Noetherini prsteni i moduli

Nuić, Mario

Sveučilište Josipa Jurja Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike

Sveučilišni diplomski studij matematike
modul: Financijska matematika i statistika

Noetherini prsteni i moduli

Diplomski rad

Mentor:
prof. dr. sc. Ivan Matić

Student:
Mario Nuić

Osijek, 2024.

Sadržaj

1 | Uvod

Emmy Noether njemačka je matematičarka i fizičarka. Rođena je 1882. godine te se od njenog rođenja, pretpostavljalo kako će Emmy kada odraste biti kućanica, poput svoje majke. Ženama u to vrijeme školovanje nije bilo dozvoljeno te se smatralo kako se samo muškarci mogu baviti znanošću. Bez obzira na prepreke s kojima se susrela, Emmy nije odustala od svoje želje da postane profesorica te je dvije godine redovno dolazila slušati predavanja, iako nije mogla polagati ispite niti dobivati povratne informacije od profesora. Svojom upornošću i trudom, uspjela je položiti završni ispit na sveučilištu u Erlangenu, nakon kojega upisuje doktorat na sveučilištu u Gottingenu. Emmy je poseban interest pokazala prema algebri u kojoj je ostavila veliki trag. U ovome radu bavit ćemo se jednim od najvećih njenih doprinosa matematici - *Noetherinim prstenima i modulima*.
U prvom dijelu rada definirat ćemo neke osnovne algebarske pojmove. Osim definicija, navest ćemo i neka osnovna svojstva navedenih matematičkih pojmova.
U drugom dijelu rada, prvo ćemo definirati Noetherin prsten te module, čime postavljamo temelj za daljnju analizu. Zatim ćemo predstaviti pridružene proste ideale, koji igraju ključnu ulogu u strukturalnim svojstvima modula. Nakon toga, ući ćemo u detaljnu analizu modula kroz dekompoziciju te ćemo pokazati što je Nakayamina lema. Objasnit ćemo što su filtrirani i gradirani moduli te korisnost Hilbertova polinoma. U zadnjem poglavlju analizirat ćemo nerazložive module.

2 | Osnovni pojmovi i svojstva

U ovom poglavlju definirat ćemo te navesti svojstva algebarskih struktura koje ćemo koristiti u nastavku ovoga rada.

2.1 Prsteni

Definicija 1. ([6], *str.* 80) *Neka je dan neprazan skup R na kojemu su definirane dvije binarne operacije zbrajanja $+ : R \times R \to R$ i množenja $\cdot : R \times R \to R$. Uređenu trojku $(R, +, \cdot)$ nazivamo prsten ukoliko za sve $a, b, c \in R$ vrijedi:*

1. *$(R, +)$ je Abelova grupa,*
2. *asocijativnost množenja:*
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$
3. *distributivnost množenja prema zbrajanju slijeva, odnosno zdesna:*
$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

Neutralni element za zbrajanje označavamo s 0, a inverzni element od a s $-a$. Dakle, u prstenu, za svaki $a \in R$ vrijedi:

$$a + (-a) = 0.$$

Definicija 2. ([6], *str.* 81) *Za prsten $(R, +, \cdot)$ kažemo da je komutativni prsten s jedinicom ukoliko je množenje u prstenu R komutativno, odnosno, ako za sve $a, b \in R$ vrijedi:*

$$a \cdot b = b \cdot a.$$

Nadalje, kažemo da je R prsten s jedinicom ukoliko postoji element $1_R \in R$ takav da za svaki $a \in R$ vrijedi sljedeće:

$$1_R \cdot a = a \cdot 1_R = a.$$

Primjer 1. ([5], *str.* 16) *Pogledajmo primjere nekih prstena:*

- *Skupovi brojeva* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *i* $\mathbb{C}$ *sa standardnim operacijama zbrajanja i množenja su primjeri prstena s jedinicom.*
- *Sa* $M(n, \mathbb{F})$ *označimo skup svih kvadratnih matrica reda* n *nad* $\mathbb{F} = \mathbb{R}$ *ili* $\mathbb{C}$. $M(n, \mathbb{F})$ *je prsten s operacijama matričnog zbrajanja i množenja, ali nije komutativan prsten jer komutativnost množenja matrica općenito ne vrijedi. Nula u prstenu je nul matrica, a jedinica je jedinična matrica.*

U sljedećem teoremu iskazat ćemo osnovna svojstva prstena. Dokaz ćemo u ovom radu izostaviti te se isti može pronaći u [6] na str. 83.

Teorem 1. ([6], *str.* 83) *Neka je* R *prsten. Za sve* $a, b, c \in R$ *vrijedi sljedeće:*

a) $a0 = 0a = 0$,

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

c) $a(b - c) = ab - ac, \quad (a - b)c = ac - bc$.

Definicija 3. ([3], *str.* 5) *Neka je* R *prsten s jedincom. Ako svaki element* $a \in R$, $a \neq 0$, *ima multiplikativni inverz* $a^{-1} \in R$, *tada* R *nazivamo prsten s dijeljenjem. Ukoliko za množenje u* R *vrijedi svojstvo komutativnosti, onda* R *nazivamo polje.*

Primjeri polja su prsteni brojeva $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$. Primjer prstena koji nije polje je skup $\mathbb{Z}$. Primijetimo kako nijedan element iz skupa $\mathbb{Z}$, osim 1 i -1, nema multiplikativni inverz u $\mathbb{Z}$.

Definicija 4. ([6], *str.* 85) *Prsten* R *u kojemu iz* $xy = 0$, $x, y \in R$ *slijedi da je* $x = 0$ *ili* $y = 0$ *nazivamo integralna domena.*

Svaki prsten R s dijeljenjem je integralna domena. Također, svako polje R je integralna domena. Međutim, obrat ne vrijedi. Primjerice, prsten $\mathbb{Z}$ je komutativna integralna domena s jedinicom, ali kao što smo ranije naveli, skup $\mathbb{Z}$ nije polje. U sljedećoj propoziciji iskazat ćemo koji uvjet mora vrijediti kako bi integralna domena bila polje.

Propozicija 1. ([6], *str.* 86) *Neka je* R *komutativna integralna domena s jedinicom. Ukoliko je* R *konačan skup, onda je* R *polje.*

U nastavku ćemo definirati još nekoliko pojmova koje ćemo koristiti u nastavku rada.

Definicija 5. ([5], *str.* 64) *Neka je* R *komutativni prsten s jedinicom. Element* $a \neq 0$ *prstena* R *nazivamo djeliteljem nule ukoliko postoji* $b \neq 0$ *takav da je* $ab = 0$.

Definicija 6. ([6], *str.* 87) *Neka je* R *prsten. Element* $a \in R$ *nazivamo nilpotentnim ukoliko postoji prirodan broj* n *za koji vrijedi:* $a^n = 0$.

U integralnoj domeni jedini nilpotentni element je neutralni element $0 \in R$.

Definicija 7. ([6], *str.* 97) *Neka je R prsten. Za neprazan podskup I prstena R kažemo da je ideal ukoliko vrijedi sljedeće:*

1. $x - y \in I, \forall x, y \in I$

2. $rx \in I$ *i* $xr \in I, \forall x \in I, r \in R$.

Kažemo da je I lijevi ideal prstena R ukoliko umjesto 2. svojstva u prethodnoj definiciji vrijedi $rx \in I, \forall x \in I, r \in R$. Također, kažemo da je desni ideal, ukoliko umjesto 2. svojstva vrijedi $xr \in I, \forall x \in I, r \in R$.

Primjer 2. ([6], *str.* 98) *Pogledajmo primjere ideala:*

- *Za svaki prsten R su* $\{0\}$ *i R ideali u R. Za ideal* $\{0\}$ *kažemo da je trivijalni ideal u prstenu R.*

- *Neka je R prsten i neka je* $a \in R$. *Tada je*

$$aR = \{ar : r \in R\}$$

desni ideal u R, a

$$Ra = \{ra : r \in R\}$$

lijevi ideal u R. Ako R nema jedinicu, a ne mora biti element skupa aR ili Ra. Pokažimo da je aR desni ideal. Odaberimo ar_1, $ar_2 \in aR$. *Tada je*

$$ar_1 - ar_2 = a(r_1 - r_2) \in aR$$

jer je $r_1 - r_2 \in R$. *Dakle, aR je Abelova podgrupa od R. Nadalje, za svaki* $r \in R$ *imamo*

$$(ar_1)r = a(r_1 r) \in aR$$

jer je $r_1 r \in R$, *pa zaključujemo da je aR desni ideal u R. Slično se pokaže i da je Ra lijevi ideal u R.*

Definicija 8. ([6], *str.* 100) *Neka je R prsten i* $S \subseteq R$. *Najmanji ideal koji sadrži S nazivamo ideal generiran skupom S i označavamo sa* (S). *Ukoliko je S konačan skup, tj.* $S = a_1, a_2, ..., a_n$, *koristi se oznaka* $(S) = (a_1, a_2, ..., a_n)$. *Nadalje, ako je ideal* (a) *generiran samo jednim elementom* $a \in R$, *nazivamo ga glavni ideal.*

Definicija 9. ([5], *str.* 69) *Neka je I ideal u prstenu R. Kažemo da je ideal I prost ukoliko je* $I \neq R$ *te ako iz* $ab \in I$ *slijedi da je ili* $a \in I$ *ili* $b \in I$.

Definicija 10. ([5], *str.* 69) *Kažemo da je ideal* $I \neq R$ *maksimalan ukoliko u R ne postoji ideal J takav da je* $I \subsetneq J \subsetneq R$.

Uočimo kako će ideal I biti različit u R ako i samo ako $1 \notin I$. Ukoliko bi vrijedilo suprotno, tj. $1 \in I$, za svaki $a \in R$ vrijedi $a = a1 \in I$, odnosno $I = R$.
Sljedeću propoziciju navest ćemo bez dokaza, a isti se može pronaći u [5] na stranici 69.

Propozicija 2. ([5], *str.* 69) *Neka je I ideal različit od R. Tada postoji maksimalan ideal u R koji sadrži I.*

Sada ćemo još definirati i kvocijentni prsten.

Neka je I ideal u prstenu R. Definirajmo relaciju ekvivalencije $\sim$ na R s

$$a \sim b \quad \text{ako i samo ako je} \quad a - b \in I.$$

Klasa ekvivalencije elementa $a \in R$ je

$$\overline{a} = \{b \in R : a - b \in I\} = \{a + r : r \in I\} = a + I.$$

Skup svih klasa ekvivalencije $\overline{a}$ označimo s

$$R/I = \{a + I : a \in R\}.$$

Definicija 11. ([6], *str.* 101) *Neka je I ideal u prstenu R. Tada prsten* $(R/I, +, \cdot)$ *nazivamo kvocijentni prsten R modulo I.*

Ako je $I = R$, onda je R/I nul-prsten jer je $\overline{r} = r + I = \overline{0}$ za svaki $x \in R$. Ako je $I = (0)$, onda se R/I može identificirati s R ako $a + (0)$ identificiramo s a.

2.2 Moduli

Module nad prstenima možemo promatrati kao generalizaciju vektorskih prostora nad poljem. U nastavku ćemo definirati te navesti osnovna svojstva modula.

Definicija 12. ([3], *str.* 30) *Neka je R prsten s jedinicom. Lijevi R-modul je Abelova grupa uz operaciju skalarnog množenja* $\cdot : R \times M \to M$ *takva da za sve elemente* $x, y \in R$ *i* $m, n \in M$ *vrijedi sljedeće:*

1. $x(m + n) = xm + xn$
2. $(x + y)m = xm + ym$
3. $(xy)m = x(ym)$
4. $1m = m$

Analogno se definira i desni R-modul.
U nastavku će se R - modul odnositi na lijevi modul, ukoliko nije drugačije naglašeno.

Primjer 3. ([6], *str.* 125) *Pogledajmo primjere nekih modula:*

- *Svaki prsten R je lijevi i desni R-modul.*
- *Ako je B aditivna Abelova grupa, onda je B lijevi* $\mathbb{Z}$*-modul jer je*

$$a(b_1 + b_2) = ab_1 + ab_2,$$

$$(a_1 + a_2)b = a_1b + a_2b,$$

$$(a_1a_2)b = a_1(a_2b),$$

$$1b = b,$$

za sve $a, a_1, a_2 \in \mathbb{Z}$ i $b, b_1, b_2 \in B$.

Definicija 13. ([6], *str.* 127) *Neka je M modul nad R. Neprazan podskup $N \subseteq M$ je podmodul od M ukoliko vrijedi*

i) $a - b \in N$ *za sve* $a, b \in N$,

ii) $ra \in N$ *za sve* $a \in N, r \in R$.

Možemo reći da je podmodul Abelova podgrupa od M koja je zatvorena na množenje elementima iz R. Jasno je da su 0 i M trivijalni podmoduli od M.

Primjer 4. ([6], *str.* 127) *Pogledajmo sada primjere nekih podmodula:*

- *Ako je I lijevi ideal u prstenu R, tada je I podmodul R-modula R.*
- *Neka je M modul nad R te neka je $x \in M$. Tada je skup*

$$Rx = \{rx : r \in R\}$$

podmodul od M.

Još ćemo definirati sumu i direktnu sumu podmodula koje ćemo koristiti u kontekstu Noetherinih prstena.

Definicija 14. ([6], *str.* 130) *Neka su $N_1, N_2, \ldots, N_k$ podmoduli $R-$modula M. Podmodul generiran unijom $\cup_{i=1}^{k} N_i$ nazivamo suma podmodula N_i i označavamo s $\sum_{i=1}^{k} N_i$.*

Definicija 15. ([6], *str.* 131) *Neka su $N_1, N_2, \ldots, N_k$ podmoduli $R-$modula M. Suma podmodula $\sum_{i=1}^{k} N_i$ naziva se direktna suma ako se svaki element $x \in \sum_{i=1}^{k} N_i$ može na jedinstven način zapisati kao $x = \sum_{i=1}^{k} x_i$, gdje je $x_i \in N_i$. Direktnu sumu obično označavamo s*

$$N_1 \bigoplus N_2 \bigoplus \ldots \bigoplus N_k.$$

Ukoliko direktna suma generira čitav modul M, pišemo

$$M = N_1 \bigoplus N_2 \bigoplus \ldots \bigoplus N_k.$$

3 | Noetherini prsteni i moduli

U ovom poglavlju bavit ćemo se specijalnom vrstom prstena te modula koji su ime dobili prema već spomenutoj Emmy Noether.

3.1 Osnovni kriteriji

Definicija 16. ([1], *str.* 157) *Neka je R komutativan prsten i M R-modul. Kažemo da je M Noetherin ukoliko je svaki podmodul od M konačno generiran.*

Propozicija 3. ([2], *str.* 413) *Neka je R komutativan prsten i neka je M R-modul. Sljedeće tvrdnje su ekvivalentne:*

(1) *Svaki podmodul od M je konačno generiran.*

(2) *Svaki rastući niz podmodula od M,*

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots,$$

takav da je $M_i \neq M_{i+1}$ je konačan.

(3) *Svaki neprazan skup S podmodula od M ima maksimalan element.*

Dokaz. (1) $\implies$ (2) Pretpostavimo da imamo rastući niz podmodula od M kao što je navedeno u svojstvu (2). Neka je N unija svih podmodula M_i $(i = 1, 2, \dots)$. Tada je N konačno generiran elementima $x_1, x_2, \dots, x_r$ i svaki element-generator je u nekome od skupova M_i. To implicira postojanje indeksa j takvog da je $x_1, x_2, \dots, x_r \in M_j$. Tada vrijedi

$$\langle x_1, x_2, \dots, x_r \rangle \subseteq M_j \subseteq N = \langle x_1, x_2, \dots, x_r \rangle,$$

što rezultira jednakošću pa je naša tvrdnja dokazana.

(2) $\implies$ (3) Neka je N_0 element skupa S. Ako N_0 nije maksimalan, sadržan je u podmodulu N_1. Ako N_1 nije maksimalan, sadržan je u podmodulu N_2. Induktivno, ako pronađemo N_i koji nije maksimalan, sadržan je u podmodulu N_{i+1}. Na ovaj način mogli bismo konstruirati beskonačan lanac, što je nemoguće.

(3) $\implies$ (1) Neka je N podmodul od M te neka je a_0 iz N. Ako $N \neq \langle a_0 \rangle$, tada postoji element $a_1 \in N$ koji se ne nalazi u $\langle a_0 \rangle$. Nastavljajući induktivno, možemo naći rastući niz podmodula od N

$$\langle a_0 \rangle \subset \langle a_0, a_1 \rangle \subset \langle a_0, a_1, a_2 \rangle \subset \dots$$

gdje je svaka inkluzija stroga. Skup ovih podmodula sadrži maksimalni element, na primjer neka je to podmodul $\langle a_0, a_1, ..., a_r \rangle$, pa je očito da ovaj konačno generirani podmodul mora biti jednak N, što je trebalo pokazati.

□

U sljedećih nekoliko propozicija iskazat ćemo te dokazati svojstva Noetherinih modula.

Propozicija 4. ([2], *str.* 414) *Neka je R komutativan prsten te neka je M Noetherin R-modul. Tada je svaki podmodul te svaki kvocijentni modul od M također Noetherin.*

Dokaz. Tvrdnja je očita za podmodule. Za kvocijentne module, neka je N podmodul i neka je $f : M \to M/N$ kanonski homomorfizam. Neka je $\overline{M}_1 \subseteq \overline{M}_2 \subseteq \dots$ rastući lanac podmodula od M/N te neka je $M_i = f^{-1}(\overline{M}_i)$. Tada $M_1 \subseteq M_2 \subseteq \dots$ čini rastući lanac podmodula od M, koji mora imati maksimalan element, na primjer M_r, takav da je $M_i = M_r$ za $r \geq i$. Tada vrijedi $f(M_i) = \overline{M}_i$ te naša tvrdnja slijedi. □

Propozicija 5. ([2], *str.* 414) *Neka je M modul, a N podmodul. Nadalje, neka su N i M/N Noetherini. Tada je i M Noetherin modul.*

Dokaz. Svakome podmodulu L od M pridružujemo par modula

$$L \mapsto (L \cap N, (L+N)/N).$$

Tvrdimo: Ako su $E \subseteq F$ dva podmodula od M takva da su im pridruženi parovi jednaki, vrijedi $E = F$. Kako bismo to vidjeli, uzmimo $x \in F$. Po pretpostavci da vrijedi
$(E+N)/N = (F+N)/N$, postoje elementi $u, v \in N$ i $y \in E$ takvi da vrijedi $y + u = x + v$. Tada je

$$x - y = u - v \in F \cap N = E \cap N.$$

S obzirom da je $y \in E$, slijedi da je i $x \in E$ te je tvrdnja dokazana. Ukoliko imamo rastući niz skupova

$$E_1 \subseteq E_2 \subseteq \dots$$

tada pridruženi parovi tvore rastući niz podmodula od N i M/N, te ovi nizovi moraju stati. Tada staje i niz $E_1 \subset E_2 \subseteq \dots$, po prethodnoj tvrdnji. □

Definicija 17. ([1], *str.* 51) *Neka su s $f : A \to B$ i $g : B \to C$ zadana dva homomorfizma R- modula. Kažemo da je par preslikavanja (f, g) složen ako vrijedi*
$g \circ f = 0 : A \to B \to C$.

Definicija se poistovjećuje sa svojstvom $Im(f) \subset ker(g)$.

Definicija 18. ([1], str. 51) *Za par složenih preslikavanja kažemo da je egzaktan ukoliko vrijedi*

$$Im(f) = ker(g).$$

Često ćemo par preslikavanja pisati kao nizove $X \xrightarrow{f} Y \xrightarrow{g} Z$ te ćemo, ukoliko je par preslikavanja egzaktan, smatrati i nizove egzaktnima. Prethodne dvije propozicije zapravo kažu da u egzaktnom nizu $0 \to M' \to M \to M'' \to 0$, vrijedi da je M Noetherin ako i samo ako su M' i M'' Noetherini.

Korolar 1. ([2], str. 415) *Neka je M modul i neka su N i N' podmoduli. Ako je $M = N + N'$ te ukoliko su N i N' Noetherini, tada je i M Noetherin. Konačna direktna suma Noetherinih modula je Noetherina.*

Dokaz. Uočimo kako je direktan produkt $N \times N'$ Noetherin jer sadrži N kao podmodul čiji je kvocijentni modul izomorfan s N', pa vrijedi Propozicija 5. Surjektivni je homomorfizam

$$N \times N' \to M$$

takav da se par (x, x'), $x \in N$ i $x' \in N'$, preslika u $x + x'$. Po Propoziciji 4., slijedi da je M Noetherin. Dokaz za konačne produkte ili sume slijedi induktivno. $\square$

Definicija 19. ([2], str. 415) *Kažemo da je prsten A Noetherin ukoliko je Noetherin kao lijevi modul nad samim sobom. Odnosno, ukoliko je svaki lijevi ideal konačno generiran.*

Propozicija 6. ([2], str. 415) *Neka je A Noetherin prsten te neka je M konačno generiran $A-$modul. Tada je M Noetherin.*

Dokaz. Neka su $x_1, \ldots, x_n$ generatori od M. Postoji homomorfizam

$$f : A \times A \times ... \times A \to M$$

produkta od A sa samim sobom n puta takav da vrijedi

$$f(a_1, \ldots, a_n) = a_1x_1 + \ldots + a_nx_n.$$

Ovaj homomorfizam je surjektivan. Prethodna propozicija kaže da je produkt Noetherin, pa je M Noetherin po Propoziciji 4. $\square$

Propozicija 7. ([2], str. 415) *Neka je A Noetherin prsten te neka je $\varphi : A \to B$ surjektivni homomorfizam prstena. Tada je B Noetherin.*

Dokaz. Neka je $b_1 \subseteq \ldots \subseteq b_n \subseteq \ldots$ rastući lanac lijevih ideala od B te neka je $a_i = \varphi^{-1}(b_i)$. Tada a_i tvore rastući lanac lijevih ideala od A koji mora stati. Pretpostavimo da je a_r zadnji u lancu. Kako je $\varphi(a_i) = b_i$, za sve i, tvrdnja je dokazana. $\square$

Definicija 20. ([1], str. 93) *Neka je A komutativan prsten i $S \subseteq A$. Kažemo da je S multiplikativni podskup od A ako je $1 \in S$ i ako je produkt bilo kojeg para elemenata iz S, element u S.*

Definicija 21. ([1], str. 94) *Neka je A komutativan prsten i S multiplikativan podskup od A. Tada je prsten razlomaka $S^{-1}A$ od A po S prirodno $A-$modul.*

Propozicija 8. ([1], *str.* 160) *Neka je A komutativan Noetherin prsten te neka je S multiplikativni podskup od A. Tada je $S^{-1}A$ Noetherin prsten.*

Dokaz. Neka je $\phi : A \to S^{-1}A$ kanonsko preslikavanje te neka je $I \subseteq S^{-1}A$ ideal. Tada je $\phi^{-1}(I) \subseteq A$ ideal, pa je konačno generiran. Slijedi da je:

$$\phi^{-1}(I)(S^{-1}A) \subseteq S^{-1}A$$

konačno generirano kao ideal u $S^{-1}A$; generatori su slike generatora od $\phi^{-1}(I)$. Sada tvrdimo da je

$$\phi^{-1}(I)(S^{-1}A) = I.$$

Inkluzija $\subseteq$ je trivijalna. Za drugu inkluziju, ako je $x/s \in I$, tada je $x \in \phi^{-1}(I)$, pa je

$$x = (1/s)x \in (S^{-1}A)\phi^{-1}(I).$$

Ovo dokazuje tvrdnju i povlači da je I konačno generiran. □

Primjer 5. ([1], *str.* 158) *Pogledajmo primjere Noetherinih prstena:*

- *Bilo koje polje je Noetherino. Dva su ideala* (1) *i* (0).
- *Bilo koja domena glavnih ideala je Noetherina: svaki ideal može biti generiran jednim elementom. Stoga,* $\mathbb{Z}$ *je Noetherin.*

3.2 Pridruženi prosti ideali

U ovome poglavlju pretpostavit ćemo da je A komutativan prsten. Moduli i homomorfizmi bit će A-moduli i A-homomorfizmi, osim ako je drugačije navedeno.

Propozicija 9. ([2], *str.* 416) *Neka je S multiplikativni podskup od A koji ne sadrži* 0. *Tada postoji ideal od A koji je maksimalan u skupu ideala koji su disjunktni sa S te je svaki takav ideal prost.*

Dokaz. Takav ideal postoji zbog Zornove leme ([5], str. 69). Neka je $\mathbf{p}$ maksimalan u promatranom skupu ideala. Neka su $a, b \in A$, $ab \in \mathbf{p}$, ali $a \notin \mathbf{p}$ i $b \notin \mathbf{p}$. Po pretpostavci vrijedi da ideali $(a, \mathbf{p})$ i $(b, \mathbf{p})$ presijecaju S, pa postoje elementi $s, s' \in S$, $c, c', x, x' \in A$, $p, p' \in \mathbf{p}$ takvi da je

$$s = ca + xp \quad \text{i} \quad s' = c'b + x'p.$$

Pomnožimo li ova dva izraza, dobivamo

$$ss' = cc'ab + p''$$

pri čemu je neki $p'' \in \mathbf{p}$, odakle zaključujemo da je $ss' \in \mathbf{p}$. To je kontradiktorno činjenici da je $\mathbf{p}$ disjunktan sa S pa je dokazano da je $\mathbf{p}$ prost. □

Korolar 2. ([2], *str.* 417) *Element $a \in A$ je nilpotentan ako i samo ako se on nalazi u svakom prostom idealu od A.*

Dokaz. Ako vrijedi $a^n = 0$, tada je $a^n \in \mathbf{p}$ za svaki prosti ideal $\mathbf{p}$, pa je i $a \in \mathbf{p}$. Ako pak postoji $n \in \mathbb{N}$ takav da vrijedi $a^n \neq 0$, uzet ćemo multiplikativni podskup potencija od a, oblika $\{1, a, a^2, \ldots\}$, te naći prosti ideal kao u Propoziciji 9. kako bismo dokazali suprotno. □

Neka je $\mathbf{x}$ ideal u A. Radikal od $\mathbf{x}$ je skup svih $a \in A$ takav da je $a^n \in \mathbf{x}$, za neki $n \geq 1$. Označavat ćemo ga s $rad(\mathbf{x})$. Očito je kako je radikal od $\mathbf{x}$ ideal.

Korolar 3. ([2], *str.* 417) *Element $a \in A$ nalazi se u radikalu ideala $\mathbf{x}$ ako i samo ako se on nalazi u svakom prostom idealu koji sadrži $\mathbf{x}$.*

Dokaz. Samo se primijeni Korolar 2. na prsten $A/\mathbf{x}$. □

Pogledajmo kako Korolar 2. možemo primijeniti i za module. Pretpostavimo da je S multiplikativni podskup od A. Ako je M modul, možemo definirati $S^{-1}M$ na način na koji smo definirali i $S^{-1}A$. Za $x \in M$ i $s \in S$ smatrat ćemo da je par (x, s) ekvivalentan paru (x', s') ako postoji $s_1 \in S$ takav da je $s_1(s'x - sx') = 0$. Klasu elemenata ekvivalentnih s (x, s) označimo s x/s. Ta je klasa zapravo aditivna grupa, odnosno $A-$modul s operacijom

$$(a, x/s) \mapsto ax/s.$$

Ovaj modul klasa ekvivalencije označit ćemo s $S^{-1}M$.
Ako je $\mathbf{p}$ prosti ideal u A, i S komplement od $\mathbf{p}$ u A, tada $S^{-1}M$ označavamo s $M_{\mathbf{p}}$. Ako je N podmodul od M, tada $S^{-1}N$ zapravo možemo promatrati kao podmodul od $S^{-1}M$. Neka je $x \in N$ i $s \in S$. Tada na x/s gledamo kao na element od $S^{-1}N$ ili $S^{-1}M$. Ako je $x/s = 0$ u $S^{-1}M$, tada postoji $s_1 \in S$ takav da je $s_1 x = 0$, pa je $x/s = 0$ i u $S^{-1}N$. Prema tome slijedi da je $N_{\mathbf{p}}$, uz pretpostavke da je N podmodul od M te da je $\mathbf{p}$ prost ideal, sadržan unutar $M_{\mathbf{p}}$. Zapravo ćemo $N_{\mathbf{p}}$ proučavati kao podmodul od $M_{\mathbf{p}}$. Uočavamo da je $M_{\mathbf{p}}$ suma svojih podmodula $(Ax)_{\mathbf{p}}$, za $x \in M$.

Definicija 22. ([3], *str.* 33) *Ako je R prsten, M $R-$modul te X podskup od M, tada anihilator skupa X označavamo s $Ann(X)$ i definiramo kao:*

$$Ann(X) = \{a \in R : ax = 0, x \in X\}.$$

Anihilator elementa x modula M je ideal koji se sastoji od elemenata $a \in A$ takvih da je $ax = 0$.

Lema 1. ([2], *str.* 418) *Neka je x element modula M, $\mathbf{a}$ njegov anihilator te neka je $\mathbf{p}$ prosti ideal od A. Tada $\mathbf{p}$ sadrži $\mathbf{a}$ ako i samo ako je $(Ax)_{\mathbf{p}} \neq 0$.*

Neka je $a \in A$ te M modul. Homomorfizam $x \mapsto ax$, za $x \in M$, nazivat ćemo glavni homomorfizam pridružen elementu a i označavat ćemo ga s a_M. Reći ćemo da je a_M lokalno nilpotentan ako za svaki $x \in M$ postoji cijeli broj $n_x \geq 1$ takav da je $a^{n_x} x = 0$. Ovo implicira da za svaki konačno generiran podmodul N od M postoji cijeli broj $n \geq 1$ takav da vrijedi $a^n x = 0$: uzimamo za n najveću potenciju od a koja anulira konačan skup generatora od N. Dakle, za konačno generiran M, vrijedi da je a_M lokalno nilpotentan ako i samo ako je nilpotentan.

Propozicija 10. ([2], *str.* 418) *Neka je M modul te $a \in A$. Tada je a_M lokalno nilpotentan ako i samo ako se a nalazi u svakom prostom idealu $\mathbf{p}$ za koji je $M_{\mathbf{p}} \neq 0$.*

Dokaz. Pretpostavimo da je a_M lokalno nilpotentan. Neka je $\mathbf{p}$ prosti ideal od A za koji je $M_{\mathbf{p}} \neq 0$. Tada postoji $x \in M$ takav da je $(Ax)_{\mathbf{p}} \neq 0$. Neka je n pozitivni cijeli broj za koji vrijedi $a^n x = 0$ te neka je $\mathbf{a}$ anihilator od x. Tada je $a^n \in A$ pa, primjenjujući Lemu 1. i Korolar 3., zaključujemo kako se a nalazi u svakom prostom idealu $\mathbf{p}$ za koji je $M_{\mathbf{p}} \neq 0$. Za dokaz druge implikacije pretpostavimo da a_M nije lokalno nilpotentan, pa postoji $x \in M$ takav da je $a^n x = 0$ za sve $n \geq 0$. Neka je $S = \{1, a, a^2, ...\}$, te koristeći Propoziciju 9. neka je $\mathbf{p}$ prosti ideal disjunktan sa S. Tada vrijedi $(Ax)_{\mathbf{p}} \neq 0$, pa je $M_{\mathbf{p}} \neq 0$ i $a \notin \mathbf{p}$ čime je tvrdnja dokazana. □

Definicija 23. ([2], *str.* 418) *Neka je M modul. Za prosti ideal* $\mathbf{p}$ *kažemo da je pridružen modulu M ako postoji* $x \in M$ *takav da je* $\mathbf{p}$ *njegov anihilator.*

Propozicija 11. ([2], *str.* 418) *Neka je M neprazan modul te neka je* $\mathbf{p}$ *maksimalan element u skupu ideala koji su anihilatori elemenata* $x_i \in M$, $x_i \neq 0$, *za sve* $i = 1, 2, ..., n$. *Tada je* $\mathbf{p}$ *prost ideal.*

Dokaz. Neka je $\mathbf{p}$ anihilator proizvoljnog $x_i \in M$, $x_i \neq 0$. Tada je $\mathbf{p} \neq A$. Neka su $a, b \in A$, $ab \in \mathbf{p}$ te $a \notin \mathbf{p}$. Tada vrijedi $ax \neq 0$, ali ideal $(b, \mathbf{p})$ anulira ax te sadrži $\mathbf{p}$. Kako je $\mathbf{p}$ maksimalan, slijedi da je $b \in \mathbf{p}$, pa je $\mathbf{p}$ prost. □

Korolar 4. ([2], *str.* 418) *Ako je A Noetherin te M neprazan modul, tada postoji prosti ideal pridružen modulu M.*

Dokaz. Skup ideala opisan u Propoziciji 11. je neprazan zbog pretpostavke da je M neprazan modul te ima maksimalan element zato što je A Noetherin. □

Korolar 5. ([2], *str.* 419) *Pretpostavimo da su A i M Noetherini te da je* $M \neq 0$. *Tada postoji niz podmodula*

$$M = M_1 \supset M_2 \supset ... \supset M_r = 0$$

takvih da je svaki kvocijentni modul M_i / M_{i+1} *izomorfan s* $A/\mathbf{p}_i$ *za neki prosti ideal* $\mathbf{p}_i$.

Dokaz. Skup podmodula opisanih u iskazu korolara nije prazan jer postoji prosti ideal $\mathbf{p}$ pridružen modulu M. Ako je $\mathbf{p}$ anihilator od x, tada vrijedi $Ax \approx A/\mathbf{p}$. Neka je N maksimalan element skupa podmodula. Ako je $N \neq M$, tada postoji podmodul N' od M koji sadrži N takav da je N'/N izomorfan s $A/\mathbf{p}$ za neki $\mathbf{p}$, što je u kontradikciji s pretpostavkom da je N maksimalan element. □

Propozicija 12. ([2], *str.* 419) *Neka je A Noetherin,* $a \in A$ *te M modul. Tada je* a_M *injekcija ako i samo ako se a ne nalazi ni u jednom prostom idealu pridruženom modulu M.*

Dokaz. Ako je a_M injekcija, tada se a ne može nalaziti niti u jednom prostom idealu pridruženom modulu M jer a ne anulira niti jedan element od M različit od 0. S druge strane, pretpostavimo da a_M nije injekcija, odnosno da vrijedi $ax = 0$ za neki $x \in M$, $x \neq 0$. Po Korolaru 4. postoji prosti ideal $\mathbf{p}$ pridružen Ax i vrijedi $a \in \mathbf{p}$ što dokazuje tvrdnju. □

Propozicija 13. ([2], *str.* 419) *Neka je A Noetherin, $a \in A$ te M modul. Sljedeće tvrdnje su ekvivalentne:*

(1) *a_M je lokalno nilpotentan.*

(2) *a se nalazi u svakom prostom idealu pridruženom M.*

(3) *a se nalazi u svakom prostom idealu $\mathbf{p}$ za koji je $M_\mathbf{p} \neq 0$.*

Ako je $\mathbf{p}$ prosti ideal za koji je $M_\mathbf{p} \neq 0$, tada $\mathbf{p}$ sadrži prosti ideal pridružen modulu M.

Dokaz. Za implikaciju (1) $\implies$ (2), koja je očita iz definicija, ne treba pretpostavka da je A Noetherin. Isto vrijedi i za implikaciju (3) $\implies$ (1) koja je dokazana u Propoziciji 10. Dokažimo implikaciju (2) $\implies$ (3) koja zapravo proizlazi iz zadnje tvrdnje. Neka je $\mathbf{p}$ prosti ideal za koji je $M_\mathbf{p} \neq 0$. Tada postoji $x \in M$ takav da je $(Ax)_\mathbf{p} \neq 0$. Po Korolaru 4., postoji prosti ideal $\mathbf{q}$ u A pridružen $(Ax)_\mathbf{p}$. Stoga, postoji element y/s iz $(Ax)_\mathbf{p}$, gdje je $y \in Ax$, $s \notin \mathbf{p}$ te $y/s \neq 0$, takvi da je $\mathbf{q}$ anihilator od y/s. Slijedi da je $\mathbf{q} \subset \mathbf{p}$, jer inače, postoji $b \in \mathbf{q}$, $b \notin \mathbf{p}$ te $0 = by/s$, odakle je $y/s = 0$ kontradikcija. Neka su $b_1, ..., b_n$ generatori za $\mathbf{q}$. Za svaki i, postoje $s_i \in A$, $s_i \notin \mathbf{p}$, takvi da vrijedi $s_i b_i y = 0$, zato što je $b_i y/s = 0$. Neka je $t = s_1 \cdots s_n$. Tada se trivijalno uočava da je $\mathbf{q}$ anihilator od ty u A, pa je $\mathbf{q} \subset \mathbf{p}$, što dokazuje tvrdnju. □

Skup svih prostih ideala $\mathbf{p}$ za koje je $M_\mathbf{p} \neq 0$ zvat ćemo nosač modula M i označavati sa $supp(M)$.

Skup svih prostih ideala pridruženih modulu M označavat ćemo s $ass(M)$.

S ovim oznakama, za konačno generiran modul M, možemo Propoziciju 13. sažeti i iskazati formulom:

$$rad(Ann(M)) = \bigcap_{\mathbf{p} \in supp(M)} \mathbf{p} = \bigcap_{\mathbf{p} \in ass(M)} \mathbf{p}.$$

Korolar 6. ([2], *str.* 420) *Neka je A Noetherin te M modul. Sljedeće tvrdnje su ekvivalentne:*

(1) *Postoji točno jedan prosti ideal pridružen modulu M.*

(2) *Modul M je neprazan te je za svaki $a \in A$ homomorfizam a_M injektivan ili lokalno nilpotentan.*

Ako su ove tvrdnje zadovoljene, tada je skup elemenata $a \in A$, takvih da je a_M lokalno nilpotentan, jednak prostom idealu pridruženom modulu M.

Dokaz. Tvrdnja je direktna posljedica Propozicije 12. te Propozicije 13. □

Propozicija 14. ([2], *str.* 420) *Neka je N podmodul od M. Svaki prosti ideal pridružen podmodulu N također je pridružen i modulu M. Prosti ideal pridružen modulu M pridružen je N ili M/N.*

Dokaz. Prva tvrdnja je očita. Kako bismo dokazali drugu tvrdnju, pretpostavimo da je $\mathbf{p}$ prost ideal pridružen modulu M koji je anihilator od $x \neq 0$. Ako vrijedi $Ax \cap N = 0$, tada je Ax izomorfan podmodulu od M/N, pa je $\mathbf{p}$ pridružen M/N. Pretpostavimo da je $Ax \cap N \neq 0$. Neka je $y = ax \in N$ takav da je $a \in A$ te $y \neq 0$. Tada $\mathbf{p}$ anulira y. Tvrdimo da je $\mathbf{p} = Ann(y)$. Neka je $b \in A$ i $by = 0$. Tada je $ba \in \mathbf{p}$, ali $a \notin \mathbf{p}$, pa je $b \in \mathbf{p}$. Stoga je $\mathbf{p}$ anihilator od y u A, pa je $\mathbf{p}$ pridružen N. □

3.3 Primarna dekompozicija

U ovome poglavlju i dalje ćemo pretpostavljati da je A komutativan prsten i da su moduli(homomorfizmi) $A-$moduli($A-$homomorfizmi), osim ako je drugačije označeno.

Definicija 24. ([2], *str.* 421) *Neka je M modul. Za podmodul Q od M reći ćemo da je primaran ako je $Q \neq M$, te ako je za dani $a \in A$, homomorfizam $a_{M/Q}$ ili injektivan ili nilpotentan.*

Ideal $\mathbf{q}$ je primaran ako i samo ako zadovoljava sljedeći uvjet:

Ako su dani $a, b \in A$, $ab \in \mathbf{q}$ te $a \notin \mathbf{q}$, tada je $b^n \in \mathbf{q}$ za neki $n \geq 1$.

Neka je Q primaran i neka je $\mathbf{p}$ ideal elemenata $a \in A$ takvih da je $a_{M/Q}$ nilpotentan. Tada je $\mathbf{p}$ prost ideal. Pretpostavimo da su $a, b \in A$, $ab \in \mathbf{p}$ i $a \notin \mathbf{p}$. Tada je $a_{M/Q}$ injektivan, i posljedično je $a^n_{M/Q}$ injektivan za sve $n \geq 1$. S obzirom da je $(ab)_{M/Q}$ nilpotentan, slijedi da $b_{M/Q}$ mora biti nilpotentan, pa je $b \in \mathbf{p}$ te je dokazano da je $\mathbf{p}$ prost. Reći ćemo da je $\mathbf{p}$ prosti ideal koji pripada Q, odnosno možemo reći i da je Q $\mathbf{p}-$primaran.
Primjećujemo odgovarajuće svojstvo za primarni modul Q s prostim idealom $\mathbf{p}$:

Neka su $b \in A$ i $x \in M$ takvi da je $bx \in Q$. Ako $x \notin Q$, tada je $b \in \mathbf{p}$.

Primjer 6. ([2], *str.* 421) *Neka je* $\mathbf{m}$ *maksimalni ideal od A, a neka je* $\mathbf{q}$ *ideal od A takav da vrijedi* $\mathbf{m}^k \subseteq \mathbf{q}$ *za neki pozitivan cijeli broj k. Tada je* $\mathbf{q}$ *primaran ideal, a* $\mathbf{m}$ *pripada* $\mathbf{q}$.

Gornji zaključak nije uvijek točan ako se $\mathbf{m}$ *zamijeni nekim prostim idealom* $\mathbf{p}$. *Na primjer, neka je R faktorijalni prsten s prostim elementom t. Definirajmo prsten A kao podprsten polinoma $f(X) \in R[X]$ takvih da vrijedi:*

$$f(X) = a_0 + a_1X + \dots$$

pri čemu je a_1 djeljiv s t. Definirajmo $\mathbf{p} = (tX, X^2)$. *Tada je* $\mathbf{p}$ *prost, ali:*

$$\mathbf{p}^2 = (t^2X^2, tX^3, X^4)$$

nije primaran ideal, što vidimo jer $X^2 \notin \mathbf{p}^2$, *ali* $t^k \notin \mathbf{p}^2$ *za sve* $k \geq 1$, *iako je* $t^2X^2 \in \mathbf{p}^2$.

Propozicija 15. ([2], *str.* 421) *Neka je M modul te $Q_1, ..., Q_r$ podmoduli koji su* $\mathbf{p}-$*primarni za isti prosti ideal* $\mathbf{p}$. *Tada je $Q_1 \cap \cdots \cap Q_r$ također* $\mathbf{p}-$*primaran.*

Dokaz. Neka je $Q = Q_1 \cap \cdots \cap Q_r$ te neka je $a \in \mathbf{p}$. Neka je n_i takav da je $(a_{M/Q_i})^{n_i} = 0$, za sve $i = 1, ..., r$, te neka je n maksimum od $n_1, ..., n_r$. Tada je $a^n_{M/Q} = 0$, tako da je $a_{M/Q}$ nilpotentan. Obratno, pretpostavimo da $a \notin \mathbf{p}$. Neka je $x \in M$, $x \notin Q_j$, za neki j. Tada za sve prirodne brojeve n vrijedi $a^n x \notin Q_j$, pa je posljedično $a_{M/Q}$ injektivan. Time je propozicija dokazana. □

Neka je N podmodul modula M. Kada se N izrazi kao konačan presjek primarnih podmodula, recimo $N = Q_1 \cap \cdots \cap Q_r$, taj izraz nazvat ćemo primarna dekompozicija modula N. Koristeći Propoziciju 15., možemo zaključiti da grupiranjem Q_i prema njihovim prostim idealima možemo iz postojeće primarne dekompozicije uvijek dobiti novu dekompoziciju gdje su prosti ideali koji pripadaju primarnim međusobno različiti. Primarnu dekompoziciju opisanog oblika, gdje su prosti ideali $p_1, \ldots, p_r$ koji pripadaju $Q_1, \ldots, Q_r$ međusobno različiti, i gdje se N ne može izraziti kao presjek prave podfamilije primarnih ideala $\{Q_1, \ldots, Q_r\}$, nazivamo reduciranom. Uklanjanjem nekih od primarnih modula iz određene dekompozicije, možemo vidjeti da, ako N ima neku primarnu dekompoziciju, onda ima i reduciranu. Dokazat ćemo rezultat koji daje određena svojstva jedinstvenosti reducirane primarne dekompozicije.

Neka je N podmodul od M i neka je $x \mapsto \bar{x}$ kanonski homomorfizam. Neka $\overline{Q}$ bude podmodul od $\overline{M} = M/N$ i neka Q bude njegova inverzna slika u M. Tada se, izravno iz definicije, može vidjeti da je $\overline{Q}$ primarni podmodul ako i samo ako je Q primarni; a ako su oni primarni, tada prosti ideal koji pripada Q također pripada i $\overline{Q}$. Nadalje, ako je $N = Q_1 \cap \cdots \cap Q_r$ primarna dekompozicija N u M, tada

$$(0) = \overline{Q}_1 \cap \cdots \cap \overline{Q}_r$$

predstavlja primarnu dekompoziciju nule u $\overline{M}$, što se lako može zaključiti iz definicija. Također, dekompozicija od N je reducirana ako i samo ako je dekompozicija nule reducirana, budući da su prosti ideali koji pripadaju $\overline{Q}$ isti kao i oni koji pripadaju Q.

Neka $Q_1 \cap \cdots \cap Q_r$ bude reducirana primarna dekompozicija, i neka $\mathbf{p_i}$ pripada Q_i. Ako $\mathbf{p_i}$ ne sadrži $\mathbf{p_j}$ $(j \neq i)$, tada kažemo da je $\mathbf{p_i}$ izoliran. Dakle, izolirani prosti ideali su minimalni u skupu prostih ideala koji pripadaju primarnim modulima Q_i.

Teorem 2. ([2], *str.* 422) *Neka je N podmodul od M, te neka je dodatno*

$$N = Q_1 \cap \cdots \cap Q_r = Q'_1 \cap \cdots \cap Q'_s$$

reducirana primarna dekompozicija podmodula N. Tada je $r = s$. Skup prostih ideala koji pripada $Q_1, \ldots, Q_r$, jednak je skupu pripadajućih ideala od $Q'_1, \ldots, Q'_s$. Ako je $\{p_1, \ldots, p_m\}$ skup izoliranih prostih ideala koji pripadaju ovim dekompozicijama, tada je $Q_i = Q'_i$ za $i = 1, \ldots, m$. Drugim riječima, primarni moduli koji odgovaraju izoliranim prostim idealima jednoznačno su određeni.

Dokaz. Jedinstvenost broja članova u reduciranoj dekompoziciji, kao i jedinstvenost skupa prostih ideala koji pripadaju komponentama primarne dekompozicije, bit će posljedica Teorema 3. niže. Preostaje još dokazati jedinstvenost primarnog modula koji pripada izoliranom prostom idealu, kojeg možemo označiti s $\mathbf{p_1}$. Po definiciji, za svaki $j = 2, \dots, r$, postoji $a_j \in \mathbf{p_j}$, ali $a_j \notin \mathbf{p_1}$. Neka je $a = a_2 \cdots a_r$ produkt. Tada je $a \in \mathbf{p_j}$ za sve $j > 1$, ali $a \notin \mathbf{p_1}$. Možemo naći neki cijeli broj $n \geq 1$ takav da je $a^n_{M/Q_j} = 0$ za sve $j = 2, \dots, r$.
Definirajmo N_1 kao skup svih $x \in M$ takvih da vrijedi $a^n x \in N$.
Tvrdnja $Q_1 = N_1$ dokazat će traženu jedinstvenost. Neka je $x \in Q_1$. Tada vrijedi $a^n x \in Q_1 \cap \cdots \cap Q_r = N$, pa je $x \in N_1$. Obrnuto, neka je $x \in N_1$, tako da je $a^n x \in N$, a posebno $a^n x \in Q_1$. Budući da $a \notin \mathbf{p_1}$, znamo po definiciji da je a_{M/Q_1} injektivna. Prema tome je $x \in Q_1$, čime je teorem dokazan. ☐

Teorem 3. ([2], *str.* 423) *Neka je M Noetherin modul. Ako N predstavlja podmodul od M, tada N dopušta primarnu dekompoziciju.*

Dokaz. Promotrimo skup svih podmodula od M koji ne dopuštaju primarnu dekompoziciju. Ako je taj skup neprazan, sadrži maksimalan element, budući da je M Noetherin modul. Neka je N taj maksimalni element. Tada N nije primaran, i postoji element $a \in A$ takav da $a_{M/N}$ nije niti injektivan niti nilpotentan. Rastući niz modula definiran s

$$Ker\ a_{M/N} \subseteq Ker\ a^2_{M/N} \subseteq Ker\ a^3_{M/N} \subseteq \dots$$

zaustavlja se, recimo na $Ker\ a^k_{M/N}$. Neka je $\varphi : M/N \to M/N$ endomorfizam $\varphi = a^k_{M/N}$. Tada je $Ker\ \varphi^2 = Ker\ \varphi$. Dakle, $0 = Ker\ \varphi \cap Im\ \varphi$ u M/N, a niti jezgra niti slika od φ nisu nula. Uzimajući inverznu sliku u M, vidimo da N predstavlja presjek dvaju podmodula od M, koji nisu jednaki N. Zaključujemo iz maksimalnosti od N da svaki od tih podmodula dopušta primarnu dekompoziciju, i stoga N također dopušta jednu, što je kontradikcija. ☐

Proučimo sada vezu između prostih ideala koji pripadaju primarnoj dekompoziciji te pridruženih prostih ideala iz prethodnog poglavlja.

Propozicija 16. ([2], *str.* 423) *Neka su A i M Noetherini moduli. Podmodul Q modula M je primaran ako i samo ako M/Q ima točno jedan pridruženi prosti ideal* $\mathbf{p}$, *i u tom slučaju,* $\mathbf{p}$ *pripada Q, to jest Q je* $\mathbf{p}$*-primaran.*

Dokaz. Slijedi izravno iz definicija i Korolara 6. ☐

Teorem 4. ([2], *str.* 423) *Neka su A i M Noetherini. Prosti ideali pridruženi modulu M su upravo oni prosti ideali koji pripadaju primarnim modulima u reduciranoj primarnoj dekompoziciji nule u M. Konkretno, skup pridruženih prostih ideala modula M je konačan.*

Dokaz. Neka je

$$0 = Q_1 \cap \cdots \cap Q_r$$

reducirana primarna dekompozicija nultog podmodula u M.

Imamo injektivni homomorfizam

$$M \to \bigoplus_{i=1}^{r} M/Q_i.$$

Prema Propozicijama 14. i 16., zaključujemo da svaki prosti ideal pridružen M pripada nekom od Q_i. Obrnuto, neka je $N = Q_2 \cap \cdots \cap Q_r$. Tada $N \neq 0$, jer je naša dekompozicija reducirana. Imamo

$$N = N/(N \cap Q_1) \approx (N + Q_1)/Q_1 \subseteq M/Q_1.$$

Prema tome, N je izomorfan podmodulu od M/Q_1, što znači da N ima pridruženi prosti ideal koji ne može biti nijedan drugi osim $\mathbf{p_1}$, koji pripada Q_1. Time je teorem dokazan. □

Teorem 5. ([2], *str.* 424) *Neka je A Noetherin prsten. Tada je skup djelitelja nule u A unija svih prostih ideala koji pripadaju primarnim idealima u reduciranoj primarnoj dekompoziciji nule.*

Dokaz. Element $a \in A$ djelitelj je nule ako i samo ako a_A nije injektivno. Prema Propoziciji 12., to je ekvivalentno činjenici da a pripada nekom pridruženom prostom idealu od A (gledanom kao modul nad samim sobom). Primjena Teorema 4. zaključuje dokaz. □

3.4 Nakayamina lema

Označimo s A komutativni prsten, koji ne mora biti Noetherin. Prilikom rada s modulima nad prstenom, često možemo prvo lokalizirati kako bismo smanjili probleme na module nad lokalnim prstenima, odnosno prstenima koji imaju jedinstven maksimalan ideal. U ovom kontekstu, ti moduli bit će konačno generirani. Ovdje ćemo pokazati da se određeni aspekti mogu svesti na vektorske prostore nad poljem, koristeći redukciju modulo maksimalan ideal u lokalnom prstenu. Modul nad poljem uvijek posjeduje bazu. Pokušavamo proširiti ovo svojstvo na module koji su konačno generirani nad lokalnim prstenom. Prve tri tvrdnje koje slijede poznate su kao Nakayamina lema.

Lema 2. ([2], *str.* 424) *Neka je $\mathbf{a}$ ideal od A koji je sadržan u svakom maksimalnom idealu od A. Neka je E konačno generiran $A-$modul te neka vrijedi $\mathbf{a}E = E$. Tada je $E = \{0\}$.*

Dokaz. Koristimo indukciju prema broju generatora od E. Neka su $x_1, \ldots, x_s$ generatori za E. Po pretpostavci, postoje elementi $a_1, \ldots, a_s \in \mathbf{a}$ takvi da je
$x_s = a_1x_1 + \cdots + a_sx_s$, pa možemo zaključiti da postoji element a takav da se $(1 + a)x_s$ nalazi u modulu generiranom s prva $s - 1$ generatora. Nadalje, $1 + a$ je jedinica u A ili je dio maksimalnog ideala, a budući da je a u svakom maksimalnom idealu, slijedi da se jedinica nalazi u maksimalnom idealu, što nije moguće. Dakle, x_s sam pripada modulu generiranom sa $s - 1$ generatora, što dovršava induktivni postupak. □

Posebno, Lema 2. vrijedi i u slučaju kada je A lokalni prsten, a $\mathbf{a} = \mathbf{m}$ maksimalni je ideal.

Lema 3. ([2], *str.* 425) *Neka je A lokalni prsten, a E konačno generiran A-modul i F podmodul. Ako je $E = F + \mathbf{m}E$, tada je $E = F$.*

Dokaz. Provodi se primjenom Leme 2. na E/F. □

Lema 4. ([2], *str.* 425) *Neka je A lokalni prsten, a E konačno generiran A-modul. Ako su $x_1, \dots, x_n$ generatori od $E/\mathbf{m}E$, tada su oni generatori i od E.*

Neka je E modul nad lokalnim prstenom A s maksimalnim idealom $\mathbf{m}$. Definirajmo
$E(\mathbf{m}) = E/\mathbf{m}E$. Ako je $f : E \to F$ homomorfizam, tada f inducira homomorfizam

$$f_{(\mathbf{m})} : E(\mathbf{m}) \to F(\mathbf{m}).$$

Ako je f surjektivno, tada trivijalno slijedi da je $f_{(\mathbf{m})}$ surjektivno.

Nakayamina lema naglašava zašto je korisno raditi nad lokalnim prstenom. Stoga je korisno svesti pitanja o općim prstenima na pitanja o lokalnim prstenima. Pogledajmo još neke tvrdnje koje proizlaze iz Nakayamine leme te ih nećemo dokazivati.

Kažemo da je modul slobodan ako ima bazu, odnosno ako postoji linearno nezavisan skup koji ga generira. Posebno, svaki vektorski prostor je modul.

Lema 5. ([2], *str.* 426) *Neka je $f : E \to F$ homomorfizam modula, konačno generiranih nad lokalnim prstenom A. Tada vrijede sljedeće tvrdnje:*

(1) *Ako je $f_{(m)}$ surjektivno, tada je i f surjektivno.*

(2) *Pretpostavimo da je f injektivno. Ako je $f_{(m)}$ surjektivno, tada je f izomorfizam.*

(3) *Pretpostavimo da su E i F slobodni. Ako je $f_{(m)}$ injektivno (izomorfizam), tada je f injektivno (izomorfizam).*

3.5 Filtrirani i gradirani moduli

Neka je A komutativan prsten, a E modul nad prstenom A. Filtracijom modula E nazivamo niz podmodula

$$E = E_0 \supseteq E_1 \supseteq E_2 \supseteq \cdots \supseteq E_n \supseteq \dots$$

Tehnički gledano, ovo bismo trebali nazvati silaznom filtracijom, ali kako razmatramo samo takvu, dovoljno je reći filtracija.

Primjer 7. ([2], *str.* 426) *Neka je $\mathbf{a}$ ideal u prstenu A, a E modul nad A. Definirajmo*

$$E_n = \mathbf{a}^n E.$$

Tada niz podmodula $\{E_n\}$ čini filtraciju modula E.

Općenitije, neka je $\{E_n\}$ bilo koja filtracija modula E. Kažemo da je to **a**-filtracija ako vrijedi $\mathbf{a}E_n \subseteq E_{n+1}$ za sve n. Prethodni je primjer upravo primjer **a**-filtracije. Kažemo da je **a**-filtracija **a**-stabilna ili samo stabilna, ako vrijedi $\mathbf{a}E_n = E_{n+1}$ za sve dovoljno velike n.

Propozicija 17. ([2], *str.* 427) *Ako su* $\{E_n\}$ *i* $\{E'_n\}$ *stabilne* **a**-*filtracije skupa* E*, tada postoji pozitivan cijeli broj* d *takav da vrijedi:*

$$E_{n+d} \subseteq E'_n \quad i \quad E'_{n+d} \subseteq E_n$$

za sve $n \geq 0$.

Dokaz. Dovoljno je dokazati propoziciju za slučaj kada je $E'_n = \mathbf{a}^n E$. Kako vrijedi $\mathbf{a}E_n \subseteq E_{n+1}$ za svaki n, imamo da je $\mathbf{a}^n E \subseteq E_n$. S obzirom na pretpostavku stabilnosti, postoji d takav da je:

$$E_{n+d} = \mathbf{a}^n E_d \subseteq \mathbf{a}^n E,$$

što dokazuje propoziciju. □

Prsten A nazivamo gradiranim ako se može zapisati kao direktna suma (kao Abelova grupa):

$$A = \bigoplus_{n=0}^{\infty} A_n,$$

tako da za sve cijele brojeve m, $n \geq 0$ vrijedi $A_n A_m \subseteq A_{n+m}$. Iz toga slijedi da je A_0 podprsten, i svaka komponenta A_n je A_0-modul.

Neka je A gradirani prsten. Modul E nazivamo gradiranim ako se može izraziti kao direktna suma (kao Abelova grupa)

$$E = \bigoplus_{n=0}^{\infty} E_n,$$

tako da je $A_n E_m \subseteq E_{n+m}$. Konkretno, skup E_n je A_0-modul. Za elemente takvog skupa E_n reći ćemo da su homogeni stupnja n. Prema definiciji, svaki element skupa E može se jedinstveno zapisati kao konačna suma homogenih elemenata.

Primjer 8. ([2], *str.* 427) *Neka je* k *polje, i neka su* $X_0, \ldots, X_r$ *nezavisne varijable. Prsten polinoma* $A = k[X_0, \ldots, X_r]$ *gradirana je algebra, gdje je* $k = A_0$*. Homogeni elementi stupnja* n *su polinomi generirani monomima u* $X_0, \ldots, X_r$ *stupnja* n*, to jest*

$$X_0^{d_0} \cdots X_r^{d_r}, \quad \textit{pri čemu vrijedi} \quad \sum_{i=0}^{r} d_i = n.$$

Ideal I od A naziva se homogenim ako je gradiran kao A-modul. U tom slučaju, kvocijentni prsten A/I također je gradirani prsten.

Teorem 6. ([1], *str.* 160) (*Hilbertov teorem*) *Ako je prsten* R *Noetherin, tada je svaki prsten polinoma konačno generiran nad* R *također Noetherin.*

Propozicija 18. ([2], *str.* 427) *Neka je A gradirani prsten. Prsten A je Noetherin ako i samo ako je A_0 Noetherin, te ako je A konačno generiran kao A_0-algebra.*

Dokaz. Algebra konačno generirana nad Noetherinim prstenom također je Noetherina, jer je homomorfna slika prstena polinoma u konačno mnogo varijabli, pa se može primijeniti Hilbertov teorem.

S druge strane, pretpostavimo da je A Noetherin. Suma

$$A^+ = \bigoplus_{n=1}^{\infty} A_n$$

ideal je od A, čiji je kvocijentni prsten A_0, koji je homomorfna slika od A, i stoga Noetherin. Nadalje, prema pretpostavci A^+ ima konačan broj generatora $x_1, \ldots, x_s$. Izražavanjem svakog generatora kao sume homogenih elemenata, možemo bez smanjenja općenitosti pretpostaviti da su ti generatori homogeni, s odgovarajućim stupnjevima $d_1, \ldots, d_s$, gdje su svi $d_i > 0$. Neka je B podprsten od A generiran nad A_0 s $x_1, \ldots, x_s$. Tvrdimo da je $A_n \subseteq B$ za sve n. Ovo je sigurno točno za $n = 0$. Neka je $n > 0$ i neka je x homogeni element stupnja n. Tada postoje elementi $a_i \in A_{n-d_i}$ takvi da vrijedi

$$x = \sum_{i=1}^{s} a_i x_i.$$

Budući da su induktivno $d_i > 0$, svaki se a_i nalazi u $A_0[x_1, \ldots, x_s] = B$, što pokazuje da je $x \in B$, čime završava dokaz. □

Sada ćemo vidjeti dva načina konstrukcije gradiranih prstena iz filtracija.

Prvo, neka je A prsten i neka je $\mathbf{a}$ ideal. Promatramo A kao filtrirani prsten s obzirom na potencije $\mathbf{a}^n$. Definiramo prvi pridruženi gradirani prsten kao

$$S_{\mathbf{a}}(A) = S = \bigoplus_{n=0}^{\infty} \mathbf{a}^n.$$

Slično, ako je E $A-$modul te je filtriran $\mathbf{a}$-filtracijom $\{E_n\}$, definiramo

$$E_S = \bigoplus_{n=0}^{\infty} E_n.$$

Odmah se može provjeriti da je E_S gradirani $S-$modul.

Primijetimo da, ako je A Noetherin, i ako je $\mathbf{a}$ generiran elementima $x_1, \ldots, x_s$, tada je S generiran kao $A-$algebra također elementima $x_1, \ldots, x_s$, te je stoga također Noetherin.

Lema 6. ([2], *str.* 428) *Neka je A Noetherin prsten, i neka je E konačno generiran modul s $\mathbf{a}$-filtracijom. Tada je E_S konačan nad S ako i samo ako je filtracija modula E $\mathbf{a}$-stabilna.*

Dokaz. Neka je

$$F_n = \bigoplus_{i=0}^{n} E_i,$$

te neka vrijedi

$$G_n = E_0 \oplus E_1 \oplus \cdots \oplus E_n \oplus \mathbf{a}E_n \oplus \mathbf{a}^2E_n \oplus \mathbf{a}^3E_n \oplus \ldots$$

Tada je G_n podmodul od E_S, i konačan je nad S jer je F_n konačan nad A. Imamo:

$$G_n \subset G_{n+1} \quad \text{i} \quad \bigcup G_n = E_S.$$

Budući da je S Noetherin, slijedi:

$$\begin{aligned} E_S \text{ je konačan nad } S &\iff E_S = G_N \text{ za neki } N \\ &\iff E_{N+m} = a^m E_N \text{ za sve } m \geq 0 \\ &\iff \text{filtracija modula } E \text{ je } \mathbf{a}-\text{stabilna.} \end{aligned}$$

Ovime je lema dokazana. □

Teorem 7. ([2], str. 429)(*Artin-Rees*) *Neka je A Noetherin prsten,* $\mathbf{a}$ *ideal, a E konačan* $A-$*modul s* $\mathbf{a}-$*stabilnom filtracijom. Neka je F podmodul, i neka vrijedi* $F_n = F \cap E_n$*. Tada je* $\{F_n\}$ $\mathbf{a}-$*stabilna filtracija od F.*

Dokaz. Imamo:

$$\mathbf{a}(F \cap E_n) \subseteq \mathbf{a}F \cap \mathbf{a}E_n \subseteq F \cap E_{n+1},$$

pa je $\{F_n\}$ $\mathbf{a}-$filtracija od F. Možemo sada formirati pridruženi gradirani $S-$modul F_S, koji je podmodul od E_S i konačan je nad S budući da je S Noetherin. Primjenjujemo Lemu 6. kako bismo zaključili dokaz. □

Ponovno formuliramo Artin-Reesov teorem u njegovom izvornom obliku kako slijedi:

Korolar 7. ([2], str. 429) *Neka je A Noetherin prsten, E konačan* $A-$*modul te F podmodul. Neka je* $\mathbf{a}$ *ideal. Postoji cijeli broj s takav da za sve cijele brojeve* $n \geq s$ *imamo:*

$$\mathbf{a}^n E \cap F = \mathbf{a}^{n-s}(\mathbf{a}^s E \cap F).$$

Dokaz. Tvrdnja je poseban slučaj Teorema 7. i definicija. □

Teorem 8. ([2], str. 429)(*Krullov teorem*) *Neka je A Noetherin prsten, i neka je* $\mathbf{a}$ *ideal sadržan u svakom maksimalnom idealu od A. Neka je E konačan* $A-$*modul. Tada vrijedi:*

$$\bigcap_{n=1}^{\infty} \mathbf{a}^n E = 0.$$

Dokaz. Neka je $F = \bigcap \mathbf{a}^n E$. Primjenom Nakayamine leme slijedi dokaz. □

Korolar 8. ([2], *str.* 430) *Neka je A lokalni Noetherin prsten s maksimalnim idealom* **m**. *Tada vrijedi:*

$$\bigcap_{n=1}^{\infty} m^n = 0.$$

Dokaz. Dokaz je poseban slučaj Teorema 8. kada je $E = A$. □

Sada ćemo navesti drugi način konstrukcije gradiranog prstena ili modula. Neka je A prsten i $\mathbf{a}$ ideal od A. Definiramo drugi pridruženi gradirani prsten na sljedeći način:

$$\mathrm{gr}_{\mathbf{a}}(A) = \bigoplus_{n=0}^{\infty} \mathbf{a}^n / \mathbf{a}^{n+1}.$$

Množenje je definirano na očit način. Neka je $a \in \mathbf{a}^n$ i neka $\bar{a}$ označava njegovu klasu ostataka modulo $\mathbf{a}^{n+1}$. Neka je $b \in \mathbf{a}^m$ i neka $\bar{b}$ označava njegovu klasu ostataka modulo $\mathbf{a}^{m+1}$. Definiramo umnožak $\bar{a}\bar{b}$ kao klasu ostataka od ab modulo $\mathbf{a}^{m+n+1}$. Lako je provjeriti da je ova definicija neovisna o izboru predstavnika klase te definira množenje na $\mathrm{gr}_{\mathbf{a}}(A)$ koje $\mathrm{gr}_{\mathbf{a}}(A)$ čini gradiranim prstenom.

Neka je E filtrirani $A-$modul. Definiramo:

$$\mathrm{gr}(E) = \bigoplus_{n=0}^{\infty} E_n / E_{n+1}.$$

Ako je filtracija $\mathbf{a}-$filtracija, tada je $\mathrm{gr}(E)$ gradirani $\mathrm{gr}_{\mathbf{a}}(A)-$modul.

Propozicija 19. ([2], *str.* 430) *Pretpostavimo da je A Noetherin prsten, i neka je* **a** *ideal od A. Tada je $gr_{\mathbf{a}}(A)$ Noetherin. Ako je E konačni $A-$modul sa stabilnom* **a**$-$*filtracijom, tada je $gr(E)$ konačni $gr_{\mathbf{a}}(A)-$modul.*

Dokaz. Neka su $x_1, \ldots, x_s$ generatori ideala $\mathbf{a}$. Neka je $\bar{x}_i$ klasa ostataka od x_i u $\mathbf{a}/\mathbf{a}^2$. Tada je

$$\mathrm{gr}_{\mathbf{a}}(A) = (A/\mathbf{a})[\bar{x}_1, \ldots, \bar{x}_s]$$

Noetherin, čime je dokazan prvi dio tvrdnje. U drugom dijelu, za neki d imamo:

$$E_{d+m} = \mathbf{a}^m E_d \quad \text{za sve} \quad m \geq 0.$$

Stoga je $\mathrm{gr}(E)$ generiran konačnom direktnom sumom

$$\mathrm{gr}(E)_0 \oplus \cdots \oplus \mathrm{gr}(E)_d.$$

No, svaki je $\mathrm{gr}(E)_n = E_n / E_{n+1}$ konačno generiran nad A, i anulira ga $\mathbf{a}$, pa je to konačni $A/\mathbf{a}-$modul. Stoga je gornja direktna suma konačni $A/\mathbf{a}-$modul. Dakle, $\mathrm{gr}(E)$ je konačni $\mathrm{gr}_{\mathbf{a}}(A)-$modul, čime završavamo dokaz propozicije. □

3.6 Hilbertov polinom

U ovome poglavlju proučit ćemo duljine određenih filtriranih modula nad lokalnim prstenima i pokazati da su one polinomi u odgovarajućim slučajevima. Međutim, najprije ćemo se osvrnuti na gradirane module, a zatim povezati filtrirane module s gradiranim koristeći konstrukciju iz prethodnog poglavlja.

Započnimo s gradiranim Noetherinim prstenom zajedno s konačnim gradiranim $A-$modulom E, pa vrijedi:

$$A = \bigoplus_{n=0}^{\infty} A_n \quad \text{i} \quad E = \bigoplus_{n=0}^{\infty} E_n.$$

Već smo u Propoziciji 18. vidjeli da je A_0 Noetherin prsten te da je A konačno generirana A_0-algebra. Slično, uočavamo da E ima konačan broj homogenih generatora te da je E_n konačan A_0-modul za sve $n \geq 0$.

Neka je φ preslikavanje koje modulima pridružuje element Abelove grupe. Ako je niz $0 \to M' \to M \to M'' \to 0$ egzaktan, tada je $\varphi(M)$ definiran ako i samo ako su definirani $\varphi(M')$ i $\varphi(M'')$, a u tom slučaju imamo

$$\varphi(M) = \varphi(M') + \varphi(M'').$$

Nadalje, $\varphi(0)$ je definiran i jednak je 0.
Takvo pravilo φ nazivat ćemo Euler-Poincaréovo preslikavanje na A-modulima.

Neka je φ Euler-Poincaréova funkcija s vrijednostima u $\mathbb{Z}$ na klasi svih konačnih A_0-modula. Definiramo Poincaréov red s obzirom na φ kao red potencija

$$P_\varphi(E,t) = \sum_{n=0}^{\infty} \varphi(E_n) t^n \in \mathbb{Z}[[t]].$$

Zbog jednostavnosti pišemo $P(E,t)$ umjesto $P_\varphi(E,t)$.

Teorem 9. ([2], *str.* 431)(*Hilbert-Serre*) *Neka s označava broj generatora prstena A kao A_0-algebre. Tada je $P(E,t)$ racionalna funkcija oblika*

$$P(E,t) = \frac{f(t)}{\prod_{i=1}^{s}(1-t^{d_i})},$$

gdje su d_i odgovarajući pozitivni cijeli brojevi, a $f(t) \in \mathbb{Z}[t]$.

Dokaz. Dokaz provodimo indukcijom po s. Za $s = 0$ tvrdnja je očigledna. Neka je $s \geq 1$. Neka je $A = A_0[x_1, \dots, x_s]$, pri čemu je d_i stupanj od x_i, $d_i \geq 1$. Množenje s x_s na E daje egzaktni niz

$$0 \to K_n \to E_n \xrightarrow{x_s} E_{n+d_s} \to L_{n+d_s} \to 0.$$

Neka su

$$K = \bigoplus K_n \quad i \quad L = \bigoplus L_n.$$

Tada su K i L konačni $A-$moduli (budući da su podmoduli i kvocijentni moduli od E), te ih anulira x_s, pa su zapravo gradirani $A_0[x_1, \dots, x_{s-1}]-$moduli.

Prema definiciji Euler-Poincaréove funkcije, slijedi

$$\varphi(K_n) - \varphi(E_n) + \varphi(E_{n+d_s}) - \varphi(L_{n+d_s}) = 0.$$

Množenjem s t^{n+d_s} i sumiranjem po n dobivamo

$$(1 - t^{d_s})P(E,t) = P(L,t) - t^{d_s}P(K,t) + g(t),$$

gdje je $g(t)$ polinom u $\mathbb{Z}[t]$. Tvrdnja slijedi induktivno. □

Sljedeći teorem govori o slučaju kada vrijedi $d_i = 1$, za svaki i.

Teorem 10. ([2], *str.* 432) *Pretpostavimo da je A generiran kao A_0-algebra pomoću homogenih elemenata stupnja* 1*. Neka je d red pola funkcije $P(E,t)$ u $t = 1$. Tada je za dovoljno velike n, $\varphi(E_n)$ polinom varijable n stupnja $d - 1$. (Za ovu se tvrdnju pretpostavlja da nulti polinom ima stupanj -1.)*

Dokaz. Prema Teoremu 9., $\varphi(E_n)$ je koeficijent uz t^n u racionalnoj funkciji

$$P(E,t) = \frac{f(t)}{(1-t)^s}.$$

Poništavanjem potencija od $1 - t$, imamo $P(E,t) = \frac{h(t)}{(1-t)^d}$, gdje je $h(1) \neq 0$, a $h(t) \in \mathbb{Z}[t]$. Neka je

$$h(t) = \sum_{k=0}^{m} a_k t^k.$$

Imamo binomni razvoj

$$(1-t)^{-d} = \sum_{k=0}^{\infty} \binom{d+k-1}{d-1} t^k.$$

Radi jednostavnosti, definiramo $\binom{n}{-1} = 0$ za $n \geq 0$ i $\binom{n}{-1} = 1$ za $n = -1$. Tada je

$$\varphi(E_n) = \sum_{k=0}^{m} a_k \binom{d+n-k-1}{d-1} \quad \text{za sve } n \geq m.$$

Suma na desnoj strani polinom je varijable n čiji je vodeći član

$$\left(\sum a_k\right) \frac{n^{d-1}}{(d-1)!} \neq 0.$$

Ovime je teorem dokazan.

□

Polinom iz Teorema 10. nazivamo Hilbertov polinom gradiranog modula E u odnosu na funkciju φ. Sada ćemo povezati rezultate iskazane u ovome poglavlju te primijeniti Teorem 10. na određene filtrirane module.

Neka je A Noetherin lokalni prsten s maksimalnim idealom $\mathbf{m}$. Neka je $\mathbf{q}$ $\mathbf{m}-$primarni ideal. Tada je $A/\mathbf{q}$ također Noetherin i lokalni prsten. Kako je neka potencija od $\mathbf{m}$ sadržana u $\mathbf{q}$, slijedi da je $\mathbf{m}/\mathbf{q}$ jedini pridruženi prosti ideal u $A/\mathbf{q}$, gledan kao modul nad samim sobom. Slično, ako je M konačan $A/\mathbf{q}-$modul, tada M ima samo jedan pridruženi prosti ideal, a jedini jednostavan $A/\mathbf{q}-$modul je zapravo $A/\mathbf{m}-$modul koji je jednodimenzionalan. Obzirom da je neka potencija od $\mathbf{m}$ sadržana u $\mathbf{q}$, slijedi da je $A/\mathbf{q}$ konačne duljine, kao i M. Koristimo funkciju duljine kao Euler-Poincaréovu funkciju u primjeni Teorema 10.

Teorem 11. ([2], *str.* 433) *Neka je A Noetherin lokalni prsten s maksimalnim idealom* $\mathbf{m}$. *Neka je* $\mathbf{q}$ $\mathbf{m}-$*primarni ideal, te neka je E konačno generirani $A-$modul sa stabilnom* $\mathbf{q}-$*filtracijom. Tada vrijede sljedeće tvrdnje:*

(i) *E/E_n konačne je duljine za $n \geq 0$.*

(ii) *Za dovoljno velike n, ova je duljina polinom $g(n)$ stupnja najviše s, gdje je s najmanji broj generatora ideala* $\mathbf{q}$.

(iii) *Stupanj i vodeći koeficijent polinoma $g(n)$ ovise samo o E i* $\mathbf{q}$, *ali ne ovise o izboru filtracije.*

Dokaz. Neka je

$$G = \mathrm{gr}_{\mathbf{q}}(A) = \bigoplus(\mathbf{q}^n/\mathbf{q}^{n+1}).$$

Tada je

$$\mathrm{gr}(E) = \bigoplus(E_n/E_{n+1})$$

gradirani $G-$modul, a $G_0 = A/\mathbf{q}$. Prema Propoziciji 19., G je Noetherin, a $\mathrm{gr}(E)$ konačni $G-$modul. Prema iskazima koji su prethodili teoremu, E/E_n konačne je duljine, u oznaci φ, te vrijedi:

$$\varphi(E/E_n) = \sum_{j=1}^{n} \varphi(E_{j-1}/E_j).$$

Ako $x_1, \ldots, x_s$ generiraju $\mathbf{q}$, tada slike $\bar{x}_1, \ldots, \bar{x}_s$ u $\mathbf{q}/\mathbf{q}^2$ generiraju G kao $A/\mathbf{q}-$algebru, i svaki $\bar{x}_i$ je stupnja 1. Prema Teoremu 10. vidimo da je

$$\varphi(E_n/E_{n+1}) = h(n)$$

polinom varijable n stupnja najviše $s-1$ za dovoljno velike n. S obzirom da je

$$\varphi(E/E_{n+1}) - \varphi(E/E_n) = h(n),$$

slijedi da je $\varphi(E/E_n)$ polinom $g(n)$ stupnja najviše s za dovoljno velike n. Ovu ćemo implikaciju potkrijepiti Lemom 7. Zadnja tvrdnja o neovisnosti stupnja polinoma g i vodećeg koeficijenta o izboru filtracije slijedi iz Propozicije 17. Time je dokaz završen. $\square$

Iz teorema možemo zaključiti da postoji polinom $\chi_{E,\mathbf{q}}$, takav da vrijedi:

$$\chi_{E,\mathbf{q}}(n) = \text{duljina}(E/\mathbf{q}^n E)$$

za dovoljno velike n. Ako je $E = A$, tada $\chi_{A,\mathbf{q}}$ nazivamo karakterističnim polinomom ideala $\mathbf{q}$. Može se vidjeti da vrijedi:

$$\chi_{A,\mathbf{q}}(n) = \text{duljina}(A/\mathbf{q}^n)$$

za dovoljno velike n.

Sada ćemo proučiti važan slučaj vezan uz ideale u prstenu polinoma. Neka je k polje te neka je

$$A = k[X_0, \ldots, X_N]$$

prsten polinoma u $N+1$ varijabli. Tada je A gradiran, pri čemu su elementi stupnja n homogeni polinomi stupnja n. Neka je $\mathbf{a}$ homogeni ideal od A. Za cijeli broj $n \geq 0$ definiramo:

$$\varphi(n) = \dim_k A_n$$
$$\varphi(n, \mathbf{a}) = \dim_k \mathbf{a}_n$$
$$\chi(n, \mathbf{a}) = \dim_k A_n/\mathbf{a}_n = \dim_k A_n - \dim_k \mathbf{a}_n = \varphi(n) - \varphi(n, \mathbf{a}).$$

Kao i ranije u ovom poglavlju, s A_n označavamo vektorski prostor homogenih elemenata stupnja n u A nad poljem k, a slično vrijedi i za $\mathbf{a}_n$. Dakle, imamo:

$$\varphi(n) = \binom{N+n}{N}.$$

Razmotrit ćemo binomni polinom

$$\binom{T}{d} = \frac{T(T-1)\cdots(T-d+1)}{d!} = \frac{T^d}{d!} + \text{članovi s nižim stupnjevima.} \tag{1}$$

Ako je f funkcija, definiramo Δf kao:

$$\Delta f(T) = f(T+1) - f(T).$$

Tada direktno dobijemo:

$$\Delta \binom{T}{d} = \binom{T}{d-1}. \tag{2}$$

Lema 7. ([2], *str.* 435) *Neka je $P \in \mathbb{Q}[T]$ polinom s racionalnim koeficijentima stupnja d.*

(a) *Ako za dovoljno velike cijele brojeve n vrijedi $P(n) \in \mathbb{Z}$, tada postoje cijeli brojevi $c_0, \dots, c_d$ takvi da je:*

$$P(T) = c_0\binom{T}{d} + c_1\binom{T}{d-1} + \dots + c_d.$$

Posebno, vrijedi $P(n) \in \mathbb{Z}$ za sve cijele brojeve n.

(b) *Ako je $f : \mathbb{Z} \to \mathbb{Z}$ proizvoljna funkcija i ako postoji polinom $Q(T) \in \mathbb{Q}[T]$ takav da je $Q(\mathbb{Z}) \subset \mathbb{Z}$ i $\Delta f(n) = Q(n)$ za dovoljno velike n, tada postoji polinom P kao u dijelu (a) takav da je $f(n) = P(n)$ za dovoljno velike n.*

Dokaz. Dokazat ćemo (a) pomoću indukcije. Ako je stupanj od P jednak 0, tvrdnja je očita. Pretpostavimo da je stupanj od P veći ili jednak 1. Prema (1) postoje racionalni brojevi $c_0, \dots, c_d$ takvi da je $P(T)$ oblika kao u (a). Međutim, polinom ΔP ima strogo manji stupanj nego P. Koristeći (2) i indukciju, zaključujemo da $c_0, \dots, c_{d-1}$ moraju biti cijeli brojevi. Na kraju, c_d je cijeli broj jer je $P(n) \in \mathbb{Z}$ za dovoljno velike n. Ovo dokazuje (a).

Za dokaz tvrdnje (b), koristit ćemo (a). Možemo napisati

$$Q(T) = c_0\binom{T}{d-1} + \dots + c_{d-1}$$

gdje su $c_0, \dots, c_{d-1}$ cijeli brojevi. Neka je P_1 oblika

$$P_1(T) = c_0\binom{T}{d} + \dots + c_{d-1}\binom{T}{1}, \quad \text{pa vrijedi} \quad \Delta P_1 = Q.$$

Tada je $\Delta(f - P_1)(n) = 0$ za dovoljno velike n. Dakle, izraz $(f - P_1)(n)$ jednak je konstanti c_d za dovoljno velike n, pa uzimamo $P = P_1 + c_d$ kako bismo zaključili dokaz. □

Propozicija 20. ([2], *str.* 435) *Neka su* **a** *i* **b** *homogeni ideali u A. Tada vrijedi*

$$\varphi(n, \mathbf{a} + \mathbf{b}) = \varphi(n, \mathbf{a}) + \varphi(n, \mathbf{b}) - \varphi(n, \mathbf{a} \cap \mathbf{b})$$
$$\chi(n, \mathbf{a} + \mathbf{b}) = \chi(n, \mathbf{a}) + \chi(n, \mathbf{b}) - \chi(n, \mathbf{a} \cap \mathbf{b}).$$

Dokaz. Prva tvrdnja je očita, a druga slijedi iz definicije funkcije χ. □

Teorem 12. ([2], *str.* 436) *Neka je F homogeni polinom stupnja d. Pretpostavimo da F nije djelitelj nule modulo* **a**, *to jest: ako vrijedi $G \in A$, $FG \in \mathbf{a}$, slijedi $G \in \mathbf{a}$. Tada je*

$$\chi(n, \mathbf{a} + (F)) = \chi(n, \mathbf{a}) - \chi(n - d, \mathbf{a}).$$

Dokaz. Najprije primijetimo da trivijalno vrijedi:

$$\varphi(n,(F)) = \varphi(n-d),$$

jer je stupanj produkta suma stupnjeva. Zatim, koristeći pretpostavku da F nije djelitelj nule modulo $\mathbf{a}$, zaključujemo:

$$\varphi(n,\mathbf{a}\cap(F)) = \varphi(n-d,\mathbf{a}).$$

Konačno, prema drugoj formuli iz Propozicije 20., dobivamo:

$$\begin{aligned}\chi(n,\mathbf{a}+(F)) &= \chi(n,\mathbf{a}) + \chi(n,(F)) - \chi(n,\mathbf{a}\cap(F))\\ &= \chi(n,\mathbf{a}) + \varphi(n) - \varphi(n,(F)) - \varphi(n) + \varphi(n,\mathbf{a}\cap(F))\\ &= \chi(n,\mathbf{a}) - \varphi(n-d) + \varphi(n-d,\mathbf{a})\\ &= \chi(n,\mathbf{a}) - \chi(n-d,\mathbf{a})\end{aligned}$$

čime je teorem dokazan. □

Označimo s $\mathbf{m} = (X_0,\dots,X_N)$ maksimalni ideal u A. Tada $\mathbf{m}$ nazivamo irelevantnim prostim idealom. Za ideal ćemo reći da je irelevantan ako sadrži neku pozitivnu potenciju ideala $\mathbf{m}$. Posebno, primarni je ideal $\mathbf{q}$ irelevantan ako i samo ako $\mathbf{m}$ pripada $\mathbf{q}$.

Propozicija 21. ([2], *str.* 436) *Neka je* $\mathbf{a}$ *homogen ideal.*

(a) *Ako je* $\mathbf{a}$ *irelevantan, tada je* $\chi(n,\mathbf{a}) = 0$ *za dovoljno velike* n.

(b) *Općenito, postoji izraz* $\mathbf{a} = \mathbf{q}_1 \cap \cdots \cap \mathbf{q}_s$ *kao reducirana primarna dekompozicija takva da su svi* $\mathbf{q}_i$ *homogeni.*

(c) *Ako se irelevantan primarni ideal pojavljuje u dekompoziciji, označit ćemo s* $\mathbf{b}$ *presjek svih ostalih primarnih ideala. Tada vrijedi:*

$$\chi(n,\mathbf{a}) = \chi(n,\mathbf{b})$$

za dovoljno velike n.

Može se pokazati da za svaki homogeni ideal $\mathbf{a}$, funkcija f oblika

$$f(n) = \chi(n,\mathbf{a})$$

zadovoljava uvjete Leme 7.(b).

Teorem 13. ([2], *str.* 437) *Neka je* $\mathbf{a}$ *homogeni ideal u* A. *Tada postoji polinom* $P \in \mathbb{Q}[T]$, *takav da je* $P(\mathbb{Z}) \subset \mathbb{Z}$ *i vrijedi*

$$P(n) = \chi(n,\mathbf{a})$$

za dovoljno velike n.

Polinom iz Teorema 13. naziva se Hilbertov polinom ideala $\mathbf{a}$.

3.7 Nerazloživi moduli

Neka je A prsten, koji ne mora biti komutativan, i E A-modul. Kažemo da je E Artinov ako zadovoljava uvjet padajućeg lanca na podmodule, odnosno za niz

$$E_1 \supseteq E_2 \supseteq E_3 \supseteq \cdots$$

postoji cijeli broj N takav da ako je $n \geq N$, tada vrijedi $E_n = E_{n+1}$.

Primjer 9. ([2], str. 439) *Ako je k polje, A k-algebra, i E konačnodimenzionalni vektorski prostor nad k koji je ujedno i $A-$modul, tada je E Artinov, ali i Noetherin.*

Primjer 10. ([2], str. 439) *Neka je A komutativni Noetherin lokalni prsten s maksimalnim idealom $\mathbf{m}$, i neka je $\mathbf{q}$ $\mathbf{m}-$primarni ideal. Tada je za svaki pozitivni cijeli broj n, $A/\mathbf{q}^n$ Artinov.*

Kao i kod Noetherinih prstena i modula, lako možemo provjeriti sljedeće tvrdnje iskazane propozicijama:

Propozicija 22. ([2], str. 439) *Neka je A prsten, te neka je*

$$0 \to E' \to E \to E'' \to 0$$

egzaktni niz $A-$modula. Tada je E Artinov ako i samo ako su E' i E'' Artinovi.

Dokaz. Dokaz se provodi slično kao i u Noetherinom slučaju. □

Propozicija 23. ([2], str. 439) *Modul E ima konačnu jednostavnu filtraciju ako i samo ako je E i Noetherin i Artinov.*

Dokaz. Jednostavni modul generiran je jednim elementom, pa je Noetherin. Budući da ne sadrži pravi podmodul različit od 0, također je Artinov. Propozicija 23. slijedi izravno iz Propozicije 22. □

Za modul E kažemo da je razloživ ako se može zapisati kao direktna suma

$$E = E_1 \oplus E_2$$

pri čemu vrijedi $E_1 \neq E, E_2 \neq E$. Ako se modul E ne može zapisati u gore navedenom obliku, kažemo da je nerazloživ. Ako je E razloživ, označimo s e_1 projekciju na prvu komponentu direktne sume, a s $e_2 = 1 - e_1$ projekciju na drugu komponentu. Tada su e_1 i e_2 idempotentni elementi za koje vrijedi

$$e_1 \neq 1, \quad e_2 \neq 1, \quad e_1 + e_2 = 1, \quad e_1e_2 = e_2e_1 = 0.$$

S druge strane, ako takvi idempotentni elementi postoje u prstenu endomorfizama od E, tada je E razloživ, a e_i je projekcija na podmodul e_iE.

Neka je $u : E \to E$ endomorfizam nekog modula E. Možemo formirati padajući niz

$$\operatorname{Im} u \supseteq \operatorname{Im} u^2 \supseteq \operatorname{Im} u^3 \supseteq \ldots$$

Ako je E Artinov, ovaj će se niz stabilizirati pa imamo:

$$\text{Im } u^n = \text{Im } u^{n+1} \quad \text{za dovoljno velike } n.$$

Ovaj podmodul zovemo $u^\infty(E)$ ili Im u^∞.

Slično, imamo i rastući niz

$$\text{Ker } u \subseteq \text{Ker } u^2 \subseteq \text{Ker } u^3 \subseteq \ldots$$

Ovaj se niz stabilizira ako je E Noetherin, i tada pišemo:

$$\text{Ker } u^\infty = \text{Ker } u^n \quad \text{za dovoljno velike } n.$$

Propozicija 24. ([2], *str.* 440)(*Fittingova lema*) *Pretpostavimo da je E Noetherin i Artinov modul. Neka je u element iz prstena endomorfizama od E. Tada se E može napisati u obliku*

$$E = Im\ u^\infty \oplus Ker\ u^\infty.$$

Nadalje, restrikcija operatora u na Im u^∞ je automorfizam, a restrikcija na Ker u^∞ je nilpotentna.

Dokaz. Odaberimo n takav da vrijedi Im u^∞ = Im u^n i Ker u^∞ = Ker u^n. Tada imamo

$$\text{Im } u^\infty \cap \text{Ker } u^\infty = \{0\},$$

jer ako x pripada presjeku, tada je $x = u^n(y)$ za neki $y \in E$, a zatim vrijedi $0 = u^n(x) = u^{2n}(y)$. Dakle, $y \in \text{Ker } u^{2n} = \text{Ker } u^n$, odakle slijedi $x = u^n(y) = 0$.

Nadalje, neka je $x \in E$. Tada za neki $y \in u^n(E)$ vrijedi

$$u^n(x) = u^n(y).$$

Pišemo

$$x = x - u^n(y) + u^n(y),$$

što pokazuje da je $E = \text{Im } u^\infty + \text{Ker } u^\infty$. U kombinaciji s prvim dijelom dokaza, slijedi da je suma direktna, kako je i navedeno.

Odmah slijedi i završna tvrdnja, jer je restrikcija operatora u na Im u^∞ surjektivna, a njegova jezgra je $\{0\}$, kao što je pokazano u prvom dijelu dokaza. Restrikcija operatora u na Ker u^∞ je nilpotentna jer je Ker u^∞ = Ker u^n. Time je dokaz završen. □

Sada ćemo generalizirati pojam lokalnog prstena na nekomutativni prsten. Prsten A je lokalan ako skup nejediničnih elemenata tvori ideal.

Propozicija 25. ([2], *str.* 441) *Neka je E nerazloživi modul nad prstenom A. Pretpostavimo da je E Noetherin i Artinov. Svaki endomorfizam od E je ili nilpotentan ili automorfizam. Nadalje, prsten endomorfizama od E je lokalan.*

Dokaz. Prema Fittingovoj lemi, znamo da za bilo koji endomorfizam u vrijedi $E = \mathrm{Im}\, u^\infty$ ili $E = \mathrm{Ker}\, u^\infty$. Neka je u endomorfizam koji nije invertibilan, pa je u nilpotentan. Za bilo koji endomorfizam v slijedi da uv i vu nisu surjektivni ni injektivni, pa nisu niti automorfizmi. Neka su u_1, u_2 endomorfizmi koji nisu invertibilni. Moramo pokazati da $u_1 + u_2$ nije invertibilan. Pretpostavimo da $u_1 + u_2$ jest invertibilan u prstenu endomorfizama od E. Neka vrijedi jednakost $v_i = u_i(u_1 + u_2)^{-1}$. Tada je $v_1 + v_2 = 1$. Nadalje, $v_1 = 1 - v_2$ jer je v_2 nilpotentan, što se može vidjeti iz raspisa od $(1 - v_2)^{-1}$. Međutim, v_1 nije invertibilan zbog prvog dijela dokaza, što daje kontradikciju. Time je završen dokaz. □

Lema 8. ([2], *str.* 442) *Neka su M i N moduli, te pretpostavimo da je N nerazloživ. Neka su $u : M \to N$ i $v : N \to M$ takvi da je vu automorfizam. Tada su u i v izomorfizmi.*

Dokaz. Neka je $e = u(vu)^{-1}v$. Tada je $e^2 = e$ idempotentan element koji pripada prstenu endomorfizama od N, te je stoga jednak 0 ili 1 jer je N po pretpostavci nerazloživ. Međutim, $e \neq 0$ jer $\mathrm{id}_M \neq 0$, te vrijedi:

$$0 \neq \mathrm{id}_M = \mathrm{id}_M^2 = (vu)^{-1}vu(vu)^{-1}vu.$$

Stoga je $e = \mathrm{id}_N$. Tada je u injektivan jer je vu automorfizam, v je injektivan jer je $e = \mathrm{id}_N$ injektivan, u je surjektivan jer je $e = \mathrm{id}_N$, a v je surjektivan jer je vu automorfizam. Ovime je dokaz završen. □

Teorem 14. ([2], *str.* 441)(*Krull-Remak-Schmidt*) *Neka je $E \neq 0$ Noetherin i Artinov modul. Tada je E konačna direktna suma nerazloživih modula. Nerazložive komponente u takvoj direktnoj sumi jedinstveno su određene do na izomorfizam, pri čemu redoslijed komponenti nije bitan.*

Dokaz. Postojanje direktne sume u dekompoziciji na nerazložive module slijedi iz Artinovog uvjeta. Ako je $E = E_1 \oplus E_2$, tada su E_1 i E_2 nerazloživi te je dokaz završen. Neka je sada, bez smanjenja općenitosti, E_1 razloživ. Ponavljajući postupak, vidimo da zbog pretpostavke da je E Artinov ova dekompozicija završava u konačno mnogo koraka. Ostaje dokazati jedinstvenost. Pretpostavimo da je

$$E = E_1 \oplus \cdots \oplus E_r = F_1 \oplus \cdots \oplus F_s,$$

gdje su E_i, F_j nerazloživi. Moramo pokazati da je $r = s$ i da, nakon neke permutacije, vrijedi $E_i \cong F_i$. Neka je e_i projekcija modula E na E_i, a u_j projekcija od E na F_j, uz gore navedene dekompozicije direktne sume. Neka je

$$v_j = e_1 u_j \quad \text{i} \quad w_j = u_j e_1.$$

Tada $\sum u_j = \mathrm{id}_E$ implicira da vrijedi

$$\textstyle\sum_{j=1}^{s} v_j w_j|_{E_1} = \mathrm{id}_{E_1}.$$

Prema Propoziciji 25., prsten endomorfizama od E_1 lokalni je prsten, te je stoga neki od izraza $v_j w_j$ automorfizam od E_1. Bez smanjenja općenitosti, pretpostavimo da je $v_1 w_1$ automorfizam od E_1. Uočimo da iz Leme 8. slijedi da v_1 i w_1 induciraju izomorfizme između E_1 i F_1.

Sada vidimo da je

$$E = F_1 \oplus (E_2 \oplus \cdots \oplus E_r).$$

Doista, e_1 inducira izomorfizam iz F_1 u E_1, a budući da je jezgra od e_1 jednaka $E_2 \oplus \cdots \oplus E_r$, slijedi da je

$$F_1 \cap (E_2 \oplus \cdots \oplus E_r) = \{0\}.$$

Također, $F_1 \equiv E_1$ (modulo $E_2 \oplus \cdots \oplus E_r$), pa je E suma od F_1 i $E_2 \oplus \cdots \oplus E_r$, odakle slijedi da je E i njihova direktna suma, što je i tvrdnja.

Ali tada je

$$E/F_1 \cong F_2 \oplus \cdots \oplus F_s \cong E_2 \oplus \cdots \oplus E_r.$$

Ostatak dokaza sada slijedi primjenom matematičke indukcije. $\square$

Literatura

[1] S. Agraqal, E. Belmont i sur., *The CRing Project*, dostupno na https://math.uchicago.edu/~amathew/CRing.pdf

[2] S. Lang, *Algebra*, Springer - Verlag, New York, 2002.

[3] I. Gut, *Komutativni prstenovi i njihovi moduli*, diplomski rad, Prirodoslovno-matematički fakultet, Matematički odsjek, Sveučilište u Zagrebu, 2014.

[4] J. Hardy, *Emmy Noether*, College of Education, University of Idaho, dostupno na https://www.lib.uidaho.edu/digital/objects/guidedreading/guidedread023.pdf

[5] H. Kraljević, *Algebra*, Odjel za matematiku, Sveučilište u Osijeku, 2008.

[6] S. Krešić-Jurić, *Algebarske strukture*, Odjel za matematiku, Prirodoslovno - matematički fakultet, Split, 2013.

Sažetak

U ovom diplomskom radu obrađuju se ključni pojmovi iz teorije Noetherinih prstena i modula. Nakon pregleda osnovnih kriterija i uvjeta za Noetherine prstene, analizirali smo pridružene proste ideale, odnosno proste ideale povezane s modulom, koji opisuju ključne elemente njegove strukture kroz dekompoziciju. Nakayamina lema kaže da u lokalnim Noetherinim prstenima injektivni moduli imaju posebnu strukturu koja ih čini projektivnima. Filtrirani i gradirani moduli omogućuju uvođenje dodatnih struktura koje pojednostavljuju analizu, a Hilbertov polinom služi za izračunavanje dimenzija tih struktura. Na kraju, obrađuju se nerazloživi moduli kao osnovni gradivni elementi.

Ključne riječi

prsten, modul, Noetherin prsten, ideal, prosti ideal, kvocijentni modul, homomorfizam, izomorfizam, gradirani modul, primarna dekompozicija, nerazloživi modul

Noetherian rings and modules

Summary

This thesis addresses key concepts from the theory of Noetherian rings and modules. After reviewing the basic criteria and conditions for Noetherian rings, we analyzed associated primes, prime ideals related to a module, which describe key elements of its structure through decomposition. Nakayama's lemma states that in local Noetherian rings, injective modules have a special structure that makes them projective. Filtered and graded modules allow the introduction of additional structures that simplify analysis, and the Hilbert polynomial is used to calculate the dimensions of these structures. Finally, indecomposable modules are discussed as fundamental building blocks.

Keywords

ring, module, Noetherian ring, ideal, prime ideal, modul factor, homomorphism, isomorphism, graded module, primary decomposition, indecomposable module

Životopis

Zovem se Mario Nuić. Rođen sam 7. srpnja 1995. godine u Filderstadtu u Njemačkoj. Pohađao sam Osnovnu školu Ljudevita Gaja u Osijeku. U Isusovačku klasičnu gimnaziju s pravom javnosti u Osijeku upisujem se 2010. godine te ju završavam 2014. godine. Iste godine upisujem Preddiplomski studij Matematike na Odjelu za matematiku, Sveučilišta Josipa Jurja Strossmayera u Osijeku. Studij završavam 2019. godine te stječem naziv prvostupnika matematike s temom završnog rada *Geometrijska preslikavanja u prostoru* pod mentorstvom izv. prof. dr. sc. Tomislava Maroševića. Nakon toga, 2019. godine upisujem Diplomski studij Matematike, na Odjelu za matematiku, Sveučilišta Josipa Jurja Strossmayera u Osijeku, smjer Financijska matematika i statistika.