijama:

$$(f + g)(n) = f(n) + g(n)$$
$$(fg)(n) = \sum_{m=0}^{n} f(m)g(n - m)$$

zovemo **prsten polinoma** u X s koeficijentima iz R.

Prisjetimo se da je neki polinom p ireducibilan ako se ne može napisati kao produkt p_1p_2 dvaju polinoma p_1 i p_2 koji su svaki stupnja barem 1.

Propozicija 1.2.10. *Pravi ideal I u ne-nul komutativnom prstenu R je maksimalan ideal ako i samo ako je R/I polje.*

Korolar 1.2.11. *Svaki maksimalan ideal I u komutativnom prstenu R je prost ideal.*

Teorem 1.2.12. *Ako je R domena glavnih ideala, onda je svaki prosti ideal koji je različit od nule zapravo maksimalan ideal.*

1.3 Moduli

Sada predstavljamo R-module gdje je R komutativan prsten. Formalno, oni generaliziraju vektorski prostor tako da je skalarima dopušteno da su iz prstena umjesto iz polja. Ako je R domena glavnih ideala onda se u sljedećem poglavlju može vidjeti da klasifikacija konačno generiranih R-modula istovremeno daje klasifikaciju svih konačno generiranih Abelovih grupa.

Definicija 35. Neka je R komutativan prsten. Tada je **R-modul** aditivna Abelova grupa M s množenjem skalarom $R \times M \to M$, definiranim s

$$(r, m) \mapsto rm,$$

ako za $m, m' \in M$ i $r, r', 1 \in R$ vrijede sljedeće tvrdnje

i) $r(m + m') = rm + rm'$

ii) $(r + r')m = rm + r'm$

iii) $(rr')m = r(r'm)$

iv) $1m = m$.

Napomena 1.3.1. *Ova definicija također ima smisla za nekomutativne prstenove R te se tada M zove lijevi R-modul.*

Primjer 1.3.2.

i) Svaki vektorski prostor nad poljem k je k-modul.

ii) Svaka Abelova grupa je $\mathbb{Z}$-modul.

iii) Svaki komutativan prsten R je modul nad samim sobom ako definiramo množenje skalarom s $R \times R \to R$. Dakle, svaki ideal I u R je R-modul zbog

$$i \in I, r \in R \Rightarrow ri \in R$$

iv) Ako je S potprsten komutativnog prstena R, onda je R S-modul s skalarnim množenjem $S \times R \to R$ $(s, r) \to sr$. Dakle, ako je k komutativni prsten, onda je $k[x]$ k-modul.

Definicija 36. Neka je R prsten i M, N R-moduli. Funkcija $f : M \to N$ je **R-homomorfizam** ako za svaki $m, m' \in M$ i za svaki $r \in R$ vrijedi:

i) $f(m + m') = f(m) + f(m')$

ii) $f(rm) = rf(m)$

Ako je R-homomorfizam bijekcija, onda se zove **R-izomorfizam**. Kažemo da su R-moduli M i N su **izomorfni**, to jest $M \cong N$ ako postoji R-izmorfizam $f : M \to N$. Kompozicija R-homomorfizama je R-homomorfizam, a ako je f R-izomorfizam onda je inverzna funkcija f^{-1} također R-izmorfizam.

Primjer 1.3.3.

i) Ako je R polje, onda je R-modul vektorski prostor i R-homomorfizam je linearna transformacija.

ii) $\mathbb{Z}$-moduli su Abelove grupe. Svaki homomorfizam Abelove grupe je $\mathbb{Z}$-homomorfizam.

Definicija 37. Neka su M, N R-moduli, onda je

$$\mathrm{Hom}_R\,(M, N) = \{\text{Svi R-homomorfizmi s } M \text{ u } N\}.$$

Ako su $f, g \in \mathrm{Hom}_R\,(M, N)$, onda definiramo $f + g : M \to N$ s

$$f + g : m \mapsto f(m) + g(m).$$

Propozicija 1.3.4. *Neka su M, N R-moduli i R je komutativan prsten. Onda je* $\mathrm{Hom}_R(M, N)$ *R-modul gdje vrijedi gore navedeno zbrajanje i množenje skalarom koje je definirano s*

$$rf : m \to (rm).$$

Nadalje, ako je

$$p : M' \to M \quad i \quad q : N \to N'$$

tada vrijedi

$$(f + g)p = fp + qp \quad i \quad q(f + g) = qf + qg$$

za sve $f, g \in \mathrm{Hom}_R(M, N)$.

Definicija 38. Neka je M R-modul. Tada je **podmodul** N od M, označen s $N \subseteq M$, aditivna podgrupa N od M zatvorena na množenje skalarom $rn \in N$ kada je $n \in N, r \in R$.

Ako je R polje, onda N nazivamo vektorski potprostor od M. Drugim riječima, podmodul je Abelova podgrupa od M koja je zatvorena na množenje skalarom.

Primjer 1.3.5.

1.) $\{0\}, M$ *su podmoduli od M. Pravi podmodul od M je podmodul $N \subseteq M, N \neq M$.*

2.) Ako je komutativan prsten R prikazan kao modul nad samim sobom, onda je podmodul od R ideal, a I je pravi podmodul kada je I pravi ideal.

3.) Podmodul od $\mathbb{Z}$-modula je podgrupa, dok je podmodul vektorskog prostora je potprostor.

4.) Ako je M R-modul i $r \in R$, onda je

$$rm = \{rM : m \in M\}$$

podmodul od M. Neka je J ideal u R te je M je R-modul, onda je

$$JM = \{\sum j_i m_i : j : i \in J, m_i \in M\}$$

je podmodul od M.

5.) Ako su S i T podmoduli modula M. tada je

$$S + T = \{s + t : s \in S, t \in T\}$$

podmodul od M koji sadrži S i T.

6.) Ako je $\{s_i : i \in I\}$ familija podmodula modula M, onda je $\bigcap_{i\in I} S_i$ podmodul od M.

*7.) M je R-modul, $m \in M$. **Ciklički podmodul generiran s m** definiramo ovako*

$$\langle m\rangle = \langle rm : r \in R\rangle,$$

generalnije ako je X podskup od R-modula M, onda je

$$\langle X\rangle = \{\sum_{i=1}^{n} r_i x_i : r_i \in R_i, x_i \in X\}.$$

*Tada je $\langle X\rangle$ skup svih R-linearnih kombinacija elemenata u X, to jest zovemo ga **podmodul generiran s X**.*

Definicija 39. Konačno generiran modul M je modul generiran konačnim skupom to jest $M = \langle X\rangle$ gdje je $X = \{x_1, x_2, ..., x_n\}$ konačan skup.

Vektorski prostor je konačno generiran ako i samo ako mu je dimenzija konačna. Nastavljamo proširivati definicije od Abelovih grupa i vektorskih prostora na module.

Definicija 40. Ako je $f : M \to N$ R-homomorfizam između R-modula onda:

$$\textbf{kernel} f = \ker f = \{m \in M : f(m) = 0\}$$

$$\textbf{image} f = \mathrm{im} f = \{n \in M : \exists m \in M \text{ tako da } n = f(m)\}.$$

Definicija 41. Ako je N podmodul R-modula, onda je **kvocijentni modul** kvocijentna grupa M/N (M je Abelova grupa te je N podgrupa) definirana množenjem skalara

$$r(m + N) = rm + N.$$

Kanonsko preslikavanje $\pi : M \to M/N$ dano s $m \mapsto m + N$ je R-homomorfizam.

Množenje skalarom u definiciji kvocijentnog modula je dobro definirano ako je $m+N = m' + N$ onda je $m - m' \in N$, iz toga slijedi $r(m - m') \in N$ (jer je N podmodul) te je $rm - rm' \in N$ i $rm + N = rm' + N$.

Teorem 1.3.6. *(Prvi teorem o izmorfizmu modula) Neka su M i N R-moduli te neka je $f : M \to N$ homomorfizam R-modula. Tada je*

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

Ostali teoremi o izomorfizmu su posljedica prvog teorema o izomorfizmu.

Teorem 1.3.7. *(Drugi teorem o izmorfizmu modula) Neka je M R modul i neka su S i T podmoduli. Tada postoji izomorfizam R-modula*

$$(S + T)/T \cong S/(S \cap T)$$

Teorem 1.3.8. *(Treći teorem o izmorfizmu modula) Neka je M R-modul i neka su T i S podmoduli od M tako da $T \subseteq S$.Tada je*

$$M/S \cong (M/T)/S/T)$$

Propozicija 1.3.9. *R-modul M je ciklički ako i samo ako je $M \cong R/I$ za neki ideal I.*

Definicija 42. Modul M je **prost ili ireducibilan** ako

i) $M \neq \{0\}$

ii) M nema pravih podmodula različitih od 0, to jest jedini podmoduli od M su: M i $\{0\}$

Korolar 1.3.10. *R-modul M je ireducibilan ako i samo ako vrijedi da je $M \cong R/I$ gdje je I maksimalan ideal.*

Egzistencija maksimalnog ideala garantira egzistenciju ireducibilnog modula. Pojam direktne sume spomenute za vektorske prostore i za Abelove grupe, proširuje se na module. Sjetimo se da je Abelova grupa unutarnja direktna suma podgrupa S i T ako

$$S + T = G \quad i \quad S \cap T = \{0\}$$

dok je vanjska direktna suma Abelova grupa čiji je osnovni skup kartezijev produkt $S \times T$ i čija je binarna operacija zbrajanje po kordinatama. Obje verzije daju izomorfnu Abelovu grupu. Unutarnje-vanjsko stajalište stoji za module.

Definicija 43. Neka su S, T R-moduli gdje je R komutativan prsten. Onda je njihova **direktna suma**, oznaka $S \sqcup T$, kartezijev produkt $S \times T$ s operacijama definiranim po kordinatama

$$(s,t) + (s' + t') = (s + s') + (t + t')$$

$$r(s,t) = (rs, rt)$$

gdje su $s, s' \in S, t, t' \in T, r \in R$.

Propozicija 1.3.11. *Sljedeće tvrdnje su ekvivalentne za R-module M, S i T.*

i) $S \sqcup T \cong M$

ii) Postoji injektivan R-homomorfizam $i : S \to M$, $j : T \to M$ tako da vrijedi:

$$M = \mathrm{Im}i + \mathrm{Im}j,$$

$$\mathrm{Im}i \cap \mathrm{Im}j = \{0\}$$

iii) Postoji R-homomorfizam $i : S \to M$, $j : T \to M$ tako da $\forall m \in M \; \exists!\; s \in S$ i $t \in T$ tako da je

$$m = is + jt$$

vi) Neka su R-homomorfizmi $i : s \to M, j : T \to M, p : M \to S, q : M \to T$ tako da je

$$pi = 1_S, qj = 1_T, pj = 0, qi = 0, ip + jq = 1_M.$$

Napomena 1.3.12. *Unutarnja direktna suma je vjerojatno najvažniji primjer modula izmorfnog direktnoj sumi.*

Definicija 44. Neka su S, T podmoduli modula M. Onda je M njihova **unutarnja direktna suma** ako

$$M \cong S \sqcup T, \qquad i : s \to M, j : T \to M.$$

Oznaka $S \oplus T$.

U ovom poglavlju ćemo vanjsku sumu označavati s $S \sqcup T$, a unutarnju ćemo označiti sa $S \oplus T$. Inače se obje sume označavaju sa $S \oplus T$.

Korolar 1.3.13. *Sljedeći uvjeti su ekvivalentni za R-modul M s podmodulima S i T.*

1.) $M = S \oplus T$

2.) $S + T = M \quad i \quad S \cap T = \{0\}$

3.) Za svaki $m \in M$ postoji jedinstven izraz $m = s + z$ gdje je $s \in S$, $t \in T$.

Definicija 45. Podmodul S modula M je **direktni sumand** od M ako postoji podmodul T od M tako da $M = S \oplus T$.

Sljedeća posljedica će povezati direktne sumande s specijalnom vrstom homomorfizma.

Korolar 1.3.14. *Ako $M = S \oplus T$ i $S \subseteq A \subseteq M$, onda $A = S \oplus (A \cap T)$.*

Konstrukcija direktne sume može biti proširena na konačno mnogo podmodula. Postoji unutarnja i vanjska verzija.

Definicija 46. Neka su $S_1, S_2, ..., S_n$ R-moduli. Definirajmo **vanjsku direktnu sumu** $S_1 \sqcup \cdots \sqcup S_n$ kao R-modul čiji je osnovni skup kartezijev produkt $S_1 \times ...S_n$ i čije su operacije:

$$(s_1, ..., s_n) + (s_1+, ..., s_n') = (s_1 + s_1', ..., s_n + s_n')$$

$$r(s_1, ..., s_n) = (rs_1, ..., rs_n)$$

Neka je M modul, a $S_1, ...S_m$ su podmoduli od M. Za M kažemo da je **unutarnja direktna suma**

$$M = S_1 \oplus ... \oplus S_n$$

ako za svaki $m \in M$ postoji jedinstven izraz oblika $m = s_1 + ... + s_n$ gdje je $s_i \in S_i$ za svaki $i = 1, 2, ..., n$. Unutarnja i vanjska verzija su izomorfne.

Propozicija 1.3.15. *Neka je $\{S_i : i \in I\}$ familija podmodula R-modula M gdje je R komutativan prsten. Ako je $M = \langle \cup_{i \in I} S_i \rangle$, onda su sljedeći uvjeti ekvivalentni.*

i) $M = \sum_{i \in I} S_i$

ii) Svaki $a \in M$ ima jedinstven izraz oblika $a = s_{i_1} + ... + s_{i_n}$, gdje je $s_{i_j} \in S_{i_j}$

iii) Za svaki $i \in I$, vrijedi

$$S_i \cap \left\langle \bigcup_{i \neq j} S_J \right\rangle = \{0\}.$$

Propozicija 1.3.16. *$M = S_1 + ... + S_n$. S_i su podmoduli tako da za svaki $m \in M$ postoji izraz oblika $m = s_1 + ... + s_n$, gdje je $s_i \in S_i$, $\forall i$. Zatim, vrijedi da je $M = S_1 \oplus ... \oplus S_n$ ako i samo ako $S_i \cap \langle S_1 + ... + \hat{S}_i + ...S_n \rangle = \{0\}$ za svaki i gdje $\hat{S}_i$ znači da je S_i izbačen iz sume.*

Propozicija 1.3.17. *Ako je R domena glavnih ideala i M R-modul koji može biti generiran s n elemenata, onda svaki podmodul od M može biti generiran s n ili manje elemenata.*

Definicija 47. Neka je F R-modul. F je **slobodan R-modul** ako je F izomorfan direktnoj sumi kopija od R, to jest

$$F = \sum_{i \in I} R_i,$$

gdje je $R_i = \langle b_i \rangle$ za svaki i. Tada $B = \{b_i \ : \ i \in I\}$ zovemo **bazom** od F.

Propozicija 1.3.18. *Neka je A podmodul modula B. Ako je B/A slobodan, onda postoji podmodul C od B tako da $C \cong B/A$ i $B = A \oplus C$.*

Poglavlje 2

Moduli nad domenama glavnih ideala

Strukturne teoreme za konačne Abelove grupe ćemo generalizirati na module nad domenama glavnih ideala. Ne samo da se generaliziraju teoremi, već se generaliziraju i dokazi.

Definicija 48. Neka je R komutativan prsten i M R-modul. Ako je $m \in M$ onda je **anihilator** od m

$$\text{ann}(m) = \{r \in R : rm = 0\}.$$

Kažemo da m ima **konačan red** (ili da je torzijski element) ako vrijedi $\text{ann}(m) \neq \{0\}$, dok u drugom slučaju kažemo da m ima **beskonačan red**.

Kada je komutativni prsten R definiran kao modul nad samim sobom, njegova jedinica ima beskonačan red jer je $\text{ann}(1) = \{0\}$.

Anihilator generalizira pojam reda elemenata. Podsjetimo se da kada je G aditivna Abelova grupa, onda element $g \in G$ ima konačan red ako je $ng = 0$ za neki pozitivan broj n, dok g ima konačan red d ako je d najmanji pozitivni broj za koji vrijedi $dg = 0$. S druge strane, $\text{ann}(g)$ je ideal u $\mathbb{Z}$ i kao svaki drugi ideal u $\mathbb{Z}$ koji je različit od nule on je generiran najmanjim pozitivnim cijelim brojem u njemu. Tada je anihilator $\text{ann}(g) = \langle d \rangle$ glavni ideal generiran redom d od g. U propoziciji 1.3.9 smo pokazali da ako je $M = \langle m \rangle$ ciklički R-modul, gdje je R neki komutativan prsten, onda je $M \cong R/I$. Ideal I je u ovoj posljedici $Ker\varphi$, gdje je $\varphi : R \to M$ homomorfizam $r \mapsto rm$, takav da $I = \text{ann}(m)$ i vrijedi

$$\langle m \rangle \cong R/\text{ann}(m).$$

Definicija 49. Neka je M R-modul gdje je R integralna domena. **Torzijski podmodul** tM od M definiran s

$$tM = \{m \in M : \text{ m ima konačan red}\}.$$

Propozicija 2.0.1. *Neka je R integralna domena i neka je M R-modul. Tada je tM podmodul od M.*

Dokaz. Ako su $m, m' \in tM$, onda postoje $r, r' \in R$ koji su različiti od 0 i za njih vrijedi $rm = 0$ i $r'm' = 0$. Očito je $rr'(m + m') = 0$. Kako je R integralna domena onda je $rr' \neq 0$ i $\text{ann}(m + m') \neq \{0\}$ te je $m + m' \in tM$.

Ako je $r \in R$, onda je $sm \in tM$, za $r \in \text{ann}(sm)$ zbog $rsm = 0$. □

Ova propozicija ne vrijedi ako R nije integralna domena.

Definicija 50. Ako je R integralna domena i M R-modul, onda je M **torzijski modul** ako vrijedi $tM = M$, dok je M **torzijski slobodan** ako vrijedi $tM = \{0\}$.

Propozicija 2.0.2. *Neka su M i M' R-moduli gdje je R integralna domena.*

i) M/tM je torzijski slobodan

ii) Ako je $M \cong M'$, onda je $tM \cong tM'$ i $M/tM \cong M'/tM'$.

Dokaz. i) Pretpostavimo da je $m + tM \neq 0$ u M/tM, to jest m ima beskonačan red. Ako $m + tM$ ima konačan red, onda imamo $r \in R$, $r \neq 0$, tako da $0 = r(m + tM) = rm + tM$ te je tada $rm \in tM$. Stoga postoji $s \in R$ tako da $s \neq 0$ i $0 = s(rm) = (sr)m$. Ali $sr \neq 0$, budući da je R integralna domena pa je $\text{ann}(m) \neq \{0\}$. Dolazimo do kontradikcije s činjenicom da m ima beskonačan red.
ii) Ako je $\varphi : M \to M'$ izomorfizam, onda je $\varphi(tM) \subseteq tM'$, jer ako je $rm = 0$ i $r \neq 0$ imamo $r\varphi(m) = \varphi(rm) = 0$, što vrijedi za svaki R-homomorfizam. Stoga je $\varphi|tM : tM \to tM'$ izomorfizam (s inverzom $\varphi^{-1}|tM'$). Za drugu činjenicu, lako je vidjeti da je homomorfizam $\overline{\varphi} : M/tM \to M'/tM'$ definiran s $\overline{\varphi} : m + tM \mapsto \varphi(m) + tM'$ izomorfizam. □

Teorem 2.0.3. *Ako je R domena glavnih ideala, onda je svaki konačno generiran, torzijski slobodan R-modul M zapravo slobodan.*

Dokaz. Dokazujemo teorem indukcijom po n, gdje je $M = \langle v_1, ..., v_n \rangle$.

Ako je $n = 1$, onda je M ciklički, stoga je $M = \langle v_1 \rangle \cong R/\text{ann}(v_1)$. Budući da je M torzijski slobodan, onda je $\text{ann}(v_1) = \{0\}$, pa je $M \cong R$ i stoga je M slobodan.

Za korak indukcije, neka je $M = \langle v_1, ..., v_n \rangle$ i definiramo

$$S = \{m \in M : r \in R, r \neq 0, \text{ tako da je } rm \in \langle v_{n+1} \rangle\}.$$

lako je provjeriti da je S podmodul od M. Sada je M/S torzijski slobodan: ako $x \in M$, $x \notin S$ i $r(x + S) = 0$, onda je $rx \in S$, stoga postoji $r' \in R$ tako da $r' \neq 0$ i $rr' \in \langle v_{n+1} \rangle$. Budući da $rr' \neq 0$, imamo kontradikciju, $x \in S$. Jednostavno, M/S može biti generiran s n elemenata, $v_1 + S, ..., v_n + S$, pa je onda M/S slobodan po pretpostavci indukcije. Sada nam propozicija 1.3.18 kaže

$$M \cong S \oplus (M/S).$$

Stoga će dokaz biti gotov kada pokažemo $S \cong R$.

Ako je $x \in S$, onda postoji $r \in R$, $r \neq 0$ tako da $rx \in \langle v_{n+1} \rangle$. Zapravo, postoji $a \in R$ tako da $rx = av_{n+1}$. Definiramo $\varphi : S \to Q$ =Frac(R), polje razlomaka od R s $\varphi : x \to a/r$. Zaključujemo da je φ dobro definiran injektivan R-homomorfizam. Ako je $D = \text{Im}\,\varphi$, onda je D konačno generiran podmodul od Q.

Dokaz će biti gotov ako možemo dokazati da je svaki konačno generiran podmodul D od Q ciklički. Sada vrijedi

$$D = \langle b_1/c_1, ..., b_m/c_m \rangle,$$

gdje je $b_i, c_i \in R$. Neka je $c = \prod_i c_i$ i definirajmo $f : D \to R$, s $f : d \to cd$ za svaki $d \in D$. Budući da je D torzijski slobodan, f je injektivan R-homomorfizam pa je D izomorfan s podmodulom od R, stoga je D izomorfan podmodulu od R. Budući da je R domena glavnih ideala, onda je svaki ideal u R koji je različit od 0, izomorfan s R. Stoga vrijedi $S \cong \text{Im}\varphi = D \cong R$. □

Korolar 2.0.4. *Ako je R domena glavnih ideala onda je svaki podmodul S, od konačno generiranog slobodnog R-modula, sam po sebi slobodan i vrijedi $dim(S) \leq dim(F)$.*

Dokaz. Po propoziciju 1.3.17 podmodul S može biti generiran s n ili manje elemenata, gdje je n =dim(F). Kako je F torzijski slobodan, stoga je i S torzijski slobodan. Sada nam iz teorema 2.0.3 slijedi da je S slobodan. □

Korolar 2.0.5.

i) Ako je R domena glavnih ideala, onda je svaki konačno generirani R-modul M direktna suma

$$M = tM \oplus F$$

gdje je F konačno generiran slobodan R-modul.

ii) Ako su M i M' konačno generirani R-moduli , gdje je R domena glavnih ideala, onda je $M \cong M'$ ako i samo ako $tM \cong tM'$ i $rang(M/tM) = rang(M'/tM')$.

Dokaz. i) Kvocijentni modul M/tM je konačno generiran jer je M konačno generiran, također je i torzijski slobodan po propoziciji 2.0.2 i). Stoga je M/tM slobodan po teoremu 2.0.3. Konačno, po propozicija 1.3.18 slijedi $M \cong tM \oplus (M/tM)$.

ii) Po propoziciji 2.0.2 ii), ako je $M \cong M'$, onda je $tM \cong tM'$ i $M/tM \cong M'/tM'$. Budući da je M/tM je konačno generiran i torzijski slobodan, onda je i slobodan modul kao što je i M'/tM'. Oni su izomorfni ako su istog ranga.

Obratno budući da su sume $M \cong tM \oplus (M/tM)$ i $M' \cong tM' \oplus (M'/tM')$ direktne, izomorfizmi sumanada induciraju izomorfizam $M \to M'$. □

Propozicija 2.0.6. *Ako je R domena glavnih ideala, onda je svaki podmodul H od konačno generiranog slobodnog R-modula F sam po sebi slobodan i vrijedi $dim(H) \leq dim\,(F)$.*

Dokaz. Dokazujemo indukcijom po n =dim(F). Ako je $n = 1$, onda $F \cong R$. Stoga je H izomorfan idealu u R, ali svi ideali su glavni pa slijedi da su izomorfni s $\{0\}$ ili s R. Znači H je slobodan modul dim ≤ 1.

Sada ćemo dokazati korak indukcije. Ako je $\{x_1, ..., x_{n+1}\}$ baza od F, definiramo $F' = \langle x_1, ...x_n\rangle$ i $H' = H \cap F'$. Po indukciji, H' je slobodan modul dimenzije $\leq n$. Sada vrijedi

$$H/H' = H/(H \cap F') \cong (H + F')/F' \subseteq F/F' \cong R.$$

Po bazi indukcije znamo da je $H/H' = \{0\}$ ili $H/H' \cong R$. U prvom slučaju je $H = H'$ i gotovi smo. U drugom slučaju propozicija 1.3.18 daje $H = H' \oplus \langle h\rangle$ za neki $h \in H$, gdje je $\langle h\rangle \cong R$ te slijedi da je H slobodan dimenzije $\leq n + 1$.

□

Sada izbacujemo pretpostavku o konačnosti.

Teorem 2.0.7. *Ako je R domena glavnih ideala, onda je svaki podmodul H slobodnog R-modula F je sam po sebi slobodan i* dim(H) $\leq$ dim(F).

Dokaz. Koristit ćemo činjenicu ekvivalentnu aksiomu izboru i Zornovoj lemi, koja nam govori da se svaki skup može dobro urediti.

Posebno, možemo pretpostaviti da je $\{x_k : k \in K\}$ baza od F koja ima dobro uređen skup indeksa K.

Za svaki $k \in K$ definiramo

$$F'_k = \langle x_j : j \prec k\rangle \quad i \quad F_k = \langle x_j : j \preceq k\rangle = F'_k \oplus \langle x_k\rangle$$

i vrijedi $F = \cup_k F_k$. Definirajmo

$$H'_k = H \cap F'_k \quad i \quad H_k = H \cap F_k.$$

Sada imamo $H'_k = H \cap F'_k = H_k \cap F'_k$, pa je

$$H_k/H'_k = H_k/(H_k \cap F'_k)$$

$$\cong (H_k + F'_k)/F'_k \subseteq F_k/F'_k \cong R.$$

Po propoziciji 1.3.18, vrijedi $H_k = H'_k$ ili $H_k = H'_k \oplus \langle h_k\rangle$ gdje je $h_k \in H_k \subseteq H$ i $\langle h_k\rangle \cong R$. Tvrdimo da je H slobodan R-modul koji za bazu ima skup svih h_k. Iz toga slijedi da je $rang(H) \leq rang(K)$.

Budući da je $F = \cup F_k$, svaki $f \in F$ leži u jednom od F_k. Budući da je K dobro uređen, onda postoji najmanji indeks $k \in K$ tako da $f \in F_k$. Taj najmanji indeks označavamo s $\mu(f)$. Posebno, ako je $h \in H$, onda

$$\mu(h) = \text{najmanji indeks } k \text{ tako da } h \in F_k.$$

Imajmo na umu da ako je $h \in H'_k \subseteq F'_k$, onda $\mu(h) \prec k$. Neka je H^* podmodul od H generiranog sa svim h_k.

Pretpostavimo da je H^* pravi podmodul od H. Neka je j najmanji indeks u

$$\{\mu(h) : h \in H \text{ i } h \notin H^*\}$$

i odaberemo $h' \in H$ da bude takav element s indeksom j, to jest $h' \notin H^*$ i $\mu(h') = j$. Sada je $h' \in H \cap F_j$ zbog $\mu(h') = j$ i također

$$h' = a + rh_j, \text{ gdje je } a \in H'_j \text{ i } r \in R.$$

Stoga, $a = h' - rh_j \in H'_j$ i $a \notin H^*$, jer bi inače bilo $h' \in H^*$ (zbog $h_j \in H^*$). Budući da je $\mu(a) \prec j$ dolazimo do kontradikcije s činjenicom da je j najmanji indeks elemenata H koji nisu u H^*. Zaključili smo $H^* = H$, to jest svaki $h \in H$ je linearna kombinacija elemenata h_k.

Preostaje nam dokazati da je prikaz svakog $h \in H$ kao linearne kombinacije elemenata h_k jedinstven. Oduzimanjem takva dva izraza vidimo da je dovoljno pokazati da ako vrijedi

$$0 = r_1 h_{k_1} + r_2 h_{k_2} + \cdots + r_n h_{k_n},$$

onda su svi koeficijenti $r_i = 0$. Uzmimo da je $k_1 \prec k_2 \prec \cdots \prec k_n$. Ako je $r_n \neq 0$, onda je $r_n h_{k_n} \in \langle h_{k_n} \rangle \cap H'_{k_n} = \{0\}$, pa dolazimo do kontradikcije. Stoga su svi $r_i = 0$ pa je H slobodan modul s bazom $\{h_k : k \in K\}$.

□

Sada se vraćamo na diskusiju konačno generiranih modula. U svijetlu propozicije 2.0.2 ii), problem klasifikacije konačno generiranih R-modula, gdje je R domena glavnih ideala, reducira se na klasifikaciju konačno generaliziranih torzijskih modula. Dakle, ovi moduli su generlizacija konačnih Abelovih grupa.

Propozicija 2.0.8. *Abelova grupa G je konačna ako i samo ako je konačno generiran torzijski $\mathbb{Z}$ -modul.*

Dokaz. Ako je G konačna onda je konačno generirana, nadalje Lagrangov teorem nam govori da je G torzijska. Da bi dokazali obrat, pretpostavimo da je $G = \langle x_1, ..., x_n \rangle$ s pozitivnim cijelim brojevima d_i za koje vrijedi $d_i x_i = 0$ za sve i. Slijedi da svaki $g \in G$ može biti zapisan kao

$$g = m_1 x_1 + \cdots + m_n x_n,$$

gdje je $0 \leq m_i < d_i$ za svaki i. Stoga, $|G| \leq \prod_i d_i$ pa je G konačna. □

karanfil

Definicija 51. Neka je R domena glavnih ideala i neka je M R-modul. Ako je $P = (p)$ prost ideal u R različit od 0, onda je M (p)-**primaran** ako za svaki $m \in M$, postoji $n \geq 1$ tako da $p^n m = 0$.

Ako je M R-modul, onda je njegova (p)-**primarna komponenta**:

$$M_P = \{m \in M \ : \ p^n m = 0 \text{ za neki } n \geq 1\}.$$

Ako ne želimo specificirati p, možemo pisati da je modul primaran umjesto (p)-primaran. Očito je da su primarne komponente zapravo podmoduli. Teoremi koji slijede su iskazani u poglavlju 1 za Abelove grupe. Sada dokazujemo njihove generalizacije na module nad prstenima glavnih ideala.

Teorem 2.0.9. ***(Primarna dekompozicija)***

i) Svaka torzijska Abelova grupa G je direktna suma p-primarnih komponenata

$$G = \sum_p G_p.$$

ii) Svaki torzijski R-modul M, gdje je R domena glavnih ideala, je direktna suma p-primarnih komponenata

$$M = \sum_P M_P.$$

Dokaz. i) Neka je $x \in G$, tako da $x \neq 0$ i neka mu je red d. Po fundamentalnom teoremu aritmetike, postoje različiti prosti brojevi $p_1, ..., p_n$ i pozitivni eksponenti $e_1, ..., e_n$ tako da

$$d = p_1^{e_1} \cdots p_n^{e_n}.$$

Definiramo $r_i = d/p_i^{e_i}$, tako da je $p_i^{e_i} = d$. Slijedi da je $r_i x \in G_{P_i}$ za svaki i. Ali najveći zajednički djelitelj od $r_1, ..., r_n$ je 1, pa postoje cijeli brojevi $s_1, ..., s_n$ tako da $1 = \sum_i s_i r_i$. Stoga vrijedi,

$$x = \sum_i s_i r_i x \in \langle \bigcup_P G_P \rangle.$$

Za svaki prost broj p, pišemo $H_p = \langle \cup_{q \neq p} G_q \rangle$. Po propoziciji 1.3.15 dovoljno je dokazati da ako

$$x \in G_p \cap H_p,$$

onda je $x = 0$. Budući da je $x \in G_p$, onda imamo $p^l x = 0$ za neki $l \geq 0$. Budući da je $x \in H_p$, onda vrijedi $ux = 0$, gdje je $u = q_1^{f_1} \cdots q_n^{f_n}$, $q_i \neq p$ i $f_i \geq 1$ za svaki i. Budući da su p^l i u relativno prosti onda postoje cijeli brojevi s i t tako da $1 = sp^l + tu$. Stoga vrijedi

$$x = (sp^l + tu)x = splx + tux = 0.$$

ii) Sada prevodimo upravo prezentirani dokaz na module. Ako je $m \in M$ različit od 0, onda je $\text{ann}(m) = (d)$, za neki $d \in R$. Po jedinstvenoj faktorizaciji, postoje ireducibilni elementi $p_1, ..., p_n$, gdje nijedno dvoje nisu asocirani, i pozitivni eksponenti $e_1, ..., e_n$ tako da

$$d = p_1^{e_1} \cdots p_n^{e_n}.$$

Po propoziciji 1.2.8, $P_i = (p_i)$ je prost ideal za svaki i. Definiramo $r_i = d/p_i$ tako da je $p_i^{e_i} r_i = d$. Slijedi da je $r_i m \in M_{p_i}$ za svaki i. Ali $\text{nzd}(r_1, ..., r_n) = 1$ pa postoje elementi $s_1, ..., s_n \in R$ tako da $1 = \sum_i s_i r_i$. Stoga,

$$m = \sum_i s_i r_i m \in \left\langle \bigcup_p M_p \right\rangle.$$

Za svaki prost P, pišemo $H_p = \left\langle \bigcup_{Q \neq P} G_Q \right\rangle$. Po propoziciji 1.3.15, dovoljno je dokazati da ako

$$m \in M_p \in H_p,$$

onda je $m = 0$. Budući da je $m \in M_p$ gdje je $P = (p)$, imamo $p^l m = 0$ za neki $l \geq 0$. Budući da je $m \in H_p$, imamo $um = 0$, gdje je $u = q_1^{f_1} \cdots q_n^{f_n}$, $Q_i = (q_i)$ i $f_i \geq 1$. Međutim p^l i u su relativno prosti pa postoje $s, t \in R$ s $1 = sp^l + tu$. Stoga vrijedi

$$m = (sp^l + tu)m = sp^l m + tum = 0.$$

□

Propozicija 2.0.10. *Neka su M i M' dva torzijska modula nad domenom glavnih ideala, oni su izomorfni ako i samo ako vrijedi $M_P \cong M'_P$ za svaki prost ideal P koji je različit od nule.*

Dokaz. Ako je $f : M \to M'$ R-homomorfizam, onda je $f(M_P) \subseteq M'_P$ za svaki prosti ideal $(P) = (p)$, jer ako je $p^l m = 0$, imamo da je $0 = f(p^l m) = p^l f(m)$. Ako je f izomorfizam, onda je $f^{-1} : M' \to M$ također izomorfizam. Slijedi da je svaka restrikcija $f|M_P : M_P \to M'_P$ izomorfizam s inverzom $f^{-1}|M'_P$. Obrnuto, ako je $f_P : M_P \to M'_P$ izomorfizam za svaki P, onda je $\varphi : \sum_P M_P \to \varphi : \sum_P M'_P$ izomorfizan definiran s $\sum_P m_p \mapsto \sum_P f_P(m_P)$.

□

Teorem 2.0.11. ***(Teorem o bazi)*** *Ako je R domena glavnih ideala, onda je svaki konačno generiran modul direktna suma cikličkih modula u kojem je svaki ciklički sumand primaran ili izomorfan s R.*

Dokaz. Iz korolara 2.0.5 slijedi da je $M = tM \oplus F$ gdje je F konačno generiran slobodan modul. □

Korolar 2.0.12. *Svaka konačno generirana Abelova grupa je direktna suma cikličkih grupa, pri čemu je red svake grupe ili potencija prostog broja ili beskonačano.*

Kada su dva konačno generirana modula M i M' nad domenom glavnih ideala izomorfni?
Prije nego što iskažemo sljedeću lemu definirajmo

$$d(M) = \dim(M/pM).$$

Posebno, $d(pM) = \dim(pM/p^2M)$, to jest generalnije,

$$d(p^nM) = \dim(p^nM/p^{n+1}M).$$

Lema 2.0.13. *Neka je M konačno generiran (p)-primaran R-modul gdje je R domena glavnih ideala, (p) prost ideal i $M = \sum_j C_j$ gdje je svaki C_j ciklički. Ako je $b_n \geq 0$ broj sumanada C_j koji imaju anihilator (p^n), onda postoji $t \geq 1$ takav da vrijedi*

$$d(p^nG) = b_{n+1} + b_{n+2} + \cdots + b_t.$$

Dokaz. Neka je B_n direktna suma svih C_j-ova s anihilatorom (p^n). Stoga,

$$M = B_1 \oplus B_2 \oplus \cdots \oplus B_t$$

za neki t. Sada imamo

$$p^nM = p^nB_{n+1} \oplus \cdots \oplus p^nB_t,$$

zbog $p^nB_j = \{0\}$ za svaki $j \leq n$. Slično,

$$p^{n+1}M = p^{n+1}B_{n+2} \oplus \cdots \oplus p^{n+1}B_t.$$

Sada imamo da je $p^{n+1}M/p^nM$ izomorfan s

$$[p^nB_{n+1}/p^{n+1}B_{n+1}] \oplus [p^nB_{n+2}/p^{n+1}B_{n+2}] \oplus \cdots \oplus [p^nB_t/p^{n+1}B_t].$$

Nadalje, lagano se vidi da je $d(p^nB_m/p^{n+1}B_m) = \dim(p^nB_m) = b_m$ za svaki $n < m$. Budući da je d aditivan nad direktnim sumama, onda imamo

$$d(p^nM) = b_{n+1} + b_{n+2} + ... + b_t.$$

□

Definicija 52. Ako je M konačno generiran (p)-primaran R-modul, gdje je R domena glavnih ideala i $P = (p)$ prost ideal, tada definiramo

$$U_P(n, M) = d(n^n M) - d(p^{n+1} M).$$

Teorem 2.0.14. *Ako je R domena glavnih ideala i $P = (p)$ prost ideal u R, tada bilo koje dvije dekompozicije konačno generiranog P-primarnog R-modula M u direktnu sumu cikličkih modula ima isti broj sumanada svakog tipa. Preciznije, za svaki $n \geq 0$, broj cikličkih sumanada koji imaju anihilator (p^{n+1}) je $U_P(n, M)$.*

Dokaz. Po teoremu o bazi postoje ciklički podmoduli C_i tako da je $M = \sum_i C_i$. Lema nam pokazuje da za svaki $n \geq 0$, broj C_i-ova koji imaju anihilator (p^{n+1}) je $U_p(n, M)$ koji je definiran bez spominjanja dane dekompozicije od M u direktnu sumu cikličkih sumanada. Stoga, ako je $M = \sum_j D_j$ još jedna dekompozicija od M gdje je svaki D_j ciklički, onda je broj D_j-ova koji imaju anihilator (p^{n+1}) također $U_p(n, M)$ kao što je traženo.

□

Korolar 2.0.15. *Ako su M i M' P-primaran R-moduli, gdje je R domena glavnih ideala, tada je $M \cong M'$ ako i samo ako $U_P(n, M) = U_P(n, M')$ za svaki $n \geq 0$.*

Dokaz. Ako je $\varphi : M \to M'$ izomorfizam, onda je $\varphi(p^n M) = p^n M'$ za svaki $n \geq 0$ i φ inducira izomorfizam od $\mathbb{Z}_P$-vektorskih prostora $p^n M / p^{n+1} M \cong p^n M' / p^{n+1} M'$ za svaki $n \geq 0$ sa $p^n m + p^{n+1} M \mapsto p^n \varphi(g) + p^{n+1} M'$. Stoga su njihove dimenzije iste, to jest vrijedi da je $U_p(n, M) = U_p(n, M')$.

Obrnuto, pretpostavimo da je $U_p(n, M) = U_p(n, M')$ za svaki $n \geq 0$. Ako je $M = \sum_i C_i$ i $M' = \sum_i C'_i$ gdje su C_i i C'_j ciklički. Tada lema 2.0.13 pokazuje da imamo isti broj sumanada svakog tipa pa je lako konstruirati izomorfizam $M \to M'$. □

Definicija 53. Ako je M P-primaran R-modul gdje je R domena glavnih ideala, onda su **elementarni divizori** od M ideali (p^{n+1}), svaki ponovljen s kratnosti $U_P(n, M)$.

Ako je M konačno generiran torzijski R-modul, onda su njegovi elementarni divizori, elementarni divizori svih primarnih komponenti.

Sljedeća definicija je motivirana korolarom 1.1.13.
Ako je G konačna Abelova grupa s elementarnim divizorima $\{p_i^{e_{ij}}\}$, onda je

$$|G| = \prod_i j p_i^{e_{ij}}.$$

Definicija 54. Ako je M konačno generiran torzijski R-modul, gdje je R domena glavnih ideala, onda je **red** od M glavni ideal generiran produktom elementarnih divizora, to jest $(\prod_{ij} p_i^{e_{ij}})$.

Primjer 2.0.16. *Ako je k polje, koliko ima $k[x]$-modula reda $(x-1)^3(x+1)^2$? Po primarnoj dekompoziciji, svaki $k[x]$-modul reda $(x-1)^3(x+1)^2$ je direktna suma primarnih modula reda $(x-1)^3$ i $(x+1)^2$. Postoje 3 modula reda $(x-1)^3$ opisanih s elementarnim divizorima*

$$(x-1, x-1, x-1), \quad (x-1, (x-1)^2), \quad (x-1)^3,$$

postoje dva modula reda $(x+1)^2$ opisani elementarnim divizorima

$$(x+1, x+1) \quad i \quad (x+1)^2.$$

Stoga, do na izomorfizam postoje 6 modula reda $(x-1)^3(x+1)^2$.

Teorem 2.0.17. ***(Fundamentalni teorem konačno generiranih modula)*** *Ako je R domena glavnih ideala, onda su dva konačno generirana R-modula izomorfna ako i samo ako njihovi torzijski podmoduli imaju iste elementarne divizore i njihovi slobodni dijelovi imaju isti dimenziju.*

Dokaz. Po teoremu 2.0.9 ii), imamo da je $M \cong M'$ ako i samo ako su primarne komponente M_P i M'_P izomorfne za sve P. Sada uz korolare 2.0.15 i 2.0.5 ii) te propoziciju 2.0.10 dovršavamo dokaz. □

Slijedi drugi tip dekompozicije konačno generiranih torzijskih R-modula M u direktnu suma cikličkih modula koji ne spominju primarne module.

Propozicija 2.0.18. *Ako je R domena glavnih ideala, onda je svaki konačno generiran torzijski R-modul M direktna suma cikličkih modula*

$$M = R/(c_1) \oplus R/(c_2) \oplus \cdots \oplus R/(c_t),$$

gdje je $t \geq 1$ i $c_1 \mid c_2 \mid \cdots \mid c_t$.

Dokaz. Neka su $p_1, ..., p_n$ prosti djelitelji reda od M. Po teoremu o bazi, za svaki p_i imamo

$$M_{p_i} = R/p_i^{e_{i1}} \oplus R/p_i^{e_{i2}} \oplus \cdots \oplus R/p_i^{e_{it}}.$$

Možemo pretpostaviti da je $0 \leq e_{i1} \leq e_{i2} \leq ... \leq e_{it}$. Nadalje, možemo dopustiti eksponente $e_{ij} = 0$ tako da zadnji indeks t može biti korišten za svaki i. Definiramo

$$c_j = p_1^{e_{ij}} p_2^{e_{2j}} \cdots p_n^{e_{nj}}.$$

Jasno je da vrijedi $c_1|c_2| \cdots |c_t$. Iz toga slijedi

$$R/p_1^{e_{1j}} \oplus R/p_2^{e_{2j}} \oplus \cdots \oplus R/p_n^{e_{nj}} \cong R/c_j$$

za svaki j. □

Definicija 55. Ako je M konačno generiran torzijski R-modul gdje je R domena glavnih ideala i ako je

$$M = R/(c_1) \oplus R/(c_2) \oplus \cdots \oplus R/(c_t),$$

gdje je $t \geq 1$ i $c_1|c_2| \cdots |c_t$, onda se $(c_1), (c_2), ..., (c_t)$ zovu **invarijantni faktori** od M.

Korolar 2.0.19. *Ako je M konačno generiran torzijski modul nad domenom glavnih ideala, onda*

$$(c_t) = \{r \in R : rm = \{0\}\},$$

gdje je (c_t) zadnji ideal koji se pojavljuje u propoziciji 2.0.18. Posebno, ako je $R = k[x]$ gdje je k polje, onda je c_t polinom najmanjeg stupnja za koji je $c_t M = \{0\}$.

Dokaz. Budući da je $c_i|c_t$ za svaki i, onda imamo da je $c_t R/(c_i) = 0$ za svaki i pa je $c_t M = \{0\}$. S druge strane, ne postoji e takav da $e|(c_t)$, $e \neq c_t$ i $eR/(c_t) = \{0\}$ pa slijedi da je (c_t) najmanji ideal koji poništava M.

Druga tvrdnja slijedi iz činjenice da je svaki ne-nul ideal u $k[x]$ generiran s polinomom najmanjeg stupnja u njemu.

□

Definicija 56. Ako je M R-modul, onda je njegov anihilator ideal

$$\text{ann}(M) = \{r \in R : rM = \{0\}\}.$$

Korolar 2.0.19 izračunava anihilator konačno generiranog torzijskog modula nad domenom glavnih ideala, to je zadnji invarijantni faktor (c_t).

Korolar 2.0.20. *Ako je M konačno generiran torzijski R-modul, gdje je R domena glavnih ideala s invarijantnim faktorima $c_1, ..., c_t$, onda je red od M upravo $(\prod_{i=1}^{t} c_i)$.*

Dokaz. Imamo

$$M \cong R/(c_1) \oplus \cdots \oplus R/(c_t)$$

Odavde slijedi da je red od M $(\prod_{i=1}^{t} c_i)$, to jest $(\prod_{ij} p_i^{e_{ij}})$. Činjenicu da je c_t eksponenet smo pokazali u korolaru 1.1.13.

□

Primjer 2.0.21. *U prethodnom primjeru smo pokazali elementarne divizore $k[x]$-modula reda $(x-1)^3(x+1)^2$, sada imamo i invarijantne faktore.*

Elementarni divizori $\leftrightarrow$ *Invarijantni faktori*

$$(x-1,\ x-1,\ x-1,\ x+1,\ x+1) \ \leftrightarrow\ x-1 \mid (x-1)(x+1) \mid (x-1)(x+1)$$

$$(x-1,\ (x-1)^2,\ x+1,\ x+1) \ \leftrightarrow\ (x-1)(x+1) \mid (x-1)^2(x+1)$$

$$((x-1)^3, x+1, x+1\ ) \leftrightarrow\ x+1 \mid (x-1)^3(x+1)$$

$$(x-1, x-1, x-1, (x+1)^2) \ \leftrightarrow\ x-1 \mid x-1 \mid (x-1)(x-1)^2$$

$$(x-1, (x-1)^2, (x+1)^2) \ \leftrightarrow\ x-1 \mid (x-1)^2(x+1)^2$$

$$(x-1)^3, (x+1)^2) \ \leftrightarrow\ (x-1)^3(x+1)^2$$

Teorem 2.0.22. ***(Teorem o invarijantnim faktorima)*** *Ako je R domena glavnih ideala, onda su dva konačno generirana R-modula izomorfni ako i samo ako njihovi torzijski podmoduli imaju iste invarijantne faktore i ako su njihovi slobodni dijelovi iste dimenzije.*

Dokaz. Po korolaru 2.0.5 i), svaki konačno generiran R-modul M je direktna suma $M = tM \oplus F$, gdje je F slobodan i $M \cong M'$ ako i samo ako $tM \cong tM'$ i $F \cong F'$. Korolar 2.0.5 ii) nam pokazuje da su slobodni dijelovi $F \cong M/tM$ i $F' \cong M'/tM'$ izomorfni, a generalizacija teorema 1.1.14. nam pokazuje da su torzijski podmoduli izomorfni. □

Bibliografija

[1] Joseph J. Rotman, *Advanced Linear Algebra*, Prentice Hall Publication, SAD, 2003

[2] B. Širola, *Algebarske strukture*, https://web.math.pmf.unizg.hr/nastava/alg/predavanja/ASpred.pdf, lipanj 2014.

Sažetak

Glavni cilj ovog rada je proučiti pojam R-modula gdje je R domena glavnih ideala. Rad se sastoji od dvaju poglavlja. U prvom poglavlju predstavljaju se osnovne algebarske strukture, grupe i prstenovi te se pojašnjavaju moduli. U drugom poglavlju detaljnije se predstavljaju moduli nad domenama glavnih ideala.

U ovom radu, glavni naglasak stavljen je na konačno generirane module čiji rezultati proizlaze iz generaliziranih tvrdnji o Abelovim grupama. Strukturne teoreme za konačne Abelove grupe generalizirat ćemo na module nad domenama glavnih ideala, iz čega zaključujemo da se ne generaliziraju samo teoremi već i dokazi.

Summary

The main objective of this paper is to study the notion of R-module where R is the principal ideal domain. This paper consists of two chapters, the first chapter presenting basic algebraic structures, groups and rings and explaining the modules. The second chapter presents the modules over principal ideal domail in more detail.

The main emphasis of this paper is placed on the finitely generated modules whose results are derived from generalized statements about Abelian groups. We will generalize the structural theorems for finite Abelian groups to modules over principal ideal domain, from which we conclude that not only the theorems are generalized but also the proofs.

Životopis

Autorica ovog rada rođena je 25. siječnja 1993. godine u Zagrebu, gdje je završila Osnovnu školu Bukovac i matematički smjer XV. Gimnazije. Na Prirodoslovno - matematičkom fakultetu, Matematičkom odsjeku u Zagrebu završila je preddiplomski studij inženjerske matematike i upisala diplomski studij Primijenjene matematike.

Tijekom završne godine studija zapošljava se u osiguravajućoj kući Allianz Zagreb d.d. kao asistent glavnom pricing aktuaru u sektoru neživotnih osiguranja.