Komutativni prsteni i moduli

Gavran, David

Master's thesis / Diplomski rad

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Applied Mathematics and Informatics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet primijenjene matematike i informatike**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:333655

Sveučilište J. J. Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike
Sveučilišni diplomski studij matematike, smjer: financijska matematika i statistika

David Gavran

Komutativni prsteni i moduli

Diplomski rad

Osijek, 2023.

Sveučilište J. J. Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike
Sveučilišni diplomski studij matematike, smjer: financijska matematika i statistika

David Gavran

Komutativni prsteni i moduli

Diplomski rad

Voditelj: prof. dr. sc. Ivan Matić

Osijek, 2023.

Sadržaj

Uvod

Glavna tema diplomskog rada su komutativni prstenovi i moduli. Kako bismo definirali komutativne prstenove i module, u prvom poglavlju ćemo definirati pojmove grupe i prstena, navesti važna svojstva vezana za njih te iskazati teoreme i definicije na koje ćemo se pozivati.
U potpoglavlju 2.1. opisat ćemo uvjete uzlaznog i silaznog lanca za prstenove i module. Glavni cilj potpoglavlja 2.2 bit će proučavanje prostih struktura komutativnih prstenova. Opisat ćemo uvjete prostih ideala, definirat ćemo pojmove primarnih ideala, radikala te navesti nekoliko teorema vezanih za te pojmove. U idućem potpoglavlju definirat ćemo primarnu dekompoziciju te proširiti znanje iz prethodnog potpoglavlja na module. U sljedećem potpoglavlju koje nazvano po Emmyju Noetheru definirat ćemo specifičnu vrstu prstenovu koja značajno pojednostavljuju idealne strukture prstena. Navest ćemo nekoliko važnih iskaza kao što je Krullov teorem, Nakayama lemu, a potpoglavlje ćemo zaokružiti s Hilbertovim teoremom o bazi. O proširenjima prstena i odnosima između prostih ideala govorit ćemo u potpoglavlju 2.5. Na kraju ćemo definirati Dedekindove domene, iskazati tvrdnje vezane za njih te navesti ekvivalencije koje povezuju Dedekindovu domenu, invertibilnost ideala i kvocijentnih ideala, projektivan ideal, Noetherinov prsten te prsten diskretne valuacije.

1. Osnovni pojmovi i svojstva

1.1. Grupa, prsten

Definicija 1.1. *[4, Definition I.1.1.] Neka je G neprazan skup. Binarna operacija na G funkcija je koja svakom uređenom paru elemenata od G pridružuje element od G, tj.*

$$(a, b) \mapsto a * b \in G \text{ za sve } a, b \in G.$$

Kažemo da je G zatvoren s obzirom na operaciju $*$ i uređeni par $(G, *)$ nazivamo grupoid.

Za početak definirajmo prsten i navedimo nekoliko osnovnih pojmova iz teorije prstenova.

Definicija 1.2. *[4, Definition I.1.1] Polugrupa je grupoid u kojem je binarna operacija asocijativna, tj. vrijedi $(ab)c = a(bc)$ za sve $a, b, c \in G$.*

Definicija 1.3. *[4, Definition I.1.1.] Kažemo da je grupoid G grupa ako vrijedi sljedeće:*
1. *Binarna operacija je asocijativna, tj. $(ab)c = a(bc)$ za sve $a, b, c \in G$.*
2. *Postoji neutralni element $e \in G$ tako da vrijedi $ae = ea = a$ za svaki $a \in G$.*
3. *Postoji inverzni element, tj. za svaki element $a \in G$ postoji $a^{-1} \in G$ tako da vrijedi $aa^{-1} = a^{-1}a = e$.*

Ako još u grupi G vrijedi komutativnost, tj. ako vrijedi $ab = ba$ za sve $a, b \in G$, tada kažemo da je G **Abelova** ili **komutativna** grupa.

Primjer 1.1. *Skup $\mathbb{Z}$ uz operaciju zbrajanja je grupa, dok skup $\mathbb{N}$ uz operaciju zbrajanja nije grupa budući da ne postoji neutralni element za zbrajanje ($0 \notin \mathbb{N}$). Skup $\mathbb{N}$ je polugrupa uz operaciju zbrajanja.*

Definicija 1.4. *[5, Definicija 3.1.1.] Prsten je neprazan skup R na kome su zadane binarne operacije zbrajanja ($(a, b) \mapsto a + b$) i množenja ($(a, b) \mapsto ab$) sa sljedećim svojstvima:*
1. *u odnosu na zbrajanje je R Abelova grupa; neutralni element u odnosu na zbrajanje označavamo s 0 i nazivamo nula (ili nula prstena R);*
2. *u odnosu na množenje je R polugrupa (tj. množenje je asocijativno);*
3. *množenje je slijeva i zdesna distributivno u odnosu na zbrajanje, tj. za sve $a, b, c \in R$ vrijedi $a(b + c) = ab + ac$ i $(a + b)c = ac + bc$.*

Prstenovi se dijele na komutativne i nekomutativne prstenove. U ovom radu bavit ćemo se komutativnim prstenovima. Kažemo da je prsten **komutativan** ako je množenje u tom prstenu komutativno.
Za svaki element a iz prstena R vrijedi $0a = a0 = 0$. Kažemo da je prsten R **unitalan** (prsten s jedinicom), ako postoji element $1 \in R$ tako da vrijedi $a1 = 1a = a$, za svaki $a \in R$. Takav element nazivamo **jedinica** prstena R.
Potprsten prstena R je podskup S koji je i sam prsten u odnosu na zadane operacije. Preciznije, $S \neq \emptyset$ i za $a, b \in S$ vrijedi $a - b \in S$ i $ab \in S$.
Neka su S i R prstenovi. Preslikavanje $\phi : R \to S$ nazivamo **homomorfizam** prstenova ako vrijedi: $\phi(a + b) = \phi(a) + \phi(b)$ i $\phi(ab) = \phi(a)\phi(b)$ za sve $a, b \in R$. Injektivni homomorfizam nazivamo **monomorfizam** prstenova, surjektivni homomorfizam nazivamo **epimorfizam** prstenova, a bijektivni homomorfizam nazivamo **izomorfizam** prstenova.
Definirajmo sada lijeve i desne ideale.

Definicija 1.5. *[4, Definition III.2.1.] Kažemo da je aditivna podgrupa J prstena R desni ideal u prstenu R ako vrijedi*

$$a \in J, b \in R \Rightarrow ab \in J,$$

a lijevi ideal u prstenu R ako vrijedi

$$a \in J, b \in R \Rightarrow ba \in J.$$

Ukoliko je J i desni i lijevi ideal u prstenu R onda J nazivamo **dvostrani** ili **obostrani** ideal u R.
Neka je J obostrani ideal u prstenu R. Tada je J podgrupa aditivne komutativne grupe prstena R pa možemo definirati kvocijentnu grupu R/J. Elementi te grupe su skupovi oblika

$$a + J = \{a + b; b \in J, a \in R\},$$

a operacija zbrajanja je zadana s

$$(a + J) + (b + J) = (a + b) + J, \ a + J, b + J \in R/J, \ \text{tj. } a, b \in R.$$

Zbog svojstva obostranog ideala ima smisla definirati i operaciju množenja na R/J:

$$(a + J)(b + J) = ab + J, \ a + J, b + J \in R/J.$$

Tako definirani prsten nazivamo **prsten s dijeljenjem**.
Neka je R komutativan unitalan prsten. Element $a \neq 0$ prstena R nazivamo **djelitelj nule** ako postoji $b \in R, b \neq 0$ tako da vrijedi $ab = 0$. Komutativan unitalan prsten $R \neq \{0\}$ u kojem nema djelitelja nule nazivamo **integralna domena**. To je prsten u kojemu vrijedi $ab = 0$ ako i samo ako je ili $a = 0$ ili $b = 0$. Prsten cijelih brojeva je jedan od primjera integralne domene. Također, svako polje je integralna domena.
Označimo s R komutativan unitalan prsten različit od 0. Kažemo da je ideal I u prstenu R je **prost** ako je $I \neq R$ i ako iz $ab \in I$ slijedi da je ili $a \in I$ ili $b \in I$.

Primjer 1.2. *U svakom prstenu R su R i $\{0\}$ ideali u R. Ideal $\{0\}$ nazivamo trivijalni ideal.*

Propozicija 1.1. *[5, Propozicija 3.3.1.] Ideal I u prstenu R je prost ako i samo ako je prsten s dijeljenjem R/I integralna domena.*

Kažemo da je ideal $I \neq R$ je **maksimalan** ako u R ne postoji ideal J takav da je $I \subsetneq J \subsetneq R$.

Propozicija 1.2. *[5, Propozicija 3.3.1.] Neka je $I \neq R$ ideal. Tada postoji maksimalan ideal u R koji sadrži I.*

Propozicija 1.3. *[5, Korolar 3.3.1.] Svaki maksimalan ideal u R je prost.*

Obrat ovog korolara ne vrijedi.
Glavni ideal u prstenu R je svaki ideal oblika $Ra = \{b \in R : ba\}$ za neki $a \in R$. Za R kažemo da je **prsten glavnih ideala** ako je svaki ideal u R glavni ideal.

Definicija 1.6. *[3, Definicija 1.1.5.] Neka je R prsten i X podskup od R. Najmanji potprsten od R koji sadrži X nazivamo potprsten generiran s X. Najmanji ideal od R koji sadrži X nazivamo ideal generiran s X i označavamo ga s $\langle X \rangle$.*

Definicija 1.7. *[2, Definicija 2.0.1] Unitalni prsten R je prsten s dijeljenjem, ako je svaki nenul element u R invertibilan.*

Primjer 1.3. *Pokažimo da je $\mathbb{Z}$, uz operacije zbrajanja i množenja definirane s*

$$a \oplus b = a + b + 1 \text{ i } a \odot b = a + b + ab$$

komutativan prsten.

Rješenje.

1. *Zatvorenost s obzirom na $\oplus$ i $\odot$ vrijedi zbog zatvorenosti zbrajanja i množenja cijelih brojeva.*

2. *Provjerimo asocijativnost zbrajanja,*
$(a \oplus b) \oplus c = (a + b + 1) \oplus c = a + b + 1 + c + 1 = a + b + c + 2$
$a \oplus (b \oplus c) = a \oplus (b + c + 5) = a + b + c + 5 + 5 = a + b + c + 10.$
Budući da imamo jednake vrijednosti, zaključujemo da vrijedi asocijativnost zbrajanja.

3. *Provjerimo komutativnost zbrajanja.*
$a \oplus b = a + b + 1 = b + a + 1 = b \oplus a$, *pa zaključujemo da vrijedi.*
Za komutativnost množenja imamo
$a \odot b = a + b + ab = b + a + ba = b \odot b$, *pa također zaključujemo da vrijedi.*

4. *Iz $a = a \odot e = a + e + 1$ zaključujemo da je $e = -1$ desni neutralni element pa s obzirom da vrijedi komutativnost zbrajanja, imamo $a = a \oplus e = e \oplus a$ te zaključujemo da je $e = -1 \in \mathbb{Z}$ neutralni element.*

5. *Iz $-1 = a \oplus b = a + b + 1$ zaključujemo da je $b = -a - 2$ desni inverzni element od a. Budući da vrijedi komutativnost, zaključujemo da je $b = -a - 2 \in \mathbb{Z}$ inverzni element od $a \in \mathbb{Z}$.*

6. *Provjerimo asocijativnost množenja.*
$(a \odot b) \odot c = (a + b + ab) \odot = a + b + ab + c + (a + b + ab)c = a + b + c + ab + ac + bc + abc.$
S druge strane imamo, $a \odot (b \odot c) = a \odot (b + c + bc) = a + b + c + bc + a(b + c + bc) = a + b + c + ab + ac + bc + abc$ *pa zaključujemo da vrijedi.*

7. *Kako je*
$(a \oplus b) \odot c = (a + b + 5) \odot c = a + b + 5 + c + (a + b + 5)c = a + b + 2c + ac + bc + 1$
jednako
$a \odot c \oplus b \odot c = (a + c + ac) \oplus (b + c + bc) = a + b + 2c + ac + bc + 1$
zaključujemo da vrijedi distributivnost zdesna, a s obzirom da vrijedi komutativnost množenja, tada vrijedi i distributivnost slijeva.

Pokazali smo da je $\mathbb{Z}$ uz zbrajanje Abelova grupa, uz množenje polugrupa te vrijedi distributivnost zdesna i slijeva, tj. $(\mathbb{Z}, \oplus, \odot)$ je komutativan prsten.

1.2. Moduli

Definicija 1.8. *[3, Definicija 2.1.1.] Neka je R prsten s jedinicom.*
Desni R-modul je Abelova grupa zajedno s operacijom množenja $\cdot : M \times R \to M$, koja za sve elemente $a, b \in R$ i $m, n \in M$ zadovoljava:

$$\begin{aligned} &1.\ (m+n)a = ma + na, \\ &2.\ m(a+b) = ma + mb, \\ &3.\ m(ab) = (ma)b, \\ &4.\ m1 = m. \end{aligned}$$

Lijevi R-modul je Abelova grupa zajedno s operacijom množenja $\cdot : R \times M \to M$, koja za sve elemente $a, b \in R$ i $m, n \in M$ zadovoljava:

$$\begin{aligned} &1.\ a(m+n) = am + an, \\ &2.\ (a+b)m = am + bm, \\ &3.\ (ab)m = a(bm), \\ &4.\ 1m = m. \end{aligned}$$

Ukoliko je R komutativni prsten i M desni R-modul, onda M postaje i lijevi R-modul ako definiramo

$$rm = mr, \quad r \in R,\ m \in M.$$

U slučaju kada je desni R-modul istovjetan s lijevim R-modulom onda takve module nazivamo R-**moduli** ili **moduli nad prstenom** R.

Primjer 1.4. (1.) *Svaki prsten R je desni i lijevi R-modul.*
(2.) *Neka je $\mathbb{R}^n$ skup svih uređenih n-torki*

$$(x_1, x_2, \ldots, x_n), \quad x_i \in \mathbb{R}.$$

Skup $\mathbb{R}$ je Abelova grupa u odnosu na zbrajanje

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n).$$

Neutralni element je

$$(0, 0, \ldots, 0) = 0,$$

a suprotni element je definiran s

$$-(x_1, x_2, \ldots, x_n) = (-x_1, -x_2, \ldots, -x_n).$$

Ako definiramo množenje $\mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$ s

$$r(x_1, x_2, \ldots, x_n) = (rx_1, rx_2, \ldots, rx_n),$$

onda $\mathbb{R}^n$ postaje modul nad $\mathbb{R}$.

Definicija 1.9. *[3, Definicija 2.1.2.] Neka je R prsten i neka su M, N R-moduli. Funkciju $\phi : M \to N$ nazivamo homomorfizam R-modula ako vrijedi:*

$$\begin{aligned} \phi(m_1 + m_2) &= \phi(m_1) + \phi(m_2),\ m_1, m_2 \in M, \\ \phi(am) &= a\phi(m),\ a \in R, m \in M. \end{aligned}$$

Definicija 1.10. *[3, Definicija 2.1.6.] Neka je R prsten i M R-modul. Za podskup N od M kažemo da je podmodul od M ako je N podgrupa aditivne grupe M s obzirom na istu operaciju množenja na M.*

Definicija 1.11. *[3, Definicija 2.1.7.] Ako je S podskup R-modula M, sa $\langle S\rangle$ označimo presjek svih podmodula od M koji sadrže S. $\langle S\rangle$ zovemo podmodul od M generiran sa S, a elemente od S nazivamo generatori od $\langle S\rangle$.*

Definicija 1.12. *[3, Definicija 2.1.8.] Kažemo da je R-modul M konačno generiran ako za neki konačan podskup S od M vrijedi $M = \langle S\rangle$.*

1.3. Teoremi

U ovom dijelu navest ćemo tvrdnje na koje ćemo se pozivati u narednim poglavljima.

Teorem 1.1. *[4, Theorem Introduction. VI.2.] Neka je S skup, $a \in S$ i za svaki $n \in \mathbb{N}$, $f_n : S \to S$ je funkcija, tada postoji jedinstvena funkcija $\phi : \mathbb{N} \to S$ takva da je $\phi(0) = a$ i $\phi(n+1) = f_n(\phi(n))$ za svaki $n \in \mathbb{N}$.*

Teorem 1.2. *[4, Theorem I.2.5.] Neka je H neprazan podskup grupe G. Tada je H podgrupa od G ako i samo ako je $ab^{-1} \in H$ za sve $a, b \in H$.*

U idućem ćemo teoremu navesti neka važna svojstva proizvoljnih prstena.

Teorem 1.3. *[4, Theorem III.1.2.] Neka je R prsten. Tada vrijedi:*
1. $0a = a0 = 0$ *za svaki* $a \in R$,
2. $(-a)b = a(-b) = -ab$ *za sve* $a, b \in R$,
3. $(-a)(-b) = ab$ *za sve* $a, b \in R$,
4. $(na)b = a(nb) = n(ab)$ *za svaki* $n \in Z$ *i sve* $a, b \in R$,
5. $(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$, $a_i, b_j \in R$.

Navedimo teorem koji je poznat pod nazivom **Binomni teorem**.

Teorem 1.4. *[4, Theorem III.1.6.] Neka je R prsten s jedinicom, $n \in \mathbb{N}$ i $a, b, a_1, a_2, \ldots, a_s \in R$.*
1. *Ako je $ab = ba$, tada je $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$,*
2. *Ako je $a_i a_j = a_j a_i$ za sve i i j, tada je $(a_1 + a_2 + \cdots + a_s)^n = \sum \frac{n!}{(i_1!)\cdots(i_s!)} a_1^{i_1} a_2^{i_2} \cdots a_s^{i_s}$, gdje suma ide po svim uređenim s - torkama $(i_1, i_2, \ldots, i_s)$ tako da je $i_1 + i_2 + \cdots + i_s = n$.*

Teorem 1.5. *[4, Theorem III.2.5.] Neka je R prsten te neka je $a \in R$ i $X \subset R$.*
1. *Glavni ideal (a) sastoji se od svih elemenata oblika $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, $(n \in \mathbb{Z}, m \in \mathbb{N}, r, s, r_i, s_i \in R)$,*
2. *Ako R ima jedinicu, tada je $(a) = \sum_{i=1}^{n} r_i a s_i$,*
3. *$Ra = \{ra | r \in R\}$ je lijevi ideal u R. Ako R ima jedinicu, tada je $a \in Ra$ i $a \in aR$,*
4. *Ako R ima jedinicu i X je u centru od R, tada se ideal (X) sastoji od svih konačnih suma $r_1 a_1 + \cdots + r_n a_n$.*

U idućem ćemo teoremu navesti neka važna svojstva proizvoljnih ideala.

Teorem 1.6. *[4, Theorem III.2.6.] Neka su $A, B, C, A_1, \ldots, A_n$ ideali u prstenu R.*
1. *$A_1 + \cdots + A_n$ i $A_1 \cdots A_n$ su ideali,*
2. $(A + B) + C = A + (B + C)$,
3. $(AB)C = ABC = A(BC)$,
4. $B(A_1 + \cdots + A_n) = BA_1 + \cdots + BA_n$ *i* $(A_1 + \cdots + A_n)C = A_1C + \cdots + A_nC$.

Definirajmo kada je ideal prost te navedimo teoreme u kojima opisujemo uvjete kada je ideal prost.

Definicija 1.13. *Kažemo da je ideal P u prstenu R prost ako je $P \neq R$ te ako za svaka dva ideala A, $B \in R$ vrijedi*

$$AB \subset P \;\Rightarrow\; A \subset P \;\; ili \;\; B \subset P.$$

Teorem 1.7. *[4, Theorem III.2.15.] Ako je P ideal u prstenu R takav da je $P \neq R$ i za sve $a, b \in R$*

$$ab \in P \;\Rightarrow\; a \in P \;\; ili \;\; b \in P$$

tada je P prost. Obrnuto, ako je P prost i R komutativan, tada P zadovoljava gornji uvjet.

Teorem 1.8. *[4, Theorem III.2.16.] U komutativnom prstenu R s jedinicom različitom od nule ideal P je prost ako i samo ako je prsten s dijeljenjem R/P integralna domena.*

U idućem ćemo teoremu navesti zahtjev koji povezuje maksimalan i prost ideal.

Teorem 1.9. *[4, Theorem III.2.19.] Ako je R komutativan prsten tako da je $R^2 = R$, tada je svaki maksimalan ideal M u R prost.*

U idućem teoremu povežimo pojmove asociranih i invertibilnih elemenata komutativnog prstena R te navedimo uvjet kada je element prstena jedinica.

Teorem 1.10. *[4, Theorem III.3.2.] Neka su a, b i u elementi komutativnog prstena R s jedinicom. Tada vrijedi:*
1. *$a|b$ ako i samo ako je $(b) \subset (a)$,*
2. *a i b su asocirani ako i samo ako je $(a) = (b)$,*
3. *u je jedinica ako i samo ako je $u|r$ za svaki $r \in R$,*
4. *Ako je $a = br$, $r \in R$ invertibilni element, tada su a i b asocirani. Ako je R integralna domena, tada vrijedi i obrnuto.*

Za elemente a i b kažemo da su asocirani ako postoji jedinica $u \in R$ tako da je $b = ua$.

Navedimo sada još neke uvjete te karakterizacije prostih i ireducibilnih elemenata integralne domene R.

Teorem 1.11. *[4, Theorem III.3.4.] Neka su p i c nenul elementi integralne domene R. Tada vrijedi:*
1. *p je prost ako i samo ako je (p) nenul prost ideal,*
2. *c je ireducibilan ako i samo ako je (c) maksimalan u skupu svih odgovarajućih ideala od R,*
3. *Svaki prost element od R je ireducibilan,*
4. *Ako je R glavna idealna domena, tada je p prost ako i samo ako je p ireducibilan,*
5. *Jedini djelitelji ireducibilnog elementa od R su njemu asocirani elementi i invertibilni elementi od R.*

Lema 1.1. *[4, Lemma III.3.6.] Ako je R prsten glavnih ideala i $(a_1) \subseteq (a_2) \subseteq \ldots$ lanac ideala u R, tada za neki prirodni broj n vrijedi $(a_j) = (a_n)$ za sve $j \geq n$.*

Teorem 1.12. *[4, Theorem III.3.7.] Svaka domena glavnih ideala R je domena jedinstvene faktorizacije.*

Neka je R komutativan prsten. Za $S \subset R$ kažemo da je **multiplikativni podskup** ako vrijedi: $1 \in S$ i za sve $s_1, s_2 \in S$ je $s_1 s_2 \in S$.
Ako je J ideal u prstenu s dijeljenjem $S^{-1}R$, tada je ϕ_S^{-1} ideal u prstenu R. ϕ_S^{-1} nazivamo **kontrakcija** od J u R.

Lema 1.2. *[4, Lemma III.4.9.] Neka je S multiplikativni podskup komutativnog prstena R s jedinicom i neka je I ideal u R. Tada vrijedi:*
1. $I \subset \phi_S^{-1}(S^{-1}I)$,
2. *Ako je $I = \phi_S^{-1}(J)$ za neki ideal J iz $S^{-1}R$, tada je $S^{-1}I = J$. Drugim riječima, ideal u $S^{-1}R$ je oblika $S^{-1}I$ za neki ideal I iz R,*
3. *Ako je P prost ideal u R i $S \cap P = \emptyset$, tada je $S^{-1}P$ prost ideal u $S^{-1}R$ i $\phi_S^{-1}(S^{-1}P) = P$.*

Neka je R komutativni prsten i P prost ideal iz R. Tada $S = R \setminus P$ nazivamo **multiplikativni podskup** od R u odnosu na P. Prsten s dijeljenjem $S^{-1}R$ nazivamo **lokalizacija** R na P i označavamo s R_P. Ako je I ideal u R, tada se ideal $S^{-1}I$ u R_P označava s I_P.

Teorem 1.13. *[4, Theorem III.4.11.] Neka je P prost ideal u komutativnom prstenu R s jedinicom.*
1. *Postoji bijekcija između skupa prostih ideala od R koji su sadržani u P i skupa prostih ideala od R_P, danog s $Q \mapsto Q_P$.*
2. *Ideal P_P iz R_P je jedinstveni maksimalni ideal od R_P.*

Za komutativni prsten s jedinicom koji ima jedinstveni maksimalni ideal kažemo da je **lokalni prsten**. U idućem teoremu navedimo neka svojstva komutativnog prstena s jedinicom.

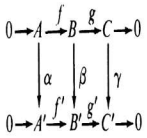
Teorem 1.14. *[4, Theorem III.4.13.] Neka je R komutativan prsten s jedinicom. Sljedeće su tvrdnje ekvivalentne:*
1. *R je lokalni prsten,*
2. *svi neinvertibilni elementi od R sadržane su u nekom idealu $M \neq R$,*
3. *neinvertibilni elementi od R tvore ideal.*

Teorem 1.15. *[4, Theorem IV.1.5.] Neka je R prsten, A R-modul, X podskup od A, $\{B_i | i \in I\}$ familija podmodula od A i $a \in A$. Neka je $Ra = \{ra | r \in R\}$.*
1. *Ra je podmodul od A i preslikavanje $R \to Ra$ dano s $r \mapsto ra$ je epimorfizam R-modula.*
2. *Ciklički podmodul generiran elementom a jednak je $\{ra + na | r \in R, n \in \mathbb{Z}\}$. Ukoliko R ima jedinicu i C unitalan, tada je $C = Ra$.*
3. *Podmodul D generiran s X je $\{\sum_{i=1}^{s} r_i a_i + \sum_{j=1}^{t} n_j b_j | s, t \in N_0, a_i, b_j \in X, r_i \in R, n_j \in \mathbb{Z}\}$. Ako R ima jedinicu i A je unitalan, tada je $D = RX = \{\sum_{i=1}^{s} r_i a_i | s \in \mathbb{N}\}$.*

Teorem 1.16. *[4, Theorem IV.1.10.] Neka je R prsten i B podmodul R-modula A, tada postoji bijekcija između skupa svih podmodula A koji sadrže B i skupa svih podmodula A/B, dano s $C \mapsto C/B$. Stoga je svaki podmodul od A/B oblika C/B, gdje je C podmodul od A koji sadrži B.*

Niz preslikavanja oblika $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ nazivamo kratki egzaktni niz, gdje je f monomorfizam, a g epimorfizam.

Lema 1.3. *[4, Lemma IV.1.17.] Neka je R prsten te neka je dan komutativni dijagram R-modula i homomorfizama R-modula [Slika1] tako da je svaki red kratki egzaktni niz.Tada vrijedi:*
1. *α, γ monomorfizmi $\to$ β je monomorfizam,*
2. *α, γ epimorfizmi $\to$ β je epimorfizam,*
3. *α, γ izomorfizmi $\to$ β je izomorfizam.*



Slika 1: Komutativni dijagram

Teorem 1.17. *[4, Theorem IV.1.18.] Neka je R prsten i $0 \to A_1 \to B \to A_2 \to 0$ kratki egzaktni niz homomorfizma R-modula. Tada su sljedeće tvrdnje ekvivalentne:*
1. Postoji homomorfizam R-modula $h : A_2 \to B$, $gh = 1_{A_2}$,
2. Postoji homomorfizam R-modula $k : B \to A_1$, $kf = 1_{A_1}$,
3. Dan je niz koji je izomorfan direktnoj sumi kratkih egzaktnih nizova $0 \to A_1 \to A_1 \oplus A_2 \to A_2 \to 0$, posebno $B \cong A_1 \oplus A_2$.

U idućem teoremu navedimo niz ekvivalencija na unitarnom R-modulu F, ali najprije definirajmo neke pojmove iz teorema.
Kažemo da je modul A **(unutarnja) direktna suma** familije podmodula $\{A_i \mid i \in I\}$ pod uvjetom da A i $\{A_i\}$ zadovoljavaju iduće:
Neka je R prsten i $\{A_i \mid i \in I\}$ familija podmodula od R-modula A tako da vrijedi:
1. A je suma familije $\{A_i \mid i \in I\}$,
2. za svaki $k \in I$ je $A_k \cap A_k^\star = \emptyset$, gdje je $A_k^\star$ suma familije $\{A_i \mid i \neq k\}$.
Definirajmo sada i bazu modula.
Kažemo da je podskup X R-modula A linearno nezavisan pod uvjetom da za različite $x_1, x_2, \ldots, x_n \in X$ i $r_i \in R$ vrijedi:

$$r_1x_1 + r_2x_2 + \cdots + r_nx_n = 0 \;\Rightarrow\; r_i = 0 \;\text{ za svaki } i.$$

Ako je A generiran kao R-modul pomoću skupa Y, tada kažemo da Y razapinje A. Linearno nezavisan podskup od A koji razapinje A nazivamo **baza** od A.

Teorem 1.18. *[4, Theorem IV.2.1.] Neka je R prsten s jedinicom. Sljedeći uvjeti na unitarnom R-modulu F su ekvivalentni:*
1. F ima nepraznu bazu.
2. F je unutarnja direktna suma familije cikličkih R-modula od kojih je svaki izomorfan R-modul kao lijevi R-modul.
3. F je R-modul izomorfan direktnoj sumi kopija lijevog R-modula R,
4. Postoji neprazan skup X i funkcija $\tau : X \to F$ sa svojstvom: dan je bilo koji unitarni R-modul A i funkcija $f : X \to A$, postoji jedinstveni homomorfizam R-modula $\bar{f} : F \to A$ tako da je $\bar{f}_\tau = f$.

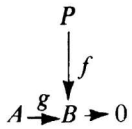
Neka je F R-modul. F je **slobodan** R-modul ukoliko je F izomorfan direktnoj sumi kopija od R, tj. $F = \sum_{i \in I} R_i$, gdje je $R_i = \langle b_i \rangle$ za svaki i.

Korolar 1.1. *[4, Corollary IV.2.2.] Svaki (unitarni) modul A nad prstenom R (s jedinicom) je homomorfna slika slobodnog R-modula F. Ako je A konačno generiran, tada se F može odabrati tako da bude konačno generiran.*

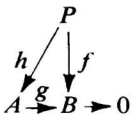
Teorem 1.19. *[4, Theorem IV.2.16.] Neka su R, S, T prsteni s dijeljenjem takvi da je $R \subset S \subset T$. Tada je $dim_R T = (dim_S T)(dim_R S)$. Nadalje, $dim_R T$ je konačna ako i samo ako su $dim_S T$ i $dim_R S$ konačne.*

Definirajmo pojam projektivnog modula te navedimo teorem u kojemu navodimo ekvivalentne uvjete na R-modulu P.

Definicija 1.14. *[4, Definition IV.3.1.] Kažemo da je modul P nad prstenom R projektivan ako je dan bilo koji dijagram homomorfizama R-modula [Slika2] s egzaktnim donjim redom (g je epimorfizam), postoji homomorfizam R-modula $h : P \to A$ takav da je dijagram [Slika3] komutativan, tj. $gh = f$.*



Slika 2: Dijagram homomorfizama



Slika 3: Komutativni dijagram

Teorem 1.20. *[4, Theorem IV.3.4.] Neka je R prsten. Sljedeći uvjeti na R-modulu P su ekvivalentni.*
1. *P je projektivan.*
2. *Svaki kratki egzaktan niz $0 \to A \to B \to P \to 0$ se egzaktno cijepa (stoga $B \cong A \oplus P$).*
3. *Postoji slobodan modul F i R-modul K takav da je $F \cong K \oplus P$.*

Teorem 1.21. *[4, Theorem V.1.5.] Ako je F proširenje polja K i $u \in F$ transcendentan nad K, tada postoji izomorfizam polja $K(u) \cong K(x)$ koji je identiteta na K.*

Napomena 1.1. *[4, Remarks, str. 171] Ako je $u \in K$, tada je u korijen od $x - u \in K[x]$ i stoga algebarski nad K. Ako je $u \in F$ algebarski nad nekim potpoljem K' od K, tada je u algebarski nad K budući je $K'[x] \subset K[x]$. Ako je $u \in F$ korijen od $f \in K[x]$ s vodećim koeficijentom $c \neq 0$, tada je u također korijen od $c^{-1}f$ koji je normiran polinom u $K[x]$.*

Aksiom izbora. Za svaku nepraznu familiju A međusobno disjunktnih nepraznih skupova A_α, postoji barem jedan skup C koji se sastoji od po točno jednog elementa iz svakog skupa A_α iz familije A.

2. Komutativni prstenovi i moduli

2.1. Uvjeti lanaca

U ovom potpoglavlju opišimo uvjete uzlaznog i silaznog lanca za prstenove i module. Navedimo prvo definiciju uvjeta uzlaznog lanca na podmodulima.

Definicija 2.1. *[4, Definition VIII.1.1.] Za modul A kažemo da zadovoljava uvjet uzlaznog lanca na podmodulima (ili da je Noetherin) ako za svaki lanac $A_1 \subseteq A_2 \subseteq \dots$ podmodula od A, postoji cijeli broj n takav da je $A_i = A_n$ za sve $i \geq n$.*

Definicija 2.2. *[4, Definition VIII.1.2.] Kažemo da je prsten R **desno [lijevo]** Noetherin ako R zadovoljava uzlazno lančani uvjet na desnim [lijevim] idealima. Kažemo da je prsten R Noetherin ako je R i desno i lijevo Noetherin.*

Primjer 2.1. 1. *Svaki prsten s dijeljenjem je Noetherin*
2. *Svaki komutativan prsten glavnih ideala je Noetherin.*
3. *Prsten $Mat_n D$ svih $n \times n$ matrica nad prstenom dijeljenja D je Noetherin.*

Desni Noetherin prsten ne mora biti lijevi Noetherin i obrnuto.
Neka je $(C, \leq)$ parcijalno uređen skup. Za element $a \in C$ kažemo da je **maksimalan** ako ne postoji element $b \in C$ tako da vrijedi $a < b$. Za $b \in C$ kažemo da je **minimalan** ako za svaki $c \in C$ koji je usporediv s b vrijedi $b \leq c$.

Definicija 2.3. *[4, Definition VIII.1.3.] Kažemo da modul A zadovoljava uvjet maksimalnosti [minimalnosti] podmodula ako svaki neprazan skup podmodula od A sadrži maksimalni [minimalni] element.*

Teorem 2.1. *[4, Theorem VIII.1.4.] Modul A zadovoljava uvjet uzlaznog [silaznog] lanca na podmodule ako i samo ako A zadovoljava uvjet maksimalnosti [minimalnosti] podmodula.*

Dokaz. Pretpostavimo da A zadovoljava uvjet minimalnosti podmodula i neka je $A_1 \supseteq A_2 \supseteq \dots$ lanac podmodula. Tada skup $\{A_i \mid i \geq 1\}$ ima minimalni element. Označimo taj minimalni element s A_n. Tada, za $i \geq n$ imamo $A_n \supseteq A_i$ te zbog minimalnosti i $A_n \subseteq A_i$ za $i \geq n$. Prema tome, $A_n = A_i$ za $i \geq n$ te A zadovoljava uvjet silaznog lanca.
Obrnuto, pretpostavimo da A zadovoljava uvjet silaznog lanca te neka je S neprazan skup podmodula od A. Tada postoji $B_0 \in S$. Ako S nema minimalnog elementa, tada za svaki podmodul B u S postoji barem jedan podmodul B' (Aksiom izbora) u S takav da je $B \supsetneq B'$. Za svaki B u S, odaberimo jedan takav B'. Definirajmo funkciju $f : S \to S$ s $B \mapsto B'$. Prema Teoremu 1.1 postoji funkcija $\phi : \mathbb{N}_0 \to S$ tako da je $\phi(0) = B_0$ i $\phi(n+1) = f(\phi(n)) = \phi(n)'$. Ako označimo $\phi(n)$ s $B_n \in S$, tada postoji niz $B_0, B_1, \dots$ takav da je $B_0 \supsetneq B_1 \supsetneq \dots$ To je u kontradikciji s uvjetom silaznog lanca. Prema tome, S mora imati minimalni element te slijedi da A zadovoljava minimalni uvjet. Dokaz za uvjete uzlaznog lanca i maksimalni element je analogan. □

Teorem 2.2. *[4, Theorem VIII.1.5.] Neka je $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ kratki egzaktni niz modula. Tada B zadovoljava uzlazni [silazni] uvjet lanca na podmodula ako i samo ako ga zadovoljavaju i A i C.*

Dokaz. Vidjeti [4]. □

Korolar 2.1. *[4, Corollary VIII.1.6.] Ako je A podmodul modula B, tada B zadovoljava uvjet uzlaznog [silaznog] lanca ako i samo ako ga zadovoljavaju A i B/A.*

Dokaz. Tvrdnja slijedi primjenom prethodnog teorema na niz $0 \to A \to B \to B/A \to 0$. □

Teorem 2.3. *[4, Theorem VIII.1.8.] Ako je R lijevi Noetherin prsten s jedinicom, tada svaki konačno generirani unitarni lijevi R-modul A zadovoljava uvjet uzlaznog lanca na podmodulima.*

Dokaz. Vidjeti [4]. □

Teorem 2.4. *[4, Theorem VIII.1.9.] Modul A zadovoljava uvjet uzlaznog lanca na podmodulima ako i samo ako je svaki podmodul od A konačno generiran. Preciznije, komutativni prsten R je Noetherin ako i samo ako je svaki ideal u R konačno generiran.*

Dokaz. Neka je B podmodul od A i S skup svih konačno generiranih modula od B. Kako skup S nije prazan ($0 \in S$) te sadrži maksimalan element C po Teoremu 2.1., C je konačno generiran sa $c_1, c_2, \ldots, c_n$. Za svaki $b \in B$ neka je D_b podmodul od B generiran s $b, c_1, c_2, \ldots, c_n$. Tada vrijedi

$$D_b \in S \text{ i } C \subset D_b.$$

Kako je C maksimalan, $D_b = C$ za svaki $b \in B$ i $B \subset C$. Budući da je $C \subset B$, tada je $B = C$ te je stoga B konačno generiran.
Neka je dan lanac podmodula $A_1 \subset A_2 \subset A_3 \subset \ldots$ Može se vidjeti da je $\cup_{i \geq 1} A_i$ podmodul od A i da je konačno generiran pomoću $a_1, a_2, \ldots, a_k$. Kako za svaki element a_i nekog A_j postoji indeks n takav da je $a_i \in A_n$ za $i = 1, 2, \ldots, k$. Prema tome, $\cup_{i \geq 1} A_i \subset A_n$, odakle je $A_i = A_n$ za $i \geq n$. □

Definirajmo nekoliko pojmova pomoću kojih ćemo dokazati idući teorem. **Normalni niz** za modul A je lanac podmodula: $A = A_0 \supset A_1 \supset A_2 \supset \ldots \supset A_n$. Faktori niza su kvocijentni moduli A_i/A_{i+1}, $i = 1, \ldots, n-1$. **Duljina niza** je broj pravilnih inkluzija (= broj netrivijalnih faktora). **Profinjenje normalnog niza** $A_0 \supset A_1 \supset \ldots \supset A_n$ je normalni niz dobiven umetanjem konačnog broja dodatnih podmodula između zadanih. **Pravilno profinjenje** je ono koje ima duljinu veću od izvornog niza. Dva normalna niza su ekvivalenta ako postoji bijekcija između netrivijalnih faktora tako da su odgovarajući faktori izmorfni moduli. Dakle, ekvivalentni nizovi nužno imaju istu duljinu. **Kompozicioni niz** za A je normalni niz $A = A_0 \supset A_1 \supset \ldots \supset A_n$ takav da je svaki faktor A_k/A_{k+1} nenul modul bez pravih podmodula. Svaka dva normalna niza modula A imaju definiranja koja su ekvivalentna. Bilo koja dva kompoziciona niza od A su ekvivalentna.

Teorem 2.5. *[4, Theorem VIII.1.11.] Modul A različit od nule ima kompozicioni niz ako i samo ako A zadovoljava uvjete uzlaznog i silaznog lanca na podmodulima.*

Dokaz. Pretpostavimo da A ima kompozicijski niz S duljine n. Ako je bilo koji od uvjeta lanaca nezadovoljen, onda se mogu pronaći podmoduli

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

koji tvore normalni niz T duljine $n+1$. S i T imaju profinjenja koja su ekvivalentna. Došli smo do kontradikcije budući da ekvivalentni nizovi imaju jednaku duljinu. Za svako definiranje kompozicije niza S mora imati istu duljinu n kao i S, dok T ima duljinu najmanje $n+1$. Stoga, A zadovoljava oba uvjeta lanca.
Neka je B nenul podmodul od A te $S(B)$ skup svih podmodula C od B tako da je $C \neq B$. Ukoliko B nema podmodule, tada je $S(B) = 0$. Neka vrijedi $S(0) = \{0\}$. Za svaki B postoji maksimalan element B' od $S(B)$. Neka je S skup svih podmodula od A i definirajmo $f : S \to S$ kao $f(B) = B'$. Postoji funkcija $\phi : \mathbb{N} \to S$ takva da je

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

Ako s A_i označimo $\phi(i)$, tada je $A \supset A_1 \supset A_2 \supset \ldots$ silazni lanac. Za neki n vrijedi $A_i = A_n$, $i \geq n$. Budući da je $A_{n+1} = A_n' = f(A_n)$ te po definiciji funkcije f vrijedi $A_{n+1} = A_n$ samo ako je $A_n = 0 = A_{n+1}$. Neka je m najmanji cijeli broj takav da je $A_m = 0$. Zatim, neka je $m \leq n$ i $A_k \neq 0$ za sve $k < m$. Nadalje, za svaki $k < m$, A_{k+1} je maksimalan podmodul od A_k takav da je $A_k \supsetneq A_{k+1}$. Prema tome, svaki A_k/A_{k+1} je različit od nule i nema prave podmodule po Teoremu 1.17. Stoga je $A \supset A_1 \supset A_2 \supset \ldots \supset A_m$ kompozicioni niz od A. □

2.2. Prosti i primarni ideali

Glavni cilj ovog potpoglavlja je proučavanje prostih struktura određenih komutativnih prstenova. Navest ćemo osnovna svojstva prostih ideala te uvesti pojam radikala. Definirat ćemo primarne ideale te na kraju raspravljati o primarnoj dekompoziciji ideala. Motivacija za većinu ovog potpoglavlja proizlazi iz proučavanja domena glavnih ideala. Konkretno, takva domena D je domena jedinstvene faktorizacije. Svaki pravi ideal od D produkt je maksimalnih (stoga i prostih) ideala, koji su određeni jedinstveno do na poredak. Svaki nenul prost ideal od D je oblika (p) gdje je p prost (ireducibilan) te vrijedi $(p)^n = (p^n)$. Prema tome, svaki pravi ideal (a) od D može se zapisati jedinstveno do na poredak u obliku $(a) = (p_1^{n_1})(p_2^{n_2}) \cdots (p_r^{n_r}) = (p_1^{n_1}) \cap (p_2^{n_2}) \cap \ldots \cap (p_r^{n_r})$, gdje je svaki $n_i > 0$ i p_i međusobno različiti prosti. Nadalje, ideal $Q = (p^n)$, p prost ima iduće svojstvo: $ab \in Q$ i $a \notin Q$ impliciraju $b^k \in Q$. Takav ideal nazivamo primarni. Prethodna diskusija pokazuje da se svaki ideal u domeni glavnih ideala na jedinstven način prikazuje kao presjek konačnih primarnih ideala. Nadalje, postoji veza između primarnih i prostih ideala. Preciznije, svaki primarni ideal $(p^n) = (p)^n$ je potencija prostog ideala.
Navedimo nekoliko činjenica o prostim idealima.

Teorem 2.6. *[4, Theorem VIII.2.1.] Ideal $P(\neq R)$ u komutativnom prstenu R je prost ako i samo ako je $R \setminus P$ multiplikativni skup.*

Dokaz. Vidjeti [4]. □

Napomena 2.1. *[4, Remark, str. 378] Skup svih prostih ideala u prstenu R nazivamo spektar prstena R.*

Teorem 2.7. *[4, Theorem VIII.2.2.] Neka je S multiplikativni podskup prstena R koji je disjunktan s idealom I od R. Tada postoji ideal P koji je maksimalan u skupu svih ideala od R koji su disjunktni sa S i sadrže I. Svaki takav ideal P je prost.*

Dokaz. Vidjeti [4]. □

Teorem 2.8. *[4, Theorem VIII.2.3.] Neka je K potprsten komutativnog prstena R. Ako su $P_1, P_2, \ldots, P_n$ prosti ideali od R takvi da je $K \subset P_1 \cup P_2 \cup \ldots \cup P_n$, tada je $K \subset P_i$ za neki i.*

Napomena 2.2. *[4, Remark, str. 378] U slučaju $n \leq 2$, sljedeći dokaz ne koristi pretpostavku da je svaki P_i prost; pretpostavka je potrebna za $n > 2$.*

Dokaz. Pretpostavimo da je $K \nsubseteq P_i$. Nadalje, pretpostavimo da je $n > 1$ i da je minimalan, tj. za svaki i, $K \nsubseteq \bigcup_{j \neq i} P_j$. Tada, za svaki i postoji $a_i \in K \setminus \bigcup_{j \neq i} P_j$. Pošto je $K \subset \bigcup_i P_i$, tada je $a_i \in P_i$. Element $a_1 + a_2 a_3 \cdots a_n$ je iz K, a stoga je i iz $\bigcup_i P_i$. Prema tome je $a_1 + a_2 a_3 \cdots a_n = b_j$, $b_j \in P_j$. Ako je $j > 1$, tada je $a_1 \in P_j$, što je kontradikcija. Ako je $j = 1$, tada je $a_2 a_3 \cdots a_n \in P_1$, odakle prema Teoremu 1.7. slijedi $a_i \in P_1$ za svaki $i > 1$, što je kontradikcija. □

Propozicija 2.1. *[4, Proposition VIII.2.4.] Ako je R komutativan prsten s jedinicom i P ideal koji je maksimalan u skupu svih ideala od R koji nisu konačno generirani, onda je P prost.*

Dokaz. Pretpostavimo da je $ab \in P$, ali $a \notin P$ i $b \notin P$. Tada su $P + (a)$ i $P + (b)$ ideali koji sadrže P pa su stoga konačno generirani. Posljednično vrijedi, $P + (a) = (p_1 + r_1a, \ldots, p_n + r_na)$ i $P + (b) = (p'_1 + r'_1b, \ldots, p'_m + r'_mb)$ za neke p_i, $p'_i \in P$ i r_i, $r'_i \in R$ (Teoremi 1.5. i 1.6.). Ako je $J = \{r \in R | ra \in P\}$, tada je J ideal. Budući da je $ab \in P$, $(p'_i + r'_ib)a = p'_ia + r'_iab \in P$ za svaki i, slijedi da je $P \subsetneq P + (b) \subset J$. Zbog maksimalnosti od P je $J = (j_1, j_2, \ldots, j_k)$ konačno generiran. Ako je $x \in P$, tada je $x \in P + (a)$ te za neki $s_i \in R$, $x = \sum_{i=1}^{n} s_i(p_i + r_ia) = \sum_{i=1}^{n} s_ip_i + \sum_{i=1}^{n} s_ir_ia$. Prema tome, $(\sum_i s_ir_i)a = x - \sum_i s_ip_i \in P$, odakle je $\sum_i s_ir_i \in J$. Za neki $t_i \in R$ vrijedi, $\sum_{i=1}^{n} s_ir_i = \sum_{i=1}^{k} t_ij_i$ i $x = \sum_{i=1}^{n} s_ip_i + \sum_{i=1}^{k} t_ij_ia$. Prema tome, P je generiran s $p_1, p_2, \ldots, p_n, j_1a, j_2a, \ldots, j_ka$, što je kontradikcija. Dakle, $a \in P$ ili $b \in P$ i P je prost prema Teoremu 1.7. □

Definirajmo sada pojam radikala ili nilradikala.

Definicija 2.4. *[4, Definition 8.2.5.] Neka je I ideal u komutativnom prstenu R. Radikal (ili nilradikal) od I s oznakom $RadI$ je presjek svih prostih ideala u R koji sadrže I. Ako skup prostih ideala koji sadrže I prazan, tada je $RadI$ definiran kao R.*

Napomena 2.3. *[4, Remark, str. 379] Ako je R prsten s jedinicom, svaki ideal $I(\neq R)$ je sadržan u maksimalnom idealu M prema Teoremu 1.9. Kako je $M \neq R$ i M nužno prost prema Teoremu 1.10. slijedi da je $RadI \neq R$. Radikal nul-ideala zove se nilradikal ili prost radikal prstena R.*

Primjer 2.2. *U svakoj je integralnoj domeni nul-ideal prost pa vrijedi $Rad0 = 0$.*
U prstenu $\mathbb{Z}$ je $Rad(12) = (2) \cap (3) = (6)$ i $Rad(4) = (2) = Rad(32)$.

Teorem 2.9. *[4, Theorem VIII.2.6.] Ako je I ideal u komutativnom prstenu R, tada je $RadI = \{r \in R \mid r^n \in I \text{ za } n > 0\}$.*

Dokaz. Ako je $RadI = R$, tada je $\{r \in R \mid r^n \in I\} \subset RadI$. Pretpostavimo da je $RadI \neq R$. Ako je $r^n \in I$ i P prost ideal koji sadrži I, tada je $r^n \in P$, odakle je $r \in P$ (Teorem 1.7.). Dakle, $\{r \in R \mid r^n \in I\} \subseteq RadI$.
Obrnuto, ako je $t \in R$ i $t^n \notin I$ za sve $n > 0$, tada je $S = \{t^n + x \mid n \in \mathbb{N},\ x \in I\}$ multiplikativan skup, takav da je $S \cap I = \emptyset$. Prema Teoremu 2.7. postoji prost ideal P disjunktan sa S koji sadrži I. Budući da $t \notin P$, vrijedi $t \notin RadI$. Dakle, $t \notin \{r \in R \mid r^n \in I\}$ implicira $t \notin RadI$ pa slijedi $RadI \subseteq \{r \in R \mid r^n \in I\}$. □

Navedimo nekoliko svojstava radikala.

Teorem 2.10. *[4, Theorem VIII.2.7.] Ako su $I_1, I_2, \ldots I_n$ ideali u komutativnom prstenu R, tada vrijedi:*
1. $Rad(RadI) = RadI$,
2. $Rad(I_1I_2 \cdots I_n) = Rad(\bigcap_{j=1}^{n} I_j) = \bigcap_{j=1}^{n} RadI_j$,
3. $Rad(I^m) = RadI$.

Dokaz. Vidjeti [4]. □

Nakon što smo na početku potpoglavlja započeli diskusiju o primarnim idealima sada ćemo ih i definirati.

Definicija 2.5. *[4, Definition VIII.2.8.] Kažemo da je ideal Q u komutativnom prstenu R ($Q \neq R$) primaran ako za sve $a, b \in R$ vrijedi:*

$$ab \in Q \text{ i } a \notin Q \Rightarrow b^n \in Q \text{ za neki } n > 0.$$

Uočimo da je svaki prost ideal ujedno i primarni.

Primjer 2.3. *Ako je F polje, ideal (x, y) je maksimalan u $F[x, y]$ pa stoga i prost. Nadalje, vrijedi $(x, y)^2 = (x^2, xy, y^2) \subsetneqq (x^2, y) \subsetneqq (x, y)$. Ideal (x^2, y) je primarni i (x, y) je jedini prost ideal koji sadrži (x^2, y). Stoga primarni ideal (x^2, y) nije potencija niti jednog prostog ideala u $F[x, y]$.*

U ostatku potpoglavlja pretpostavljamo da svi promatrani prstenovi imaju jedinicu.

Teorem 2.11. *[4, Theorem VIII.2.9.] Ako je Q primaran ideal u komutativnom prstenu R, tada je $RadQ$ prost ideal.*

Dokaz. Pretpostavimo da $ab \in RadQ$ i $a \notin RadQ$. Tada je $a^n b^n = (ab)^n \in Q$ za neki n. Budući da je Q primarni, postoji cijeli broj $m > 0$ takav da je $(b^n)^m \in Q$, odakle je $b \in RadQ$. Prema tome je $RadQ$ prost po Teoremu 1.7. □

Ako je Q primarni ideal u komutativnom prstenu R, tada radikal P od Q nazivamo **pridruženim** prostim idealom od Q. Kaže se da je Q primarni ideal koji pripada prostom P ili da je Q primaran za P ili da je Q P - primarni. Za dani primarni ideal Q, pridruženi prost ideal $RadQ$ je jedinstven. Međutim, dani prost ideal može biti pridruženi prost ideal i za više različitih primarnih ideala.

Teorem 2.12. *[4, Theorem VIII.2.10.] Neka su Q i P ideali u komutativnom prstenu R. Tada je Q primaran za P ako i samo ako:*
1. *$Q \subset P \subset RadQ$ i*
2. *ako je $ab \in Q$ i $a \notin Q$, tada je $b \in P$.*

Dokaz. Vidjeti u [4]. □

Teorem 2.13. *[4, Theorem VIII.2.11.] Ako su $Q_1, Q_2, \ldots, Q_n$ primarni ideali u komutativnom prstenu R, od kojih su svi primarni za prost ideal P, tada je $\bigcap_{i=1}^n Q_i$ također primarni ideal koji pripada P.*

Dokaz. Neka je $Q = \bigcap_{i=1}^n Q_i$. Tada je prema Teoremu 2.10.(2.) $RadQ = \bigcap_{i=1}^n RadQ_i = \bigcap_{i=1}^n P = P$ te posebno $Q \subset P \subset RadQ$. Ako $ab \in Q$ i $a \notin Q$, tada je $ab \in Q_i$ i $a \notin Q_i$ za neki i. Budući da je Q_i P - primaran, tada je $b \in P$ prema Teoremu 2.12.(2.). Prema tome, Q je P - primaran prema Teoremu 2.12. □

Na kraju potpoglavlja definirajmo primarnu dekompoziciju o kojoj ćemo puno više pisati u idućem potpoglavlju.

Definicija 2.6. *[4, Definition VIII.2.12.] Kažemo da ideal I u komutativnom prstenu R ima primarnu dekompoziciju ako je $I = Q_1 \cap Q_2 \cap \ldots \cap Q_n$, Q_i primaran. Ako Q_i ne sadrži $Q_1 \cap \ldots \cap Q_{i-1} \cap Q_{i+1} \cap \ldots \cap Q_n$ i radikali od Q_i su svi međusobno različiti, tada se kaže da je primarna dekompozicija reducirana.*

Teorem 2.14. *[4, Theorem VIII.2.13.] Neka je I ideal u komutativnom prstenu R. Ako I ima primarnu dekompoziciju, tada I ima reduciranu primarnu dekompoziciju.*

Dokaz. Ako je $I = Q_1 \cap Q_2 \cap \ldots Q_n$ te neki Q_i sadrži $Q_1 \cap Q_2 \cap Q_{i-1} \cap Q_{i+1} \ldots \cap Q_n$, tada je $I = Q_1 \cap Q_2 \cap Q_{i-1} \cap Q_{i+1} \ldots \cap Q_n$ također primarna dekompozicija. Uklanjanjem Q_i imamo $I = Q_1 \cap Q_2 \cap \ldots \cap Q_k$ bez Q_i koji sadrži presjek nekog drugog Q_j. Neka su $P_1, P_2, \ldots, P_r$ različiti prosti ideali u skupu $\{RadQ_1, RadQ_2, \ldots, RadQ_k\}$ i neka je Q_i' $(1 \leq i \leq r)$ presjek svih Q'-ova koji pripadaju prostom P_i. Prema Teoremu 2.13. svaki Q_i' je primaran za P_i. Niti jedan Q_i' ne sadrži presjek svih ostalih Q_j'. Prema tome, $I = \bigcap_{i=1}^{k} Q_i = \bigcap_{i=1}^{r} Q_i'$ pa I ima reduciranu primarnu dekompoziciju. □

2.3. Primarna dekompozicija

U ovom potpoglavlju proširit ćemo rezultate iz prethodnog potpoglavlja na module. Iskaz o jedinstvenosti za reducirane primarne dekpomozicije (ideala ili podmodula) dokazat će se kao i činjenica da svaki podmodul (ideal) Noetherina modula (prstena) ima primarnu dekompoziciju. Kroz čitavo ovo potpoglavlje svi su prstenovi komutativni s jedinicom te su svi moduli jedinstveni.

Definicija 2.7. *[4, Definition VIII.3.1.] Neka je R komutativan prsten s jedinicom i B R-modul. Podmodul $A(\neq B)$ je primarni pod uvjetom:*

$$r \in R,\ b \notin A \text{ i } rb \in A \Rightarrow r^n B \subset A \text{ za neki prirodan broj } n.$$

Primjer 2.4. *Promotrimo prsten R kao R-modul i neka je Q primarni ideal (time je i podmodul) od R. Ako je $rb \in Q$, $r \in R$, $b \notin Q$, tada je $r^n \in Q$ za neki n. Kako je Q ideal, imamo $r^n R \subset Q$. Stoga je Q primarni podmodul od modula R. Obrnuto, svaki primarni podmodul od R je primarni ideal. Prema tome, svi rezultati o primarnim podmodulima primjenjuju se i na primarne ideale.*

Teorem 2.15. *[4, Theorem VIII.3.2.] Neka je R komutativan prsten s jedinicom i A primarni podmodul R-modula B. Tada je $Q_A = \{r \in R \mid rB \subset A\}$ primarni ideal u R.*

Dokaz. Budući da je $A \neq B$, $1_R \notin Q_A$, vrijedi $Q_A \neq R$. Ako je $rs \in Q_A$ i $s \notin Q_A$, tada je $sB \nsubseteq A$. Stoga, za neke $b \in B$, $sb \notin A$, ali $r(sb) \in A$. Budući da je A primaran $r^n B \subset A$ za neke n, tj. $r^n \in Q_A$. Stoga je Q_A primaran. □

Neka su R, A, B i Q_A iz Teorema 2.15. Prema Teoremu 2.11. $RadQ_A = P_1$ je prost ideal gdje je $P_1 = \{r \in R \mid r^n B \subset A \text{ za neki } n > 0\}$. Kaže se da primarni podmodul A modula B pripada prostom idealu P ili da je P- primarni podmodul od B ako je $P = RadQ_A = \{r \in R \mid r^n B \subset A \text{ za neki } n > 0\}$. Posebno, ako je J primarni ideal, tada je $Q_J = J$.

Definicija 2.8. *[4, Definition VIII.3.3.] Neka je R komutativan prsten s jedinicom i B R-modul. Podmodul C od B ima primarnu dekompoziciju ako je $C = A_1 \cap A_2 \cap \ldots \cap A_n$, sa svakim A_i P_i- primarnim podmodulom od B za neki prost ideal P_i od R. Ako niti jedan A_i ne sadrži $A_1 \cap A_2 \cap \ldots \cap A_{i-1} \cap A_{i+1} \cap \ldots \cap A_n$ i ako su svi ideali $P_1, \ldots, P_n$ različiti, tada za primarnu dekompoziciju kaže se da je reducirana.*

Ako su C, A_i i P_i kao iz prethodne definicije i $P_j \nsubseteq P_i$ za svaki $j \neq i$, tada se za P_i kaže da je **izolirani** prost ideal od C. P_i je izoliran ako je minimalan u skupu $\{P_1, \ldots, P_n\}$. Za P_i koji nije izoliran kažemo da je uložen.

Teorem 2.16. *[4, Theorem VIII.3.4.] Neka je R komutativan prsten s jedinicom i B R-modul. Ako podmodul C od B ima primarnu dekompoziciju, tada C ima reduciranu primarnu dekompoziciju.*

Dokaz. Vidjeti u [4]. □

Teorem 2.17. *[4, Theorem VIII.3.5.] Neka je R komutativan prsten s jedinicom i B R-modul. Nadalje, neka je $C(\neq B)$ podmodul od B s dvije reducirane primarne dekompozicije,*

$$A_1 \cap A_2 \cap \ldots \cap A_k = C = A'_1 \cap A'_2 \cap \ldots \cap A'_s,$$

gdje je A_i P_i- primaran i A'_j P'_j- primaran. Tada je $k = s$ i $P_i = P'_i$ za $i = 1, 2, \ldots, k$. Nadalje, ako su A_i i A'_i zajedno P_i primarni i P_i izolirani prost, tada je $A_i = A'_i$.

Dokaz. Pretpostavimo da je P_1 maksimalan u skupu $\{P_1, P_2, \ldots, P_k, P'_1, P'_2, \ldots, P'_s\}$. Pokažimo prvo da je $P_1 = P'_j$ za neki j. Pretpostavimo suprotno, tj. neka je $P_1 \neq P'_j$, za $j = 1, 2, \ldots, s$. Kako je P_1 maksimalan, tada je $P_1 \nsubseteq P'_j$ za $j = 1, 2, \ldots, s$. Budući da je prva dekompozicija reducirana, $P_1, P_2, \ldots, P_k$ različiti, slijedi da je $P_1 \nsubseteq P_i$, za $i = 1, 2, \ldots, k$. Po kontrapoziciji teorema 2.8. vrijedi $P_1 \nsubseteq P_2 \cup P_3 \cup \ldots \cup P_k \cup P'_1 \cup P'_2 \ldots \cup P'_s$. Stoga postoji $r \in P_1$ takav da je $r \notin P_i$ $(i \geq 2)$ i $r \notin P'_j$ $(j \geq 1)$. Budući da je $A_1 P_1$- primaran, vrijedi $r^n B \subset A_1$ za prirodan broj n. Neka je $C^\star$ skup podmodula $\{x \in B \mid r^n x \in C\}$. Ako je $k = 1$, tada je $C = A_1$ i stoga $C^\star = B$. Tvrdimo da je za $k \geq 1$, $C^\star = C$ i za $k > 1$, $C^\star = A_2 \cap A_3 \cap \ldots \cap A_k$. Tada vrijedi $A_2 \cap A_3 \ldots \cap A_k \subset C^\star$ i $A'_1 \cap A'_2 \cap \ldots \cap A'_k = C \subset C^\star$ za $k > 1$. Obrnuto, ako $x \notin A_i (i > 2)$, tada $r^n x \notin A_i$. Prema tome, $r^n x \notin C$, odakle slijedi $x \notin C^\star$. Dakle, $C^\star \subset A_2 \cap A_3 \cap \ldots \cap A_k$ za $k > 1$. Slično se pokazuje da je $C^\star \subset A'_1 \cap A'_2 \ldots \cap A'_s = C$ pa je $C^\star = C$ za $k \geq 1$ i $C^\star = A_2 \cap A_3 \cap \ldots A_k$ za $k > 1$. Ako je $k = 1$, tada je $C^\star = B$. Dakle, $C = C^\star = B$ što je u kontradikciji s pretpostavkom $C \neq B$. Ako je $k > 1$, tada je

$$A_2 \cap A_3 \cap \ldots \cap A_k = C^\star = C = A_1 \cap A_2 \cap \ldots \cap A_k$$

te odatle slijedi da je $A_2 \cap A_3 \cap \ldots \cap A_k \subset A_1$. Ovo je u kontradikciji sa činjenicom da je prva dekompozicija reducirana. Dakle, pretpostavka $P_1 \neq P'_j$ za svaki j dovodi do kontradikcije. Vrijedi, $P_1 = P'_j$ za neki j, npr. za $j = 1$. Dokazujemo sada indukcijom po k. Ako je $k = 1$, tada je također i $s = 1$. Ukoliko je $s > 1$, tada gornji dokaz s $P_1 = P'_1$ i ulogama A_i, A'_i obrnut, pokazuje da je $B = C^\star = A'_2 \cap A'_3 \cap \ldots \cap A'_s$, odakle slijedi da je $A'_j = B$ za neki $j \geq 2$. Dakle, druga dekompozicija od C nije reducirana što je kontradikcija. Stoga je $s = 1 = k$ i $A_1 = C = A'_1$. Pretpostavimo sada da je $k > 1$ te da je teorem točan za sve podmodule koji imaju reduciranu primarnu dekompoziciju manje od k članova. Dokaz iz prethodnog dijela (s $P_1 = P'_1$) pokazuje da za $k > 1$ podmodul $C^\star$ ima dvije reducirane primarne dekompozicije:

$$A_2 \cap A_3 \cap \ldots \cap A_k = C^\star = A'_2 \cap A'_3 \cap \ldots \cap A'_s.$$

Indukcijom za $k = s$ i $P_i = P'_i$ za sve i. Time je završen induktivni dokaz prvog dijela teorema.
Pretpostavimo da su A_i i A'_i oba P_i -primarna i da je P_i izolirano prost. Radi jednostavnosti pretpostavimo da je $i = 1$. Kako je P_1 izoliran, za svaki $j \geq 2$ je $r_j \in P_j - P_1$. Tada je $t = r_2 r_3 \cdots r_k \in P_j$ za $j > 1$, ali $t \notin P_1$. Budući da je A_j P_j- primaran, za $j \geq 2$ postoji cijeli broj n_j takav da je $r^{n_j} B \subset A_j$. Slično, za svaki $j \geq 2$ postoji m_j takav da je $t^{m_j} B \subset A'_j$. Nadalje, neka je $n = \max\{n_2, \ldots, n_k, m_2, \ldots, m_k\}$, tada vrijedi $r^n B \subset A_j$ i $t^n B \subset A'_j$ za svaki $j \geq 2$. Neka je D podmodul $\{x \in B \mid t^n x \in C\}$. Pokažimo da je $A_1 = D = A'_1$. Ako je $x \in A_1$, tada je $t^n x \in A_1 \cap A_2 \cap \ldots \cap A_k = C$, odakle je $x \in D$ i $A_1 \subset D$. Ako je $x \in D$, tada je $t^n x \in C \subset A_1$. Kako je A_1 P_1- primaran i $t \notin P_1$, imamo $t^m B \nsubseteq A_1$, za svaki $m > 0$. Budući da je A_1 primaran, mora vrijediti $x \in A_1$ (u suprotnom, $t^n x \in A_1$ i $x \notin A_1$ impliciraju $t^{nq} B \subset A_1$ za neki pozitivan q). Dakle, $D = A_1$. Identičan argument pokazuje da je $D = A'_1$. Prema tome je $A_1 = A'_1$. □

Navedimo sada teorem u kojemu ćemo navesti koji moduli (ideali) imaju primarnu dekompoziciju.

Teorem 2.18. *[4, Theorem VIII.3.6.] Neka je R komutativan prsten s jedinicom i B R-modul koji zadovoljava stanje uzlaznog lanca na podmodule. Tada svaki podmodul $A(\neq B)$ ima reduciranu primarnu dekompoziciju. Konkretno, svaki podmodul $A(\neq B)$ konačno generiranog modula B nad komutativnim Noetherinim prstenom R i svaki ideal $(\neq R)$ od R ima reduciranu primarnu dekompoziciju.*

Dokaz. Neka je S skup svih podmodula od B koji nemaju primarnu dekompoziciju. Trebamo pokazati da je S prazan. Ukoliko S nije prazan, tada sadrži maksimalan element od C prema Teoremu 2.1. Kako C nije primaran, postoji $r \in R$ i $b \in B \setminus C$ tako da je $rb \in C$, ali $r^n B \nsubseteq C$ za sve $n > 0$. Neka je $B_n = \{x \in B \mid r^n x \in C\}$. Tada je svaki B_n podmodul od B i $B_1 \subset B_2 \subset \ldots$ Prema pretpostavci postoji $k > 0$ takav da je $B_i = B_k$ za $i \geq k$. Neka je D podmodul $\{x \in B \mid x = r^k y + c \text{ za neke } y \in B, c \in C\}$. Vrijedi $C \subset B_k \cap D$. Obrnuto, ako $x \in B_k \cap D$, tada $x = r^k y + c$ i $r^k x \in C$, slijedi $r^{2k} y = r^k(r^k y) = r^k(x - c) = r^k x - r^k c \in C$. Dakle, $y \in B_{2k} = B_k$. Dakle, $r^k y \in C$ pa stoga $x = r^k y + c \in C$. Prema tome je $B_k \cap D \subset C$ pa slijedi $B_k \cap D = C$. Kako je $b \in B_k \setminus C$ i $r^k B \nsubseteq C$ vrijedi, $C \neq B_k \neq B$ i $C \neq D \neq B$. Prema maksimumu od C u S, D i B_k moraju imati primarnu dekompoziciju. Dakle, C ima primarnu dekompoziciju što je kontradikcija. Prema tome, S je prazan i svaki podmodul ima primarnu dekompoziciju. Posljedično, svaki podmodul ima reduciranu primarnu dekompoziciju. □

2.4. Noetherini prstenovi i moduli

U prvom dijelu ovog potpoglavlja bavit ćemo se Noetherinim modulima koji zadovoljavaju uvjet uzlaznog lanca. Iskazat i dokazat ćemo Krullov teorem. Također, navest ćemo i Nakayaminu lemu te nekoliko posljedica te leme. U drugom dijelu ovog potpoglavlja, koji ne ovisi o prvom dijelu, iskazat ćemo i dokazati Hilbertov teorem o bazi te teorem koji pokazuje da je $R[[x]]$ komutativan Noetherinov prsten s jedinicom. Podsjetimo se, komutativan prsten R je Noetherin ako i samo ako R zadovoljava maksimalni uvjet na (obostrane) ideale (Definicija 2.2. i Teorem 2.1.).

Propozicija 2.2. *[4, Theorem VIII.4.1.] Komutativan prsten R s jedinicom je Noetherin ako i samo ako je svaki prost ideal od R konačno generiran.*

Dokaz. Vidjeti u [4]. □

Sada navedimo potrebne podatke za dokazivanje Krullovog teorema. Ako je B modul nad komutativnim prstenom R, tada je $I = \{r \in R \mid rb = 0 \text{ za svaki } b \in B\}$ ideal od R. Ideal I nazivamo **anhilator** od B u R.

Lema 2.1. *[4, Lemma VIII.4.2.] Neka je B konačno generirani modul nad komutativnim prstenom R s jedinicom i neka je I anhilator od B u R. Tada B zadovoljava uvjet uzlaznog lanca na podmodulima ako i samo ako je R/I Noetherin.*

Dokaz. Vidjeti u [4]. □

Ukoliko je I bilo koji ideal u prstenu R s jedinicom i B R-modul, tada je $IB = \{\sum_{i=1}^{n} r_i b_i \mid r_i \in I, b_i \in B, n \in N\}$ podmodul od B.

Lema 2.2. *[4, Lemma VIII.4.3.] Neka je P prost ideal u komutativnom prstenu R s jedinicom. Ako je C P primaran podmodul Noetherinovog R-modula A, tada postoji pozitivan cijeli broj m takav da je $P^m A \subset C$.*

Dokaz. Neka je I anhilator od A u R i definirajmo prsten $\bar{R} = R/I$. Označimo $r + I \in \bar{R}$ s $\bar{r}$. Vrijedi $I \subset \{r \in R \mid rA \subset C\} \subset P$ te slijedi da je $\bar{P} = P/I$ ideal od $\bar{R}$. A i C su $\bar{R}$-moduli uz $\bar{r}a = ra$, gdje je $r \in R, a \in A$. Tvrdimo da je tada C primarni $\bar{R}$-podmodul od A. Ako je $\bar{r}a \in C$, $r \in R$ i $a \in A \setminus C$, tada je $ra \in C$. Kako je C primarni R-podmodul, $r^n A \subset C$ za neki n, slijedi da je $\bar{r}^n A \subset C$ i C je $\bar{R}$-primaran. Budući da je $\{\bar{r} \in \bar{R} \mid \bar{r}^k A \subset C,\ za\ neki\ k > 0\} = \{\bar{r} \in \bar{R} \mid r^k A \subset C\} = \{\bar{r} \in \bar{R} \mid r \in P\} = \bar{P}$, $\bar{P}$ je prost ideal od $\bar{R}$ i C je $\bar{P}$-primaran $\bar{R}$-podmodul od A. Kako je $\bar{R}$ Noetherin, $\bar{P}$ je konačno generiran. Neka su $\bar{p_1}, \bar{p_2}, \ldots, \bar{p_s}$, $p_i \in P$ generatori od $\bar{P}$. Za svaki i postoji n_i takav da je $\bar{p_i}^{n_i} A \subset C$. Ako je $m = n_1 + n_2 + \cdots + n_s$, tada prema Teoremima 1.3. i 1.5. vrijedi $\bar{P}^m A \subset C$. Tada $\bar{P} = P/I$ i $IA = 0$ impliciraju da je $P^m A \subset C$. □

Teorem 2.19. *(Krull) [4, Theorem VIII.4.4.] Neka je R komutativan prsten s jedinicom, I ideal od R i A Noetherin R-modul. Ako je $B = \bigcap_{n=1}^{\infty} I^n A$, tada je $IB = B$.*

Dokaz. Ako je $IB = A$, tada je $A = IB \subset B$ pa slijedi $B = A = IB$. Ako je $IB \neq A$, tada prema Teoremu 2.18. IB ima primarnu dekompoziciju: $IB = A_1 \cap A_2 \cap \ldots \cap A_s$, gdje je svaki A_i P_i- primarni podmodul od A za svaki prost ideal P_i od R. Budući da je $IB \subset B$, trebamo pokazati da je $B \subset A_i$ za svaki i kako bismo zaključili da je $B \subset IB$ pa stoga i $B = IB$. Neka je i, $1 \leq i \leq s$ fiksan. Pretpostavimo da je $I \subset P_i$. Prema prethodnoj lemi postoji cijeli broj m takav da je $P_i^m A \subset A_i$, odakle slijedi $B = \bigcap_n I^n A \subset I^m A \bigcap P_i^m A \subset A_i$. Sada pretpostavimo $I \nsubseteq P_i$. Tada postoji $r \in I \setminus P_i$. Ako je $B \nsubseteq A_i$, tada postoji $b \in B \setminus A_i$. Budući da je $rb \in IB \subset A_i$, $b \notin A_i$ i A_i je primaran, tada je $r^n A \subset A_i$ za neki $n > 0$. Stoga, $r \in P_i$ (budući da je A_i P_i- primarni podmodul). Ovo je u kontradikciji s izborom $r \in I \setminus P_i$. Dakle, $B \subset A_i$. □

Lema 2.3. *(Nakayama) [4, Lemma VIII.4.5.] Ako je J ideal u komutativnom prstenu R s jedinicom, tada su sljedeće tvrdnje ekvivalentne:*
1. *J je sadržan u svakom maksimalnom idealu od R.*
2. *$1_R - j$ je invertibilan za svaki $j \in J$.*
3. *Ako je A konačno generirani R-modul takav da je $JA = A$, tada je $A = 0$.*
4. *Ako je B podmodul konačno generiranog R-modula A takav da je $A = JA + B$, tada je $A = B$.*

Dokaz. 1. $\Rightarrow$ 2. Ako $j \in J$ i $1_R - j$ nije invertibilan, tada ideal $(1_R - j)$ različit od R (Teorem 1.11.) i stoga je sadržan u maksimalnom idealu $M \neq R$ (Teorem 1.9.). Kako $1_R - j \in M$ i $j \in J \subset M$ impliciraju da je $1_R \in M$ dolazimo do kontradikcije. Dakle, $1_R - j$ je invertibilan.
2. $\Rightarrow$ 3. Kako je A konačno generiran, mora postojati minimalan skup $X = \{a_1, a_2, \ldots, a_n\}$ koji generira A. Ako je $A \neq 0$, tada je $a_1 \neq 0$ minimalan. Budući da je $JA = A$, $a_1 = j_1 a_1 + j_2 a_2 + \cdots + j_n a_n$ $(j_i \in J)$, vrijedi $1_R a_1 = a_1$ tako da je $(1_R - j_1)a_1 = 0$ ako je $n = 1$ i $(1_R - j_1)a_1 = j_2 a_2 + \cdots + j_n a_n$ za $n > 1$. Kako je $1_R - j_1$ jedinica u R, $a_1 = (1_R - j_1)^{-1}(1_R - j_1)a_1$. Dakle, za $n = 1$ je $a_1 = 0$ što je kontradikcija. Za $n > 1$, a_1 je linearna kombinacija od $a_2, a_3, \ldots, a_n$. Dakle, $\{a_2, a_3, \ldots, a_n\}$ generira A, što je u kontradikciji s izborom od X.
3. $\Rightarrow$ 4. Kvocijentni modul A/B je takav da vrijedi $J(A/B) = A/B$ pa slijedi $A/B = 0$ i $A = B$.
4. $\Rightarrow$ 1. Ako je M maksimalni ideal, tada ideal $JR + M$ sadrži M. Vrijedi, $JR + M \neq R$

jer bi u suprotnosti bilo $R = M$. Prema tome, $JR + M = M$ prema maksimalnosti. Dakle, $J = JR \subset M$. □

Sada ćemo navesti nekoliko posljedica Nakayamine leme.

Propozicija 2.3. *[4, Proposition 8.4.6.] Neka je J ideal u komutativnom prstenu s jedinicom. Tada je J sadržan u svakom maksimalnom idealu od R ako i samo ako za svaki R-modul A koji zadovoljava uvjet uzlaznog lanca na podmodule vrijedi $\bigcap_{n=1}^{\infty} J^n A = 0$.*

Dokaz. ($\Rightarrow$) Za $B = \bigcap_n J^n A$, vrijedi $JB = B$. Budući da je B konačno generiran prema Teoremu 2.4., tada je $B = 0$ prema Nakayama lemi.
($\Leftarrow$) Pretpostavimo da je $R \neq 0$. Ako je M maksimalan ideal od R, tada je $M \neq R$ i $A = R/M$ nenul R-modul koji nema prave podmodule (Teorem 1.17.). Stoga A zadovoljava uvjet uzlaznog lanca, odakle je $\bigcap_n J^n A = 0$ prema pretpostavci. Kako je JA podmodul od A, ili je $JA = A$ ili $JA = 0$. Ako je $JA = A$, tada je $J^n A = A$ za sve n. Dakle, $\bigcap_n J^n A = A \neq 0$, što je kontradikcija. Tada je $JA = 0$. Dakle, $0 = JA = J(R/M)$ implicira da je $J \subset JR \subset M$. □

Korolar 2.2. *[4, Corollary VIII.4.7.] Ako je R Noetherin lokalni prsten s maksimalnim idealom M, tada je $\bigcap_{n=1}^{\infty} M^n = 0$.*

Dokaz. Vidjeti u [4]. □

Propozicija 2.4. *[4, Proposition VIII.4.8.] Ako je R lokalni prsten, tada je svaki konačno generirani projektivni R-modul slobodan.*

Dokaz. Ako je P konačno generirani projektivni R-modul, tada prema Korolaru 1.2. postoji slobodni R-modul F s konačnom bazom i epimorfizam $\pi : F \to P$. Među svim slobodnim R-modulima s ovim svojstvom odaberimo onaj s bazom $\{x_1, x_2, \ldots, x_n\}$ koji ima minimalan broj elemenata. Kako je π epimorfizam, $\{\pi(x_1), \pi(x_2), \ldots, \pi(x_n)\}$ nužno generira P. Pokažimo prvo da je $K = Ker\pi$ sadržan u MF, gdje je M jedinstveni maksimalan ideal od R. Za $K \nsubseteq MF$ postoji $k \in K$ takav da $k \notin MF$. Sada je $k = r_1x_1 + r_2x_2 + \cdots + r_nx_n$, $r_i \in R$, jedinstveno određen. Budući da $k \notin MF$, neki r_i, recimo r_1, nije element od M. Prema Teoremu 1.15., r_1 je invertibilan pa vrijedi $x_1 - r_1^{-1}k = -r_1^{-1}r_2x_2 - \cdots - r_1^{-1}r_nx_n$. Stoga, budući da je $k \in Ker\pi$, $\pi(x_1) = \pi(x_1 - r_1^{-1}k) = \pi(\sum_{i=2}^{n} -r_1^{-1}r_ix_i) = \sum_{i=2}^{n} -r_1r_i\pi(x_i)$. Dakle, $\{\pi(x_2), \pi(x_3), \ldots, \pi(x_n)\}$ generira P. Ako je F' slobodan podmodul od F s bazom $\{x_2, x_3, \ldots, x_n\}$ i $\pi' : F' \to P$ restrikcija od π na F', tada je π' epimorfizam. Ovo je u kontradikciji s izborom baze minimalne kardinalnosti. Dakle, $K \subset MF$. Budući da je $0 \to K \xrightarrow{\subseteq} F \xrightarrow{\pi} P \to 0$ i P je projektivan, tada je $K \oplus P \cong F$ po Teoremu 1.21. Iz izomorfizma $(k, 0) \mapsto k$ za sve $k \in K$, slijedi da je F unutarnja direktna suma $F = K \oplus P'$, gdje je $P' \cong P$. Dakle, $F = K + P' \subset MF + P'$. Ako je $u \in F$, tada je $u = \sum_i m_iv_i + p_i$ gdje su $m_i \in M$, $v_i \in F$, $p_i \in P'$. Tada u R-modulu F/P' vrijedi $u + P' = \sum_i m_iv_i + P' = \sum_i m_i(v_i + P') \in M(F/P')$ pa vrijedi $M(F/P') = F/P'$. Kako je F konačno generiran, takav je i F/P'. Stoga vrijedi $K \cong F/P' = 0$ po Nakayaminoj lemi. Dakle, $P \cong P' = F$ i P je slobodan. □

Zaključimo ovo poglvlje s dva teorema čiji dokazi su neovisni s prethodnim iskazima.

Teorem 2.20. *(Hilbertov teorem o bazi) [4, Theorem VIII.4.9.] Ako je R komutativni Noetherin prsten s jedinicom, onda je takav i $R[x_1, \ldots, x_n]$.*

Dokaz. Pokazat ćemo samo da je $R[x]$ Noetherin. Prema Teoremu 2.4. trebamo pokazati da je svaki ideal J u $R[x]$ konačno generiran. Neka je $n \geq 0$ te definirajmo I_n kao skup svih $r \in R$ takvi da je $r = 0$ ili je vodeći koeficijent polinoma $f \in J$ stupnja n. Provjerimo je li svaki I_n ideal R. Ako je r nenul element od I_n i $f \in J$ polinom stupnja n s vodećim koeficijentom r, tada je r također vodeći koeficijent od xf, koji je polinom u J i stupnja je $n+1$. Stoga vrijedi $I_0 \subset I_1 \subset I_2 \subset \ldots$ Budući da je R Noetherin, postoji cijeli broj t takav da je $I_n = I_t$ za svaki $n \geq t$. Nadalje, prema Teoremu 2.4. svaki I_n je konačno generiran, gdje je $I_n = (r_{n_1}, r_{n_2}, \ldots, r_{ni_n})$. Za svaki r_{n_j}, $0 \leq n \leq t$ i $1 \leq j \leq i_n$ neka je $f_{n_j} \in J$ polinom stupnja n s vodećim koeficijentom r_{n_j}. Primjetimo da je $f_{0_j} = r_{0_j} \in R \subset R[x]$. Pokažimo da je ideal J od $R[x]$ konačno generiran skupom polinoma $X = \{f_{n_j} \mid 0 \leq n \leq t; 1 \leq j \leq i_n\}$. Vrijedi $(X) \subset J$. Obrnuto, polinomi stupnja 0 u J su elementi od I_0 i stoga su sadržani u (X). Nastavljajući induktivno, pretpostavimo da (X) sadrži sve polinome od J stupnja manjeg od k i neka $g \in J$ ima stupanj k i da mu je vodeći koeficijent $r \neq 0$. Ako je $k \leq t$, tada je $r \in I_k$ i stoga je $r = s_1 r_{k_1} + s_2 r_{k_2} + \cdots + s_{i_k} r_{i_k}$ za neki $s_j \in R$. Stoga polinom $\sum_{j=1}^{i_k} s_j f_{k_j} \in (X)$ ima vodeći koeficijent r i stupnja k. Prema tome, $g - \sum_j s_j f_{k_j}$ ima stupanj najviše $k-1$. Prema pretpostavci indukcije $g - \sum_j s_j f_{k_j} \in (X)$, vrijedi $g \in (X)$. Ako je $k \geq t$, tada je $r \in I_k = I_t$ i $r = \sum_{j=1}^{i_t} s_j r_{t_j}$, gdje je $s_j \in R$. Nadalje, $\sum_{j=1}^{i_t} s_j x^{k-t} f_{tj} \in (X)$ ima vodeći koeficijent r i stupanj k. Stoga $g - \sum_j s_j x^{k-t} f_{tj}$ ima stupanj najviše $k-1$ i pripada (X) prema pretpostavci indukcije. Prema tome, $g \in (X)$. Dakle, $J = (X)$. □

Propozicija 2.5. *[4, Theorem VIII.4.10.] Ako je R komutativni Noetherin prsten s jedinicom, onda je takav i $R[[x]]$.*

Dokaz. Dovoljno je, prema Propoziciji 2.2. dokazati da je svaki prost ideal P u $R[[x]]$ konačno generiran. Definirajmo epimorfizam prstenova $R[[x]] \to R$ preslikavanjem svakog $f = \sum_{i=0}^{\infty} a_i x^i$ na njegov konstantan član a_0. Neka je $P^\star$ slika od P ovog preslikavanja. Tada je $P^\star$ konačno generiran ideal u R, $P^\star = (r_1, r_2, \ldots, r_n)$. Za svaki r_i odaberimo $f_i \in P$ s konstantnim članom r_i. Ako je $x \in P$, tvrdimo da je P generiran s $r_1, r_2, \ldots, r_n, x$. Primjetimo ako je $f_k = r_k + \sum_{i=1}^{\infty} a_i x^i$, tada je $r_k = f_k - x(\sum_{j=0}^{\infty} a_{j+1} x^j) \in P$. Nadalje, ako je $g = \sum_{i=0}^{\infty} b_i x^i \in P$, tada je $b_0 = s_1 r_1 + s_2 r_2 + \cdots + s_n r_n$ za neki $s_i \in R$. Prema tome, $g - \sum_{i=1}^{n} s_i r_i$ ima konstantan član jednak nuli, tj. $g - \sum_i s_i r_i = x g_1$ ($g_1 \in R[[x]]$). Stoga je $g = \sum_i s_i r_i + x g_1$ i P je generiran s $r_1, r_2, \ldots, r_n, x$. Ako $x \notin P$, tvrdimo da je P generiran s $f_1, f_2, \ldots, f_n \in P$. Za $h = \sum_{i=0}^{\infty} c_i x^i \in P$ vrijedi $c_0 = t_1 r_1 + t_2 r_2 + \cdots + t_n r_n$, za neki $t_i \in R$. Dakle, $h - \sum_{i=1}^{n} t_i f_i = x h^\star$ za neki $h^\star \in R[[x]]$. Budući da $x \notin P$, $x h^\star = h - \sum_i t_i f_i \in P$ i P je prost, imamo $h^\star \in P$. Za svaki $h \in P$, odaberimo $t_i \in R$ i $h^\star \in P$ tako da je $h = \sum_{i=1}^{m} t_i f_i + x h^\star$. Neka je $\lambda : P \to P$ preslikavanje definirano s $h \mapsto h^\star$. Neka je g bilo koji element od P. Tada prema Teoremu o rekurziji imamo funkciju $\phi : N \to P$ tako da je $\phi(0) = g$ i $\phi(k+1) = \lambda(\phi(k)) = \phi(k)^\star$. Neka je $\phi(k) = h_k \in R[[x]]$ i označimo s t_{ki} prethodno odabrane elemente iz R tako da je $h_k = \sum_{i=1}^{n} t_{ki} f_i + x h_k^\star = \sum_{i=1}^{n} t_{ki} f_i + x h_{k+1}$. Za svaki i, $1 \leq i \leq n$ neka je $g_i = \sum_{k=0}^{\infty} t_{ki} x^k \in R[[x]]$. Tada vrijedi,

$$g_1 f_1 + g_2 f_2 + \cdots + g_n f_n = \sum_{i=1}^{n} (\sum_{k=0}^{\infty} t_{ki} x^k) f_i = \sum_{k=0}^{\infty} (\sum_{i=1}^{n} t_{ki} f_i) x^k = \sum_{k=0}^{\infty} (h_k - x h_{k+1}) x^k.$$

Prema tome, za svaki $m \geq 0$ koeficijent uz x^m u $g_1 f_1 + g_2 f_2 + \cdots + g_n f_n$ je isti kao i koeficijent uz x^m u $\sum_{k=0}^{m} (h_k - x h_{k+1}) x^k$. Budući da je $\sum_{k=0}^{m} (h_k - x h_{k+1}) x^k = h_0 - x^{m+1} h_{m+1} = g - x^{m+1} h_{m+1}$, tada koeficijent uz x^m u $f_1 g_1 + f_2 g_2 + \cdots + f_n g_n$ je upravo koeficijent uz x^m u g. Dakle, $g = g_1 f_1 + g_2 f_2 + \cdots + g_n f_n$ i $f_1, f_2, \ldots, f_n$ generiraju P. □

2.5. Proširenja prstenova

U prvom dijelu potpoglavlja definirat ćemo proširenje prstena te ćemo navesti bitna svojstva cijelih proširenja. Drugi dio ovog potpoglavlja odnosi se na proučavanje odnosa između prostih ideala u prstenovima R i S, gdje je S proširenje prstena R. U ovom potpoglavlju svi prstenovi su komutativni s jedinicom.

Definicija 2.9. *[4, Definition VIII.5.1.] Neka je S komutativan prsten s jedinicom i R potprsten od S koji sadrži 1_S. Tada za S kažemo da je proširenje prstena R.*

Primjer 2.5. *Svako proširenje polja F od K je proširenje prstena$K$. Ako je R komutativan prsten s jedinicom, tada su $R[x_1, x_2, \ldots, x_n]$ i $R[[x]]$ proširenja prstena R. Prsten cijelih brojeva nije proširenje potprstena parnih cijelih brojeva P jer P ne sadrži 1.*

Definicija 2.10. *[4, Definition VIII.5.2.] Neka je S proširenje prstena R i $s \in S$. Ako postoji normirani polinom $f(x) \in R[x]$ takav da je s korijen od f (tj. $f(s) = 0$), tada kažemo da je s cijeli nad R. Ako je svaki element iz S cijeli nad R, tada se za S kaže da je cijelo proširenje od R.*

Primjer 2.6. *Svako algebarsko proširenje polja F od polja K je cijelo proširenje prstena. Prsten $\mathbb{R}$ je cijeli nad samim sobom budući je $r \in \mathbb{R}$ korijen od $x - r \in \mathbb{R}[x]$. U proširenju $\mathbb{Z}$ s poljem realnih brojeva $\mathbb{R}$, $1/\sqrt{3}$ je algebarski nad $\mathbb{Z}$ budući je korijen od $3x^2 - 1$, ali $1/\sqrt{3}$ nije cijeli nad $\mathbb{Z}$. Također, $1/\sqrt{3}$ je cijeli nad poljem racionalnih brojeva $\mathbb{Q}$.*

Neka je S proširenje prstena R i X podskup od S. Kažemo da je presjek svih potprstena od S koji sadrže $X \cup R$ potprsten od S generiran s X nad R, te označavamo s $R[X]$. $R[X]$ sastoji od svih elemenata $f(s_1, \ldots s_n), n \in \mathbb{N}, f \in R[x_1, \ldots, x_n]$ i $s_i \in X$. Posebno, za bilo koji $s_1, \ldots, s_t \in S$ potprsten generiran s $s_1, \ldots, s_t$ nad R, u oznaci s $R[s_1, \ldots, s_t]$, sadrži sve elemente $f(s_1, \ldots, s_t), f \in R[x_1, \ldots, x_t]$. $R[s_1, \ldots, s_t]$ ne mora biti izomorfan prstenu $R[x_1, \ldots, x_t]$. Za svaki $i, 1 \leq i \leq t$, vrijedi $R[s_1, \ldots, s_{i-1}][s_i] = R[s_1, \ldots, s_i]$. Kako je $R[s_1, \ldots, s_t]$ prsten koji sadrži R, $R[s_1, \ldots, s_t]$ je R-modul. Također vrijedi, svaki modul nad $R[s_1, \ldots, s_t]$ je ujedno i R-modul.

Teorem 2.21. *[4, Theorem VIII.5.3.] Neka je S proširenje prstena R i $s \in S$. Tada su sljedeće tvrdnje ekvivalentne:*
1. *s je cijeli nad R,*
2. *$R[s]$ je konačno generirani R-modul,*
3. *postoji potprsten T od S koji sadrži 1_S i $R[s]$ koji je konačno generiran kao R-modul.*

Dokaz. Vidjeti u [4]. □

Korolar 2.3. *[4, Corollary VIII.5.4.] Ako je S proširenje prstena R i S konačno generiran kao R-modul, tada je S cijelo proširenje od R.*

Dokaz. Vidjeti u [4]. □

Dokazi sljedećih tvrdnji ovise o sljedećem: Ako su $R \subset S \subset T$ prstenovi tako da je T konačno generirani S-modul i S je konačan generirani R-modul, tada je T konačno generirani R-modul.

Teorem 2.22. *[4, Theorem VIII.5.5.] Ako je S proširenje prstena R i $s_1, s_2, \ldots, s_t \in S$ cijeli nad R, tada je $R[s_1, s_2, \ldots, s_t]$ konačno generirani R-modul i cijelo proširenje prstena R.*

Dokaz. Vrijedi iduće: $R \subset R[s_1] \subset R[s_1, s_2] \subset \ldots \subset R[s_1, s_2, \ldots, s_t]$. Za svaki i, s_i je cijeli nad R i prema tome cijeli nad $R[s_1, \ldots, s_{i-1}]$. Budući da je $R[s_1, \ldots, s_i] = R[s_1, \ldots, s_{i-1}][s_i]$, $R[s_1, \ldots, s_i]$ je konačno generirani modul nad $R[s_1, \ldots, s_{i-1}]$ po Teoremu 2.21. Primjenom prethodne napomene dobivamo da je $R[s_1, \ldots, s_n]$ konačno generirani R-modul. Dakle, $R[s_1, \ldots, s_n]$ je cijelo proširenje prstena R prema prethodnom korolaru. □

Teorem 2.23. *[4, Theorem VIII.5.6.] Ako je T cijelo proširenje prstena S i S cijelo proširenje prstena R, tada je T cijelo proširenje prstena R.*

Dokaz. Neka je T proširenje prstena R. Ako je $t \in T$, tada je t cijel nad S i prema tome korijen nekog polinoma $f \in S[x]$ kojemu je vodeći koeficijent 1, primjerice $f = \sum_{i=0}^{n} s_i x^i$. Kako je f također polinom nad prstenom $R[s_0, s_1, \ldots, s_{n-1}]$, t je cijel nad $R[s_0, s_1, \ldots, s_{n-1}]$. Prema Teoremu 2.21. $R[s_0, \ldots, s_{n-1}][t]$ je konačno generirani $R[s_0, \ldots, s_{n-1}]$ - modul. Kako je S cijeli nad R, $R[s_0, \ldots, s_{n-1}]$ je konačno generirani R-modul prema Teoremu 2.22. Napomena koja prethodila Teoremu 2.22 pokazuje da je

$$R[s_0, \ldots, s_{n-1}][t] = R[s_0, \ldots, s_{n-1}, t]$$

konačno generirani R-modul. Budući da je $R[t] \subset R[s_0, \ldots, s_{n-1}, t]$, t je cijeli nad R po Teoremu 2.21. □

Teorem 2.24. *[4, Theorem VIII.5.7.] Neka je S proširenje prstena R i neka je $\hat{R}$ skup svih elemenata od S koji su cijeli nad R. Tada je $\hat{R}$ cijelo proširenje prstena R koje sadrži svaki potprsten od S koji je cijeli nad R.*

Dokaz. Ako su $s, t \in \hat{R}$, tada su $s, t \in R[s, t]$ pa slijedi da je $t - s \in R[s, t]$ i $ts \in R[s, t]$. Neka su s i t cijeli nad R tako da je $R[s, t]$ prsten. Nadalje vrijedi $t - s \in \hat{R}$ i $ts \in \hat{R}$. Prema tome, $\hat{R}$ je potprsten od S. $\hat{R}$ sadrži R jer je svaki element od R trivijalno cijeli nad R. Definicija od $\hat{R}$ osigurava da je $\hat{R}$ cijeli nad R i sadrži sve potprstene od S koji su cijeli nad R. □

Ako je S proširenje prstena R, tada prsten $\hat{R}$ iz prethodnog teorema nazivamo **cijeli zatvarač** od R u S. Ukoliko je $R = \hat{R}$, tada se za R kaže da je **cijelo zatvoren** u S.

Napomena 2.4. *[4, Remarks, str. 397]*
1. *Kako je $1_R \in R \subset \hat{R}$, S je proširenje prstena $\hat{R}$. Teoremi* 2.23. *i* 2.24. *impliciraju da je $\hat{R}$ cijelo zatvoren u S.*
2. *Pojmovi cijelih zatvarača i cijelih zatvorenih prstenova se odnose na prsten R i određeno proširenje S. Stoga ne možemo reći da je R cijelo zatvoren ukoliko nije specificirano proširenje S. Međutim, u jednom slučaju nije potrebno specificirati proširenje S. Za integralnu domenu R kaže se da je cijelo zatvorena pod uvjetom da je R cijelo zatvorena u svom polju kvocijenata.*

Primjer 2.7. 1. *Integralna domena $\mathbb{Z}$ je cijelo zatvorena (u svom polju kvocijenata $\mathbb{Q}$).*
2. *$\mathbb{Z}$ nije cijelo zatvoren u polju kompleksnih brojeva jer je $i \in \mathbb{C}$ cijel nad $\mathbb{Z}$.*
3. *Svaka domena jedinstvene faktorizacije je cijelo zatvorena.*
4. *Neka je F polje. Prsten polinoma $F[x_1, \ldots, x_n]$ je cijelo zatvoren u svom polju kvocijenata $F(x_1, \ldots, x_n)$.*

Teorem 2.25. *[4, Theorem VIII.5.8.] Neka je T multiplikativni podskup integralne domene R tako da je $0 \notin T$. Ako je R cijelo zatvorena, tada je $T^{-1}R$ cijelo zatvorena integralna domena.*

Dokaz. Vidjeti u [4]. □

U idućem dijelu potpoglavlja raspravljamo o odnosima između (prostih) ideala u prstenima R i S, gdje je S proširenje prstena R.
Ako je S proširenje prstena R i $I(\neq S)$ ideal od S, tada vrijedi:
1. $I \cap R \neq R$ i
2. $I \cap R$ je ideal od R kojeg nazivamo kontrakcija od I na R i kažemo da I leži nad J.
Ako je Q prost ideal u S, gdje je S proširenje prstena R, tada je kontrakcija $Q \cap R$ od Q na R prost ideal od R. Neka je P prost ideal u R. Pitamo se, postoji li prost ideal Q u S koji leži nad P? Jedan od kontraprimjera je proširenje $\mathbb{Z}$ poljem $\mathbb{Q}$. Djelomično rješenje problema daje idući teorem.

Teorem 2.26. *[4, Theorem VIII.5.9.] Neka je S cijelo proširenje prstena R i P prost ideal od R. Tada postoji prost ideal Q u S za koji vrijedi $Q \cap R = P$.*

Dokaz. Budući da je P prost, $R \setminus P$ je multiplikativni podskup od R, a time i multiplikativni podskup od S. Očigledno da $0 \notin R \setminus P$. Prema Teoremu 2.7. postoji ideal Q od S koji je maksimalan u skupu svih ideala I od S tako da je $I \cap (R \setminus P) = \emptyset$. Nadalje, svaki takav ideal Q je prost u S. Vrijedi i $Q \cap R \subset P$. Za $Q \cap R \neq P$, odaberimo $u \in P$ takav da $u \notin Q$. Tada ideal $Q + (u)$ u S sadrži Q. Prema maksimalnosti postoji $c \in (Q + (u)) \cap (R \setminus P)$, $c = q + su$, $q \in Q$, $s \in S$. Budući da je s cijeli nad R, postoje $r_0, r_1, \ldots, r_{n-1} \in R$ takvi da je

$$s^n + r_{n-1}s^{n-1} + \cdots + r_1 s + r_0 = 0.$$

Ako pomnožimo prethodnu jednakost s u^n dobivamo

$$(su)^n + r_{n-1}u(su)^{n-1} + \cdots + r_1 u^{n-1}(su) + r_0 u^n = 0.$$

Kako je $su = c - q$, Binomni teorem 1.4. implicira da je $v = c^n + r_{n-1}uc^{n-1} + \cdots + r_1 u^{n-1}c + r_0 u^n \in Q$. Također, $v \in R$ i stoga je $v \in R \cap Q \subset P$. Nadalje, $u \in P$ i $v \in P$ impliciraju da je $c^n \in P$. Budući da je P prost, c mora biti u P, što je kontradikcija. □

Idući korolar slijedi iz prethodnog teorema.

Korolar 2.4. *[4, Corollary VIII.5.10.] Neka je S cijelo proširenje prstena R i P_1, P prost ideal u R tako da je $P_1 \subset P$. Ako je Q_1 prost ideal od S koji se nalazi nad P_1, tada postoji prost ideal Q od S takav da je $Q_1 \subset Q$ i Q se nalazi nad P.*

Teorem 2.27. *[4, Theorem VIII.5.11.] Neka je S cijelo proširenje prstena R i P prost ideal u R. Ako su Q i Q_1 prosti ideali u S tako da je $Q_1 \subseteq Q$ i oba Q i Q_1 se nalaze nad P, tada je $Q = Q_1$.*

Dokaz. Dovoljno je pokazati da ako je Q prost ideal u S takav da je $Q \cap R = P$, tada je Q maksimalan u skupu A svih ideala I u S sa svojstvom $I \cap (R \setminus P) = \emptyset$. Ako Q nije maksimalan u A, tada postoji ideal I u S tako da vrijedi

$$Q \subsetneq I \text{ i } I \cap (R \setminus P) = \emptyset.$$

Prema tome, $I \cap R \subset P$. Odaberimo $u \in I \setminus Q$. Budući da je u cijeli nad R, skup normiranih polinoma $f \in R[x]$ takvih da vrijedi $deg f \geq 1$ i $f(u) \in Q$ je neprazan. Odaberimo takav polinom f najmanjeg stupnja, primjerice $f = \sum_{i=0}^{n} r_i x_i$. Tada iz

$$u^n + r_{n-1}u^{n-1} + \cdots + r_1 u + r_0 \in Q \subset I,$$

slijedi $r_0 \in I \cap R \subset P = Q \cap R \subset Q$. Stoga vrijedi

$$u(u^{n-1} + r_{n-1}u^{n-2} + \cdots + r_2 u + r_1) \in Q.$$

Po minimalnosti stupnja f, $(u^{n-1} + r_{n-1}u^{n-2} + \cdots + r_1) \notin Q$. Kako $u \notin Q$, slijedi da Q nije prost ideal, što je u suprotnosti s našom pretpostavkom. Ovo je u kontradikciji budući da je Q prost (Teorem 1.7.). Dakle, Q je maksimalan u S. □

Teorem 2.28. *[4, Theorem VIII.5.12.] Neka je S cijelo proširenje prstena R i neka je Q prost ideal u S koji se nalazi nad prostim idealom P u R. Tada je Q maksimalan u S ako i samo ako je P maksimalan u R.*

Dokaz. Pretpostavimo da je Q maksimalan u S. Prema Teoremu 1.9. postoji maksimalan ideal M od R koji sadrži P. Prema Teoremu 1.10. je M prost. Korolar 2.4. tvrdi da postoji prost ideal Q' u S takav da je $Q \subset Q'$ i Q' se nalazi nad M. Budući da je Q' prost, vrijedi $Q' \neq S$. Maksimalnost od Q implicira da je $Q = Q'$, odakle slijedi da je $P = Q \cap R = Q' \cap R = M$. Dakle, P je maksimalan u R.
Nasuprot tome, pretpostavimo da je P maksimalan u R. Kako je Q prost u S, $Q \neq S$ te postoji maksimalan ideal N od S koji sadrži Q (Teorem 1.9.). Prema Teoremu 1.10. je N prost pa vrijedi $1_R = 1_S \notin N$. Kako je $P = R \cap Q \subset R \cap N \subsetneq R$, po maksimalnosti mora vrijediti $P = R \cap N$. Dakle, Q i N oba leže nad P i $Q \subset N$. Stoga, $Q = N$ prema Teoremu 2.27. □

2.6. Dedekindove domene

U ovom potpoglavlju ispitujemo klasu Dedekindovih domena koje su vrlo važne u teoriji algebarskih krivulja i algebarskoj teoriji brojeva.
Iduća definicija je motivirana idućim činjenicama: prema Lemi 1.1. je svaki glavni ideal domene D Noetherin. Prema tome, svaki ideal ($\neq D$) ima primarnu dekompoziciju.

Definicija 2.11. *[4, Definition VIII.6.1.] Dedekindova domena je integralna domena R u kojoj je svaki ideal ($\neq R$) produkt konačnog broja prostih ideala.*

Napomena 2.5. *Prethodno smo naveli da je svaka domena glavnih ideala Dedekindova. Međutim, obrat ne vrijedi, tj. postoji Dedekindova domena koja nije domena glavnih ideala.*

Da bi pokazali da je svaka Dedekindova domena zapravo Noetherin moramo uvesti pojam kvocijentnog ili frakcionalnog ideala.

Definicija 2.12. *[4, Definition VIII.6.2.] Neka je R integralna domena s poljem kvocijenata K. Kvocijentni ideal od R je R-podmodul I od K takav da je $aI \subset R$ za neki nenul $a \in R$.*

Primjer 2.8. *Svaki nenul ideal I u integralnoj domeni R je R-podmodul od R, a samim time i kvocijentni ideal od R. Obrnuto, svaki kvocijentni ideal od R koji je sadržan od R je obični ideal od R.*

Napomena 2.6. *[4, Remark, str. 401] Ako je I kvocijentni ideal integralne domene R i $aI \subset R, a \in R$, tada je aI ideal u R i preslikavanje $I \mapsto aI$ dano s $x \mapsto ax$ je izomorfizam R-modula.*

Teorem 2.29. *[4, Theorem VIII.6.3.] Ako je R integralna domena s poljem kvocijenata K, tada je skup svih kvocijentnih ideala u R komutativan monoid s jedinicom R i množenjem danim s $IJ = \{\sum_{i=1}^{n} a_i b_i | a_i \in I, b_i \in J, n \in \mathbb{N}\}$.*

Dokaz. Vidjeti u [4]. □

Kažemo da je kvocijentni ideal I integralne domene R je **invertibilan** ako je $IJ = R$ za neki kvocijentni ideal J od R. Dakle, invertibilni kvocijentni ideali su oni koji imaju inverze u monoidu svih kvocijentnih ideala.

Napomena 2.7. *[4, Remarks, str. 402]*
1. *Inverz invertibilnog kvocijentnog ideala I je jedinstven te ga definiramo kao $I^{-1} = \{a \in K \mid aI \subset R\}$. Za svaki kvocijentni ideal vrijedi $I^{-1}I = II^{-1} \subset R$. Ako je I invertibilan i $IJ = JI = R$, tada vrijedi da je $J \subset I^{-1}$. Obratno, kako su I^{-1} i J R-podmoduli od K, $I^{-1} = RI^{-1} = (JI)I^{-1} = J(II^{-1}) \subset JR = RJ \subset J$, slijedi da je $J = I^{-1}$.*
2. *Ako su A, B, I kvocijentni ideali od R takvi da je $IA = IB$ i I invertibilan, tada je $A = RA = (I^{-1}I)A = I^{-1}(IB) = RB = B$.*
3. *Ako je I običan ideal u R, tada je $R \subset I^{-1}$.*

Primjer 2.9. *Svaki nenul glavni ideal u integralnoj domeni R je invertibilan.*
Neka je K polje kvocijenata od R i $I = (b), b \neq 0$ te neka je $J = Rc \subset K, c = 1_R/b$. Tada je J kvocijentni ideal od R takav da je $IJ = R$.

Idući rezultati pokazuju neke činjenice o invertibilnim kvocijentnim idealima.

Lema 2.4. *[4, Lemma VIII.6.4.] Neka su $I, I_1, \ldots, I_n$ ideali u integralnoj domeni od R. Tada vrijedi:*
1. *Ideal $I_1 I_2 \cdots I_n$ je invertibilan ako i samo ako je svaki I_j invertibilan.*
2. *Ako je $P_1 P_2 \cdots P_m = I = Q_1 Q_2 \cdots Q_n$, gdje su P_i i Q_j prosti ideali u R i svaki P_i je invertibilan, tada je $m = n$ i $P_i = Q_i$ za svaki $i = 1, 2, \ldots, m$.*

Dokaz. 1. Ako je J kvocijentni ideal takav da je $J(I_1 \cdots I_n) = R$, tada za svaki $j = 1, 2, \ldots n$ vrijedi, $I_j(JI_1 \cdots I_{j-1} I_{j+1} \cdots I_n) = R$ pa je tada I_j invertibilan. Obratno, ako je I_j invertibilan, tada je $(I_1 \cdots I_n)(I_1^{-1} \cdots I_n^{-1}) = R$ pa slijedi da je $I_1 \cdots I_n$ invertibilan.
2. Dokaz provodimo indukcijom po m. Za $m > 1$, odabiremo P_i, npr. P_1, tako da P_1 ne sadrži P_i za $i = 2, \ldots, m$. Vrijedi, $Q_1 \cdots Q_n = P_1 \cdots P_m \subset P_1$ i P_1 je neki prost Q_j, npr. Q_1 i on je sadržan u P_1 (Definicija 1.11.). Slično, $P_1 \cdots P_m = Q_1 \cdots Q_n \subset Q_1$, $P_i \subset Q_1$ za neki i. Stoga je $P_i \subset Q_1 \subset P_1$. Po minimalnosti od P_1 imamo $P_i = Q_1 = P_1$. Budući da je $P_1 = Q_1$ invertibilno, prethodna napomena pod 2. implicira $P_2 P_3 \cdots P_m = Q_2 Q_3 \cdots Q_n$. Dakle, prema pretpostavci indukcije $m = n$ i $P_i = Q_i$ za $i = 1, 2, \ldots, m$. □

Primjer prije Leme 2.4. i Teorem 1.12. pokazuju da je svaki nenul prost ideal u domeni glavnih ideala maksimalan i invertibilan.

Teorem 2.30. *[4, Theorem VIII.6.5.] Ako je R Dedekindova domena, tada je svaki nenul prost ideal od R invertibilan i maksimalan.*

Dokaz. Najprije pokažimo da je svaki invertibilan prosti ideal P maksimalan. Ako je $a \in R \setminus P$, moramo pokazati da je ideal $P + Ra$ s P i a jednak R. Ako $P + Ra \neq R$, tada budući da je R Dedekindova domena, postoje prosti ideali P_i i Q_i takvi da vrijedi

$$P + Ra = P_1 P_2 \cdots P_m \text{ i } P + Ra^2 = Q_1 Q_2 \cdots Q_n.$$

Neka je $\pi : R \to R/P$ kanonski epimorfizam i razmotrimo glavne ideale u R/P koji generiraju redom $\pi(a)$ i $\pi(a^2)$. Vrijedi

$$(\pi(a)) = \pi(P_1) \cdots \pi(P_m) \text{ i } (\pi(a^2)) = \pi(Q_1) \cdots \pi(Q_n).$$

Budući da je $Ker\pi = P \subset P_i$ i $P \subset Q_i$ za svaki i, ideali $\pi(P_i)$ i $\pi(Q_i)$ su prosti u R/P. Kako je prema Teoremu 1.8. R/P integralna domena, svaki glavni ideal u R/P je invertibilan. Prema tome, $\pi(P_i)$ i $\pi(Q_j)$ su invertibilni prema Lemi 2.4. Budući da je

$$\pi(Q_1)\cdots\pi(Q_n) = (\pi(a^2)) = (\pi(a))^2 = \pi(P_1)^2\cdots\pi(P_m)^2,$$

Lema 2.4. implicira $n = 2m$ i $\pi(P_i) = \pi(Q_{2i}) = \pi(Q_{2i-1})$ za $i = 1, 2, \ldots, m$. Iz $Ker\pi = P \subset P_i$ i $P \subset Q_j$ za svaki i, j, je

$$P_i = \pi^{-1}(\pi(P_i)) = \pi^{-1}(\pi(Q_{2i})) = Q_{2i}$$

i isto tako $P_i = Q_{2i-1}$ za $i = 1, 2, \ldots, m$. Stoga, $P + Ra^2 = (P + Ra)^2$ i $P \subset P + Ra^2 \subset (P + Ra)^2 \subset P^2 + Ra$. Za $b = c + ra \in P, c \in P^2, r \in R$ je $ra \in P$. Dakle, $r \in P$ jer je P prost i $a \notin P$. Nadalje, $P \subset P^2 + Pa \subset P$, što implicira $P = P^2 + Pa = P(P + Ra)$. Kako je P invertibilan, $R = P^{-1}P = P^{-1}P(P + Ra) = R(P + Ra) = P + Ra$, što nije moguće. Dakle, svaki invertibilan prost ideal P je maksimalan. Sada pretpostavimo da je P svaki nenul prost ideal u R i da je c nenul element iz P. Tada je $(c) = P_1P_2\cdots P_n$ za neke proste ideale P_i. Za $P_1P_2\cdots P_n = (c) \subset P$, imamo za neki k, $P_k \subset P$. Glavni ideal (c) je invertibilan pa stoga i P_k. U prvom dijelu dokaza je P_k maksimalan pa vrijedi $P_k = P$. Dakle, P je maksimalan i invertibilan. □

Lema 2.5. *[4, Lemma VIII.6.6.] Ako je I kvocijentni ideal integralne domene R s poljem kvocijenata K i $f \in Hom_R(I, R)$, tada za sve $a, b \in I$ vrijedi $af(b) = bf(a)$.*

Dokaz. Neka je $a = r/s$ i $b = v/t$, gdje su $r, s, v, t \in R; s, t \neq 0$. Tada vrijedi $sa = r$ i $tb = v$. Stoga $sab = rb \in I$ i $tab = va \in I$. Dakle, $sf(tab) = f(stab) = tf(sab) \in R$. Prema tome, $af(b) = saf(b)/s = f(sab)/s = f(tab)/t = tbf(a)/t = bf(a)$. □

Lema 2.6. *[4, Lemma VIII.6.7.] Svaki invertibilan kvocijentni ideal integralne domene R s poljem kvocijenata K je konačno generirani R-modul.*

Dokaz. Kako je $I^{-1}I = R$, postoje $a_i \in I^{-1}$, $b_i \in I$ takvi da je $1_R = \sum_{i=1}^n a_ib_i$. Za $c \in I$ vrijedi $c = \sum_{i=1}^n (ca_i)b_i$. Nadalje, svaki $ca_i \in R$ jer je $a_i \in I^{-1} = \{a \in K \mid aI \subset R\}$. Stoga je I generiran kao R-modul pomoću $b_1, \ldots, b_n$ (Teorem 1.16.). □

Već smo naveli da je svaki nenul ideal I u domeni glavnih ideala D invertibilan. Također je I izomorfan D kao D-modul (Teorem 1.16.). Prema tome, I je slobodan i stoga projektivan D-modul.

Teorem 2.31. *[4, Theorem VIII.6.8.] Neka je R integralna domena i I kvocijentni ideal od R. Tada je I invertibilan ako i samo ako je I projektivni R-modul.*

Dokaz. ($\Rightarrow$) Prema Lemi 2.6. i Teoremu 1.16., $I = Rb_1 + \cdots + Rb_n$, $b_i \in I$ i $1_R = \sum_{i=1}^n a_ib_i, a_i \in I^{-1}$. Neka je F slobodan R-modul s bazom $e_1, \ldots, e_n$. Preslikavanje $\pi : F \to I$ definirano s $e_i \mapsto b_i$ je R-modul epimorfizam (Teorem 1.19.) i postoji kratak egzaktan niz $0 \to Ker\pi \xrightarrow{\pi} F \to I \to 0$. Definirajmo $\zeta : I \to F$, $\zeta(c) = ca_1e_1 + \cdots + ca_ne_n, c \in I$ tako da je ζ R-modul homomorfizam i da vrijedi $\pi\zeta = 1_I$. Posljedično, prethodni se egzaktni niz cijepa i I je direktna suma slobodnih R-modula (Teorem 1.18.). Dakle, I je projektivan prema Teoremu 1.21.
($\Leftarrow$) Neka je $X = \{b_j \mid j \in J\}$ skup nenul generatora projektivnog R-modula I. Neka je $b_0 \in X$ fiksan. Nadalje, neka je F slobodan R-modul s bazom $\{e_j \mid j \in J\}$ i $\phi : F \to I, e_i \mapsto b_i$ epimorfizam R-modula (Teorem 1.19.). Kako je I projektivan, postoji homomorfizam R-modula $\psi : I \to F$ tako da je $\phi\psi = 1_I$. Za svaki $j \in J$, neka je $\pi_j : F \to R$, $e_j \cong R$

kanonska projekcija koja preslikava $\sum_i r_i e_i \in F$ na $r_j \in R$. Zatim, za svaki j preslikavanje $\theta_i = \pi_j\psi : I \to R$ je homomorfizam R-modula. Neka je $c_j = \theta_j(b_0)$. Za svaki $c \in I$, $cc_j = c\theta_j(b_0) = b_0\theta_j(c)$ prema Lemi 2.5., odakle u polju kvocijenata K od R vrijedi $c(c_j/b_0) = cc_j/b_0 = b_0\theta_j(c)/b_0 = \theta_j(c) \in R$. Stoga

$$c_j/b_0 \in I^{-1} = \{a \in K \mid aI \subset R\}.$$

Prema tome, za bilo koji $c \in I$

$$\psi(c) = \textstyle\sum_{j\in J_1} \theta_j(c)e_j = \sum_{j\in J_1} c(c_j/b_0)e_j,$$

gdje je J_1 konačan podskup $\{j \in J \mid \theta_j(c) \neq 0\}$. Dakle, za svaki nenul $c \in I$,

$$c = \phi\psi(c) = \phi(\textstyle\sum_{j\in J_1} c(c_j/b_0)e_j) = \sum_{j\in J_1} c(c_j/b_0)b_j = c(\sum_{j\in J_1}(c_j/b_0)b_j),$$

odakle $1_R = \sum_{j\in J_1}(c_j/b_0)b_j$, $c_j/b_0 \in I^{-1}$. Slijedi, $R \subset I^{-1}I$. Kako je $I^{-1}I \subset R$ vrijedi $R = I^{-1}I$. Dakle, I je invertibilan. □

Za navođenje karakterizacija Dedekindovih domena potrebno je uvesti još jedan pojam, **prsten diskretne valuacije**. To je domena glavnih ideala koja sadrži jedinstven nenul prost ideal.

Lema 2.7. *[4, Lemma VIII.6.9.] Ako je R Noetherin cijelo zatvorena integralna domena koja sadrži jedinstven nenul prost ideal, tada je R prsten diskretne valuacije.*

Dokaz. Pokažimo da je svaki pravi ideal u R glavni. Za to su potrebne iduće tvrdnje koje se dokazuju u nastavku:
1. Neka je K polje kvocijenata od R. Za svaki kvocijentni ideal I od R skup $\bar{I} = \{a \in K \mid aI \subset I\}$ jednak je upravo R,
2. $R \subsetneq P^{-1}$,
3. P je invertibilan,
4. $\bigcap_{n\in\mathbb{N}} P^n = 0$,
5. P je glavni.
Pretpostavimo da vrijedi 1. - 5. te neka je I bilo koji odgovarajući ideal od R. Tada je I sadržan u nenul maksimalnom idealu M od R (Teorem 1.9.) koji je nužno prost (Teorem 1.10.). Prema jedinstvenosti $M = P$, slijedi $I \subset P$. Kako je prema 4. $\cap_{n\in\mathbb{N}} P^n = 0$, m najveći cijeli broj takav da vrijedi $I \subset P^m$ i $I \nsubseteq P^{m+1}$. Odaberimo $b \in I - P^{m+1}$. Budući da je prema 5. $P = (a), a \in R$, vrijedi $P^m = (a)^m = (a^m)$. Kako je $b \in P^m$, tada je $b = ua^m$. Nadalje, $u \notin P = (a)$. Prema tome, u je invertibilan u R. Stoga prema Teoremu 1.11. $P^m = (a^m) = (ua^m) = (b) \subset I$, odakle je I glavni ideal $P^m = (a^m)$.
1. Vrijedi $R \subset \bar{I}$. Prema Napomeni 2.7. vrijedi da je $\bar{I}$ potprsten od K i kvocijentni ideal od R, odakle je $\bar{I}$ izomorfizam u idealu od R. Dakle, budući da je R Noetherin, $\bar{I}$ je konačno generiran (Teorem 2.4.). Teorem 2.21. (za $T = \bar{I}$) implicira da je svaki element iz $\bar{I}$ cijeli nad R. Prema tome, $\bar{I} \subset R$ budući da je R cijelo zatvorena. Dakle, $\bar{I} = R$.
2. Podsjetimo se da je $R \subset J^{-1}$ za svaki ideal J u R. Neka je F skup svih ideala J u R tako da je $R \subsetneq J^{-1}$. Budući da je P odgovarajući ideal (Definicija 1.11.), svaki nenul element iz P nije jedinica prema Teoremu 1.11. Ako je $J = (a), 0 \neq a \in P$, tada je $1_R/a \in J^{-1}$, ali $1_R/a \notin R$ pa slijedi $R \subsetneq J^{-1}$. Dakle, F nije prazan. Budući da je R Noetherin, F sadrži maksimalan element od M (Teorem 2.1.). Tvrdimo da je M prost ideal od R. Za $ab \in M, a, b \in R$ i $a \notin M$, odaberimo $c \in M^{-1} \setminus R$. Tada je $c(ab) \in R$ pa slijedi $bc(aR + M) \subset R$ i $bc \in (aR + M)^{-1}$. Dakle, $bc \in R$ (inače, $aR + M \in F$ je u kontradikciji s maksimalnošću od M). Prema tome, $c(bR + M) \subset R$ i dakle $c \in (bR + M)^{-1}$. Kako $c \notin R$, maksimalnost od M implicira $bR + M = M$ pa slijedi da je $b \in M$. Stoga je M prost

prema Teoremu 1.7. Kako je $M \neq 0$, zbog jedinstvenosti moramo imati $P = M$. Dakle, $R \subsetneqq M^{-1} = P^{-1}$.
3. Vrijedi $P \subset PP^{-1} \subset R$. Vidjeli smo da je P jedinstveni maksimalni ideal u R pa odatle slijedi $P = PP^{-1}$ ili $PP^{-1} = R$. Ako je $P = PP^{-1}$, tada je $P^{-1} \subset \bar{P}$ i prema 1. i 2. je $R \subsetneqq P^{-1} \subset \bar{P} = R$ što je kontradikcija. Dakle, $PP^{-1} = R$ i P je invertibilan.
4. Ako je $\cap_{n\in\mathbb{N}} P^n \neq 0$, tada je $\cap_{n\in\mathbb{N}} P^n$ kvocijentni ideal od R. Iskoristimo činjenicu da je $P^{-1} \subset \cap_{n\in\mathbb{N}} P^n$. Tada prema 1. i 2. vrijedi $R \subsetneqq P^{-1} \subset \cap_{n\in\mathbb{N}} P^n = R$ što je kontradikcija.
5. Postoji $a \in P$ takav da $a \notin P^2$ (inače, $P = P^2$ pa slijedi $\cap_{n\in\mathbb{N}} P^n = P \neq 0$ što je kontradikcija prema 4.). Tada je aP^{-1} nenul ideal u R takav da $aP^{-1} \nsubseteq P$ (inače, $a \in aR = aP^{-1}P \subset P^2$). U prvom dijelu dokaza pokazano je da svaki pravi ideal u R sadržan u P, a odatle je $aP^{-1} = R$. Stoga prema 3., $(a) = (a)R = (a)P^{-1}P = (aP^{-1})P = RP = P$. □

Definicija 2.13. *[3, Definicija 1.8.2] Neka je R komutativni prsten i neka je $S \subset R$, neprazan multiplikativni podskup u R koji nema djelitelja nule. Lokalizacija od R po S je komutativni prsten R_S s jedinicom i injektivni homomorfizam prstenova $\phi : R \to R_S$ takav da za sve $a \in R_S$ postoji $b \in R$ i $c \in S$ takav da je $\phi(c)$ invertibilan u R_S i $a = \phi(b)\phi(c)^1$.*

Teorem 2.32. *[4, Theorem VIII.6.10.] Neka je R integralna domena. Sljedeće tvrdnje su ekvivalentne:*
1. *R je Dedekindova domena,*
2. *svaki pravi ideal u R se može na jedinstven način prikazati kao produkt konačnog broja prostih ideala,*
3. *svaki ideal različit od nule u R je invertibilan,*
4. *svaki kvocijentni ideal od R je invertibilan,*
5. *skup svih kvocijentnih ideala od R je grupa obzirom na množenje,*
6. *svaki ideal u R je projektivan,*
7. *svaki kvocijentni ideal od R je projektivan*
8. *R je Noetherin, cijelo zatvoren i svaki prost ideal različit od nule je maksimalan,*
9. *R je Noetherin i za svaki primarni ideal različit od nule P od R, lokalizacija R_P od R u P je prsten diskretne valuacije.*

Dokaz. Pokazat ćemo samo neke ekvivalencije.
4. $\Rightarrow$ 5. Svaki ideal od R je invertibilan prema 4. i prema tome konačno generiran prema Lemi 2.6. Stoga je R Noetherin prema Teoremu 2.4. Neka je K polje kvocijenata od R. Ako je $u \in K$ cijeli nad R, tada je $R[u]$ konačno generiran R-podmodul od K prema Teoremu 2.21. Također, Primjer 2.8. pokazuje da je $R[u]$ kvocijentni ideal od R. Stoga je $R[u]$ invertibilan prema 4. Dakle, budući da je

$$R[u]R[u] = R[u], R[u] = RR[u] = (R[u]^{-1}R[u])R[u] = R[u]^{-1}R[u] = R,$$

slijedi da je $u \in R$. Prema tome, R je cijelo zatvoren. Ako je P nenul prost ideal u R, tada postoji maksimalan ideal M od R koji sadrži P (Teorem 1.9.). M je invertibilan prema 4. Prema tome, $M^{-1}P$ je kvocijentni ideal od R s $M^{-1}P \subset M^{-1}M = R$ pa slijedi da je $M^{-1}P$ ideal u R. Budući da je $M(M^{-1}P) = RP = P$ i P prost ili je $M \subset P$ ili $M^{-1}P \subset P$. Ako je $M^{-1}P \subset P$, tada je $R \subset M^{-1} = M^{-1}R = M^{-1}PP^{-1} \subset PP^{-1} \subset R$ odakle slijedi $M^{-1} = R$. Dakle, $R = MM^{-1} = MR = M$, što je kontradikcija s pretpostavkom da je M maksimalan. Prema tome, $M \subset P$ i stoga $M = P$. Dakle, P je maksimalan.
8. $\Rightarrow$ 9. R_P je cijelo zatvorena integralna domena prema Teoremu 2.25. Prema Lemi 1.2. svaki ideal u R_P je oblika $I_P = \{i/s \mid i \in I, s \notin P\}$, gdje je I ideal od R. Budući da je svaki ideal od R konačno generiran prema 8. i Teoremu 2.4., slijedi da je svaki ideal od R_P konačno generiran. Prema tome, R_P je Noetherin prema Teoremu 2.4. Prema Teoremu 1.14., svaki

nenul prost ideal od R_P je oblika I_P, gdje je I nenul prost ideal od R koji je sadržan u P. Kako je prema 8. svaki nenul prost ideal od R maksimalan, P_P mora biti jedinstveni nenul prost ideal u R_P. Dakle, R_P je diskretna vrijednost prstena prema Lemi 2.7.
9. $\Rightarrow$ 1. Prvo pokažimo da je svaki ideal $I \neq 0$ invertibilan. II^{-1} je kvocijentni ideal od R sadržan u R (Napomena 2.8.) pa slijedi da je II^{-1} ideal u R. Za $II^{-1} \neq R$ postoji maksimalan ideal M koji sadrži II^{-1} (Teorem 1.9.). Kako je M prost (Teorem 1.10.), ideal I_M u R_M je glavni prema 9. i neka je $I_M = (a/s), a \in I, s \in R \setminus M$. Budući da je R Noetherin, I je konačno generiran i neka je $I = (b_1, \ldots, b_n)$. Za svaki i, $b_i/I_R \in I_M$, odakle u R_M, $b_i/I_R = (r_i/s_i)(a/s)$ za neke $r_i \in R$ i $s_i \in R \setminus M$. Prema tome, $s_i s b_i = r_i a \in I$. Neka je $t = ss_1 \cdots s_n$. Kako je $R \setminus M$ multiplikativno, $t \in R \setminus M$. U polju kvocijenata od R imamo za svaki t, $(t/a)b_i = tb_i/a = s_1 \cdots s_{i-1} s_{i+1} \cdots s_n r_i \in R$ pa vrijedi $t/a \in I^{-1}$. Prema tome, $t = (t/a)a \in I^{-1}I \subset M$, što je kontradikcija s činjenicom da je $t \in R \setminus M$. Stoga, $II^{-1} = R$ i I je invertibilno. Za svaki ideal $I \neq R$ od R odaberimo maksimalni ideal M_I od R tako da $I \subset M_I \subsetneq R$. Za $I = R$ neka je $M_R = R$. Tada je IM_I^{-1} kvocijentni ideal od R te vrijedi $IM_I^{-1} \subset M_I M_I^{-1} \subset R$. Prema tome, IM_I^{-1} je ideal od R koji sadrži I. Također, ako je I pravi, tada je $I \subsetneq IM_I^{-1}$ (inače, kako su I i M_I invertibilni, $R = RR = (I^{-1}I)(M_I^{-1}M_I) = I^{-1}(IM_I^{-1})M_I = I^{-1}IM_I = RM_I = M_I$, što je kontradikcija s odabirom M_I). Neka je S skup svih ideala od R te definirajmo funkciju $f : S \to S$, $I \mapsto IM_I^{-1}$. S obzirom na pravi ideal J, prema Teoremu 1.1. ($f_n = f$ za svaki n) postoji funkcija $\phi : \mathbb{N}_0 \to S$ takva da je $\phi(0) = J$ i $\phi(n+1) = f(\phi(n))$. Ako $\phi(n)$ označimo s J_n i M_{J_n} s M_n, dobivamo uzlazni lanac ideala $J = J_0 \subseteq J_1 \subseteq J_2 \subseteq \ldots$ tako da je $J = J_0$ i $J_{n+1} = f(J_n) = J_n M_n^{-1}$. Budući da je R Noetherin i J je pravi, postoji cijeli broj k tako da je

$$J = J_0 \subsetneq J_1 \subsetneq \ldots \subsetneq J_{k-1} \subsetneq J_k = J_{k+1}.$$

Dakle, $J_k = J_{k+1} = f(J_k) = J_k M_k^{-1}$. Gornje napomene pokazuju da se to može dogoditi samo ako je $J_k = R$. Prema tome, $R = J_k = f(J_{k-1}) = J_{k-1}M_{k-1}^{-1}$ pa vrijedi

$$J_{k-1} = J_{k-1}R = J_{k-1}M_{k-1}^{-1}M_{k-1} = RM_{k-1} = M_{k-1}.$$

Kako je $M_{k-1} = J_{k-1} \subsetneq J_k = R$, M_{k-1} je maksimalni ideal. Minimalnost od k osigurava da je svaki $M_0, \ldots, M_{k-2}$ maksimalan (inače bi vrijedilo $M_j = R$ pa slijedi $J_{j+1} = J_j M_j^{-1} = J_j R^{-1} = J_j R = J_j$). Nadalje, vrijedi

$$M_{k-1} = J_{k-1} = J_{k-2}M_{k-2}^{-1} = J_{k-3}M_{k-3}^{-1}M_{k-2}^{-1} = \ldots = JM_0^{-1}M_1^{-1}\cdots M_{k-2}^{-1}.$$

Prema tome, budući da je M_i invertibilan,

$$M_{k-1}(M_0 \cdots M_{k-2}) = JM_0^{-1} \cdots M_{k-2}^{-1}(M_0 \cdots M_{k-2}) = J.$$

Dakle, J je produkt maksimalnih ideala pa prema tome R je Dedekindov. $\square$

Sažetak

U ovom diplomskom radu napravljen je koncpet komuntativnih prstenova i modula. Nakon definiranja osnovnih pojmova i teorema iz teorije prstenova, baziramo se na komutativne prstenove i module. Upoznali smo se s uvjetima lanaca, primarnih idealima, primarnom dekompozicijom, Noetherinim prstenovima, proširenja prstenova te Dedekindovim domenama. Naveli smo važne teoreme algebre kao što su Krullov teorem, Hilbertov teorem o bazi, teorem koji povezuje pojmove Dedekindove domene, invertibilnih ideala, projektivnih ideala te Noetherinih prstenova. Upoznali smo se s pojmovima normalnog niza, kompozicionog niza, izoliranog ideala, anhilatora i prstena diskretne valuacije.
Ključne riječi: grupa, prsten, modul, ideal, komutativan prsten, primarni ideal, primarna dekompozicija, Noetherini prstenovi, proširenje prstena, Dedekindova domena, Hilbertov teorem o bazi, Krull

Commutative rings and modules

Summary

In this master's thesis, a concept of commutative rings and modules is developed. After defining the basic concepts and theorems from ring theory, the focus shifts to commutative rings and modules. We become acquainted with chain conditions, primary ideals, primary decomposition, Noetherian rings, ring extensions, and Dedekind domains. Important algebraic theorems are stated, such as Krull's theorem, Hilbert's basis theorem, and a theorem connecting the concepts of Dedekind domains, invertible ideals, projective ideals, and Noetherian rings. We familiarize ourselves with the notions of a normal sequence, a composition series, an isolated ideal, an annihilator, and a ring of discrete valuation.
Keywords: group, ring, module, ideal, commutative ring, primary ideal, primary decomposition, Noetherian rings, ring extension, Dedekind domain, Hilbert's basis theorem, Krull's theorem

Životopis

Moje ime je David Gavran. Rođen sam 13. Siječnja 1998. godine u Slavonskom Brodu. Pohađao sam Osnovnu školu „Viktor Car Emin“ u Donjim Andrijevcima u razdoblju od 2004. do 2012. godine. Po završetku osnovne škole upisao sam Srednju školu „Matije Antuna Reljkovića“ – smjer Tehničar za geodeziju i geoinformatiku u Slavonskom Brodu. Naziv sveučilišnog prvostupnika stječem 2021. godine završnim radom pod nazivom „Verižni razlomci“ pod mentorstvom doc.dr.sc Mirele Jukić Bokun. Iste godine upisuje Diplomski studij Matematike, smjer Financijska matematika i statistika na Odjelu za Matematiku u Osijeku.

Literatura

[1] D. Brajković, *Algebra kroz primjere*, Sveučilište u Osijeku, Osijek, 2018. http://www.mathos.unios.hr/images/uploads/774.pdf

[2] P. Dević, *Konačnodimenzionalne algebre s dijeljenjem*, Diplomski rad, Zagreb, 2019.

[3] I. Gut, *Komutativni prstenovi i njihovi moduli*, Diplomski rad, Zagreb, 2014.

[4] T. W. Hungerford, *Algebra*, Springer, New York, 1974.

[5] H. Kraljević, *Algebra*, Odjel za matematiku, Sveučilište u Osijeku (skripta), 2007.