Dedekindove metode

Gregurec, Matea

Sveučilište Josipa Jurja Strossmayera u Osijeku

Fakultet primijenjene matematike i informatike

Sveučilišni prijediplomski studij Matematika

Matea Gregurec

Dedekindove domene

Završni rad

Osijek, 2023.

Sveučilište Josipa Jurja Strossmayera u Osijeku

Fakultet primijenjene matematike i informatike

Sveučilišni prijediplomski studij Matematika

Matea Gregurec

Dedekindove domene

Završni rad

Mentor: prof.dr.sc. Ivan Matić

Osijek, 2023.

Sažetak: U ovome radu upoznat ćemo se s Dedekindovom domenom. Najprije ćemo navesti pojmove i tvrdnje iz algebre prstenova, kao što su prsten, ideal i modul, koji su potrebni za razumijevanje njezine definicije. Zatim ćemo uvesti pojam Noetherinog prstena i neke njegove karakterizacije, nakon čega ćemo definirati i samu Dedekindovu domenu. Na kraju ćemo napraviti pregled nekih svojstava i primjera Dedekindovih domena.

Ključne riječi: prsten, ideal, Dedekindova domena, Noetherin prsten

Dedekind domains

Abstract: In this paper, we will be introduced to the concept of Dedekind domains. Firstly, we will name the basic terms and statements concerning the algebra of rings, such as ring, ideal and module, needed to understand it's definition. Thus, we will introduce the concept of Noetherian and some of it's characterization, and afterwards we will define the Dedekind domain. Lastly, we will overview some characterization and examples of Dedekind domains.

Keywords: ring, ideal, Dedekind domain, Noetherian ring

Sadržaj

1 Uvod

Algebra je jedna od temeljnih grana matematike. Podrazumijeva širok raspon pojmova, od najjednostavnijih matematičkih jednadžbi do nešto apstraktnijih algebarskih struktura kao što su polja i prstenovi. Poznavanje osnova algebre nužno je za razumijevanje i rad u gotovo svim područjima znanosti. Iako toga uglavnom nismo svjesni, ova znanja koristimo i u svakodnevnome životu. Dok računamo "u glavi", zapravo rješavamo jednostavnu algebarsku jednadžbu i pritom koristimo niz algebarskih operacija i svojstava.

U prvoj točki drugog poglavlja navest ćemo definicije i tvrdnje koje su potrebne za daljnje shvaćanje ovoga rada. Tu se nalaze definicije grupe, prstena i modula te ideal i vrste ideala. Osim toga, ponovit ćemo i definiciju homomorfizma te navesti neka svojstva i primjere navedenog. U drugoj točki uvest ćemo pojam Noetherinog[1] prstena i Dedekindove[2] domene uz pripadne karakterizacije. Također ćemo i definirati kvocijentni ideal te objasniti što je njegov inverz.

U trećem i posljednjem poglavlju iskazat ćemo i dokazati svojstva Dedekindove domene, kao i navesti neke primjere. Nadalje ćemo definirati prsten diskretne valuacije. Na kraju ćemo se osvrnuti na tvrdnju koja objedinjuje Dedekindovu domenu, kvocijentne ideale i Noetherin prsten.

[1] Amalie Emmy Noether (1882. - 1935.) - njemačka matematičarka
[2] Julius Wilhelm Richard Dedekind (1831. - 1916.) - njemački matematičar

2 Pojam Dedekindove domene

U ovome poglavlju ponovit ćemo osnovne pojmove i tvrdnje potrebne za razumijevanje Dedekindovih domena. Definirat ćemo Dedekindovu domenu.

2.1 Temeljne algebarske strukture i pojmovi

Neki od osnovnih pojmova u algebri koje ćemo spominjati u ovome radu su monoid i grupa. Pojam grupe zauzima posebno važno mjesto u matematici.

Definicija 1. *[4, Definition I.1.1.ii.] Algebarsku strukturu s jednom asocijativnom binarnom operacijom i neutralnim elementom nazivamo monoidom.*

Definicija 2. *[4, Definition I.1.1.iii.] Neprazan skup G s binarnom operacijom množenja $\cdot$ nazivamo grupom ako vrijede sljedeća svojstva:*

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

(ii) postoji element $e \in G$ takav da je $x \cdot e = e \cdot x = x$ za svaki $x \in G$ i takav e nazivamo neutralni element ili jedinica

(iii) za proizvoljan $x \in G$ postoji element $y \in G$ takav da je $x \cdot y = y \cdot x = e$ i takav y nazivamo inverzni element elementa x.

Ovako zadanu grupu s binarnom operacijom množenja $\cdot$ označavamo kao uređeni par $(G, \cdot)$. Osnovni pojam za razumijevanje Dedekindove domene je prsten u kojemu, za razliku od grupe, imamo dvije binarne operacije.

Definicija 3. *[4, Definition III.1.1.] Neprazan skup R na kojemu su zadane dvije binarne operacije, zbrajanje $+ : (x, y) \mapsto x + y$ i množenje $\cdot : (x, y) \mapsto xy$, nazivamo prstenom ako vrijede sljedeća svojstva:*

(i) $(R, +)$ je Abelova komutativna grupa s neutralnim elementom koji označavamo s 0 i zovemo nula

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

(iii) i slijeva i zdesna vrijedi distributivnost množenja u odnosu na zbrajanje, odnosno $\forall x, y, z \in R$ vrijedi $x(y + z) = xy + xz$ i $(x + y)z = xz + yz$.

Nadalje, ako je operacija množenja komutativna, onda kažemo da je prsten *komutativan*, odnosno ako $\forall x, y \in R$ vrijedi $xy = yx$. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ su primjeri komutativnih prstenova uz zbrajanje i množenje. Također je i potprsten komutativnog prstena komutativan.

Definicija 4. *[4, Definition III.2.1.] Neka je R prsten. Aditivnu podgrupu J prstena R nazivamo lijevim idealom od R ako za $a \in J$ i $b \in R$ vrijedi $ba \in J$. Aditivnu podgrupu J prstena R nazivamo desnim idealom od R ako za $a \in J$ i $b \in R$ vrijedi $ab \in J$. Kažemo da je ideal obostran ako je i lijevi i desni.*

U komutativnom prstenu svaki je ideal obostran. U prstenu R postoje dva trivijalna ideala, $\{0\}$ i sam R. Za ideal koji nije trivijalan kažemo da je pravi ideal.

Definicija 5. *[4, Definition III.2.14.] Neka je R komutativan prsten s $1, 1 \neq 0$. Za ideal I u prstenu R kažemo da je prost ako je $I \neq R$ te ako iz $x \cdot y \in I$ slijedi $x \in I$ ili $y \in I$.*

Definicija 6. *[4, Definition III.2.17.] Ako za ideal I u prstenu R, $I \neq R$, ne postoji ideal J u R za koji vrijedi $I \subsetneq J \subsetneq R$, onda I nazivamo maksimalnim idealom.*

U prstenu R postoje maksimalni ideali. Svaki je ideal $I \neq R$ sadržan u nekom maksimalnom idealu u R.

Primjer 1. (3) je maksimalan ideal u $\mathbb{Z}$. Ideal (4) nije maksimalan jer vrijedi $(4) \subsetneq (2) \subsetneq \mathbb{Z}$. Ideal (2) je i prost i maksimalan ideal u $\mathbb{Z}$.

Definicija 7. *[4, Definition III.1.3.] Kažemo da je $c \in R, c \neq 0$, djelitelj nule ako postoji $d \in R, d \neq 0$, takav da je $cd = 0$.*

Definicija 8. *[4, Definition III.1.5.] Komutativan prsten s jedinicom, $1 \neq 0$, u kojemu ne postoje djelitelji nule nazivamo integralnom domenom.*

U prstenu R za element $b \in R$ se ideal u R generiran elementom b označava s (b). To je najmanji ideal u R koji sadrži taj element. Ideal generiran jednim elementom nazivamo *glavni ideal*. Prema tome (b) je glavni ideal generiran elementom $b \in R$.
Ako je svaki ideal u prstenu R glavni, onda kažemo da je R *prsten glavnih ideala*. Integralnu domenu koja je prsten glavnih ideala nazivamo *domenom glavnih ideala*.

Ako je R komutativan prsten s jedinicom i P prost ideal u R, tada je $S = R\backslash P$ multiplikativan podskup od R. Na skupu $R \times S$ definiramo relaciju ekvivalencije $(x, y) \sim (u, v)$ ako postoji $t \in S$ tako da je $(xv - yu)t = 0$. Skup klasa ekvivalencije obzirom na ovu relaciju je prsten koji označavamo sa $S^{-1}R$ te nazivamo *lokalizacijom od R u P*. Također koristimo i oznaku R_P. Ukoliko je I ideal u R, onda ideal $S^{-1}I$ u R označavamo I_P.

Definicija 9. *[4, Definition I.2.1.] Neka su G_1, G_2 grupe. Kažemo da je preslikavanje $\varphi : G_1 \to G_2$ homomorfizam grupa ako za sve $x, y \in G$ vrijedi $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$.*

U skladu s definicijom homomorfizma uvodimo i sljedeće pojmove.
Ako je homomorfizam ujedno i injekcija, nazivamo ga *monomorfizmom.* Ako je homomorfizam surjekcija, onda ga nazivamo *epimorfizmom.* Ako je homomorfizam i injekcija i surjekcija, odnosno ako je bijekcija, nazivamo ga *izomorfizmom.*
Automorfizam je izomorfizam strukture prema samoj sebi. *Kanonski izomorfizam* je izomorfizam između dvije strukture koji je jedinstven.

Definicija 10. *[4, Definition IV.1.1.] Neka je R prsten. Lijevim R-modulom nazivamo aditivnu Abelovu grupu M s djelovanjem $R \times M \to M$, $(r, m) \mapsto rm$ pri čemu $\forall r, s \in R$ i $\forall m, n \in M$ vrijedi sljedeće:*

(1) $r(m + n) = rm + rn$

(2) $(r + s)n = rn + sn$

(3) $r(sn) = (rs)n.$

Ukoliko postoji jedinica 1_R te dodatno vrijedi i

(4) $1_R n = n, \forall n \in M,$

onda M nazivamo unitalnim R-modulom.

Desni R-modul definira se analogno, uz funkciju $M \times R \to M$.

Definicija 11. *[4, Definition IV.1.3.] Neka je M modul nad R. Kažemo da je podskup $N \subset M$, $N \neq \emptyset$, podmodul modula M ako vrijedi:*

(1) $m - n \in N$, $\forall m, n \in N$

(2) $rn \in N$, $\forall n \in N, r \in R.$

Ukoliko je M R-modul i $u \in M$, tada skup $Ru = \{au : a \in R\}$ nazivamo lijevim podmodulom modula M generiranim elementom u.

Analogno se definira i desni podmodul.

Definicija 12. *[1, Definition III.4.3.] Neka je M R-modul. Kažemo da je skup $S \subseteq M$ baza od $M \neq 0$ ako se svaki $m \in M$ može na jedinstven način prikazati u obliku:*

$$m = a_1 m_1 + \cdots + a_n m_n,$$

pri čemu su $m_1, \ldots, m_n \in S$ i $a_1, ..., a_n \in R$.

R-modul koji ima bazu nazivamo *slobodnim* modulom. Kažemo da je R-modul M *projektivan* ako postoji R-modul N tako da je direktna suma $M \oplus N$ slobodan R-modul. U prstenu R s jedinicom je svaki slobodan R-modul projektivan modul.
Za module M i N nad prstenom R je funkcija $f : M \to N$ homomorfizam R-modula ako za sve $a, b \in M$ te za svaki $r \in R$ vrijedi sljedeće:

$$f(a + b) = f(a) + f(b) \text{ i } f(ra) = rf(a).$$

Oznakom $Hom_R(I, R)$ dan je skup svih homomorfizama R-modula s I u R.

Ako su dana polja K i L za koja vrijedi $K \subset L$, odnosno K je pravi podskup od L, onda kažemo da je L proširenje polja K. Primjer takvog proširenja je polje realnih brojeva $\mathbb{R}$ koje je proširenje polja racionalnih brojeva $\mathbb{Q}$, $\mathbb{Q} \subset \mathbb{R}$.
Nadalje, za element $\alpha \in L$ kažemo da je algebarski nad poljem K ako postoji nekonstantan polinom $P \in K[x]$ tako da $P(\alpha) = 0$, odnosno ako se polinom P poništava u α.

Neka je X integralna domena i L polje koje sadrži X. Element $\alpha \in L$ je *cijeli element* nad X ako je on korijen normiranog polinoma s koeficijentima u X, odnosno ako zadovoljava jednadžbu

$$\alpha^n + x_1 \alpha^{n-1} + \cdots + x_n = 0$$

za neke $x_i \in X$, $i = 1, \ldots, n$. Skup elemenata iz L koji su cijeli nad X tvori prsten koji nazivamo *cijelo zatvorenje* od X u L. Kažemo da je prsten X *cijelo zatvoren* ako je jednak svom cijelom zatvorenju u vlastitom polju kvocijenata K.

2.2 Noetherin prsten i Dedekindova domena

Definicija 13. *[1, Definition II.5.9.] Neka je R prsten. Prsten R nazivamo Noetherinim prstenom ako za svaki niz*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

ideala u R postoji prirodan broj n za koji vrijedi $I_k = I_n, \forall k \geq n$.

U sljedećoj karakterizaciji Noetherinih prstenova koristi se pojam maksimalnog elementa u parcijalno uređenom skupu. Maksimalni element parcijalno uređenog skupa X je element $m \in X$ takav da je $m \geq x$ za bilo koji $x \in X$. Odnosno, najveći element je onaj element koji nije strogo manji niti od jednog drugog elementa tog skupa.

Propozicija 1. *[1, Proposition II.5.10.] Neka je R prsten. Tada je sljedeće ekvivalentno:*

(1) R je Noetherin prsten.

(2) Svi ideali u R su konačno generirani.

(3) U svakom nepraznom podskupu ideala iz R postoji maksimalan element.

Posebno, svaka je domena glavnih ideala Noetherin prsten.

Dokaz. Dokažimo najprije (1) $\Rightarrow$ (3). Pretpostavit ćemo suprotno, odnosno da familija $\mathcal{S} = \{J_\alpha\}_{\alpha \in A}$, koja je neprazan skup ideala iz R, ne sadrži maksimalan element. Zatim odaberemo $J_1 \in \mathcal{S}$. Budući da skup $\mathcal{S}$ nema maksimalan element, postoji $J_2 \in \mathcal{S}$ takav da $J_1 \subsetneq J_2$. Slično, ni J_2 nije maksimalan element pa postoji $J_3 \in \mathcal{S}$ takav da $J_2 \subsetneq J_3$. Slijedeći isti postupak, dobivamo strogo rastući niz ideala iz R. Stoga $\mathcal{S}$ mora imati maksimalan element. Dolazimo do kontradikcije, čime je ova implikacija dokazana.

Nadalje dokažimo (3) $\Rightarrow$ (2). Uzmimo da je J ideal u R te označimo sa $\mathcal{S}$ familiju svih konačno generiranih ideala iz R sadržanih u J. Prema pretpostavci, tada postoji maksimalan element $I \in \mathcal{S}$. Neka je $b \in J$. Tada se ideal $I + (b)$ nalazi u familiji $\mathcal{S}$.
Budući da je I maksimalan u $\mathcal{S}$, vrijedi da je $I = I + (b)$. Slijedi da je $J = I$ i J je konačno generiran.

Konačno, dokažimo (2) $\Rightarrow$ (1). Neka su svi ideali u R konačno generirani te neka je

$$J_1 \subseteq J_2 \subseteq J_3 \subseteq \cdots$$

niz ideala u R. Uzmimo da je $J = \bigcup_{n=1}^{\infty} J_n$. Tada je J ideal u R takav da je $J = (r_1, r_2, ..., r_m)$ za neke $r_i \in R$. Kako je $r_i \in J = \bigcup_{n=1}^{\infty} J_n, 1 \leq i \leq m$, tada je $r_i \in J_{n_i}$ za neki n_i. Imamo niz ideala pa slijedi da postoji neki n sa svojstvom da je $r_i \in J_n$ za svaki i. Tada će za bilo koji $k \geq n$ za koji $J_k = J = J_n$, $\forall k \geq n$ vrijediti

$$(r_1, \ldots, r_m) \subseteq J_k \subseteq J = (r_1, \ldots, r_m).$$

Tada je R Noetherin prsten.

□

Sada možemo definirati Dedekindovu domenu.

Definicija 14. *[2, Corollary 9.4.]* ***Dedekindova domena*** *je integralna domena R u kojoj je svaki ideal različit od R konačan produkt prostih ideala.*

Postoji i alternativna definicija ovog pojma:
Dedekindova domena je komutativan prsten A sa sljedećim svojstvima:

(i) prsten A je Noetherin prsten i integralna domena

(ii) prsten A je cijelo zatvoren

(iii) svaki nenul prost ideal je i maksimalan ideal.

Iz definicije nije odmah uočljivo da je svaka Dedekindova domena ujedno i Noethererin prsten. Kako bismo to pokazali i objasnili svojstva Dedekindove domene, uvest ćemo pojam kvocijentnog ideala.

Definicija 15. *[4, Definition VIII.6.2.] Neka je R integralna domena s poljem kvocijenata K. Kvocijentni ideal od R je svaki nenul podmodul I od K za koji vrijedi $aI \subset R$, $\forall a \in R$, $a \neq 0$.*

Svaki nenul ideal I u integralnoj domeni R je podmodul od R, a posljedično i kvocijentni ideal od R. Vrijedi i obrat, svaki kvocijentni ideal od R koji je sadržan u R je ideal u R.

Napomena 1. *[4, Chapter VIII] Ako je I kvocijentni ideal domene R i $aI \subset R$ $(0 \neq a \in R)$, onda je aI ideal u R i preslikavanje $I \to aI$ dano s $x \mapsto ax$ je izomorfizam R-modula.*

Sljedeći je teorem dan bez dokaza.

Teorem 1. *[4, Theorem VIII.6.3.] Ako je R integralna domena s poljem kvocijenata K, onda skup svih kvocijentih ideala u R čini komutativni monoid s neutralnim elementom R i operacijom množenja danom s*

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J, n \in \mathbb{N} \right\}.$$

Primijetimo da ako su I i J ideali u R, onda je IJ običan produkt ideala.
Za kvocijentni ideal I integralne domene R kažemo da je *invertibilan* ako za neki kvocijentni ideal J u R vrijedi $IJ = R$. Iz toga slijedi da su invertibilni kvocijentni ideali točno oni koji imaju inverzan element u monoidu svih kvocijentnih ideala. Često invertibilne kvocijentne ideale nazivamo samo invertibilnim idealima. Skup svih nenul kvocijentnih ideala Dedekindove domene R čini grupu obzirom na množenje koju nazivamo *grupom ideala* od R.

Napomena 2. *[4, Chapter VIII]*

(i) Inverzni element invertibilnog kvocijentnog ideala I je jedinstven i zadan je kao $I^{-1} = \{a \in K : aI \subset R\}$. Lako je uočljivo da je za svaki kvocijentni ideal I skup $I^{-1} = \{a \in K : aI \subset R\}$ kvocijentni ideal takav da je $I^{-1}I = II^{-1} \subset R$. Ako je I invertibilan i vrijedi $IJ = JI = R$, onda je $J \subset I^{-1}$. Obratno, kako su I^{-1} i J podmoduli od K u R, $I^{-1} = RI^{-1} = (JI)I^{-1} = J(II^{-1}) \subset JR = RJ \subset J$, odakle je $J = I^{-1}$.

(ii) Ako su I, A, B kvocijentni ideali iz R za koje je $IA = IB$ i I je invertibilan, onda vrijedi $A = RA = (I^{-1}I)A = I^{-1}(IB) = RB = B$.

(iii) Ako je I ideal u R, onda je $R \subset I^{-1}$.

Svaki nenul glavni ideal u integralnoj domeni R je invertibilan. Ako je K polje kvocijenata od R i $I = (c)$ za $c \neq 0$, neka je $J = Rd \subset K$ za $d = 1_R/c$. Tada je J kvocijentni ideal u R za koji je $IJ = R$.
Integralne domene u kojima je svaki ideal invertibilan su upravo Dedekindove domene.

Primjer 2. [2, Chapter IX] Neka je K konačno proširenje polja racionalnih brojeva $\mathbb{Q}$. Njegov prsten cijelih brojeva M je cijelo zatvorenje od $\mathbb{Z}$ u K. Uzmimo da je, na primjer, $K = \mathbb{Q}(i)$. U tom je slučaju je $M = \mathbb{Z}[i]$. Tada je M Dedekindova domena.

Općenito, prsten cijelih brojeva u algebarskom polju brojeva K je Dedekindova domena.

3 Svojstva Dedekindove domene

Razmotrit ćemo svojstva Dedekindove domene, kao i tvrdnje koje slijede iz njezine definicije. Svaka je domena glavnih ideala ujedno i Dedekindova domena. Obrat ne vrijedi, što možemo vidjeti u sljedećem primjeru koji je detaljnije obrađen u literaturi [4].

Primjer 3. [4, Chapter VIII] Neka integralna domena $\mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} : a, b \in \mathbb{Z}\}$ ima polje kvocijenata $\mathbb{Q}(\sqrt{10}) = \{c + d\sqrt{10} : c, d \in \mathbb{Q}\}$. Može se pokazati da je domena $\mathbb{Z}[\sqrt{10}]$ cijelo zatvorena. Kako je preslikavanje $\mathbb{Z}[x] \to \mathbb{Z}[\sqrt{10}]$ dano funkcijom $f(x) \mapsto f(\sqrt{10})$ epimorfizam te je $\mathbb{Z}[x]$ Noetherin prsten, onda je i $\mathbb{Z}[\sqrt{10}]$ Noetherin prsten. Također se može pokazati i da je svaki nenul prost ideal u $\mathbb{Z}[\sqrt{10}]$ maksimalan ideal. Tada je $\mathbb{Z}[\sqrt{10}]$ Dedekindova domena, ali nije domena glavnih ideala.

Svaki je nenul glavni ideal u domeni glavnih ideala invertibilan i maksimalan, a poopćenje toga dano je sljedećom tvrdnjom.

Teorem 2. *[4, Theorem VIII.6.5.] Ako je R Dedekindova domena, onda je svaki nenul prost ideal u R ujedno i invertibilan i maksimalan.*

Dokaz. Najprije pokažimo da je svaki invertibilan prost ideal P maksimalan. Ako je $a \in R \setminus P$, treba pokazati da je ideal $P + Ra$ koji je generiran pomoću P i a jednak R. Ako $P + Ra \neq R$, budući da je R Dedekindova domena, postoje prosti ideali P_i, Q_i takvi da vrijedi $P + Ra = P_1P_2 \cdots P_m$ i $P + Ra^2 = Q_1Q_2 \cdots Q_n$. Nadalje neka je $\pi : R \to R \setminus P$ kanonski epimorfizam te neka su glavni ideali u $R \setminus P$ generirani redom s $\pi(a), \pi(a^2)$. Očito slijedi

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

Budući da je $\mathrm{Ker}(\pi) = P \subset P_i$ i $P \subset Q_i$ za svaki i, slijedi da su ideali $\pi(P_i)$ i $\pi(Q_i)$ prosti u $R \setminus P$. Kako je $R \setminus P$ integralna domena, svaki ideal u $R \setminus P$ je invertibilan, stoga su i $\pi(P_i), \pi(Q_i)$ invertibilni. Iz

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

slijedi da je $n = 2m$. Nakon zamjene indeksa imamo $\pi(P_i) = \pi(Q_{2i}) = \pi(Q_{2i-1})$ za $i = 1, 2, \ldots, m$.

Nadalje, zbog $\mathrm{Ker}(\pi) = P \subset P_i$ i $P \subset Q_i$ za sve i, slijedi

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

te na sličan način dobijemo $P_i = Q_{2i-1}$ za sve $i = 1, 2, \ldots, m$.
Posljedično, $P + Ra^2 = (P + Ra)^2$ i $P \subset P + Ra^2 \subset (P + Ra)^2 \subset P^2 + Ra$. Ako $b = c + ra \in P (c \in P^2, r \in R)$, onda je $ra \in P$. S obzirom da je P prost i $a \notin P$, vrijedi da je $r \in P$. Zato je $P \subset P^2 + Pa \subset P$, odakle je $P = P^2 + Pa = P(P + Ra)$. Kako je P invertibilan, vrijedi $R = P^{-1}P = P^{-1}P(P + Ra) = R(P + Ra) = P + Ra$. Dobili smo kontradikciju. Zaključujemo da je svaki invertibilni prost ideal P ujedno i maksimalan.
Uzmimo sada da je P bilo koji nenul prost ideal u R te neka je $c \in P$, $c \neq 0$. Tada je $(c) = P_1 P_2 \cdots P_n$ za neke proste ideale P_i. Budući da je $P_1 P_2 \cdots P_n = (c) \subset P$, vrijedi $P_k \subset P$ za neke k. Glavni ideal (c) je invertibilan pa su stoga i svi $P_1, \ldots, P_n$ invertibilni. Iz prvog dijela dokaza zaključujemo da je P_k maksimalan ideal, zbog čega je $P_k = P$. Konačno, P je maksimalan i invertibilan ideal.

□

Sljedećim primjerom ilustrirano je da nije svaki Noetherin prsten ujedno i Dedekindova domena.

Primjer 4. [4, Chapter VIII] Ako je F polje, onda su glavni ideali (x_1) i (x_2) u prstenu polinoma $F[x_1, x_2]$ prosti, ali ne i maksimalni (zbog toga što je $(x_i) \subsetneq (x_1, x_2) \subsetneq F[x_2, x_2]$). Stoga $F[x_1, x_2]$ nije Dedekindova domena. Kako je $F[x_1, x_2]$ Noetherin prsten, vidimo da je klasa Dedekindovih domena pravi podskup klase Noetherinih domena.

Lema 1. *[4, Lemma VIII.6.6.] Ako je I kvocijentni ideal integralne domene R s poljem kvocijenata K i ako je $h \in Hom_R(I, R)$ onda za sve $a, b \in I$ vrijedi $ah(b) = bh(a)$.*

Dokaz. Neka je $a = x/y$ i $b = z/w$ za $x, y, z, w \in R$ pri čemu su $y, w \neq 0$. Tada je $ya = x$ i $wb = z$, odakle slijedi $yab = xb \in I$ te $wab = za \in I$. Nadalje imamo $yh(wab) = h(ywab) = wh(yab)$ u R. Konačno $ah(b) = yah(b)/y = h(yab)/y = h(wab)/w = wbh(a)/w = bh(a)$.

□

Lema 2. *[4, Lemma VIII.6.7.] Svaki invertibilan kvocijentni ideal integralne domene R s poljem kvocijenata K je konačno generiran R-modul.*

Dokaz. Kako je $I^{-1}I = R$, slijedi da postoje $a_i \in I^{-1}, b_i \in I$ takvi da $1_R = \sum_{i=1}^{n} a_i b_i$. Ako je $c \in I$, tada $c = \sum_{i=1}^{n} (ca_i)b_i$. Također je svaki $ca_i \in R$ jer $a_i \in I^{-1} = \{a \in K : aI \subset R\}$.
Stoga je I generiran elementima $b_1, \ldots, b_n$ kao R-modul.

□

Ranije smo vidjeli da je svaki nenul ideal I u domeni glavnih ideala D invertibilan. Nadalje, ovako dan ideal I je izomorfan s domenom D kao D-modul. Stoga je I slobodan pa i projektivan D-modul. Navedeno vrijedi u proizvoljnoj integralnoj domeni. Sljedeći teorem navodimo bez dokaza, a dokaz je dostupan u [4].

Teorem 3. *[4, Theorem VIII.6.8.] Ako je R integralna domena i I kvocijentni ideal od R, onda je I invertibilan ako i samo ako je I projektivni R-modul.*

Za sljedeću karakterizaciju Dedekindove domene potrebno je uvesti novi pojam. *Prsten diskretne valuacije* je domena glavnih ideala koja ima točno jedan nenul prost ideal (uzimamo u obzir da je nul-ideal prost u svakoj integralnoj domeni).

Lema 3. *[4, Lemma VIII.6.4.] Neka su $I, I_1, I_2, \ldots, I_p$ ideali u integralnoj domeni R.*

(i) Ideal $I_1 I_2 \cdots I_p$ je invertibilan ako i samo ako je svaki od I_j invertibilan.

(ii) Ako je $P_1 \cdots P_r = I = Q_1 \cdots Q_p$, pri čemu su P_i i Q_j prosti ideali u R i svaki je P_i invertibilan, onda je $p = r$ te je $P_i = Q_i$ za svaki $i = 1, 2, \ldots, r$.

Dokaz. (i) $\Rightarrow$ Ako je J kvocijentni ideal takav da je $J(I_1 \cdots I_p) = R$, onda za svaki $j = 1, 2, \ldots, p$, vrijedi $I_j(JI_1 \cdots I_{j-1} I_{j+1} \cdots I_p) = R$, odakle znamo da je svaki I_j invertibilan.
$\Leftarrow$ Ako je svaki od I_j invertibilan, onda vrijedi $(I_1 \cdots I_p)(I_1^{-1} \cdots I_p^{-1}) = R$, zbog čega je produkt $I_1 \cdots I_p$ invertibilan.
(ii) Dokaz se provodi indukcijom po indeksu r. Za $r = 1$ je dokaz trivijalan. Ako je $r > 1$, onda biramo jedan P_i, recimo P_1, takav da P_i nije pravi podskup od P_1 za $i = 2, \ldots, r$. Kako je $Q_1 \cdots Q_p = P_1 \cdots P_r \subset P_1$ i P_1 je prost, slijedi da je neki Q_j, recimo Q_1, sadržan u P_1. Slično, kako je $P_1 \cdots P_r = Q_1 \cdots Q_p \subset Q_1$, onda je i $P_i \subset Q_1$ za neki indeks i. Iz toga slijedi niz implikacija $P_i \subset Q_1 \subset P_1$. Zbog minimalnosti elementa P_1, mora vrijediti $P_1 = P_i = Q_1$. Budući da je $P_1 = Q_1$ invertibilan, slijedi

$$P_2 P_3 \cdots P_r = Q_2 Q_3 \cdots Q_p.$$

Iz pretpostavke indukcije slijedi $p = r$ i $P_i = Q_i$ za svaki $i = 1, 2, \ldots, r$.

□

Lema 4. *[4, Lemma VIII.6.9.] Ako je R Noetherin prsten koji je cijelo zatvorena integralna domena te ako R sadrži jedinstven nenul prost ideal P, onda je R prsten diskretne valuacije.*

Dokaz leme može se pronaći u [4].
Iskazat ćemo i djelomično dokazati sljedeći teorem koji govori o svojstvima integralne domene R.

Teorem 4. *[4, Theorem VIII.6.10.] Neka je R integralna domena. Sljedeća svojstva su ekvivalentna.*

(i) *R je Dedekindova domena.*

(ii) *Svaki pravi ideal u R je na jedinstven način zadan kao produkt konačno mnogo prostih ideala.*

(iii) *Svaki nenul ideal u R je invertibilan.*

(iv) *Svaki kvocijentni ideal od R je invertibilan.*

(v) *Skup svih kvocijentnih ideala od R je grupa uz operaciju množenja.*

(vi) *Svaki ideal u R je projektivan.*

(vii) *Svaki kvocijentni ideal u R je projektivan.*

(viii) *R je Noetherin prsten koji je cijelo zatvoren i svaki je nenul prost ideal maksimalan.*

(ix) *R je Noetherin prsten i za svaki nenul prost ideal P od lokalizacija R_P od R u P je prsten diskretne valuacije.*

Dokaz. Ekvivalencija $(iv) \Leftrightarrow (v)$ je trivijalna. Implikacija $(i) \Rightarrow (ii)$, kao i implikacija $(ii) \Rightarrow (iii)$, slijedi iz teorema 2 i leme 3. Nadalje, ekvivalencije $(iii) \Leftrightarrow (vi)$ i $(vii) \Leftrightarrow (iv)$ su direktna posljedica teorema 3. Implikaciju $(vi) \Rightarrow (vii)$ lako dobijemo iz napomene 2. Za dovršavanje dokaza preostalo je jedino pokazati implikacije $(iv) \Rightarrow (viii), (viii) \Rightarrow (ix)$ i $(ix) \Rightarrow (i)$.

$(iv) \Rightarrow (vii)$ Neka je svaki ideal u R invertibilan. Tada je po lemi 2 i konačno generiran.

Dakle, R je Noetherin prsten. Uzmimo da je K polje kvocijenata integralne domene R. Ako je $t \in K$ cijeli nad R, tada je $R[t]$ konačno generiran R-podmodul od K. Tada je $R[t]$ kvocijentni ideal od R. Prema pretpostavci tvrdnje je $R[t]$ invertibilan. Kako je $R[t]R[t] = R[t]$, $R[t] = RR[t] = (R[t]^{-1}R[t])R[t] = R[t]^{-1}R[t] = R$, dobivamo da je $t \in R$. Prema tome, R je cijelo zatvoreno. Ako je P nenul prost ideal u R, onda postoji maksimalan ideal M u R koji sadrži upravo P, odnosno $P \subset M$. Prema pretpostavci je M invertibilan. Slijedi da je $M^{-1}P$ kvocijentni ideal od R, pri čemu je $M^{-1}P \subset M^{-1}M = R$, zbog čega je i $M^{-1}P$ ideal u R. Budući da je $M(M^{-1}P) = RP = P$ i P je prost, vrijedi ili $M \subset P$ ili je $M^{-1}P$ ideal u R. Ako vrijedi $M^{-1}P \subset P$, onda je $R \subset M^{-1} = M^{-1}R = M^{-1}PP^{-1} \subset PP^{-1} \subset R$, odakle slijedi da je $M^{-1} = R$. Stoga je $R = MM^{-1} = MR = M$, a to je kontradikcija s činjenicom da je M maksimalan ideal. Dakle, vrijedi da je $M \subset P$ pa imamo $M = P$. Time je dokazano da je P maksimalan ideal.

$(viii) \Rightarrow (ix)$ Iz pretpostavki slijedi da je R_P cijelo zatvorena domena. Znamo da je svaki ideal u R_P oblika $I_P = \{i/a : i \in I, a \notin P\}$, gdje je I ideal u R. Kako je prema pretpostavci svaki ideal u R konačno generiran, slijedi da je i svaki ideal u R_P također konačno generiran. Stoga je R_P Noetherin prsten. Znamo da je svaki nenul prost ideal u R_P oblika I_P, pri čemu je I nenul prost ideal u R koji je sadržan u P. Kako je svaki nenul prost ideal od R maksimalan (tvrdnja $(viii)$), onda P_P mora biti jedinstven nenul prost ideal u R_P. Dakle, R_P je prsten diskretne valuacije prema lemi 4.

Dokaz implikacije $(ix) \Rightarrow (i)$ dostupan je u literaturi [4, Theorem VIII.6.10.].

□

Teorem 5. *[3, Theorem I.6.3A.] Cijelo zatvorenje Dedekindove domene u konačnom proširenju njezinog polja kvocijenata je opet Dedekindova domena.*

Literatura

[1] W.A. Adkins, S.H. Weintraub, *Algebra: An Approach via Module Theory*, Springer New York, 1992.

[2] M.F. Atiyah, I.G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[3] R. Hartshorne, *Algebraic Geometry*, Encyclopaedia of mathematical sciences, Springer, 1977.

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