Prsteni

Jukić, Josipa

Sveučilište J. J. Strossmayera u Osijeku
Fakultet primjenjene matematike i informatike
Sveučilišni prijediplomski studij Matematika

Josipa Jukić

Prsteni

Završni rad

Osijek, 2023.

Sveučilište J. J. Strossmayera u Osijeku
Fakultet primjenjene matematike i informatike
Sveučilišni prijediplomski studij Matematika

Josipa Jukić

Prsteni

Završni rad

Mentor: prof. dr. sc. Ivan Matić

Osijek, 2023.

Sažetak

Glavna ideja ovog završnog rada je upoznavanje s algebarskom strukturom prsteni. Upoznali smo najvažnije karakteristike i najbitnije definicije prstena. Nadalje smo analizirali i proste i maksimalne ideale, te operacije nad idealima i spektar prostih ideala. Kako bi svojstva i definicije bile što razumljivije, potkrijepili smo ih primjerima.

Ključne riječi:. psteni, ideali, prosti ideali, maksimalni ideali, spektar

Rings

Summary

The main idea of this Final Paper is to introduce the algebraic structure of rings. We have explored the most important characteristics and essential definitions of rings. Furthermore, we analyzed prime and maximal ideals, as well as operations on ideals and the spectrum of prime ideals. To enhance the understanding of properties and definitions, we supported them with examples.

Keywords: rings, ideals, prime ideals, maximal ideals, spectrum

Sadržaj

Uvod

Algebra je osnovna grana matematike koja se bavi proučavanjem algebarskih struktura. Za većinu matematičara danas, algebra označava "asocijativnu algebru nad poljem" (ili komutativnim prstenom), što je vektorski prostor V nad poljem (komutativnim prstenom) koji sadrži bilinearnu i asocijativnu operaciju množenja.

U matematici, algebarske strukture mogu se podijeliti u tri osnovne kategorije: grupe, prstene i polja. U ovom radu ćemo se fokusirati na prstene. Naš cilj je prikazati definiciju prstena, njihove ključne karakteristike i pružiti primjere takvih struktura.

1. Prsteni

1.1. Karakteristike prstena

Definicija 1.1 (vidjeti [1], Definicija 1.1.1). *Komutativni prsten s jediničnim elementom definiramo kao strukturu $(R, +, \cdot, 1)$ koja zadovoljava sljedeće aksiome:*

(1) $(R, +)$ je Abelova grupa, što znači da je skup $(R, +)$ opremljen binarnom operacijom zbrajanja "+" koja je asocijativna, ima neutralni element (označen obično s 0) i za svaki element a u R postoji suprotni element $-a$.

(2) Množenje (označeno s $\cdot$) je asocijativno i distributivno u odnosu na zbrajanje. To znači da za sve elemente a, b, c u R vrijedi:

- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *(asocijativnost množenja)*
- $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ *i* $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ *(distributivnost množenja u odnosu na zbrajanje).*

(3) Množenje je komutativno, što znači da za sve elemente a i b u R vrijedi:

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

(4) Množenje ima jedinični element 1, što znači da postoji element u R, označen s 1, za koji vrijedi:

$$a \cdot 1 = 1 \cdot a = a, \forall a \in R.$$

Od sada ćemo koristiti termin "prsten" kao sinonim za "komutativni prsten s jediničnim elementom".

Napomena 1.1 (vidjeti [1], Napomena 1.1.2). *Iz određenih tehničkih razloga, dopuštamo postojanje **nultog prstena**. U nultom prstenu vrijedi jedinstvena jednakost $0 = 1$. To znači da svi elementi ovog prstena postaju identični, što dalje implicira da za bilo koji element x iz prstena R, vrijedi sljedeće:*

$$x = x \cdot 1 = x \cdot 0 = 0.$$

Primjer 1.1. *Skupovi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su prstenovi.*

Definicija 1.2. *Neka je R prsten i $S \subseteq R$. Skup S se naziva **podprsten** od R, ako je S prsten s operacijama definiranim na R.*
Naprimjer, prstenovi $\mathbb{Z}$, $\mathbb{Q}$ i $\mathbb{R}$ su podprstenovi od $\mathbb{C}$.

Definicija 1.3. *Ako imamo skup X i prsten R, tada možemo stvoriti novi prsten $F(X, R)$ koji se sastoji od svih funkcija $f : X \to R$. Operacija zbrajanja u ovom prstenu definirana je kao $f + g$, što znači da se $\forall x \in X$, vrijednosti funkcija $f(x)$ i $g(x)$ zbrajaju. Slično tome, operacija množenja u ovom prstenu definirana je kao fg, što znači da se $\forall x \in X$, vrijednosti funkcija $f(x)$ i $g(x)$ množe.*
U ovom prstenu, konstantne funkcije 0 i 1 predstavljaju neutralne elemente.

Primjer 1.2 (vidjeti [1], Primjer 1.1.7). *Ako imamo prsten R, tada je skup polinoma $R[X]$ također prsten. U ovom skupu, polinom 0 predstavlja neutralni element, a polinom 1 predstavlja jedinični element. Operacije zbrajanja i množenja polinoma definirane su na uobičajeni*

način.

$$\left(\sum_{i=0}^{n} a_i X^i\right) + \left(\sum_{j=0}^{m} b_j X^j\right) = \sum_{k=0}^{\max\{n,m\}} (a_k + b_k)^k, \qquad (a_k = 0 \ za \ k > n \ i \ b_k = 0 \ za \ k > m)$$

$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot \left(\sum_{j=0}^{m} b_j X^j\right) = \sum_{k=0}^{n+m} \left(\sum_{h=0}^{k} (a_h b_{k-h}) X^k\right)$$

ako je $a_i = 0$ za $i > n$ i $b_j = 0$ za $j > m$, iteracijom dobivamo prstene polinoma $R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$ i prsten polinoma s beskonačno mnogo varijabli $R[X_1, \ldots, X_n, \ldots]$.

Definicija 1.4 (vidjeti [1], Definicija 1.1.8)**.** *Neka su R i S prsteni.* ***Homomorfizam prstena*** *je preslikavanje $\varphi\colon R \to S$ za koje vrijedi:*

- $\varphi(x + y) = \varphi(x) + \varphi(y), \qquad \forall x, y \in R$
- $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y), \qquad \forall x, y \in R.$

Ako dodatno vrijedi i $\varphi(1) = 1$ kažemo da je homomorfizam unitalan.
Homomorfizam koji je bijekcija nazivamo ***izomorfizam****.*

Ako imamo dva homomorfizma prstena $\gamma\colon R \to A$ i $\psi\colon R \to B$, gdje su R, A i B prsteni, tada je njihova kompozicija $\psi\gamma\colon R \to A$ također homomorfizam prstena. To znači da kompozicija čuva strukturu prstena, odnosno $(\psi\gamma)(x+y) = (\psi\gamma)(x) + (\psi\gamma)(y)$ i $(\psi\gamma)(xy) = (\psi\gamma)(x) \cdot (\psi\gamma)(y)$, $\forall x, y \in R$.

Primjer 1.3 (vidjeti [1], Primjer 1.1.10)**.** *Ako je R prsten, S skup i $x_0 \in S$. Preslikavanje*

$$\begin{aligned} F(S, R) &\longrightarrow R \\ f &\longmapsto f(x_0) \end{aligned}$$

je homomorfizam prstena.

Propozicija 1.1. *Ako je $\varphi\colon R \to S$ homomorfizam prstena, tada je $Im\varphi$ podprsten od S.*

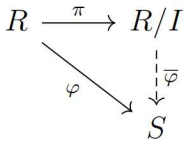
Dokaz: Slijedi iz Definicije 1.4. Primjetimo $1 = \varphi(1) \in Im\varphi$. □

Definicija 1.5 (vidjeti [1], Definicija 1.1.12)**.** *Podskup $I \subset R$ nazivamo* ***idealom*** *ako je $(I, +)$ podgrupa od $(R, +)$ i $xy \in I$, $\forall x \in R$ i $\forall y \in I$.*

Propozicija 1.2. *Ako je $\varphi\colon R \to S$ homomorfizam prstena i $J \subseteq S$ ideal od S, tada je $\varphi^{-1}(J) = \{x \in R \mid \varphi(x) \in J\}$ ideal u prstenu R.*
$Ker\varphi = \varphi^{-1}(0)$ je ideal u R.

Dokaz: Lako se može vidjeti da je skup $\varphi^{-1}(J)$ podgrupa, i $\forall x \in R$ i $y \in \varphi^{-1}(J)$ vrijedi $\varphi(xy) = \varphi(x)\varphi(y) \in J$, jer je $\varphi(y) \in J$. □

Propozicija 1.3 (vidjeti [1], Propozicija 1.1.14)**.** *Ako je $I \subseteq R$ ideal, R/I je kvocijentni prsten i preslikavanje $\pi\colon R \to R/I$ je homomorfizam prstena. Svaki homomorfizam prstena $\varphi\colon R \to S$ takav da je $I \subseteq Ker\varphi$ se na jedinstven način faktorizira kroz homomorfizam prstena $\overline{\varphi}\colon R/I \to S$:*



Primjer 1.4. *(a) Za bilo koji prsten R postoji jedinstveni homomorfizam prstena $\varphi\colon \mathbb{Z} \to R$ definiran s $\varphi(1) = 1$. Jezgra tog homomorfizma je ideal od $\mathbb{Z}$. Stoga, $Ker\varphi = m\mathbb{Z}$ za neki $m \in \mathbb{N}$ se naziva* ***karakteristika*** *prstena.*

(b) Ako je $I = R$, tada je R/I nul-prsten. U mnogim argumentima bit će potrebno uzeti cijeli prsten kao ideal, a to je jedan od razloga za uključivanje praznog prstena ($R/I = \{0\}$).

Definicija 1.6 (vidjeti [1], Definicija 1.1.18)**.** *Neka je R prsten i $S \subseteq R$. Skup $(S) = \{\sum_i x_i s_i | x_i \in R, s_i \in S\}$ je ideal kojeg nazivamo* ***ideal generiran*** *skupom S. Ideal je* ***konačno generiran*** *ako je generiran konačnim podskupom. Na primjer, skup svih višekratnika od $x \in R$ je* ***glavni ideal****, označen s (x) ili xR.*

Definicija 1.7 (vidjeti [1], Definicija 1.1.19)**.** *Neka je R prsten i $x \in R$. Vrijedi:*

a) x je ***djelitelj nule*** *ako je $xy = 0$ za neki $y \neq 0$*

b) x je ***nilpotentan*** *ako je $x^m = 0$ za neki $m \in \mathbb{N}$*

c) x je ***unitalan*** *ili* ***invertibilan*** *ako je $xy = 1$ za neki $y \in R$.*

Primjer 1.5. *U $\mathbb{Z}/6\mathbb{Z}$, broj 2 je djelitelj nule, jer je $2 \cdot 3 = 0$, a i 5 je unitalan, jer je $5 \cdot 5 = 1$.*

Definicija 1.8 (vidjeti [1], Definicija 1.1.23)**.** ***Nul-radikal*** *prstena R je skup svih nilpotentnih elemenata prstena R. Označujemo ga s $\mathfrak{N}_R$.*

Definicija 1.9 (vidjeti [1], Definicija 1.1.25)**.** ***Integralna domena*** *je prsten u kojemu je jedini djelitelj nule 0.*

Primjer 1.6. *Prsteni $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su integralne domene.*

Definicija 1.10 (vidjeti [1], Definicija 1.1.28)**.** ***Polje*** *je prsten u kojem je svaki nenul element invertibilan.*

Primjer 1.7. *Prsteni $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su polja. Za $p > 1$, prsten $\mathbb{Z}/p\mathbb{Z}$ je polje ako i samo ako je p prost broj.*

Propozicija 1.4 (vidjeti [1], Propozicija 1.1.30)**.** *Neka je R nenul prsten. Sljedeće tvrdnje su ekvivalentne:*

(1) R je polje.

(2) Bilo koji nenul homomorfizam $\varphi\colon R \to S$ je injekcija.

(3) Jedini ideali u prstenu R su 0 i R.

Dokaz: (1) $\Rightarrow$ (2) Ako je $x \in Ker\varphi$, $x \neq 0$, onda je $1 = x^{-1}x \in Ker\varphi$, iz toga slijedi da je φ nul-homomorfizam.

(2) $\Rightarrow$ (3) Ako je $I \subsetneq R$ pravi ideal, tada $\pi\colon R \to R/I$ ne može biti nul-preslikavanje, nego mora biti injekcija. Tada je $I = Ker\varphi = \{0\}$.

(3) $\Rightarrow$ (1) Ako je $x \neq 0$, tada $(x) \neq 0$, stoga $(x) = R$ i iz toga slijedi da je 1 višekratnik od x. $\square$

Definicija 1.11. ***Domena glavnih ideala****, ili skraćeno DGI, je integralna domena koja je prsten glavnih ideala, tj. prsten u kojem je svaki ideal glavni.*

Primjer 1.8. *Prsten $\mathbb{Z}$ je domena glavnih ideala.*

Definicija 1.12 (vidjeti [1], Definicija 1.1.33)**.** *Kažemo da je $x \in R$* ***ireducibilan*** *ako $x \neq R^\times$ ($R^\times = R \setminus \{0\}$), i kada je $x = yz \in R$ tada je ili y i z unitalan.*
Integralna domena je ***domena jedinstvene faktorizacije****, ili skraćeno DJF, ako se svaki element može napisati kao produkt ireducibilnih elemenata pomnoženih s jediničnim elementima, pri čemu su ireducibilni faktori jedinstveni do na poredak i množenje invertibilnim elementima.*

Primjer 1.9. *Prsten $\mathbb{Z}$ je domena jedinstvene faktorizacije.*

1.2. Prosti i maksimalni ideali

Definicija 1.13 (vidjeti [1], Definicija 1.1.36). *Pravi ideal $\mathfrak{p} \subsetneq R$, nazivamo **prostim idealom**, ako za bilo koje $x, y \in R$, za koje vrijedi $xy \in \mathfrak{p}$, je ili $x \in \mathfrak{p}$ ili $y \in \mathfrak{p}$.*

Primjer 1.10. *Ideal $p\mathbb{Z}$ je prost ideal ako i samo ako je p prost broj.*

Propozicija 1.5 (vidjeti [1], Propozicija 1.1.38). *Neka je R prsten i $\mathfrak{p} \subsetneq R$ pravi ideal. Sljedeće tvrdnje su ekvivalentne:*

a) $\mathfrak{p}$ je prost

b) $R/\mathfrak{p}$ je domena glavnih ideala.

Dokaz: Prema definiciji, $\overline{x} \cdot \overline{y} = \overline{xy} = 0$ u $R/\mathfrak{p}$ ako i samo ako $xy \in \mathfrak{p}$. □

Korolar 1.1. *Nul-ideal je prost ideal ako i samo ako je R integralna domena.*

Primjer 1.11 (vidjeti [1], Primjer 1.1.40). *Ako je p prost broj, $p\mathbb{Z}[X] \subset \mathbb{Z}[X]$ je prost ideal. Naime, $p\mathbb{Z}[X] = Ker\pi$, gdje je $\pi\colon \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$ definirana s $\pi(\sum a_i X^i) = \sum \overline{a}_i X^i$. Stoga je, $\mathbb{Z}[X]/p\mathbb{Z}[X] \cong (\mathbb{Z}/p\mathbb{Z})[X]$.*

Napomena 1.2. *Ako je R integralna domena, element $x \in R$ možemo nazvati **prostim** ako je ideal generiran s x, tj. (x) prost ideal. Prost element je također i ireducibilan, takav da, ako postoji izraz $x = yz$ tada su ili y ili z iz (x). Osim toga, ako postoji element $u \in R$ takav da je $y = uz$, tada možemo pokazati da je $uz = 1$, što znači da je z invertibilan u R.*

Propozicija 1.6. *Neka je R prsten i $\varphi\colon R \to S$ homomorfizam prstena. Ako je $\mathfrak{q} \subset S$ prost ideal, tada je $\varphi^{-1}(\mathfrak{q}) \subset R$ također prost ideal.*

Dokaz: Prema Propoziciji 1.3, $R/\varphi^{-1}(\mathfrak{q}) \hookrightarrow S/\mathfrak{q}$ i potonji je integralna domena. □

Definicija 1.14. *Pravi ideal $\mathfrak{m} \subsetneq R$ naziva se **maksmalni ideal** ako ne postoji pravi ideal u R koji strogo sadrži $\mathfrak{m}$. Drugim rijecima, ako je $I \subset R$ ideal takav da je $\mathfrak{m} \subset I \subset R$, tada je ili $\mathfrak{m} = I$ ili $I = R$.*

Propozicija 1.7 (vidjeti [1], Propozicija 1.1.45). *Neka je R prsten i $\mathfrak{m} \subsetneq R$ pravi ideal. Sljedeće tvrdnje su ekvivalentne:*

a) $\mathfrak{m}$ je maksimalan

b) $R/\mathfrak{m}$ je polje.

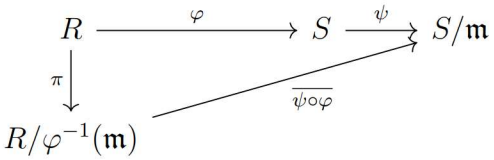
Dokaz: Ako je $\mathfrak{m}$ maksimalan ideal i $x \neq R$ tada je ideal generiran s $\mathfrak{m}$ i x jednak cijelom prstenu R, tj. ako postoji $z \in \mathfrak{m}$ i $y \in R$ takav da vrijedi $1 = xy + z$. Nadalje, x je invertibilan u $R/\mathfrak{m}$ takav da je y inverz. Obratno, ako je $R/\mathfrak{m}$ polje, promotrimo $\mathfrak{m} \subseteq I \subseteq R$. Ako I sadrži element $x \neq \mathfrak{m}$, budući je x invertibilan modulo $\mathfrak{m}$, postoje $z \in \mathfrak{m}$ i $y \in R$ takvi da vrijedi $1 = xy + z$, pa je $I = R$. □

Korolar 1.2. *Svaki maksimalan ideal je prost.*

Ako je $\varphi\colon R \to S$ homomorfizam prstena i $\mathfrak{m} \subset S$ maksimalan ideal, općenito $\varphi^{-1}(\mathfrak{m}) \subset R$ nije maksimalan. Na primjer, promotrimo preslikavanje $\varphi\colon \mathbb{Z} \to \mathbb{Q}$ i $\varphi^{-1}(0) = 0$. Međutim, vrijedi sljedeća tvrdnja:

Propozicija 1.8. *Neka je $\varphi\colon R \to S$ surjektivni homomorfizam prstena. Ako je $\mathfrak{m} \subset S$ maksimalan ideal, tada je i $\varphi^{-1}(\mathfrak{m}) \subset R$ maksimalan.*

Dokaz: Promotrimo dijagram



Budući da je $\psi \circ \varphi$ surjekcija, $\overline{\psi \circ \varphi} \circ \pi$ je također surjekcija, iz toga slijedi da je i $\overline{\psi \circ \varphi}$ surjekcija. Prema Propoziciji 1.3, $\overline{\psi \circ \varphi}$ je injekcija. Stoga, $R/\varphi^{-1}(\mathfrak{m}) \simeq S/\mathfrak{m}$ je polje, pa je $\varphi^{-1}(\mathfrak{m})$ maksimalan. □

Maksimalni i prosti ideali uvijek postoje. Ovo se može vidjeti pomoću Zornove leme koju ćemo u nastavku spomenuti. Skup Σ je **parcijalno uređen** ako zadovoljava refleksivno i tranzitivno svojstvo relacije $\leq$ takvo da vrijedi

$$\begin{cases} x \leq y \\ y \leq x \end{cases} \implies \quad x = y$$

Element $m \in \Sigma$ je **maksimalan** ako uvjet $x \geq m$ slijedi $x = m$. **Lanac** je podskup $C \subseteq \Sigma$, takav da $\forall x, y \in C$ vrijedi da je ili $x \leq y$ ili $y \leq x$.

Teorem 1.1 (**Zornova lema**, vidjeti [1], Teorem 1.1.50)**.** *Neka je Σ parcijalno uređen neprazan skup. Ako za svaki $C \subseteq \Sigma$, postoji $s \in \Sigma$ takav da je $x \leq s$, $\forall x \in C$, tada Σ ima maksimalne elemente.*

Korolar 1.3. *Ako je R ne-nul prsten, tada R sadrži maksimalni ideal.*

Korolar 1.4. *Svaki pravi ideal I u prstenu R sadržan je u nekom maksimalnom idealu.*

Korolar 1.5. *U ne-nul prstenu R, svaki $x \in R^\times$ sadržan je u nekom maksimalnom idealu.*

Dokaz: Primjenimo Korolar 1.4 na ideal (x).

Propozicija 1.9 (vidjeti [1], Propozicija 1.1.54)**.** *Nul-radikal je presjek svih prostih ideala.*

Dokaz: Da bismo pokazali tvrdnju, razmotrit ćemo dvije strane: prvo, da svaki nilpotentni element pripada svakom prostom idealu, a zatim, da za svaki ne-nilpotentni element postoji pripadajući prosti ideal koji ga ne sadrži.
Za prvu stranu, pretpostavimo da je x nilpotentan element, tj. da postoji $n \in \mathbb{N}$ za koji vrijedi $x^n = 0$. Nadalje, za bilo koji ideal $\mathfrak{p}$ vrijedi da je $x^n = 0 \in \mathfrak{p}$, što znači da x pripada tom idealu.
S druge strane, pretpostavimo da je x ne-nilpotentni element. Promotrimo skup Σ svih ideala $\mathfrak{s} \subset R$, takav da $x^n \notin \mathfrak{s}$, $\forall n \in \mathbb{N}$. Budući da x nije nilpotentan, $0 \in \Sigma$, što znači da je skup Σ neprazan. Neka je $C = \{\mathfrak{s}_n\}$ skup lanaca u Σ. Definirajmo $\mathfrak{s} = \bigcup_{n\in\mathbb{N}} \mathfrak{s}_n$, što je također ideal. Sada, $\forall y \in \mathfrak{s}$, postoji $\mathfrak{s}_n$ koji ga sadrži, pa slijedi da je $y^n \in \mathfrak{s}_n$, za neki $n \in \mathbb{N}$. No, to znači da $y^n \notin \mathfrak{s}$, $\forall n \in \mathbb{N}$, pa prema tome $y \notin \mathfrak{s}$. To pokazuje da je $\mathfrak{s} \in \Sigma$. Kako je svaki lanac u Σ ograničen, primjenjujemo Zornovu lemu i zaključujemo da skup Σ sadrži maksimalni element, koji označimo s $\mathfrak{p}$.
Sada želimo pokazati da je $\mathfrak{p}$ prost ideal. Ako y,$z \notin \mathfrak{p}$, tada je $\mathfrak{p}$ sadržan u $(y, \mathfrak{p})$ i $(z, \mathfrak{p})$, pa ovi ideali nisu u skupu Σ: postoje m,$n \in \mathbb{N}$ i elementi a,$c \in R$ te b,$d \in \mathfrak{p}$ takvi da $x^n = ay + b$ i $x^m = cz + d$. Da je $yz \in \mathfrak{p}$, slijedilo bi $x^{m+n} = acyz + (ayd + czb + bd) \in (yz, \mathfrak{p}) = \mathfrak{p}$, što je kontradikcija s pretpostavkom da x nije nilpotentan element. □

Definicija 1.15. ***Jacobsonov radikal*** *je presjek svih maksimalnih ideala u prstenu R, označavamo ga s $\mathfrak{R}_R$.*

Propozicija 1.10. *Vrijedi $x \in \mathfrak{R}_R$ ako i samo ako $1 - xy \in R^\times$, $\forall y \in R$.*

Definicija 1.16. *Prsten je* ***lokalni*** *ako sadrži jedinstveni maksimalni ideal.* ***Semi-lokalni*** *prsten je prsten s konačnim brojem maksimalnih ideala.*

Primjer 1.12. *Prsten $\mathbb{Z}/6\mathbb{Z}$ je semi-lokalni prsten, s maksimalnim idealima $2\mathbb{Z}/6\mathbb{Z}$ i $3\mathbb{Z}/6\mathbb{Z}$. Zaista, skup maksimalnih ideala u $\mathbb{Z}/6\mathbb{Z}$ je u bijekciji sa skupom ideala u $\mathbb{Z}$ koji sadrže 6: jedini takvi su $2\mathbb{Z}$ i $3\mathbb{Z}$.*

Propozicija 1.11 (vidjeti [1], Propozicija 1.1.60)**.** *Neka je R prsten.*

a) Ako je $\mathfrak{s} \subset R$ pravi ideal od R, takav da $R - \mathfrak{s} \subseteq R^\times$, tada je R lokalni prsten s maksimalnim idealom $\mathfrak{s}$.

b) Ako je $\mathfrak{m} \subset R$ maksimalni ideal i ako je za $\forall x \in \mathfrak{m}$ izraz $1 + x$ jedinični element u R (tj. ima inverzni element za množenje), tada je R lokalni prsten.

Dokaz:

a) Neka je $\mathfrak{s} \subseteq I \subseteq R$. Ako je $\mathfrak{s} \neq I$, tada I sadrži element iz $R - \mathfrak{s}$, odnosno, jedinični element. Dakle, $I = R$, što znači da je $\mathfrak{s}$ maksimalni ideal. Također, $\mathfrak{s}$ je jedinstveni maksimalni ideal jer bilo koji drugi ideal koji nije sadržan u $\mathfrak{s}$ sadrži jedinični element.

b) Neka je $\mathfrak{b} \subset R$ bilo koji ideal. Ako $\mathfrak{b} \neq \mathfrak{m}$, tada $\exists y \in \mathfrak{b}$, takav da $y \notin \mathfrak{m}$. Prema maksimalnosti vrijedi $(y,\mathfrak{m}) = R$. Neka je $1 = ay + x$ za neki $a \in R$, $x \in \mathfrak{m}$. Tada je $ay = 1 - x \in \mathfrak{b}$ jedinični element, stoga $\mathfrak{b} = R$. Dakle, svaki pravi ideal je sadržan u $\mathfrak{m}$.

□

1.3. Operacije nad idealima

Propozicija 1.12 (vidjeti [1], Propozicija 1.1.61)**.** *Neka je R prsten, i $\{I_\alpha\}_\alpha$ familija ideala. Presjek $\bigcap_\alpha I_\alpha$ i suma $\sum_\alpha I_\alpha = \{\sum_\alpha x_\alpha, x_\alpha \in I_\alpha,\ x_\alpha = 0,$ za sve, osim konačno mnogo $\alpha\}$ su ideali od R.*

Propozicija 1.13 (vidjeti [1], Propozicija 1.1.62)**.** *Neka su I i J ideali u prstenu R. Skup $IJ = \{\sum_i x_i y_i, \forall x \in I, y \in J\}$, koji se sastoji od konačnih suma produkta elemenata iz I i elemenata iz J, je ideal, kojeg nazivamo* ***produkt ideala****.*

Dokaz: Skup IJ nije prazan, jer sadrži 0. Suma dvaju elemenata iz IJ je konačna, pa i pripada skupu IJ. Za svaki $s \in R$ imamo $s(\sum_i x_i y_i) = \sum_i (sx_i)y_i \in IJ$ jer je svaki $sx_i \in I$. □

Definicija 1.17. *Neka je R komutativni prsten.* ***Najveći zajednički djelitelj****, skraćeno nzd, prstena R je element $z \in R$ takav da vrijedi $z|x$ i $z|y$ $\forall x, y \in R$.*

Definicija 1.18. *Neka je R komutativni prsten.* ***Najmanji zajednički višekratnik****, skraćeno nzv, elemenata $x, y \in R$ je zajednički višekratnik $z \in R$ takav da je svaki zajednički višekratnik elemenata x i y također višekratnik od z.*

Primjer 1.13 (vidjeti [1], Primjer 1.1.63)**.** *Neka je R DGI, $I = (x)$ i $J = (y)$. Tada je $I + J = (nzd(x,y))$, $I \cup J = (nzv(x,y))$ i $IJ = (xy)$. Posebno, $IJ = I \cup J$ ako i samo ako $nzd(x,y) = 1$.*

Definicija 1.19 (vidjeti [1], Definicija 1.1.64)**.** *Kažemo da su dva ideala I,$J \subseteq R$* ***relativno prosti*** *ako vrijedi $I + J = R$.*

Propozicija 1.14 (vidjeti [1], Propozicija 1.1.65)**.** *Neka su I i J ideali prstena R. Tada vrijedi $IJ \subseteq I \cup J$ ako su I i J relativno prosti.*

Dokaz: Inkluzija $IJ \subseteq I \cup J$ vidljiva je iz definicija. Pretpostavimo da vrijedi $I + J = R$, tada je $1 = x + y$, za $x \in I$ i $y \in J$. Tada $\forall z \in I \cup J$, slijedi da je $xz \in I$ i $yz \in J$, stoga $z = 1z = xz + yz \in IJ$. □

Korolar 1.6 (vidjeti [1], Korolar 1.1.66)**.** *Neka su $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideali R. Tada $\prod_{i=1}^n \mathfrak{a}_i \subseteq \bigcup_{i=1}^n \mathfrak{a}_i$ vrijedi ako su ideali relativno prosti: $\mathfrak{a}_i + \mathfrak{a}_j = R, \forall i \neq j$.*

Definicija 1.20 (vidjeti [1], Definicija 1.1.67)**.** *Neka je $\{R_\alpha\}_\alpha$ familija prstena. Produkt Abelovih grupa $\prod_\alpha R_\alpha$ je također prsten, koji nazivamo* ***direktan produkt****, s operacijom množenja $(\ldots, a_\alpha, \ldots) \cdot (\ldots, b_\alpha, \ldots) = (\ldots, a_\alpha b_\alpha, \ldots)$ i $1 = (\ldots, 1, \ldots)$. Preslikavanje $\pi\colon \prod_\alpha R_\alpha \to R_\alpha$ je homomorfizam prstena.*

Neka su $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideali u R. Tada preslikavanje $\pi_i\colon R \to R/\mathfrak{a}_i$ definira trivijalni homomorfizam prstena

$$\begin{aligned} \varphi : R &\longrightarrow \prod_{i=1}^{n} R/\mathfrak{a}_i \\ x &\longmapsto (\pi_i(x), \ldots, \pi_n(x)). \end{aligned} \tag{1}$$

Dodatno vrijedi: $Ker\varphi = \bigcap_{i=1}^n \mathfrak{a}_i$.

Korolar 1.7 (**Kineski teorem o ostatcima**, vidjeti [1], Korolar 1.1.68)**.** *Preslikavanje φ u (1) je surjekcija ako i samo ako su ideali $\mathfrak{a}_i$ relativno prosti.*

Dokaz:

- Ako je φ surjektivno preslikavanje, $\forall i \neq j$, kompozicijsko preslikavanje $R \to \prod_{i=1}^{n} R/\mathfrak{a}_i \to R/\mathfrak{a}_i \times R/\mathfrak{a}_j$ je također surjekcija, onda odaberimo $x \in R$ koji se preslikava u $(1,0)$, tj. $x \equiv 1 \pmod{\mathfrak{a}_i}$ i $x \equiv 0 \pmod{\mathfrak{a}_j}$. Tada $1 = (1-x) + x \in \mathfrak{a}_i + \mathfrak{a}_j$.

- Obratno, ako su $\mathfrak{a}_i$ reativno prosti, za $i = 2, \ldots, n$, odaberemo $x_i \in \mathfrak{a}_i$ i $y_i \in \mathfrak{a}_i$ takav da $x_i + y_i = 1$. Tada vrijedi $y = \prod_{i=2}^{n} y_i \in \mathfrak{a}_i$ za $\forall i \in \{2, \ldots, n\}$ i $y = \prod_{i=2}^{n} (1 - x_i) \equiv 1 \mod \mathfrak{a}_i$, nadalje je $\varphi(y) = (1, 0, \ldots, 0)$. Permutirajući indekse, vidimo da je φ surjekcija.

□

1.4. Spektar prostih ideala

Gotovo cijela moderna komutativna algebra bila je inspirirana i potaknuta algebarskom geometrijom i teorijom brojeva. Klasično, algebarska geometrija proučava svojstva algebarskih skupova, što su skupovi u afinom ili projektivnom prostoru definirani sustavima polinomnih jednadžbi. Nulto mjesto polinoma u jednoj varijabli nad algebarski zatvorenim poljem K jednostavno su konačne skupine točaka u afinom pravcu, tj. korijeni polinoma. Ako želimo da polinomi budu kontinuirane funkcije u afinom prostoru K^n, prirodna topologija koju bismo trebali koristiti je *topologija Zarinskog*, koja kaže da su otvoreni skupovi oni koji su komplementarni konačnim unijama nultočaka polinoma.

Dakle, $K[X_1, \ldots, X_n]$ se može shvatiti kao prsten neprekidnih funkcija na posebnom topološkom prostoru, koji predstavlja afini n-dimenzionalni prostor. Jedna od Grothendieckova spoznaja bila je preskočiti određene situacije i promatrati svaki prsten R kao prsten neprekidnih funkcija na topološkom prostoru koji mu je intrinzički pripojen, njegov spektar *Spec R*. Ovaj konceptualni napredak omogućuje da se geometrija može primjenjivati s proizvoljnim prstenovima koeficijenata, a ne samo s algebarski zatvorenim poljima. Na taj način, Algebarska geometrija i Teorija brojeva spajaju se u jednu cjelinu - Aritmetičku geometriju.

Definicija 1.21 (vidjeti [1], Definicija 1.1.69)**.** *Neka je R prsten i $I \subseteq R$ ideal.* ***Nulto mjesto*** *u idealu I je skup $\mathcal{Z}(I)$ koji se sastoji od svih prostih ideala u R koji sadrže I.*

Primjer 1.14 (vidjeti [1], Primjer 1.1.70)**.** *U svakom prstenu R vrijedi $\mathcal{Z}(1) = \emptyset$ (ako pretpostavimo da su svi prosti ideali pravi), dok je $\mathcal{Z}(0)$ skup prostih ideala. Ako je $\mathfrak{m} \subset R$ maksimalni ideal, tada je $\mathcal{Z}(\mathfrak{m}) = \{\mathfrak{m}\}$.*

Primjer 1.15 (vidjeti [1], Primjer 1.1.71)**.** *U $R = \mathbb{Z}$ je $\mathcal{Z}((30)) = \{(2), (3), (5)\}$.*

Propozicija 1.15 (vidjeti [1], Propozicija 1.1.73)**.** *Neka je R prsten, i neka su $I, J, \{I_\alpha\}_\alpha$ ideali. Tada vrijedi:*

a) Ako $I \subseteq J$ tada je $\mathcal{Z}(J) \subseteq \mathcal{Z}(I)$

b) $\mathcal{Z}(IJ) = \mathcal{Z}(I) \cup \mathcal{Z}(J)$

c) $\mathcal{Z}(\Sigma_\alpha I_\alpha) = \cap_\alpha \mathcal{Z}(I_\alpha)$.

Dokaz: a) slijedi iz Definicije 1.19. Budući da je IJ sadržan i u I i u J, to pokazuje da je $\mathcal{Z}(IJ) \supseteq \mathcal{Z}(I) \cup \mathcal{Z}(J)$. S druge strane, ako je $IJ \subseteq \mathfrak{p}$ i $I \subsetneq \mathfrak{p}$, tada $x \in I, x \notin \mathfrak{p}$. Budući da $\forall y \in J$ imamo $xy \in IJ \subseteq \mathfrak{p}$ i $y \in \mathfrak{p}$. Stoga $J \subseteq \mathfrak{p}$, pa slijedi b).

c) Svaki prosti ideal koji sadrži svaki od I_α sadrži i njihovu sumu, i obratno, stoga svaki prosti ideal koji sadrži sumu sadrži svaki I_α. □

Definicija 1.22 (vidjeti [1], Definicija 1.1.74)**.** ***Spektar*** *prstena R je skup Spec R svih prostih ideala u R, opisan Zarinski topologijom u kojoj su otvoreni podskupovi oblika Spec $R \setminus \mathcal{Z}(I)$ za neki ideal $I \subseteq R$.*

Propozicija 1.16 (vidjeti [1], Propozicija 1.1.75)**.** *Ako je $\varphi\colon R \to S$ homomorfizam prstena, tada φ određuje neprekidno preslikavanje*

$$\begin{aligned} \varphi^\sharp : Spec\ S &\longrightarrow Spec\ R \\ \mathfrak{p} &\longmapsto \varphi^{-1}(\mathfrak{p}). \end{aligned}$$

Dokaz: Preslikavanje $\varphi^\sharp$ je dobro definirano po Propoziciji 1.6. Ako je $I \subseteq R$ ideal, tada

$$\begin{aligned}(\varphi^\sharp)^{-1}\mathcal{Z}(I) &= \{\mathfrak{q} \in Spec\ S \mid \varphi^\sharp(\mathfrak{q}) \in \mathcal{Z}(I)\} \\ &= \{\mathfrak{q} \in Spec\ S \mid I \subseteq \varphi^{-1}(\mathfrak{q})\} \\ &= \{\mathfrak{q} \in Spec\ S \mid \varphi(I) \subseteq \mathfrak{q}\} \\ &= \mathcal{Z}(\varphi(I)).\end{aligned}$$

Stoga, $\varphi^\sharp$ je neprekidno preslikavanje. □

Korespondencija između ideala u R i zatvorenih podskupova u $Spec\ R$ nije savršena: ako je $I \subseteq R$ ideal, prema Propoziciji 1.15, $\mathcal{Z}(I^2) = \mathcal{Z}(I) \cup \mathcal{Z}(I) = \mathcal{Z}(I)$, ali općenito $I \neq I^2$. To nas potiče na sljedeću definiciju.

Definicija 1.23 (vidjeti [1], Definicija 1.1.76)**.** *Neka je R prsten i $I \subseteq R$ ideal.* ***Radikal*** *od I je ideal*

$$\sqrt{I} = \{x \in R \mid \exists n \in \mathbb{N}, x^n \in I\}.$$

Ako je $I = \sqrt{I}$, kažemo da je I ***radikalni ideal****.*

Primjer 1.16. *Svaki prosti ideal je radikalni. Ideal $6\mathbb{Z}$ je radikalni ideal u $\mathbb{Z}$ i $\sqrt{12\mathbb{Z}} = 6\mathbb{Z}$.*

Stoga možemo precizirati tvrdnju iz Propozicije 1.15 a):

Korolar 1.8 (vidjeti [1], Korolar 1.1.78)**.** *Ako su I i J ideali, tada $\mathcal{Z}(J) \subseteq \mathcal{Z}(I) \iff \sqrt{I} \subseteq \sqrt{J}$.*

Dokaz: Budući da je $\mathcal{Z}(I) = \mathcal{Z}(\sqrt{I})$ jedna implikacija slijedi iz Propozicije 1.15 a). Ako $\mathcal{Z}(J) \subseteq \mathcal{Z}(I)$, svaki prosti ideal koji sadrži J također sadrži i I. Dakle, $\sqrt{I} = \cap_{I \subseteq \mathfrak{p}} \mathfrak{p} \subseteq \cap_{J \subseteq \mathfrak{p}} \mathfrak{p} = \sqrt{J}$. □

Napomena 1.3 (vidjeti [1], Napomena 1.1.79)**.** *Spec R kao topološki prostor ima svojstva koja su značajno drugačija od intuicije stjecane radom s uobičajenom realnom ili kompleksnom topologijom. Primjerice, nije Hausdorffov: ako je R integralna domena, tada je 0 prosti ideal koji je sadržan u okolini svake točke. Također, točke nisu nužno zatvorene: ponovno, u integralnoj domeni je 0 točka čiji je zatvarač cijeli prostor. Općenito, zatvarač točke $\mathfrak{p} \in Spec\ R$ je*

$$\overline{\{\mathfrak{p}\}} = \bigcap_{I \subseteq \mathfrak{p}} \mathcal{Z}(I) = \bigcap_{I \subseteq \mathfrak{p}} \{\mathfrak{q} \supseteq I\} = \mathcal{Z}(\mathfrak{p}).$$

U $Spec\ R$, zatvorene točke su posebno značajne jer odgovaraju maksimalnim idealima. U klasičnoj Algebarskoj geometriji, obično se promatraju samo zatvorene točke. Međutim, treba napomenuti da se maksimalni ideali ne ponašaju dobro s obzirom na homomorfizam prstenova, i cjelokupnu sliku dobivamo samo kada razmatramo sve glavne ideale.

Literatura

[1] M. A. Garuti, *Commutative Algebra Lecture Notes*, https://www.math.unipd.it/~mgaruti/CA/50sNak.pdf

[2] T. W. Hungerford, *Algebra*, Springer-Verlag, New York-Berlin, 1980.

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