SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Marina Zrno

KOMUTATIVNI PRSTENI

Diplomski rad

Voditelj rada:
prof.dr.sc. Ozren Perše

Zagreb, 2014

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

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

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Roditeljima, Željku i Ružici. Hvala vam na beskrajnoj ljubavi i razumijevanju.

Sadržaj

Uvod

Cilj ovog diplomskog rada je upozavanje s nekim pojmovima i objektima, od kojih je centralan pojam komutativan prsten. Prsteni su jedna od osnovnih algebarskih struktura u matematici. Osnovna podjela prstena je na komutativne i nekomutativne. Iako je u pravilu proučavanje strukture nekomutativnih prstena puno kompliciranije nego kod onih koji su komutativni, često baš komutativnost u određenom smislu daje 'bogatstvo strukture', tj. u mnogim komutativnim prstenima će biti cijelo mnoštvo potprstena i ideala.

Prsteni se pojavljuju u analizi, u algebri, u teoriji brojeva, u algebarskoj geometriji i u mnogim drugim granama matematike. Za razliku od grupa gdje imamo samo jednu binarnu operaciju, kod prstena imamo dvije operacije; imajući na umu prsten $(\mathbb{Z}, +, \cdot)$, kao prvi 'pravi' i osnovni primjer, te se operacije sada zovu 'zbrajanje' i 'množenje'. Poseban naglasak ćemo smo staviti na prsten polinoma. Vidjeti ćemo da, kada je k polje, svi poznati teoremi koji vrijede u $\mathbb{Z}$, imaju analogon u $k[x]$; štoviše, vidjet ćemo da se svi poznati dokazi mogu prenijeti ovdje. Prezentirat ćemo algoritam dijeljenja za polinome s koeficijentima iz polja.

U ovom diplomskom radu ćemo proučiti elementarna svojstva komutativnog prstena, posebno konstrukcije koje su analogne onim u teoriji grupa kao što su potprsteni, ideali (koji su analogni normalnim podgrupama), kvocijentni prsteni i homomorfizmi prstena.

Upoznat ćemo se s dva zanimljiva tipa ideala: prostim idealima i maksimalnim idealima. Pokazat ćemo da je svaki maksimalan ideal prost ideal, vidjeti primjer prostog ideala koji nije maksimalan i na kraju dokazati da ako je komutativan prsten R domena glavnih ideala, tada je svaki ne-nul prost ideal maksimalan.

Poglavlje 1

Definicije i osnovna svojstva

U ovom poglavlju uvodimo pojam komutativnog prstena, dajemo njegova svojstva i neke primjere počevši sa poznatim skupovima $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$. Također su navedeni osnovni rezultati iz grupa koji su nam bili potrebni za cjelovitost ovog diplomskog rada.

Definicija 1.1 *Binarna operacija na skupu G je funkcija*

$$* : G \times G \to G.$$

Definicija 1.2 *Skup G s binarnom operacijom $*$ se zove **grupa** ako vrijedi*
(i) zakon asocijativnosti: za sve $x, y, z \in G$,

$$x * (y * z) = (x * y) * z;$$

*(ii) postoji element e, kojeg nazivamo **neutralni element**, tako da vrijedi $e * x = x * e = x$ za sve $x \in G$;*
*(iii) svaki $x \in G$ ima **inverzni element**, tj., postoji $x' \in G$ tako da vrijedi $x * x' = x' * x = e$.*

Definicija 1.3 *Ako je G grupa i $a \in G$, definiramo **potencije** a^n, za $n \geq 1$, induktivno:*

$$a^1 = a \text{ i } a^{n+1} = aa^n.$$

Definiramo $a^0 = 1$ i ako je n pozitivan cijeli broj, definiramo

$$a^{-n} = (a^{-1})^n.$$

Definicija 1.4 *Grupa G se naziva **Abelova grupa,** ako vrijedi dodatni uvjet, **zakon komutativnosti**,*

$$x * y = y * x,$$

za sve $x, y \in G$.

Primjer 1.5 *(i) Skup $\mathbb{Q}^\times$, svih ne-nul racionalnih brojeva, s binarnom operacijom $*$ množenja, je Abelova grupa. Neutralni element je 1. Inverzni element od $r \in \mathbb{Q}^\times$ je $1/r$. Slično, $\mathbb{R}^\times$ i $\mathbb{C}^\times$ su Abelove grupe.*

(ii) Skup cijelih brojeva $\mathbb{Z}$ s binarnom operacijom zbrajanja $+$, je Abelova grupa. Neutralni element je 0. Inverzni element od $n \in \mathbb{Z}$ je $-n$. Slično, $\mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$ su Abelove grupe s binarnom operacijom zbrajanja.

Definicija 1.6 *Podskup H grupe G je podgrupa ako vrijedi*
(i) $1 \in H$;
(ii) ako je $x, y \in H$, tada je $xy \in H$;
(iii) ako je $x \in H$, tada je $x^{-1} \in H$.

Ako je H podgrupa od G, tada išemo $H \leq G$; ako je H prava podgrupa od G, tj., $H \neq G$, tada pišemo $H < G$.

Definicija 1.7 *Ako su $(G, *)$ i $(H, \circ)$ grupe tada je funkcija $f : G \to H$ **homomorfizam** (grupa) ako vrijedi*

$$f(x * y) = f(x) \circ f(y)$$

*za sve $x, y \in G$. Homomorfizam koji je također bijekcija naziva se **izomorfizam**. Za dvije grupe G i H reći cemo da su **izomorfne**, ako postoji neki izomorfizam f medju njima; tu činjenicu označavamo sa $G \cong H$.*

Definicija 1.8 *Za proizvoljan homomorfizam grupa $f : G \to H$, definirajmo njegovu **jezgru***

$$\ker\ f = \{x \in G \mid f(x) = 1\}$$

*i njegovu **sliku***

$$im\ f = \{h \in h \mid h = f(x)\ za\ neki\ x \in G\}.$$

Definicija 1.9 *Podgrupa N grupe G se naziva **normalna podgrupa** ako $n \in N$ i $g \in G$ povlače $gng^{-1} \in N$. Ako je N normalna podgrupa od G, tada pišemo $N \lhd G$.*

Primijetimo da je u Abelovoj grupi svaka podgrupa očito normalna.

Teorem 1.10 *Neka je G proizvoljna grupa i N neka njezina normalna podgrupa. Tada kvocijentni skup*

$$G/N = \{xN \mid x \in G\}$$

sa operacijom

$$G/N \times G/N \to G/N, \qquad (xN, yN) \longmapsto xyN,$$

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

$$\pi : G \to G/N, \qquad x \longmapsto xN,$$

*je epimorfizam grupa sa jezgrom $\ker \pi = N$; π zovemo **kanonski epimorfizam**, ili **kanonska surjekcija**.*

Teorem 1.11 ***(Prvi teorem o izomorfizmu.)*** *Ako je $f : G \to H$ homomorfizam, tada je*

$$\ker\ f \lhd G \text{ i } G/\ker\ f \cong im\ f.$$

Ako je $\ker\ f = K$ *i* $\varphi : G/K \to im\ f \leq H$ *dano s* $\varphi : aK \longmapsto f(a)$, *tada je* φ *izomorfizam.*

Teorem 1.12 ***(Teorem o korespondenciji za grupe)*** *Neka je G grupa, neka je $K \lhd G$, i neka je $\pi : G \to G/K$ prirodno preslikavanje. Tada je*

$$S \longmapsto \pi(S) = S/K$$

je bijekcija između familije svih podgrupa S od G koje sadrže K i familije svih podgrupa grupe G/K.

Definicija 1.13 ***Komutativan prsten*** *R je skup na kojem su definirane dvije binarne operacije, zbrajanje i množenje, tako da vrijedi:*

(i) R je Abelova grupa za zbrajanje;
*(ii) (**komutativnost**) $ab = ba$ za sve $a, b \in R$;*
*(iii) (**asocijativnost**) $a(bc) = (ab)c$ za sve $a, b, c \in R$;*
(iv) postoji jedinični element $1 \in R$ takav da je $1a = a$ za sve $a \in R$;
*(v) (**distributivnost**) $a(b + c) = ab + ac$ za sve $a, b, c \in R$.*

Jedinični element prstena R se zove još i jedinica ili identiteta u R.

Primjer 1.14 *(i) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$ su komutativni prsteni sa zbrajanjem i množenjem.*

*(ii) Neka je $\mathbb{Z}[i]$ skup svih kompleksnih brojeva oblika $a+bi$, gdje su $a, b \in \mathbb{Z}$, $i^2 = -1$. $\mathbb{Z}[i]$ se zove prsten **Gaussovih cijelih brojeva.***

(iii) Neka je R skup svih realnih brojeva x oblika

$$x = a + b\omega,$$

gdje su $a, b \in \mathbb{Q}$ i $\omega = \sqrt[3]{2}$. Lako je za vidjeti da je R zatvoren za zbrajanje. Međutim, kada bi R bio zatvoren za množenje, tada je $\omega^2 \in R$ i postoje racionalni a i b tako da je

$$\omega^2 = a + b\omega$$

Množenje obje strane s ω i s b daje jednadžbe

$$2 = a\omega + b\omega^2$$

$$b\omega^2 = ab + b^2\omega.$$

Stoga, $2 - a\omega = ab + b^2\omega$ i

$$2 - ab = (b^2 + a)\omega.$$

Ako je $b^2 + a \neq 0$, tada je $\omega = \sqrt[3]{2}$ racionalan; ako je $b^2 + a = 0$, tada iz toga u kombinaciji s $2 - ab = 0$ slijedi $2 = (-b)^3$. Dakle $\sqrt[3]{2}$ bi bio racionalan, odnosno, ova kontradikcija pokazuje da R nije komutativan prsten.

Propozicija 1.15 *Neka je R komutativan prsten.*

(i) $0 \cdot a = 0$ *za svaki* $a \in R$.

(ii) Ako je $1 = 0$, *tada se* R *sadrži samo jedan element* 0. *U tom slučaju,* R *nazivamo* ***nulprstenom.***

(iii) Ako je $-a$ *inverzan element od* a *za zbrajanje, tada je* $(-1)(-a) = a$.

(iv) $(-1)a = -a$ *za svaki* $a \in R$.

(v) Ako je $n \in \mathbb{N}$ *i* $n1 = 0$, *tada je* $na = 0$ *za svaki* $a \in R$.

(vi) Vrijedi binomni teorem: Ako su $a, b \in R$, *tada*

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}.$$

Dokaz. (Skica.) (i) $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$.

(ii) $a = 1 \cdot a = 0 \cdot a = 0$.

(iii) $0 = (-1+1)(-a) = (-1)(-a) + (-a)$.

(iv) Budući da je $(-1)(-a) = a$, imamo $(-1)(-1)(-a) = (-1)a$. Ali $(-1)(-1) = 1$.

(v) Budući da se radi o grupi obzirom na operaciju zbrajanja, na je prikladnija oznaka nego a^n, i na je, za $n \in \mathbb{Z}$ i $a \in R$ zbroj $a-$ova n puta. Ako je $a \in R$ i $n \in \mathbb{Z}$ pozitivan, tada $n1 = 0$ povlači $na = n(1a) = (n1)a = 0a = 0$.

(vi) Indukcijom za $n \geq 0$ koristeći $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$ za $0 < r < n+1$. ∎

Potprsten S komutativnog prtena R je komutativan prsten sadržan u većem komutativnom prstenu R tako da S i R imaju iste operacije zbrajanja i množenja i isti jedinični element.

Definicija 1.16 *Podskup* S *komutativnog prstena* R *je* ***potprsten*** *od* R *ako*

(i) $1 \in S$;

(ii) ako je $a, b \in S$ *tada je* $a - b \in S$;

(iii) ako je $a, b \in S$ *tada je* $ab \in S$.

Propozicija 1.17 *Potprsten* S *komutativnog prstena* R *je komutativan prsten.*

Primjer 1.18 *Ako je* $n \geq 3$ *cijeli broj, neka je* $\zeta_n = e^{2\pi i/n}$ *primitivni* $n-ti$ *korijen iz jedinice. Definiramo*

$$\mathbb{Z}[\zeta_n] = \{z \in \mathbb{C} : z = a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{n-1},\ \text{za sve } a_i \in \mathbb{Z}\}.$$

(Kada je $n = 4$, *tada je* $\mathbb{Z}[\zeta_4]$ *prsten Gaussovih cijelih brojeva* $\mathbb{Z}[i]$*). Lako je provjeriti da je* $\mathbb{Z}[\zeta_n]$ *potprsten od* $\mathbb{C}$.

Definicija 1.19 ***Integralna domena****, ili kraće* ***domena****, je komutativan prsten* R *koji zadovoljava dva dodatna aksioma: prvi,*

$$1 \neq 0;$$

drugi, za sve $a, b, c \in R$,

$$\text{ako je } ca = cb \text{ i } c \neq 0, \text{ tada je } a = b.$$

Poznati primjeri komutativnih prstena $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$ su domene; nulprsten nije domena.

Propozicija 1.20 *Ne-nul komutativan prsten R je domena ako i samo ako je umnožak bilo koja dva ne-nul elementa od R ne-nul element.*

Definicija 1.21 *Neka su a i b elementi komutativnog prstena R. Tada a **dijeli** b u R (ili a je **djelitelj** od b), u oznaci $a \mid b$, ako postoji element $c \in R$ tako da je $b = ca$.*

Kao primjer, ako $0 \mid a$, tada je $a = 0 \cdot b$ za neki $b \in R$. Kako je $0 \cdot b = 0$, mora vrijediti $a = 0$. Stoga, $0 \mid a$ ako i samo ako $a = 0$.

Primjetimo da $a \mid b$ ne ovisi samo o elementima a i b nego i o ambijentnom prstenu R. Npr., 3 dijeli 2 u $\mathbb{Q}$, za $2 = 3 \times \frac{2}{3}$, i $\frac{2}{3} \in \mathbb{Q}$; s druge strane, 3 ne dijeli 2 u $\mathbb{Z}$, jer ne postoji cijeli broj c tako da $3c = 2$.

Definicija 1.22 *Element u u komutativnom prstenu R nazivamo **jedinicom** ako $u \mid 1$ u R, tj., ako postoji $v \in R$ tako da je $uv = 1$; element v nazivamo **inverz** od u i v često označavamo s u^{-1}.*

Kako $a \mid b$ ne ovise samo o elementima a i b nego i o ambijentnom prstenu R; slično, jedinica $u \in R$ također ovisi o ambijentnom prstenu R. Npr., 2 je jedinica u $\mathbb{Q}$, $\frac{1}{2} \in \mathbb{Q}$ i $2 \times \frac{1}{2} = 1$, ali nije jedinica u $\mathbb{Z}$, jer ne postoji cijeli broj v tako da je $2v = 1$. Zapravo, jedine jedinice u $\mathbb{Z}$ su 1 i -1.

Propozicija 1.23 *Neka je R domena i neka su $a, b \in R$ ne-nul elementi od R. Tada $a \mid b$ i $b \mid a$ ako i samo ako je $b = ua$ za neku jedinicu $u \in R$.*

Definicija 1.24 *Ako je R komutativan prsten, tada definiramo **grupu jedinica** od R kao*

$$U(R) = \{\text{sve jedinice u } R\}$$

Definicija 1.25 ***Polje*** *F je komutativan prsten u kojem je $1 \neq 0$ i svaki ne-nul element a je jedinica; tj., postoji $a^{-1} \in F$ tako da je $a^{-1}a = 1$.*

Primjeri polja su $\mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$.

Definicija polja može biti izražena u terminima grupe jedinica; komutativan prsten R je polje ako i samo ako je $U(R) = R^{\times}$, ne-nul elementi od R.

Propozicija 1.26 *Svako polje F je domena.*

Dokaz. (Skica.) Ako je $ab = ac$ i $a = 0$, tada je $b = a^{-1}(ab) = a^{-1}(ac) = c$. ∎

Teorem 1.27 *Ako je R domena, tada postoji polje F koje sadrži R kao potprsten. Štoviše, F možemo odabrati tako da, za svaki $f \in F$ postoje $a, b \in R$, $b \neq 0$ i $f = ab^{-1}$.*

Dokaz. (Skica.) Neka je $X = \{(a, b) \in R \times R \mid b \neq 0\}$. Definiramo relaciju $\equiv$ na X s $(a, b) \equiv (c, d)$ ako je $ad = bc$. Tvrdimo da je $\equiv$ relacija ekvivalencije. Vrijede refleksivnost i simetričnost; ovdje je dokaz tranzitivnosti. Ako je $(a, b) \equiv (c, d)$ i $(c, d) \equiv (e, f)$, tada je $ad = bc$ i $cf = de$. Ali $ad = bc$ daje $adf = b(cf) = bde$. Poništavajći d, koji je ne-nul, dobijemo $af = be$; tj., $(a, b) \equiv (e, f)$.Klasu ekvivalencije od (a, b) označavamo s $[a, b]$ i definiramo F kao skup svih klasa ekvivalencije $[a, b]$. Definiramo operacije zbrajanja i množenja na F s:

$$[a, b] + [c, d] = [ad + bc, bd]$$

i

$$[a, b][c, d] = [ac, bd].$$

Kako je $b \neq 0$ i $d \neq 0$, slijedi $bd \neq 0$, jer je R domena i stoga gornje formule imaju smisla. Pokažimo još da je zbrajanje dobro definirano. Ako je $[a, b] = [a', b']$ (tj., $ab' = a'b$) i $[c, d] = [c', d']$ (tj., $cd' = c'd$), tada moramo pokazati da je $[ad + bc, bd] = [a'd' + b'c', b'd']$. Ali ovo je istinito:

$$(ad + bc)b'd' = ab'dd' + bb'c'd = a'bdd' + bb'c'd = (a'd' + b'c')bd.$$

Sličnim argumentima možemo pokazati da je množenje dobro definirano.

F je komutativan prsten: Nul element je $[0, 1]$, jedinica je $[1, 1]$, inverzni element za zbrajanje od $[a, b]$ je $[-a, b]$. Lako je vidjeti da je familija $R' = \{[a, 1] \mid a \in R\}$ potprsten od F i $a \in R$ poistovjećujemo s $[a, 1] \in R'$.

Da bi vidjeli da je F polje, primjetimo da, ako je $[a, b] \neq [0, 1]$, tada je $a \neq 0$ i inverz od $[a, b]$ je $[b, a]$.

Konačno, ako je $b \neq 0$, tada je $[1, b] = [b, 1]^{-1}$ i stoga $[a, b] = [a, 1][b, 1]^{-1}$. ■

Definicija 1.28 *Polje F konstruirano iz R u Teoremu 1.27 naziva se* ***polje razlomaka*** *od R, označavamo s $Frac(R)$, a $[a, b] \in Frac(R)$ označavamo s a/b.*

Definicija 1.29 *Potpolje polja K je potprsten k od K koje je također polje.*

Poglavlje 2

Polinomi

Iako pretpostavljamo da je čitatelj upoznat s polinomima, u ovom poglavlju ih uvodimo aksiomatski. Skup svih polinoma činit će prsten polinoma i predstavljat će važanu strukturu za proučavanje.

Definicija 2.1 *Ako je R komutativan prsten, tada **niz** σ u R definiramo sa*

$$\sigma = (s_0, s_1, s_2, ..., s_i, ...);$$

pri čemu su svi $s_i \in R$, za sve $i \geq 0$. s_i se nazivaju koeficijentima od σ.

Niz σ je zapravo funkcija $\sigma : \mathbb{N} \to R$, gdje je $\mathbb{N}$ skup prirodnih brojeva, sa $\sigma(i) = s_i$ za sve $i \geq 0$. Ako je $\tau = (t_0, t_1, t_2, ..., t_i, ...)$ niz, tada je $\sigma = \tau$ ako i samo ako $\sigma(i) = \tau(i)$ za sve $i \geq 0$; tj., $\sigma = \tau$ ako i samo ako je $s_i = t_i$ za sve $i \geq 0$.

Definicija 2.2 *Niz $\sigma = (s_0, s_1, s_2, ..., s_i, ...)$ u komutativnom prstenu R naziva se **polinom** ako postoji neki cijeli broj $m \geq 0$ tako da je $s_i = 0$ za sve $i > m$; tj.,*

$$\sigma = (s_0, s_1, ..., s_m, 0, 0, ...).$$

Polinom ima konačno mnogo ne-nul koeficijenata. **Nul-polinom**, u oznaci $\sigma = 0$, je niz $\sigma = (0, 0, 0, ...)$.

Definicija 2.3 *Ako je $\sigma = (s_0, s_1, ..., s_n, 0, 0, ...) \neq 0$ polinom, tada postoji $s_n \neq 0$ tako da je $s_i = 0$ za sve $i > n$. s_n se zove **vodeći koeficijent** od σ, n se zove **stupanj** od σ (označavamo s $\deg(\sigma)$).*

Ako je R komutativan prsten, tada skup svih polinoma s koeficijentima u R označavamo s $R[x]$.

Propozicija 2.4 *Ako je R komutativan prsten, tada je $R[x]$ komutativan prsten koji sadrži R kao potprsten.*

Dokaz. (Skica.) Definiramo zbrajanje i množenje polinoma na sljedeći način: Ako je $\sigma = (s_0, s_1, ...)$ i $\tau = (t_0, t_1, ...)$, tada je

$$\sigma + \tau = (s_0 + t_0, s_1 + t_1, ..., s_n + t_n, ...)$$

i

$$\sigma\tau = (c_0, c_1, c_2, ...),$$

gdje je $c_k = \sum_{i+j=k} s_i t_j = \sum_{i=0}^{k} s_i t_{k-i}$. Aksiomi iz definicije komutativnog prstena se rutinski provjeravaju. Podskup $\{(r, 0, 0, ...) \mid r \in R\}$ je potprsten od $R[x]$ kojeg poistovjećujemo s R. ∎

Lema 2.5 *Neka je R komutativan prsten i neka su $\sigma, \tau \in R[x]$ ne-nul polinomi.*
(i) Ili je $\sigma\tau = 0$ ili $\deg(\sigma\tau) \leq \deg(\sigma) + \deg(\tau)$.
(ii) Ako je R domena, tada je $\sigma\tau \neq 0$ i

$$\deg(\sigma\tau) = \deg(\sigma) + \deg(\tau).$$

(iii) Ako je R domena, tada je $R[x]$ domena.

Dokaz. (Skica.) Neka su $\sigma = (s_0, s_1, ...)$ i $\tau = (t_0, t_1, ...)$ redom stupnja m i n.
(i) Ako je $k > m + n$, tada je svaki član u $\sum_i s_i t_{k-i}$ jednak 0 ($s_i = 0$ ili $t_{k-i} = 0$).
(ii) Svaki član u $\sum_i s_i t_{m+n-i}$ je jednak 0, s mogućom iznimkom $s_m t_n$. Kako je R domena, $s_m \neq 0$ i $t_n \neq 0$ povlače $s_m t_n \neq 0$.
(iii) Slijedi iz dijela (ii) jer je produkt dva ne-nul polinoma ne-nul. ∎

Definicija 2.6 *Definiramo element $x \in R[x]$ sa*

$$x = (0, 1, 0, 0, ...).$$

Propozicija 2.7 *Ako je $\sigma = (s_0, s_1, ..., s_n, 0, 0, ...)$, tada je*

$$\sigma = s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n,$$

gdje je svaki element $s \in R$ jednak polinomu $(s, 0, 0, ...)$.

Dokaz.

$$\begin{aligned}
\sigma &= (s_0, s_1, ..., s_n, 0, 0, ...) \\
&= (s_0, 0, 0, ...) + (0, s_1, 0, 0, ...) + \cdots + (0, 0, ..., s_n, 0, ...) \\
&= s_0(1, 0, 0, ...) + s_1(0, 1, 0, 0, ...) + \cdots + s_n(0, 0, ..., 1, 0, ...) \\
&= s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n.
\end{aligned}$$

∎

Nadalje ćemo upotrebljavati standardne oznake, tj., umjesto

$$\sigma = (s_0, s_1, ..., s_n, 0, 0, ...)$$

ćemo pisati

$$f(x) = s_0 + s_1x + s_2x^2 + \cdots + s_nx^n.$$

Ako je $f(x) = s_0 + s_1x + s_2x^2 + \cdots + s_nx^n$, gdje je $s_n \neq 0$, tada se s_0 zove **slobodni koeficijent**, a s_n se zove, kao što što smo već rekli, **vodeći koeficijent**. Ako je vodeći koeficijent $s_n = 1$, tada se $f(x)$ zove normiran. Svaki polinom osim nul-polinoma ima stupanj. **Konstantan polinom** je ili nul-polinom ili polinom stupnja 0. Polinom stupnja 1, $ax + b, b \neq 0$, se zove **linearan**, polinom stupnja 2 se zove **kvadratan**, stupnja 3 **kuban**, itd.

Korolar 2.8 *Polinomi $f(x) = s_0 + s_1x + s_2x^2 + \cdots + s_nx^n$ i $g(x) = t_0 + t_1x + t_2x^2 + \cdots + t_mx^m$ stupnja n i m su jednaki ako i samo ako je $n = m$ i $s_i = t_i$ za sve i.*

Definicija 2.9 *Neka je k polje. Polje razlomaka od $k[x]$, označava se $k(x)$ i zove **polje racionalnih funkcija** nad k.*

Sljedeća Propozicija je direktna posljedica Teorema 1.27:

Propozicija 2.10 *Ako je k polje, tada elementi od $k(x)$ imaju oblik $f(x)/g(x)$, gdje su $f(x), g(x) \in k[x]$ i $g(x) \neq 0$.*

Poglavlje 3

Najveći zajednički djelitelji

U ovom poglavlju ćemo vidjeti da, kada je k polje, svi poznati teoremi koji vrijede u $\mathbb{Z}$, imaju analogon u $k[x]$; štoviše, vidjet ćemo da se svi poznati dokazi mogu prenijeti ovdje. Prezentiramo algoritam dijeljenja za polinome s koeficijentima iz polja.

Teorem 3.1 ***(Algoritam dijeljenja).*** *Pretpostavimo da je k polje i da su $f(x), g(x) \in k[x]$ te $f(x) \neq 0$. Tada postoje jedinstveni polinomi $q(x), r(x) \in k[x]$ takvi da vrijedi*

$$g(x) = q(x)f(x) + r(x)$$

i vrijedi ili $r(x) = 0$ ili $\deg(r) < \deg(f)$.

Dokaz. Prvo, pokažimo postojanje takvih q i r. Ako $f \mid g$, tada je $g = qf$ za neke q; definiramo ostatak $r = 0$, i tvrdnja je dokazana. Ako $f \nmid g$, tada promatramo sve (obavezno ne-nul) polinome oblika $g - qf$ gdje q varira po $k[x]$. Aksiom o najmanjem cijelom broju osigurava da postoji polinom $r = g - qf$ koji ima najmanji stupanj među svim takvim polinomima. Kako je $g = qf + r$, dovoljno je pokazati da je $\deg(r) < \deg(f)$. Zapišimo polinome $f(x)$ i $r(x)$ u standardnom obliku: $f(x) = s_n x^n + \cdots + s_1 x + s_0$ i $g(x) = t_m x^m + \cdots + t_1 x + t_0$. Sada $s_n \neq 0$ povlači da je s_n jedinica, jer je k polje i stoga s_n^{-1} postoji u k. Ako je $\deg(r) \geq \deg(f)$, definiramo

$$h(x) = r(x) - t_m s_n^{-1} x^{m-n} f(x);$$

tj., ako je $V\check{C}(f) = s_n x^n$, gdje $V\check{C}$ označava **vodeći član**, tada je

$$h = r - \frac{V\check{C}(r)}{V\check{C}(f)} f;$$

primijetimo da je $h = 0$ ili je $\deg(h) < \deg(r)$. Ako je $h = 0$, tada je $r = [V\check{C}(r)/V\check{C}(f)]f$ i

$$\begin{aligned} g &= qf + r \\ &= qf + \frac{V\check{C}(r)}{V\check{C}(f)}f \\ &= [q + \frac{V\check{C}(r)}{V\check{C}(f)}]f, \end{aligned}$$

što je kontradikcija s $f \nmid g$. Ako $h \neq 0$, tada je $\deg(h) < \deg(r)$ i

$$g - qf = r = h + \frac{V\check{C}(r)}{V\check{C}(f)}f.$$

Prema tome, $g - [q + V\check{C}(r)/V\check{C}(f)]f = h$ što je u kontradikciji s tim da je r polinom najmanjeg stupnja ovakvog oblika. Stoga, $\deg(r) < \deg(f)$.

Da bi dokazali jednistvenost od $q(x)$ i $r(x)$, pretpostavimo da je $g = q'f + r'$, gdje je $\deg(r') < \deg(f)$. Tada

$$(q - q')f = r' - r.$$

Ako je $r' \neq r$, tada svaka strana ima stupanj. Ali $\deg((q - q')f) = \deg(q - q') + \deg(f) \geq \deg(f)$, dok je $\deg(r' - r) \leq \max\{\deg(r'), \deg(r)\} < \deg(f)$, kontradikcija. Stoga je $r' = r$ i $(q - q')f = 0$. Kako je $k[x]$ domena i $f \neq 0$, slijedi da je $q - q' = 0$ i $q = q'$. ∎

Definicija 3.2 *Ako su $f(x)$ i $g(x)$ polinomi u $k[x]$, gdje je k polje, tada se polinomi $q(x)$ i $r(x)$ koji se pojavljuju u algoritmu dijeljenja nazivaju* ***količnik*** *i* ***ostatak*** *nakon dijeljenja $g(x)$ s $f(x)$.*

Korolar 3.3 *Neka je R komutativan prsten i neka je $f(x) \in R[x]$ normiran polinom. Ako je $g(x) \in R[x]$, tada postoje $q(x), r(x) \in R[x]$ tako da vrijedi*

$$g(x) = q(x)f(x) + r(x),$$

gdje je ili $r(x) = 0$ ili $\deg(r) < \deg(f)$.

Dokaz. (Skica) Ovdje možemo ponoviti algoritam dijeljenja jednom kada vidimo da je $V\check{C}(r)/V\check{C}(f) \in R$ jer je $f(x)$ normiran. ∎

Definicija 3.4 *Ako je $f(x) \in k[x]$, gdje je k polje, tada definiramo* ***korijen*** *od $f(x)$ u k kao element $a \in k$ takav da je $f(a) = 0$.*

Lema 3.5 *Neka je $f(x) \in k[x]$, gdje je k polje, i neka je $u \in k$. Tada postoji $q(x) \in k[x]$ takav da vrijedi*

$$f(x) = q(x)(x - u) + f(u).$$

Dokaz. Algoritam dijeljenja daje

$$f(x) = q(x)(x-u) + r;$$

ostatak r je konstanta jer je $x-u$ stupnja 1. Sada uvrštavamo

$$f(u) = q(u)(u-u) + r,$$

i dobivamo $r = f(u)$. ∎

Propozicija 3.6 *Ako je $f(x) \in k[x]$, gdje je k polje, tada je a korijen od $f(x)$ u k ako i samo ako $x-a$ dijeli $f(x)$ u $k[x]$.*

Dokaz. Ako je a korijen od $f(x)$ u k, tada je $f(a) = 0$ i Lema 3.5 daje $f(x) = q(x)(x-a)$.

Obrnuto, ako je $f(x) = g(x)(x-a)$, tada uvršavanje a daje $f(a) = g(a)(a-a) = 0$. ∎

Teorem 3.7 *Neka je k polje i neka je $f(x) \in k[x]$. Ako je $f(x)$ stupnja n, tada $f(x)$ ima najviše n korijena u k.*

Dokaz. Dokazujemo tvrdnju indukcijom po $n \geq 0$. Ako je $n = 0$, tada je $f(x)$ konstanta različila od nule i broj njegovih korijena u k je nula. Neka je sada $n > 0$. Ako $f(x)$ nema korijena u k, tvrdnja je dokazana, jer je $0 \leq n$. U suprotnom, možemo pretpostaviti da postoji $a \in k$, takav da je a korijen od $f(x)$; stoga po Propoziciji 3.6,

$$f(x) = q(x)(x-a);$$

štoviše, $q(x) \in k[x]$ je stupnja $n-1$. Ako postoji korijen $b \in k$ takav da je $b \neq a$, tada je

$$0 = f(b) = q(b)(b-a).$$

Kako je $b-a \neq 0$, vrijedi $q(b) = 0$ (jer je k polje pa je i domena), stoga je taj b korijen od $q(x)$. $\deg(q) = n-1$, pa po pretpostavci indukcije slijedi da $q(x)$ ima najviše $n-1$ korijena u k. Stoga, $f(x)$ ima najviše n korijena u k. ∎

Korolar 3.8 *Neka je k beskonačno polje i neka su $f(x)$ i $g(x)$ polinomi u $k[x]$. Ako $f(x)$ i $g(x)$ određuju istu polinomijalnu funkciju [tj., ako je $f(a) = g(a)$ za svaki $a \in k$], tada je $f(x) = g(x)$.*

Dokaz. Ako je $f(x) \neq g(x)$, tada je polinom $h(x) = f(x) - g(x)$ različit od nule i ima neki stupanj, recimo n. Sada je svaki element od k korijen od $h(x)$; kako je k beskonačan, $h(x)$ ima više od n korijena, a ovo je u kontradikciji s Teoremom 3.7. ∎

Korolar 3.9 *Neka je k bilo kakvo polje, možda i konačno. Ako je $f(x), g(x) \in k[x]$, ako je $\deg(f) \leq \deg(g) \leq n$ i ako je $f(a) = g(a)$ za $n+1$ elemenata $a \in k$, tada je $f(x) = g(x)$.*

Dokaz. (*Skica.*) Ako je $f \neq g$, tada je $\deg(f-g)$ definiran i $\deg(f-g) \leq n$. ■

Definicija 3.10 *Neka su su $f(x)$ i $g(x)$ polinomi u $k[x]$, pri čemu je k polje. Polinom $c(x) \in k(x)$ nazivamo* ***zajednički djelitelj*** *polinoma $f(x)$ i $g(x)$ ako $c(x) \mid f(x)$ i $c(x) \mid g(x)$. Ako $f(x)$ i $g(x)$ nisu oba 0, definiramo njihov* ***najveći zajednički djelitelj****, nzd, kao normiran zajednički djelitelj s najvećim stupnjem. Ako je $f(x) = 0 = g(x)$, definiramo njihov $nzd = 0$. nzd od $f(x)$ i $g(x)$ se često označava i s (f, g).*

Teorem 3.11 *Ako je k polje i $f(x)$, $g(x) \in k[x]$, tada je njihov nzd $d(x)$ linearna kombinacija od $f(x)$ i $g(x)$; tj., postoje $s(x), t(x) \in k[x]$ tako da vrijedi*

$$d(x) = s(x)f(x) + t(x)g(x).$$

Dokaz. (*Skica.*) Ovaj Teorem je poseban slučaj Teorema 4.15 kojeg dokazujemo u Poglavlju 4. ■

Direktno iz ovog Teorema slijedi:

Korolar 3.12 *Neka je k polje i neka su $f(x)$, $g(x) \in k[x]$. Normiran zajednički djelitelj $d(x)$ je nzd ako i samo ako je $d(x)$ djeljiv sa svakim zajedničkim djeliteljem; tj., ako je $c(x)$ zajednički djelitelj, tada $c(x) \mid d(x)$.*

Štoviše, $f(x)$ i $g(x)$ imaju jedinstven nzd.

Definicija 3.13 *Kažemo da je element p u domeni R* ***ireducibilan*** *ako su ispunjena sljedeća dva uvjeta:*

(i) $p \neq 0$ i p nije jedinica;

(ii) ako je $p = uv$, tada je u ili v jedinica.

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

Propozicija 3.14 *Ako je k polje, tada je polinom $p(x) \in k[x]$ ireducibilan ako i samo ako je $\deg(p) = n \geq 1$ i ne postoji faktorizacija u $k[x]$ oblika $p(x) = g(x)h(x)$ u kojoj su oba faktora stupnja manjeg od n.*

Dokaz. Prvo ćemo pokazati da je $h(x) \in k[x]$ jedinica ako i samo ako je $\deg(h) = 0$. Ako je $h(x)u(x) = 1$, tada je $\deg(h) + \deg(u) = \deg(1) = 0$; kako je stupanj nenegativan, slijedi $\deg(h) = 0$.

Obrnuto, ako je $\deg(h) = 0$, tada je $h(x)$ konstanta različita od nula; tj., $h \in k$; kako je k polje, k ima inverz.

Ako je $p(x)$ ireducibilan, tada su sve njegove faktorizacije oblika $p(x) = g(x)h(x)$, gdje su $h(x)$ ili $g(x)$ jedinica; tj., gdje je ili $\deg(g) = 0$ ili $\deg(h) = 0$. Stoga, $p(x)$ nema faktorizaciju u kojoj su oba faktora manjeg stupnja.

Obrnuto, ako $p(x)$ nije ireducibilan, tada ima faktorizaciju $p(x) = g(x)h(x)$, gdje nisu niti $h(x)$ niti $g(x)$ jedinice; tj., niti $h(x)$ niti $g(x)$ nemaju stupanj 0. Stoga, $p(x)$ ima faktorizaciju kao produkt polinoma manjeg stupnja. ■

Korolar 3.15 *Neka je k polje i neka je $f(x) \in k[x]$ kvadratan ili kuban polinom. Tada je $f(x)$ ireducibilan u $k[x]$ ako i samo ako $f(x)$ nema korijen u k.*

Dokaz. (*Skica.*) Ako je $f(x) = g(x)h(x)$ i nijedan od g i h nije konstanta, tada $\deg(f) = \deg(g) + \deg(h)$ povlači da je barem jedan od faktora stupnja 1. ∎

Lema 3.16 *Neka je k polje i neka su $p(x)$, $f(x) \in k[x]$ i neka je $d(x) = (p, f)$ njihov nzd. Ako je $p(x)$ normiran ireducibilan polinom, tada*

$$d(x) = \begin{cases} 1 \text{ ako } p(x) \nmid f(x) \\ p(x) \text{ ako } p(x) \mid f(x). \end{cases}$$

Dokaz. (*Skica.*) Kako $d(x) \mid p(x)$, imamo $d(x) = 1$ ili $d(x) = p(x)$. ∎

Teorem 3.17 ***(Euklidova lema)***. *Neka je k polje i neka su $f(x)$, $g(x) \in k[x]$. Ako je $p(x)$ ireducibilan polinom u $k[x]$ i $p(x) \mid f(x)g(x)$ tada vrijedi ili*

$$p(x) \mid f(x) \text{ ili } p(x) \mid f(x).$$

Općenito, ako $p(x) \mid f_1(x) \cdots f_n(x)$, tada $p(x) \mid f_i(x)$ za neki i.

Dokaz. (*Skica.*) Pretpostavimo da $p \mid fg$, ali da $p \nmid f$. Kako je p ireducibilan, $(p, f) = 1$, i stoga vrijedi $1 = sp + tf$ za neke polinome s i t. Dakle,

$$g = spg + tfg.$$

Ali $p \mid fg$, po pretpostavci, i stoga $p \mid g$. ∎

Lagano se vidi da vrijedi i obrat Euklidove leme. Naime, neka je k polje i neka je $f(x) \in k[x]$ polinom stupnja ≥ 1; ako, kada $f(x)$ dijeli produkt dva polinoma, nužno dijeli jedan od faktora, tada je $f(x)$ ireducibilan.

Definicija 3.18 *Za dva polinoma $f(x)$, $g(x) \in k[x]$, gdje je k polje, kažemo da su* ***relativno prosti*** *ako je njihov nzd jednak* 1.

Korolar 3.19 *Neka su $f(x)$, $g(x), h(x) \in k[x]$, gdje je k polje, i neka su $h(x)$ i $f(x)$ relativno prosti. Ako $h(x) \mid f(x)g(x)$, tada $h(x) \mid g(x)$.*

Dokaz. (*Skica.*) Dokaz Euklidove leme također vrijedi ovdje: Kako je $(h, f) = 1$, vrijedi $1 = sh + tf$, i stoga $g = shg + tfg$. ∎

Teorem 3.20 ***(Euklidov algoritam)***. *Ako je k polje i $f(x)$, $g(x) \in k[x]$, tada postoje algoritmi za računanje nzd (f, g), kao i za traženje para polinoma $s(x)$ i $t(x)$ tako da vrijedi*

$$(f, g) = s(x)f(x) + t(x)g(x).$$

Dokaz. Dokaz je u suštini ponavljanje algoritama dijeljenja:

$$\begin{aligned} g &= q_1 f + r_1 \\ f &= q_2 r_1 + r_1 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-4} &= q_{n-2} r_{n-3} + r_{n-2} \\ r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n. \end{aligned}$$

Kako su stupnjevi ostataka strogo padajući, ovaj se postupak se mora zaustaviti nakon konačnog broja koraka. Tvrdimo da je $d = r_n$ *nzd*, jednom kad je normiran. Vidimo da je d zajednički djelitelj od f i g unatrag supstitucijom: idemo odozdo prema gore. Da bi vidjeli da je d *nzd*, idemo odozgo prema dolje da bi pokazali da ako je c bilo koji zajednički djelitelj od f i g, tada $c \mid r_i$ za svaki i. Konačno, da bi pronašli s i t tako da vrijedi $d = sf + tg$, ponovno idemo odozdo prema gore.

$$\begin{aligned} r_n &= r_{n-2} - q_n r_{n-1} \\ &= r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) \\ &= (1 + q_{n-1}) r_{n-2} - q_n r_{n-3} \\ &= (1 + q_{n-1})(r_{n-4} - q_{n-2} r_{n-3}) - q_n r_{n-3} \\ &= (1 + q_{n-1}) r_{n-4} - [(1 + q_{n-1}) q_{n-2} + q_n] r_{n-3} \\ &\vdots \\ &= sf + tg \end{aligned}$$

■

Korolar 3.21 *Neka je k potpolje polja K, stoga je $k[x]$ potprsten prstena $K[x]$. Ako su $f(x), g(x) \in k[x]$, tada je njihov nzd u $k[x]$ jednak njihovom nzd u $K[x]$.*

Dokaz. Algoritam dijeljenja u $K[x]$ daje

$$g(x) = Q(x) f(x) + R(x),$$

gdje su $Q(x), R(x) \in K[x]$; kako su $f(x), g(x) \in k[x]$, algoritam dijeljenja u $k[x]$ daje

$$g(x) = q(x) f(x) + r(x),$$

gdje su $q(x), r(x) \in k[x]$. Ali jednadžba $g(x) = q(x) f(x) + r(x)$ također vrijedi u $K[x]$ jer je $k[x] \subseteq K[x]$, stoga jedinstvenost kvocijenta i ostatka u algoritmu dijeljenja u $K[x]$ daje $Q(x) = q(x) \in k[x]$ i $R(x) = r(x) \in k[x]$. Stoga, lista jednadžbi koje se pojavljuju u Euklidovom algoritmu u $K[x]$ je točno ista lista koja se pojavljuje u Euklidovom algoritmu u manjem prstenu $k[x]$, dakle, isti *nzd* je dobiven u oba prstena polinoma. ■

Teorem 3.22 ***(Jedinstvena faktorizacija.)*** *Ako je k polje, tada je svaki polinom $f(x) \in k[x]$ stupnja ≥ 1 produkt ne-nul konstante i normiranih ireducibilnih polinoma. Štoviše, ako $f(x)$ ima dvije takve faktorizacije*

$$f(x) = ap_1(x)\cdots p_m(x) \text{ i } f(x) = bq_1(x)\cdots q_n(x),$$

tj., a i b su ne-nul konstante, a $p-ovi$ i $q-ovi$ su normirani ireducibilni polinomi, tada je $a = b$, $m = n$, i $q_i = p_i$ za sve i.

Dokaz. Dokazujemo postojanje faktorizacije za polinom $f(x)$ indukcijom po $\deg(f) \geq 1$. Ako je $\deg(f) = 1$, tada je $f(x) = ax + c = a(x + a^{-1}c)$. Kao i svaki linearni polinom, $x+a^{-1}c$ je ireducibilan i stoga je i produkt ireducibilnih. Pretpostavimo sada da je $\deg(f) \geq 1$. Ako je $f(x)$ ireducibilan i njegov vodeći koeficijent je a, tada je $f(x) = a(a^{-1}f(x))$; gotovi smo, jer je $a^{-1}f(x)$ normiran. Ako $f(x)$ nije ireducibilan, tada je $f(x) = g(x)h(x)$, gdje je $\deg(g) < \deg(f)$ i $\deg(h) < \deg(f)$. Po pretpostavci indukcije, postoje faktorizacije $g(x) = bp_1(x)\cdots p_m(x)$ i $h(x) = cq_1(x)\cdots q_n(x)$, gdje su $p-ovi$ i $q-ovi$ normirani ireducibilni. Slijedi da je

$$f(x) = (bc)p_1(x)\cdots p_m(x)q_1(x)\cdots q_n(x),$$

kao što je traženo.

Sada dokazujemo, indukcijom po $M = \max\{m, n\} \geq 1$, da ako postoji jednadžba

$$ap_1(x)\cdots p_m(x) = bq_1(x)\cdots q_n(x)$$

u kojoj su a i b ne-nul konstante i $p-ovi$ i $q-ovi$ su normirani ireducibilni, tada je $a = b$, $m = n$, i $q_i = p_i$ za sve i. Za bazu indukcije $M = 1$, pretpostavka daje polinom $g(x) = ap_1(x) = bq_1(x)$. Sada je a vodeći koeficijent od $g(x)$, jer je $p_1(x)$ normiran; slično, b vodeći koeficijent od $g(x)$, jer je $q_1(x)$. Stoga je $a = b$ i $p_1(x) = q_1(x)$. Za korak indukcije, dana jednadžba pokazuje da $p_m(x) \mid q_1(x)\cdots q_n(x)$. Po Euklidovoj lemi za polinome, postoji i takav da $p_m(x) \mid q_i(x)$. Ali $q_i(x)$ je normiran ireducibilan pa osim samog sebe i 1 nema drugih normiranih djelitelja, stoga $q_i(x) = p_m(x)$. Ponovnim indeksiranjem možemo pretpostaviti da je $q_n(x) = p_m(x)$. Poništavanjem ovog faktora dobijemo $ap_1(x)\cdots p_{m-1}(x) = bq_1(x)\cdots q_{n-1}(x)$. Po pretpostavci indukcije, $a = b, m-1 = n-1$ (stoga $m = n$), i $q_i = p_i$ za sve i. ∎

Poglavlje 4

Homomorfizmi

U ovom poglavlju ćemo promatrati ona preslikavanja koja 'čuvaju strukturu'; tj., preslikavanja među prstenima koja respektiraju obje operacije, zbrajanje i množenje u prstenu. Zatim uvodimo pojam ideala u prstenu, koji čini centralno mjesto u teoriji prstena.

Definicija 4.1 *Neka su A i R komutativni prsteni.* ***Homomorfizam*** *(prstena) je funkcija $f : A \to R$ takva da vrijedi*
(i) $f(1) = 1$;
(ii) $f(a + a') = f(a) + f(a')$ *za sve* $a, a' \in A$;
(ii) $f(aa') = f(a)f(a')$ *za sve* $a, a' \in A$.

Homomorfizam koji je također bijekcija naziva se **izomorfizam**. Za dva komutativna prstena A i R reći cemo da su **izomorfni**, ako postoji neki izomorfizam f medju njima; tu činjenicu označavamo sa $A \cong R$.

Primjer 4.2 *(i) Neka je R domena i s $F = Frac(R)$ označimo njegovo polje razlomaka. U Teoremu 1.27 rekli smo da je R potprsten od F, ali to nije istina; R čak nije ni podskup od F. Pronašli smo međutim potprsten R' od F koji ima veliku sličnost s R; $R' = \{[a, 1] : a \in R\} \subseteq F$. Funkcija $f : R \to R'$, dana s $f(a) = [a, 1]$ je izomorfizam.*

(ii) Podskup R' komtativnog prstena R, definiran s $R' = \{(r, 0, 0, ...) : r \in R\}$ je potprsten od $R[x]$, a funkcija $f : R \to R'$, definirana s $f(r) = (r, 0, 0, ...)$, je izomorfizam.

(iii) $z = a+ib \to \overline{z} = a-ib$ ($\overline{z}$ je kompleksno konjugiran od z) je izomorfizam $\mathbb{C} \to \mathbb{C}$ jer je $\overline{1} = 1, \overline{z + w} = \overline{z} + \overline{w}$ i $\overline{zw} = \overline{z}\,\overline{w}$.

(iv) Neka je R komutativan prsten s jedinicom označenom s ε, tada je funkcija $\chi : \mathbb{Z} \to R$, definirana s $\chi(n) = n\varepsilon$, homomorfizam prstena.

Lema 4.3 *Ako je $f : A \to R$ homomorfizam prstena, tada, za sve $a \in A$,*
(i) $f(a^n) = f(a)^n$ *za sve* $n \geq 0$;
(ii) ako je a jedinica, tada je $f(a)$ jedinica te $f(a^{-1}) = f(a)^{-1}$; štoviše, ako je a jedinica tada je $f(a^{-n}) = f(a)^{-n}$ za sve $n \geq 1$;

(iii) ako je $f : A \to R$ homomorfizam prstena, tada je

$$f(U(A)) \leq U(R),$$

gdje je $U(A)$ grupa jedinica od A; ako je f izomorfizam, tada je

$$U(A) \cong U(R).$$

Definicija 4.4 *Za proizvoljan homomorfizam prstena $f : A \to R$, definirajmo njegovu* ***jezgru***

$$\ker\ f = \{a \in A \mid f(a) = 0\}$$

i njegovu ***sliku***

$$im\ f = \{r \in R \mid r = f(a)\ za\ neki\ a \in R\}$$

Definicija 4.5 ***Ideal*** *u komutativnom prstenu R je podskup I od R tako da vrijedi*
(i) $0 \in I$;
(ii) ako su $a, b \in I$, tada je $a + b \in I$;
(iii) ako je $a \in I$ i $r \in R$, tada je $ra \in I$.

Nadalje, reći ćemo da je ideal I od R **pravi ideal** ako je $I \neq R$ i $I \neq \{0\}$; ovdje je sa $\{0\}$ označen nul-ideal.

Primjer 4.6 *Ako su $b_1, b_2, ..., b_n \in R$, tada je skup svih linearnih kombinacija*

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

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

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

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

Propozicija 4.7 *Ako je $f : A \to R$ homomorfizam prstena, tada je* $\ker f$ *ideal u A i $im\ f$ je potprsten od R. Štoviše, ako su A i R nenul prsteni, tada je* $\ker f$ *pravi ideal.*

Propozicija 4.8 *Homomorfizam prstena $f : A \to R$ je injekcija ako i samo ako je* $\ker f = \{0\}$.

Korolar 4.9 *Ako je $f : k \to R$ homomorfizam prstena, gdje je k polje i R nije nul-prsten, tada je f injekcija.*

Teorem 4.10 *Ako je k polje, tada je svaki ideal I u $k[x]$ glavni ideal. Štoviše, ako je $I \neq 0$, tada postoji normiran polinom koji generira I.*

Dokaz. (*Skica.*) Ako je k polje, tada je $k[x]$ primjer Euklidovog prstena. U Teoremu 5.3 dokazat ćemo da je svaki ideal u Euklidovom prstenu glavni ideal. ■

Definicija 4.11 *Domena R je **domena glavnih ideala** ako je svaki ideal u R glavni ideal.*

Primjer 4.12 *(i) Prsten cijelih brojeva je domena glavnih ideala.*

(ii) Svako polje je domena glavnih ideala.

(iii) Ako je k polje, tada je prsten polinoma $k[x]$ domena glavnih ideala, po Teoremu 4.10.

Primjer 4.13 *Nisu svi ideali u proizvoljnim komutativnim prstenima glavni ideali. Neka je $R = \mathbb{Z}[x]$, komutativan prsten svih polinoma u $\mathbb{Z}$. Lako je vidjeti da je skup I svih konstantnih polinoma ideal u $\mathbb{Z}[x]$. Međutim, I nije glavni ideal.*

Definicija 4.14 *Element δ u komutativnom prstenu R je **najveći zajednički djelitelj**, nzd, elemenata $\alpha, \beta \in R$ ako vrijedi*

(i) δ je zajednički djelitelj od α i β;

(ii) ako je γ bilo koji zajednički djelitelj od α i β, tada $\gamma \mid \delta$.

Teorem 4.15 *Neka je R domena glavnih ideala.*

(i) Za sve $\alpha, \beta \in R$ postoji nzd, δ, koji je linearna kombinacija od α i β :

$$\delta = \sigma\alpha + \tau\beta,$$

gdje su $\sigma, \tau \in R$.

(ii) Ako ireducibilan element $\pi \in R$ dijeli umnožak $\alpha\beta$, tada ili $\pi \mid \alpha$ ili $\pi \mid \beta$.

Dokaz. Možemo pretpostaviti da je barem jedan od α i β ne-nul (u suprotnom, nzd je 0 i rezultat je očit). Neka je I skup svih linearnih kombinacija:

$$I = \{\sigma\alpha + \tau\beta \mid \sigma, \tau \in R\}.$$

Sada su α i β sadržani u I (stavimo $\sigma = 1$ i $\tau = 0$ ili obrnuto). Lako je provjeriti da je I ideal u R, stoga postoji $\delta \in I$, $I = (\delta)$, jer je R domena glavnih ideala; tvrdimo da je δ nzd od α i β.

Kako je $\alpha \in I = (\delta)$, imamo $\alpha = \rho\delta$ za neki $\rho \in R$; tj., δ je djelitelj od α; slično δ je djelitelj od β, odnosno δ je zajednički djelitelj od α i β.

$\delta \in I$ je linearna kombinacija od α i β pa postoje $\sigma, \tau \in R$ tako da je

$$\delta = \sigma\alpha + \tau\beta.$$

Konačno, ako je γ bilo koji zajednički djelitelj od α i β, tada je $\alpha = \gamma\alpha'$ i $\beta = \gamma\beta'$, stoga γ dijeli δ za $\delta = \sigma\alpha + \tau\beta = \gamma(\sigma\alpha' + \tau\beta')$. Zaključujemo da je δ nzd.

(ii) Ako $\pi \mid \alpha$, tvrdnja vrijedi. Ako $\pi \nmid \alpha$ tada je 1 nzd od π i α, tj., postoje $\sigma, \tau \in R$ tako da je $1 = \sigma\pi + \tau\alpha$ te stoga

$$\beta = \sigma\pi\beta + \tau\alpha\beta.$$

Kako $\pi \mid \alpha\beta$, slijedi $\pi \mid \beta$. ■

Poglavlje 5

Euklidovi prsteni

U ovom kratkom poglavlju uvodimo pojam Euklidovog prstena i donosimo važan teorem koji kaže da je svaki Euklidov prsten domena glavnih ideala.

Definicija 5.1 *Domena R je **Euklidov prsten** ako postoji funkcija*

$$\partial : R\backslash\{0\} \to \mathbb{N},$$

*koju nazivamo **funkcija stupnja**, takva da*
(i) $\partial(f) \leq \partial(fg)$ za sve $f, g \in R, f, g \neq 0$;
(ii) za sve $f, g \in R, f \neq 0$, postoje $q, r \in R$ tako da je

$$g = qf + r,$$

gdje je ili $r = 0$ ili $\partial(r) \leq \partial(f)$.

Primjer 5.2 *(i) Skup cijelih brojeva $\mathbb{Z}$ je Euklidov prsten s funkcijom stupnja $\partial(m) = |m|$. Imamo*

$$\partial(mn) = |mn| = |m||n| = \partial(m)\partial(n).$$

(ii) Kada je k polje, domena $k[x]$ je Euklidov prsten s funkcijom stupnja, stupnja ne-nul polinoma. U $k[x]$, imamo

$$\begin{aligned} \partial(fg) &= \deg(fg) \\ &= \deg(f) + \deg(g) \\ &= \partial(f) + \partial(g). \end{aligned}$$

Ako je funkcija stupnja ∂ multiplikativna, tj.,

$$\partial(fg) = \partial(f)\partial(g)$$

*tada se ∂ zove **norma**.*

Teorem 5.3 *Svaki Euklidov prsten R je domena glavnih ideala.*

Dokaz. Neka je I ideal u R. Ako je $I = \{0\}$, tada je $I = (0)$ glavni; stoga možemo pretpostaviti da je $I \neq (0)$. Skup svih stupnjeva nenul elemenata u I ima najmanji element, neka je to n; odaberemo $d \in I$ tako da je $\partial(d) = n$. Očito je $(d) \subseteq I$ pa je dovoljno dokazati obrnutu inkluziju. Ako je $a \in I$ tada postoje $q, r \in R$ tako da je $a = qd + r$, gdje je ili $r = 0$ ili $\partial(r) < \partial(d)$. Ali, $r = a - qd \in I$ pa slijedi $r = 0$. Stoga, $a = qd \in (d)$ i $I = (d)$. ∎

Korolar 5.4 *Prsten Gaussovih cijelih brojeva $\mathbb{Z}[i]$ je domena glavnih ideala.*

Primjer 5.5 *Prsten*

$$R = \{a + b\alpha \mid a, b \in \mathbb{Z}\},$$

gdje je $\alpha = \frac{1}{2}(1 + \sqrt{-19})$, je domena glavnih ideala.

Poglavlje 6

Kvocijentni prsteni

U ovom poglavlju definiramo kvocijentni prsten i navodimo Prvi teorem o izomorfizmu za prstene.

Neka je I ideal u komutativnom prstenu R. Ako zaboravimo na operaciju množenja, tada je I podgrupa aditivne grupe R; kako je R Abelova grupa, podgrupa I je nužno normalna, stoga je kvocijentna grupa R/I definirana, kao i preslikavanje $\pi : R \to R/I$ dano s $\pi(a) = a + I$. Sada vrijedi $a + I = b + I$ u R/I ako i samo ako je $a - b \in I$. Prisjetimo se da je zbrajanje na R/I dano s:

$$(a + I) + (b + I) = a + b + I$$

Teorem 6.1 *Ako je I ideal u komutativnom prstenu R, tada se aditivna Abelova grupa R/I može 'organizirati' u komutativan prsten na način da je preslikavanje $\pi : R \to R/I$ surjektivan homomorfizam prstena.*

Skica dokaza. Definiramo množenje na aditivnoj Abelovoj grupi R/I s

$$(a + I)(b + I) = ab + I.$$

Da bi vidjeli da je ovo dobro definirana funkcija $R/I \times R/I \to R/I$, pretpostavimo da je $a + I = a' + I$ i $b + I = b' + I$, tj., $a - a' \in I$ i $b - b' \in I$. Moramo pokazati da vrijedi $(a' + I)(b' + I) = a'b' + I = ab + I$, tj., $ab - a'b' \in I$. Ali

$$\begin{aligned} ab - a'b' &= ab - a'b + a'b - a'b' \\ &= (a - a')b + a'(b - b') \in I, \end{aligned}$$

kao što je traženo.

Da bi dokazali da je R/I komutativan prsten, dovoljno je pokazati da vrijede asocijativnost i komutativnost množenja, distributivnost i da je jedinica $1 + I$. Dokazi ovih svojstava su trivijalni. Npr., množenje u R/I je komutativno jer

$$(a + I)(b + I) = ab + I = ba + I = (b + I)(a + I).$$

Ponovnim zapisivanjem jednadžbe $(a + I)(b + I) = ab + I$ upotrebljavajući definiciju od π, $a + I = \pi(a)$, dobijemo $\pi(a)\pi(b) = \pi(ab)$. Kako je $\pi(1) = 1 + I$,

slijedi da je π homomorfizam prstena. Konačno, π je surjekcija jer je $a + I = \pi(a)$.

Korolar 6.2 *Ako je I ideal u komutativnom prstenu R, tada postoje komutativan prsten A i homomorfizam prstena $\pi : R \to A$ tako da vrijedi $I = \ker \pi$.*

Dokaz. Ako zaboravimo na množenje, tada je preslikavanje $\pi : R \to R/I$ homomorfizam između aditivnih grupa, te vrijedi

$$I = \ker \pi = \{r \in R \mid \pi(a) = 0 + I = I\}.$$

Sada se sjetimo množenja: $(a + I)(b + I) = ab + I$; tj., $\pi(a)\pi(b) = \pi(ab)$. Stoga, π je homomorfizam prstena i $\ker \pi$ je jednaka I bez obzira da li je funkcija π homomorfizam prstena ili homomorfizam aditivnih grupa. ∎

Teorem 6.3 ***(Prvi teorem o izomorfizmu)*** *Ako je $f : R \to A$ homomorfizam prstena, tada je* ker f *ideal u A, $im\ f$ potprsten od A i*

$$R/\ker\ f \cong im\ f.$$

Dokaz. Neka je $I = \ker f$. Već smo vidjeli u Propoziciji 4.7 da je I ideal u R i da je $im\ f$ potprsten od A.

Ako zaboravimo na množenje u prstenima, tada je funkcija $\varphi : R/I \to A$, definirana s $\varphi(r + I) = f(r)$, izomorfizam aditivnih grupa. Kako je $\varphi(1 + I) = f(1) = 1$, dovoljno je dokazati da φ čuva množenje. Ali $\varphi((r + I)(s + I)) = \varphi(rs + I) = f(rs) = f(r)f(s) = \varphi(r + I)\varphi(s + I)$. Stoga je φ homomorfizam prstena. ∎

Poglavlje 7

Prosti ideali i maksimalni ideali

U ovom poglavlju uvodimo dva zanimljiva tipa ideala: proste ideale i maksimalne ideale.

Propozicija 7.1 ***(Teorem o korespondenciji za prstene)*** *Ako je I pravi ideal u komutativnom prstenu R, tada postoji bijekcija φ sa skupa svih srednjih ideala J koji sadrže I, tj., $I \subseteq J \subseteq R$, u skup svih ideala u R/I, dana s*

$$\varphi : J \longmapsto \pi(J) = J/I = \{a + I \mid a \in J\},$$

gdje je $\pi : R \to R/I$ prirodno preslikavanje.

Dokaz. Ako zaboravimo na množenje, komutativan prsten R je samo aditivna Abelova grupa i njegov ideal I je normalna podgrupa. Po teoremu o korespondenciji za grupe sada imamo bijekciju

$$\Phi : \{\text{sve podgrupe od } R \text{ koje sadže } I\} \to \{\text{sve podgrupe od } R/I\},$$

gdje je $\Phi(J) = \pi(J) = J/I$.

Ako je J ideal, tada je $\Phi(J)$ također ideal, jer ako je $r \in R$ i $a \in J$, tada je $ra \in J$ i stoga

$$(r + I)(a + I) = ra + I \in J/I.$$

Neka je φ restrikcija od Φ na skup svih srednjih idala; φ je injekcija jer je Φ bijekcija. Da bi vidjeli da je φ surjekcija, neka je J^* ideal u R/I. Sada je $\pi^{-1}(J^*)$ srednji ideal u R [sadrži $I = \pi^{-1}(\{0\})$] i $\varphi(\pi^{-1}(J^*)) = J^*$. ∎

Definicija 7.2 *Za ideal I u komutativnom prstenu R kažemo da je* ***prost ideal*** *ako je pravi ideal, tj., $I \neq R$, i ako $ab \in I$ povlači $a \in I$ ili $b \in I$.*

Primjer 7.3 *U prstenu $\mathbb{Z}[x]$, svih polinoma čiji su koeficijenti cijeli brojevi, ideal generiran s 2 i x je prost ideal. Sadrži sve one polinome čiji su konstantni koeficijenti parni.*

Primjer 7.4 *Prisjetimo se da je ne-nul komutativan prsten R domena ako i samo ako $ab = 0$ u R povlači da je $a = 0$ ili $b = 0$. Prema tome, $(0) = \{0\}$ u R je prost ideal ako i samo ako je R domena.*

Propozicija 7.5 *Ideal I u komutativnom prstenu R je prost ideal ako i samo ako je R/I domena.*

Dokaz. Neka je I prost ideal. Kako je I pravi ideal, imamo $1 \notin I$ i stoga je $1 + I \neq 0 + I$ u R/I. Ako je $0 = (a + I)(b + I) = ab + I$, tada je $ab \in I$. Kako je I prost ideal, tada je ili $a \in I$ ili $b \in I$; tj., ili je $a + I = 0$ ili $b + I = 0$. Stoga, R/I je domena. Obrat je sličan. ∎

Propozicija 7.6 *Ako je k polje, tada je ne-nul polinom $p(x) \in k[x]$ ireducibilan ako i samo ako je $((p(x))$ prost ideal.*

Dokaz. Pretpostavimo da je $p(x)$ ireducibilan. Prvo, (p) je pravi ideal; u suprotnom, $k[x] = (p)$ i stoga $1 \in (p)$ pa postoji polinom $f(x)$ tako da je $1 = p(x)f(x)$. Ali $p(x)$ je stupnja najmanje 1, jer je

$$0 = \deg(1) = \deg(pf) = \deg(p) + \deg(f) \geq \deg(p) \geq 1.$$

Kontradicija pokazuje da je (p) pravi ideal. Drugo, ako je $ab \in (p)$, tada $p \mid ab$, i po Euklidovoj lemi vrijedi $p \mid a$ ili $p \mid b$. Tj., $a \in (p)$ ili $b \in (p)$. Slijedi da je (p) prost ideal.

Obratno, ako je $(p(x))$ prost ideal, tada $fg \in (p)$ povlače da je $f \in (p)$ ili $g \in (p)$; tj., $p \mid f$ ili $p \mid g$. Sada po obratu Euklidove leme slijedi da je p ireducibilan. ∎

Ako je I ideal u komutativnom prstenu R, možemo pisati $I \subsetneq R$ ako je I pravi ideal. Općenito, ako su I i J ideali, možemo pisati $I \subsetneq J$ ako je $I \subseteq J$ i $I \neq J$.

Definicija 7.7 *Za ideal I u komutativnom prstenu R kažemo da je* ***maksimalan ideal*** *ako je pravi ideal i ne postoji ideal J tako da vrijedi $I \subsetneq J \subsetneq R$.*

Primjer 7.8 *Ideal $\{0\}$ je maksimalan ideal u komutativnom prstenu R ako i samo ako je R polje. Svaki ne-nul ideal I u R je jednak samom R ako i samo ako je svaki ne-nul element u R jedinica. Tj., $\{0\}$ je maksimalan ideal ako i samo ako je R polje.*

Propozicija 7.9 *Pravi ideal I u ne-nul komutativnom prstenu R je maksimalan ideal ako i samo ako je R/I polje.*

Dokaz. Teorem o korespondenciji za prstene pokazuje da je I maksimalan ideal ako i samo ako R/I nema drugih ideala osim $\{0\}$ i samog R/I; Primjer 7.9 pokazuje da ovo svojstvo vrijedi ako i samo ako je R/I polje. ∎

Korolar 7.10 *Svaki maksimalan ideal u komutativnom prstenu R je prost ideal.*

Dokaz. Ako je I maksimalan ideal, tada je R/I polje. Kako je svako polje domena, R/I je domena i stoga je I prost ideal. ∎

Primjer 7.11 *Ne vrijedi obrat Korolara 7.11. Na primjer, uzmimo u obzir glavni ideal (x) u $\mathbb{Z}[x]$. Vrijedi*

$$\mathbb{Z}[x]/(x) \cong \mathbb{Z};$$

kako je $\mathbb{Z}$ domena, (x) je prost ideal; kako $\mathbb{Z}$ nije polje, (x) nije maksimalan ideal.

Međutim, ako je komutativan prsten R domena glavnih ideala, vrijedi obrat Korolara 7.11.

Teorem 7.12 *Ako je R domena glavnih ideala, tada je svaki ne-nul prost ideal I maksimalan ideal.*

Dokaz. Pretpostavimo da postoji pravi ideal J tako da vrijedi $I \subseteq J$. Kako je R domena glavnih ideala, $I = (a)$ i $J = (b)$ za neke $a, b \in R$. Sada $a \in J$ povlači da je $a = rb$ za neki $r \in R$ i stoga je $rb \in I$; ali I je prost ideal, stoga je $r \in I$ ili $b \in I$. Ako je $r \in I$, tada je $r = sa$ za neki $s \in R$, i stoga $a = rb = sab$. Kako je R domena, $1 = sb$ i vrijedi $J = (b) = R$, što je u kontradikciji s pretpostavkom da je J pravi ideal. Ako je $b \in I$, tada je $J \subseteq I$, i stoga je $J = I$. Slijedi da je I maksimalan ideal. ∎

Korolar 7.13 *Ako je k polje i $p(x) \in k[x]$ je ireducibilan, tada je kvocijentni prsten $k[x]/(p(x))$ polje.*

Dokaz. Kako je $p(x)$ ireducibilan, glavni ideal $I = (p(x))$ je ne-nul prost ideal; kako je $k[x]$ domena glavnih ideala, I je maksimalan ideal i stoga je $k[x]/I$ polje. ∎

Propozicija 7.14 *Neka je P prost ideal u komutativnom prstenu R. Ako su I i J ideali takvi da vrijedi $IJ \subseteq P$, tada $I \subseteq P$ ili $J \subseteq P$.*

Dokaz. Pretpostavimo suprotno, da je $I \nsubseteq P$ i $J \nsubseteq P$; tj., postoje $a \in I$ i $b \in J$ takvi da je $a, b \notin P$. Ali $ab \in IJ \subseteq P$, što je u kontradikciji s tim da je P prost. ∎

Poglavlje 8

Domene s jedistvenom faktorizacijom

U ovom poglavlju ćemo, nakon što uvedemo pojam domene s jedinstvenom faktorizacijom, dokazati da je svaka domena glavnih ideala domena s jedinstvenom faktorizacijom.

Definicija 8.1 *Za elemente a i b u komutativnom prstenu R kažemo da su* ***asocirani*** *ako postoji jedinica $u \in R$ takva da vrijedi $b = ua$.*

Na primjer, u $\mathbb{Z}$, jedinice su ± 1, stoga jedini asociran od cijelog broja m je $\pm m$; u $k[x]$, gdje je k polje, jedinice su ne-nul konstante, i stoga jedini asocirani od polinoma $f(x) \in k[x]$ je polinom $uf(x)$, gdje je $u \in k$ i $u \neq 0$.

Propozicija 8.2 *Neka je R domena i neka su $a, b \in R$.*
(i) $a \mid b$ i $b \mid a$ ako i samo ako su a i b asocirani.
(ii) Glavni ideali (a) i (b) su jednaki ako i samo ako su a i b asocirani.

Dokaz. (i) Ako $a \mid b$ i $b \mid a$, tada postoje $r, s \in R$ takvi da vrijedi $b = ra$ i $a = sb$, i stoga $b = ra = rsb$. Ako je $b = 0$, tada je $a = 0$ (zato što $b \mid a$); ako je $b \neq 0$, tada ga možemo poništiti (R je domena) i dobijemo $1 = rs$. Stoga su r i s jedinice, i a i b su asocirani. Obrat je očit.

(ii) Ako je $(a) = (b)$, tada je $a \in (b)$; stoga je $a = rb$ za neki $r \in R$, i onda $b \mid a$. Slično, $b \in (a)$ povlači $a \mid b$, i stoga prema (i) slijedi da su a i b asocirani.

Obratno, ako je $a = ub$, gdje je u jedinica, tada je $a \in (b)$ i $(a) \subseteq (b)$. Slično, $b = u^{-1}a$ povlači $(b) \subseteq (a)$, i stoga je $(a) = (b)$. ∎

Korolar 8.3 *Ako je R domena glavnih ideala i $p \in R$ ireducibilan, tada je (p) prost ideal.*

Dokaz. Neka je I ideal takav da je $(p) \subseteq I$. Kako je R domena glavnih ideala, postoji $q \in R$ takav da je $I = (q)$. Stoga, $p \in (q)$ i slijedi $p = rq$ za neki $r \in R$. Ireducibilnost od p kaže da su ili p i q asocirani ili je q jedinica. U prvom

slučaju, $(p) = (q)$ po Propoziciji 8.2; u drugom slučaju, $(q) = R$. Slijedi da je (p) maksimalan ideal, i stoga je i prost ideal. ∎

Definicija 8.4 *Za domenu R kažemo da je* ***domena s jedinstvenom faktorizacijom*** *ako vrijedi*

(i) svaki $r \in R$, koji nije ni 0 ni jedinica, je produkt ireducibilnih.

(ii) ako je $up_1 \cdots p_m = vq_1 \cdots q_n$, gdje su u i v jedinice i svi p_i i q_j su ireducibilni, tada je $m = n$ i postoji permutacija $\sigma \in S_n$ takva da su p_i i $q_{\sigma(i)}$ asocirani za sve i.

Propozicija 8.5 *Neka je R domena u kojoj je svaki $r \in R$, koji nije ni 0 ni jedinica , produkt ireducibilnih. Tada je R domena s jedinstvenom faktorizacijom ako i samo ako je (p) prost ideal u R za svaki ireucibilni element $p \in R$.*

Dokaz. Pretpostavimo da je R domena s jedinstvenom faktorizacijom. Ako je $a, b \in R$ i $ab \in (p)$, tada postoji $r \in R$ takav da je

$$ab = rp.$$

Faktorizirajmo svaki a, b i r u ireducibilne; po jedinstvenoj faktorizaciji, lijeva strana jednadžbe mora sadžavati asociran element od p.Taj asocirani je nastao kao faktor od a i b, i stoga je $a \in (p)$ ili $b \in (p)$.

Obratno, pretpostavimo da vrijedi

$$up_1 \cdots p_m = vq_1 \cdots q_n,$$

gdje su u i v jedinice i svi p_i i q_j su ireducibilni elementi. Dokazujemo, indukcijom po $\max\{m, n\} \geq 1$, da je $m = n$ i da $q-$ove možemo ponovno indeksirati tako da su q_i i p_i asocirani elementi za sve i. Ako je $\max\{m, n\} = 1$, tada je $up_1 = vq_1, up_1 = v$ ili $u = vq_1$. Posljednja dva slučaja se ne mogu dogoditi za ireducibilne elemente koji nisu jedinice i stoga vrijedi baza indukcije. Za korak indukcije, dana jednadžba pokazuje da $p_1 \mid q_1 \cdots q_n$. Po pretpostavci, (p_1) je prost ideal i stoga postoje neki q_j takav da vrijedi $p_1 \mid q_j$. Ali q_j, jer su ireducibilni, nemaju drugih djelitelja osim jedinica i asociranih elemenata, stoga su q_j i p_1 asocirani: $q_j = up_1$ za neku jedinicu u. Poništavanjem p_1 s obje strane, dobijemo $p_2 \cdots p_m = uq_1 \cdots \widehat{q_j} \cdots q_n$. Po pretpostavci indukcije, $m - 1 = n - 1$ (i stoga $m = n$), i nakon ponovnog indeksiranja, q_i i p_i su asocirani za sve i. ∎

Lema 8.6 *(i) Ako je R komutativan prsten i*

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

je rastući lanac ideala u R, tada je $J = \bigcup_{n \geq 1} I_n$ ideal u R.

(ii) Ako je R domena glavnih ideala, tada ne sadrži beskonačan strogo rastući lanac ideala

$$I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subsetneq I_{n+1} \subsetneq \cdots .$$

(iii) Neka je R domena glavnih ideala. Ako je $r \in R$, koji nije ni 0 ni jedinica, tada je r produkt ireducibilnih.

Dokaz. (i) Tvrdimo da je J ideal. Ako je $a \in J$, tada je $a \in I_n$ za neki n; ako je $r \in R$, tada je $ra \in I_n$, jer je I_n ideal; stoga $ra \in J$. Ako je $a, b \in J$, tada postoje ideali I_n i I_m takvi da je $a \in I_n$ i $b \in I_m$; kako je lanac rastući, možemo pretpostaviti da $I_n \subseteq I_m$, i stoga je $a, b \in I_m$. Kako je I_m ideal, $a + b \in I_m$ i stoga $a + b \in J$. Stoga je J ideal.

(ii) Ako, u suprotnom,beskonačan strogo rastući lanac postoji, tada definiramo $J = \bigcup_{n \geq 1} I_n$. Po (i) J je ideal; kako je R domena glavnih ideala, vrijedi $J = (d)$ za neki $d \in J$. Odavde slijedi da je d sadržan u I_n, za neki n. Stoga je

$$J = (d) \subseteq I_n \subsetneq I_{n+1} \subseteq J,$$

što je kontradikcija.

(iii) Djelitelj r elementa $a \in R$ se naziva *pravi djelitelj* od a ako r nije ni jedinica ni asociran od a. Ako je r djelitelj od a, tada je $(a) \subseteq (r)$; ako je r pravi djelitelj, tada je $(a) \subsetneq (r)$, ako nejednakost nije stroga, tada $(a) = (r)$, i zbog toga a i b moraju biti asocirani po Propoziciji 8.2.

Za ne-nul $a \in R$, koji nije ni jedinica kažemo da je *dobar* ako je produkt ireducibilnih, u suprotnom za a kažemo da je *loš*. Moramo pokazati da ne postoje loši elementi. Ako je a loš, nije ireducibilan i stoga je $a = rs$, gdje su oba r i s pravi djelitelji. Ali produkt dobrih elemenata je dobar i stoga je barem jedan od faktora, npr. r, loš. Kako je $(a) \subsetneq (r)$, slijedi, indukcijom, da postoji niz $a_1 = a, a_2 = r, a_3, ..., a_n, ...$ loših elemenata tako da je svaki a_{n+1} pravi djelitelj od a_n, i ovaj niz nam daje strogo rastući lanac

$$(a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \subsetneq (a_{n+1}) \subsetneq \cdots,$$

što je u kontradikciji s (i). ∎

Teorem 8.7 *Ako je R domena glavnih ideala, tada je R domena s jedinstvenom faktorizacijom. Posebno, svaki Euklidov prsten je domena s jedinstvenom faktorizacijom.*

Dokaz. Gledajći posljednja dva rezultata, dovoljno je dokazati da je (p) prost ideal kad god je p ireducibilan. Kako je R domena glavnih ideala, Korolar 8.3 pokazuje da je (p) prost ideal. ∎

Pojam najvećeg zajedničkog djelitelja možemo lagano poopćiti na proizvoljan komutativan prsten. Tada vrijedi:

Propozicija 8.8 *Ako je R domena glavnih ideala, tada nzd od bilo kojeg konačnog skupa elemenata $a_1, ..., a_n$ iz R postoji.*

Dokaz. Dovoljno je pokazati da tvrdnja vrijedi za dva elementa a i b; općenit rezultat slijedi indukcijom.

Postoje jedinice u i v i različiti ireducibilni elementi $p_1, ..., p_t$ takvi da vrijedi

$$a = up_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$$

i

$$b = vp_1^{f_1} p_2^{f_2} \cdots p_t^{f_t},$$

gdje su $e_i \geq 0$ i $f_i \geq 0$ za sve i. Lako je vidjeti da ako $c \mid a$, tada je faktorizacija od c na ireducibilne dana s $a = wp_1^{g_1} p_2^{g_2} \cdots p_t^{g_t}$, gdje je w jedinica i vrijedi $0 \leq g_i \leq e_i$ za sve i. Odnosno, c je zajednički djelitelj od a i b ako i samo ako $g_i \leq m_i$ za sve i, gdje je

$$m_i = \min\{e_i, f_i\}.$$

Sada je jasno da je $p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ *nzd* od a i b. ■

Bibliografija

[1] J. J. Rotman, Advanced Modern Algebra, Prentice Hall; 1st edition (2002); 2nd printing (2003)

[2] M. Artin, Algebra, Prentice-Hall, 1991

[3] S. Lang, Algebra, 3d ed., Addison–Wesley, Reading, 1993.

[4] N. H McCoy and G. J. Janusz, Introduction to Modern Algebra, 5th ed., Wm. C. Brown Publishers, Dubuque, Iowa, 1992.

[5] B. Širola, Algebarske strukture, http://web.math.pmf.unizg.hr/nastava/alg/predavanja/ASpred.pdf

Sažetak

Centralni pojam ovog diplomskog rada je komutativan prsten, jedna od osnovnih algebarskih struktura u matematici.

U Poglavlju 1 uvodimo neke osnovne definicije koje će nam biti potrebne za daljnje analize, kao na primjer, domene i polje razlomaka.

Poseban naglasak smo stavili na prsten polinoma. Poglavlje 2 počinje s definicijom polinoma, vodećih koeficijenata polinoma, stupnja polinoma i prstena polinoma.

U Poglavlju 3 ćemo vidjeti da, kada je k polje, svi poznati teoremi koji vrijede u $\mathbb{Z}$, imaju analogon u $k[x]$; štoviše, vidjet ćemo da se svi poznati dokazi mogu prenijeti ovdje. Prezentiramo algoritam dijeljenja za polinome s koeficijentima iz polja.

U Poglavlju 4 ćemo promatrati ona preslikavanja koja 'čuvaju strukturu'; tj., preslikavanja među prstenima koja respektiraju obje operacije, zbrajanje i množenje u prstenu. Zatim uvodimo pojam ideala u prstenu, koji čini centralno mjesto u teoriji prstena.

U Poglavlju 5 uvodimo pojam Euklidovog prstena i donosimo važan teorem koji kaže da je svaki Euklidov prsten domena glavnih ideala.

U Poglavlju 6 definiramo kvocijentni prsten i navodimo Prvi teorem o izomorfizmu za prstene.

U Poglavlju 7 i Poglavlju 8 uvodimo dva zanimljiva tipa ideala: proste ideale i maksimalne ideale. Onda ćemo, nakon što uvedemo pojam domene s jedinstvenom faktorizacijom, dokazati da je svaka domena glavnih ideala domena s jedinstvenom faktorizacijom.

Summary

The main focus of this work are commutative rings, which are one of the basic algebraic structures in mathematics.

In Chapter 1 we introduce some basic defnitions that will be needed for further analysis, like for example, domains and fraction fields.

In this work we give a special attention to the ring of polynomials. Chapter 2 begins with definitions of polynomial, leading coefficient of polynomial, degree of polynomial and ring of polynomials.

In Chapter 3 we are going to see that, when k is a field, virtually all the familiar theorems valid in $\mathbb{Z}$ have polynomial analogs in $k[x]$; moreover, we shall see that the familiar proofs can be translated into proofs here. We present division algorithm for polynomials with coefficients in a field.

In Chapter 4 we observe those mappings that preserve the structure, the (ring) homomorphism. Afterwards we introduce the notion of ideals that makes the central point in the theory of rings.

Chapter 5 defines euclidean ring and proves that every euclidean ring is a principal ideal domain.

Chapter 6 defines quotient ring and proves first isomorphism theorem.

Chapter 7 and Chapter 8 introduce two interesting type of ideals: prime and maximal ideals in commutative rings, and define unique factorization domains. Afterwards we are going to prove a common generalization: Every principal ideal domain has a unique factorization.

Životopis

Rođen sam 26.12.1987. godine u Zenici, Bosna i Hercegovina. U Žepču, Bosna i Hercegovina, sam živjela do 1995. godine. Nakon vojno-redarstvene operacije Oluja selim se s obitelji u Knin, gdje sam 2006. godine završila opću gimnaziju u Srednjoj školi Lovre Montija. Iste godine upisujem Prirodoslovno-matematički fakultet, Matematički odsjek Sveučilišta u Zagrebu. Nakon završenog preddiplomskog studija matematike upisujem Diplomski sveučilišni studij Matematičke statistike na istom odsjeku. Zadnje tri godine zaposlena sam u kompaniji Synergy Sports Technology gdje kao P1 Logger statistički obrađujem košarkaške utakmice.