Komutativni prstenovi i njihovi moduli

Gut, Ivana

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Ivana Gut

KOMUTATIVNI PRSTENOVI I NJIHOVI MODULI

Diplomski rad

Voditelj rada:
prof. dr. sc. Dražen Adamović

Zagreb, rujan, 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. _____

Sadržaj

Uvod

Prstenovi su pojam koji se koristi u mnogim područjima matematike, kao što je teorija brojeva ili analiza.
Neprazan skup R, zajedno s dvije binarne operacije $+ : R \times R \to R$ i $\cdot : R \times R \to R$ nazivamo prsten ako zadovoljava sljedeće uvjete:

(1) $(R, +)$ *je Abelova grupa,*

(2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \quad a, b, c \in R,$

(3) $a \cdot (b + c) = a \cdot b + a \cdot c$ *i* $(b + c) \cdot a = b \cdot a + c \cdot a, \quad a, b, c \in R.$

Prstenovi se, generalno, mogu podijeliti na komutativne i nekomutativne prstenove. U ovom radu bavit ćemo se komutativnim prstenovima, odnosno onim prstenovima u kojima je operacija množenja komutativna.
Uz prstenove, prirodno se nadovezuju homomorfizmi prstenova, odnosno preslikavanja s jednog prstena u drugi u skladu s operacijama definiranima na prstenu.
Za dva prstena reći ćemo da su izomorfna ako između njih možemo uspostaviti izomorfizam. U radu ćemo navesti teoreme o izomorfizmima prstenova.
Nadalje, dokazat ćemo generalizaciju Kineskog teorema o ostacima, koja vrijedi za komutativne prstenove s jedinicom.
Integralna domena u kojoj je svaki ideal glavni naziva se domena glavnih ideala. Dokazat ćemo da osnovni teorem aritmetike vrijedi za domene glavnih ideala:

Teorem 1. *Neka je R domena glavnih ideala. Tada svaki nenul element $a \in R$ možemo zapisati kao*

$$a = up_1p_2 \cdots p_n,$$

gdje je u invertibilni element i svaki p_i je prost. Štoviše, faktorizacija je jedinstvena. Tako, ako je

$$a = vq_1q_2 \cdots q_m,$$

gdje je v invertibilan, a svaki q_i prost, tada je $m = n$ i postoji permutacija $\sigma \in S_n$, takva da je q_i asociran s $p_{\sigma(i)}$ za $1 \leq i \leq n$.

Integralnu domenu R nazivamo euklidska domena ako postoji funkcija $v : R \setminus \{0\} \to \mathbb{Z}^+$ takva da:

i) za svaki $a, b \in R \setminus \{0\}$, $v(a) \leq v(ab)$ i

ii) za dane $a, b \in R, a \neq 0$, postoje $q, r \in R$, $b = aq + r$ takvi da je $r = 0$ ili $v(r) < v(a)$.

U radu ćemo dokazati da je svaka euklidska domena ujedno i domena glavnih ideala.

Skup svih polinoma s koeficijentima iz nekog komutativnog prstena s jedinicom, uz standardne operacije zbrajanja i množenja polinoma, čini prsten, i nazivamo ga prsten polinoma. Pokazat ćemo da je prsten polinoma nad poljem domena glavnih ideala. Vezano uz prsten polinoma, dokazat ćemo Hilbertov teorem o bazi:

Teorem 2. *Neka je R komutativni prsten s jedinicom u kojemu je svaki ideal konačno generiran. Tada je svaki ideal u prstenu polinoma $R[X]$ također konačno generiran.*

Uvest ćemo pojam primitivni polinom te dokazati da je prsten polinoma $R[X]$ domena jedinstvene faktorizacije ako je R domena jedinstvene faktorizacije.
Ovo poglavlje završit ćemo dokazom Eisensteinovog kriterija.

U drugom dijelu obradit ćemo module.
Neka je R prsten s jedinicom. Lijevi R-modul je Abelova grupa zajedno s operacijom skalarnog množenja $\cdot : R \times M \to M$, koja za sve elemente a, b iz R i m, n iz M zadovoljava sljedeće aksiome:

(i) $a(m + n) = am + an$

(ii) $(a+b)m = am + bm$

(iii) $(ab)m = a(bm)$

(iv) $1m = m.$

Analogno se definira i desni R-modul. Slično kao kod prstenova, definirat ćemo homomorfizam modula i navesti teoreme o izomorfizmima modula.
Nadalje, za prsten R i R-modul M uvest ćemo pojmove R-linearne nezavisnosti podskupa od M i definirati bazu:
Neka je M R-modul. Podskup S od M je baza od M ako S generira M kao R-modul i ako je S R-linearno nezavisan.
Posebno ćemo definirati i dati primjere slobodnih modula: *R-modul M nazivamo slobodni R-modul ako ima bazu.*
Rad zaključujemo dokazom teorema:

Teorem 3. *Neka je D prsten s dijeljenjem i neka je V D-modul. Tada je V slobodan D-modul. Posebno, svaki vektorski prostor V ima bazu.*

Poglavlje 1

Komutativni prstenovi

1.1 Osnovne definicije i teoremi iz teorije prstenova

Osnovni pojam koji se proteže kroz ovaj rad je prsten. Prstenovi su algebarske strukture koji imaju dvije operacije, koje uobičajeno nazivamo zbrajanje i množenje.

Definicija 1.1.1. *Neprazan skup R, zajedno s dvije binarne operacije $+ : R\times R \to R$ i $\cdot : R \times R \to R$ nazivamo prsten (označavamo: $(R, +, \cdot)$) ako zadovoljava sljedeće uvjete:*

(1) $(R, +)$ *je Abelova grupa,*

(2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \;\; a, b, c \in R,$

(3) $a \cdot (b + c) = a \cdot b + a \cdot c \;\; i \;\; (b + c) \cdot a = b \cdot a + c \cdot a, \quad a, b, c \in R.$

Neutralni element grupe $(R, +)$ nazivamo nula prstena i označavamo s 0. Ako je $R \neq \{0\}$ i množenje ima neutralni element za svaki $a \in R$, onda $(R, +, \cdot)$ nazivamo prsten s jedinicom.
U prstenu s jedinicom, a je invertibilni element ako a ima multiplikativni inverz, odnosno ako u prstenu postoji b takav da je $ab = 1 = ba$.

Skup svih invertibilnih elementa u prstenu R označavat ćemo s R^*. Nadalje ćemo umjesto $(R, +, \cdot)$ pisati R, a umjesto $a \cdot b$ pisati ab.
Podskup S prstena R nazivamo potprsten, ako je $(S+, \cdot)$ i sam prsten.
Ako su a i b elementi prstena R, takvi da je $a \neq 0$ i $b \neq 0$, a $ab = 0$, onda a i b nazivamo djelitelji nule prstena R. Ako je množenje u prstenu R komutativno, tada R nazivamo komutativni prsten.
Prsten R nazivamo integralna domena ako je R komutativan prsten s jedinicom i ako nema djelitelja nule.
Za prsten s jedinicom kažemo da je prsten s dijeljenjem ako svaki nenul element prstena ima multiplikativni inverz, tj. ako je $R^* = R\backslash\{0\}$.
Komutativni prsten s dijeljenjem nazivamo polje.

Propozicija 1.1.2. *Konačna integralna domena je polje.*

Dokaz. Neka je R konačna integralna domena, neka je $a \in R$, $a \neq 0$. Definirajmo funkciju $\phi_a : R \to R$, $\phi_a(b) = ab$. Dovoljno je pokazati da je funkcija ϕ_a injekcija. Pretpostavimo da je $\phi_a(b) = \phi_a(c)$. Iz toga nam slijedi $ab = ac$, odnosno
$ab - ac = 0 \Rightarrow a(b - c) = 0$. Jer je $a \neq 0$, a R integralna domena, slijedi da je $b = c$, odnosno ϕ_a je injekcija. Kako je R konačan, ϕ_a je surjekcija, stoga i bijekcija pa je a invertibilan, iz čega slijedi da je R prsten s dijeljenjem, a zbog komutativnosti, R je i polje. □

Primjer 1.1.3. *Neka je R prsten s jedinicom i neka je $M_{m,n}(R)$ skup svih $m \times n$ matrica čiji elementi su iz R. Za $m = n$ pisat ćemo $M_n(R)$. Označimo s a_{ij} element u i-tom retku i j-tom stupcu matrice $A = (a_{ij})$, $1 \leq i \leq m$, $1 \leq j \leq n$.*
Za $A = (a_{ij}), B = (b_{ij}) \in M_{m,n}(R)$ definirajmo zbrajanje s:

$$A + B = (c_{ij}) \in M_{m,n}(R),$$

gdje je

$$c_{ij} = a_{ij} + b_{ij}, \text{ za svaki } i = 1, 2, \ldots, m, j = 1, 2, \ldots, n.$$

Za $A \in M_{m,n}(R)$ i $B \in M_{n,p}(R)$ definirajmo množenje s:

$$AB = (c_{ij}) \in M_{m,p}(R),$$

pri čemu je

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}, \text{ za svaki } i = 1, 2, \ldots, m, j = 1, 2, \ldots, p.$$

Ove operacije zbrajanja i množenja uvijek su dobro definirane za matrice iz $M_n(R)$ i uz te operacije, $M_n(R)$ je prsten s jedinicom. Jedinica u tom prstenu je matrica I_n, definirana s $I_n = (\delta_{ij})$, gdje je δ_{ij} Kroneckerov delta:

$$\delta_{ij} = \begin{cases} 1, \text{ za } i = j \\ 0, \text{ za } i \neq j. \end{cases}$$

Definicija 1.1.4. *Neka je R prsten i neka je $I \subseteq R$. Kažemo da je I ideal u R ako i samo ako vrijedi:*

1. *I je aditivna podgrupa u R*
2. *$rI = \{ra : a \in I\} \subseteq I$, za svaki $r \in R$*
3. *$Ir = \{ar : a \in I\} \subseteq I$, za svaki $r \in R$.*

Svaki prsten R ima barem dva ideala: R i $\{0\}$. Jedini ideali u prstenu s dijeljenjem R su $\{0\}$ i R.
Neka je $I \subseteq R$ ideal. Tada je kvocijentni skup R/I, uz operacije zbrajanja

$$(r + I) + (s + I) = (r + s) + I, \qquad r, s \in I$$

i množenja

$$(r + I)(s + I) = rs + I, \qquad r, s \in I$$

prsten i nazivamo ga kvocijentni prsten R po idealu I.

Definicija 1.1.5. *Neka je R prsten i X podskup od R. Najmanji potprsten od R koji sadrži X nazivamo potprsten generiran s X. Najmanji ideal od R koji sadrži X*

nazivamo ideal generiran s X i označavamo s $\langle X \rangle$. Ako je $X = \{a\}$, ideal generiran s a u komutativnom prstenu s jedinicom je skup $\langle a \rangle = \{ra : r \in R\}$. Takav ideal nazivamo glavni ideal.

Ideal M u prstenu R nazivamo maksimalni ideal ako je $M \neq R$ i M je takav da ako je I ideal, $M \subseteq I \subseteq R$, tada je $I = M$ ili $I = R$.
Ideal u komutativnom prstenu R nazivamo prost ideal ako je $P \neq R$ i P je takav da ako je $ab \in P$, tada je $a \in P$ ili $b \in P$.

Definicija 1.1.6. *Neka su R, S prstenovi. Preslikavanje $f : R \to S$ nazivamo homomorfizam prstenova ako*

$$f(a+b) = f(a) + f(b) \quad i$$
$$f(ab) = f(a)f(b)$$

vrijedi za svaki $a, b \in R$.

Dakle, homomorfizam prstenova je preslikavanje koje poštuje dane strukture prstenova. Jezgra homomorfizma je skup $\mathrm{Ker}\,(f) = \{a \in R : f(a) = 0\}$. Slika homomorfizma je skup $\mathrm{Im}\,(f) = \{f(a), a \in R\}$.

1.2 Teoremi o izmorfizmima prstenova

Neka su R, S prstenovi te neka je $f : R \to S$ homomorfizam prstenova. Ako je f invertibilna funkcija, odnosno ako postoji homomorfizam prstenova $g : S \to R$ takav da je $f \circ g = 1_S$ i $g \circ f = 1_R$, tada kažemo da je f izomorfizam prstenova. U tom slučaju je i g izomorfizam prstenova, a za prstenove R i S kažemo da su izomorfni i označavamo $R \cong S$. Teoreme o izomorfizmima prstenova navodimo bez dokaza, koji se mogu pronaći u [1]

Teorem 1.2.1 (Prvi teorem o izomorfizmu)**.** *Neka je $f : R \to S$ homomorfizam prstenova. Tada je $R/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$.*

Teorem 1.2.2 (Drugi teorem o izomorfizmu)**.** *Neka je R prsten, $I \subseteq R$ ideal, $S \subseteq R$ potprsten. Tada je $S + I$ potprsten u R, I je ideal u $S + I$, $S \cap I$ je ideal u S i $(S + I)/I \cong S/(S \cap I)$.*

Teorem 1.2.3 (Treći teorem o izomorfizmu)**.** *Neka je R prsten i I i J ideali u R takvi da je $I \subseteq J$. Tada je J/I ideal u R/I i $R/J \cong (R/I)/(J/I)$.*

1.3 Kineski teorem o ostacima

Dokazat ćemo generalizaciju klasičnog Kineskog teorema o ostacima koja vrijedi za komutativne prstenove.

Definicija 1.3.1. *Neka je R prsten i neka je I ideal u R. Za elemente $a, b \in R$ kažemo da su kongruentni modulo I i pišemo $b \equiv a (\mathrm{mod}\, I)$ ako je $b - a \in I$.*

Teorem 1.3.2 (Kineski teorem o ostacima)**.** *Neka je R komutativan prsten s jedinicom i neka su $I_1, I_2, ..., I_n$ ideali u R takvi da je $I_i + I_j = R$ za sve $i \neq j$. Za dane elemente $a_1, a_2, \ldots, a_n \in R$ postoji $a \in R$ takav da je*

$$a \equiv (a_i \bmod I_i),\ za\ 1 \leq i \leq n.$$

Također, $b \in R$ je rješenje sustava kongruencija

$$x \equiv a_i (\mathrm{mod} I_i),\ za\ 1 \leq i \leq n$$

ako i samo ako

$$b \equiv a (\mathrm{mod} I_1 \cap I_2 \cap \cdots \cap I_n).$$

Dokaz. Prvo ćemo dokazati specijalni slučaj gdje je $a_1 = 1$ i $a_j = 0$ za $j > 1$. Za svaki $j > 1$ možemo naći $b_j \in I_1$ i $c_j \in I_j$ takvi da su $b_j + c_j = 1$. Tada je

$$\prod_{j=1}^{n} (b_j + c_j) = 1.$$

Budući da je $b_j \in I_1$, tada je

$$1 = \prod_{j=1}^{n} (b_j + c_j) \in I_1 + \prod_{j=2}^{n} I_j.$$

Tada postoje $\alpha_1 \in I_1$ i $\beta_1 \in \prod_{j=2}^{n} I_j$ i $\alpha_1 + \beta_1 = 1$. Uočimo da je β_1 rješenje specijalnog slučaja sustava kongruencija, odnosno

$$\beta_1 \equiv 1 (\mathrm{mod} I_1)$$
$$\beta_1 \equiv 0 (\mathrm{mod} I_j), \quad \text{za } j \neq 1.$$

Na isti način možemo naći $\beta_2, \beta_3, \ldots, \beta_n$ takve da je

$$\beta_i \equiv 1 (\mathrm{mod} I_i)$$
$$\beta_i \equiv 0 (\mathrm{mod} I_j), \quad \text{za } j \neq i.$$

Neka je $a = a_1\beta_1 + a_2\beta_2 + \cdots + a_n\beta_n$. Tada je

$$a \equiv a_i (\mathrm{mod} I_i),\ 1 \leq i \leq n.$$

Pretpostavimo sada da je $b \equiv a_i (\mathrm{mod} I_i), \qquad 1 \leq i \leq n.$

$$b \equiv a_i (\mathrm{mod} I_i) \Leftrightarrow b - a \equiv 0 (\mathrm{mod} I_i) \Leftrightarrow b - a \in I_i \Leftrightarrow$$
$$\Leftrightarrow b - a \in \bigcap_{i=1}^{n} I_i \Leftrightarrow b \equiv a (\mathrm{mod} I_1 \cap I_2 \cap \cdots \cap I_n).$$

Dokaz obrata je jednostavan. □

1.4 Domena glavnih ideala

Integralnu domenu u kojoj je svaki ideal glavni nazivamo domena glavnih ideala. Neka je R integralna domena i neka su a,$b \in R \setminus \{0\}$. Za a i b kažemo da su asocirani i koristimo oznaku $a \sim b$ ako postoji invertibilni element $u \in R$ takav da je $a = ub$.
Nadalje, kažemo da a dijeli b i pišemo $a|b$ ako postoji $c \in R$ takav da je $b = ac$.
Neinvertibilni element a je ireducibilan ako $a = bc$ povlači da su b ili c invertibilni elementi.
Neinvertibilni element a je prost ako $a|bc$ povlači $a|b$ ili $a|c$.

Definicija 1.4.1. *Neka je R integralna domena i neka je A neprazan podskup od $R \setminus \{0\}$. Kažemo da je $d \in R$ najveći zajednički djelitelj od A ako*

i) $d|a$ *za svaki* $a \in A$

ii) ako je $e \in R$ *i* $e|a$ *za svaki* $a \in A$*, tada* $e|d$.

Ako je 1 najveći zajednički djelitelj od A, tada kažemo da je skup A relativno prost.

Teorem 1.4.2. *Neka je R domena glavnih ideala i neka je A neprazan podskup od $R \setminus \{0\}$. Tada je element $d \in R$ je najveći zajednički djelitelj od A ako i samo ako je d generator od $\langle A \rangle$.*

Dokaz. Neka je d generator ideala $\langle A \rangle$. Tada $d|a$ za svaki $a \in A$ Također, budući da je $d \in \langle A \rangle$, slijedi da je $d = \sum_{i=1}^{n} r_i a_i$ za $r_1, r_2, \ldots, r_n \in R$ i $a_1, a_2, \ldots, a_n \in A$. Ako $e|a$ za svaki $a \in A$, tada $e|d$ pa je d najveći zajednički djelitelj od A.
Pretpostavimo sada da je d najveći zajednički djelitelj od A i neka je $\langle A \rangle = \langle c \rangle$. Tada $d|a$ za svaki $a \in A$ pa je $a \in \langle d \rangle$. Dakle,

$$\langle c \rangle = \langle A \rangle \subseteq \langle d \rangle.$$

No, za $a \in A$, $a \in \langle c \rangle$ pa $c|a$. Kako je d najveći zajednički djelitelj od A, slijedi da je $\langle d \rangle \subseteq \langle c \rangle$, pa je $\langle d \rangle = \langle c \rangle$ te je d generator od $\langle A \rangle$. □

Korolar 1.4.3. *Neka je R domena glavnih ideala i neka je $a \in R \setminus \{0\}$. Tada je a prost ako i samo ako je a ireducibilan.*

Korolar 1.4.4. *Neka je R domena glavnih ideala i neka je $I \subseteq R$ nenul ideal. Tada je I prost ako i samo ako je I maksimalni ideal.*

1.5 Noetherini prstenovi

Definicija 1.5.1. *Neka je R prsten s jedinicom. Kažemo da je R Noetherin prsten ako za svaki rastući niz*

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

ideala u R postoji n takav da je $I_k = I_n$ za sve $k \geq n$.

Propozicija 1.5.2. *Neka je R prsten. Sljedeće tvrdnje su ekvivalentne:*

(1) *R je Noetherin prsten.*

(2) *Svaki ideal u R je konačno generiran.*

(3) *Svaki neprazan podskup ideala u R ima maksimalni element.*

Posebno, domena glavnih ideala je Noetherin prsten.

Dokaz. (1) $\Rightarrow$ (3) Pretpostavimo da je $\mathcal{S} = \{I_\alpha\}_{\alpha \in A}$ neprazan skup ideala u R koji nema maksimalni element. Izaberimo $I_1 \in \mathcal{S}$. Kako $\mathcal{S}$ nema maksimalni element, onda postoji $I_2 \in \mathcal{S}$ takav da je $I_1 \subset I_2$. Isto tako, I_2 nije maksimalni element pa postoji $I_3 \in \mathcal{S}$ takav da je $I_2 \subset I_3$. Na ovaj način možemo konstruirati beskonačan strogo rastući niz ideala u R, što je u kontradikciji s činjenicom da je R Noetherin prsten.

(3) $\Rightarrow$ (2) Neka je I ideal u R i neka je $\mathcal{S}$ familija svih konačno generiranih ideala u R koji su sadržani u I. Tada postoji maksimalni element $J \in \mathcal{S}$. Neka je $a \in I$. Tada je ideal $J + \langle a \rangle \in \mathcal{S}$ i sadrži J. Kako je J maksimalni element u $\mathcal{S}$, slijedi da je $J = J + \langle a \rangle$. Tada je $I = J$ i I je konačno generiran.

(2) $\Rightarrow$ (1) Pretpostavimo da je svaki ideal u R konačno generiran. Neka je

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

niz ideala u R i neka je $I = \bigcup_{n=1}^{\infty} I_n$. Tada je I ideal u R takav da je $I = \langle a_1, a_2, \ldots, a_m \rangle$ za neke $a_i \in R$.

$$a_i \in I = \bigcup_{n=1}^{\infty} I_n,\ 1 \leq i \leq m$$

i $a_i \in I_{n_i}$ za neki n_i. Kako imamo niz ideala, slijedi da postoji n takav da je $a_i \in I_n$ za svaki i. Odnosno, za svaki $k \geq n$ je

$$\langle a_1, a_2, \ldots, a_m \rangle \subseteq I_k \subseteq I = \langle a_1, a_2, \ldots, a_m \rangle$$

takvih da je $I_k = I = I_n$ za svaki $k \geq n$ pa je R Noetherin prsten. □

1.6 Osnovni teorem aritmetike

Osnovni teorem aritmetike tvrdi da se svaki prirodni broj veći od 1 može jednoznačno (do na poredak faktora) napisati kao umnožak prostih brojeva. Analogon osnovnog teorem aritmetike vrijedi za domene glavnih ideala.

Teorem 1.6.1 (Osnovni teorem aritmetike)**.** *Neka je R domena glavnih ideala. Tada svaki nenul element $a \in R$ možemo zapisati kao*

$$a = up_1p_2 \cdots p_n,$$

gdje je u invertibilni element i svaki p_i je prost. Štoviše, faktorizacija je jedinstvena. Tako, ako je

$$a = vq_1q_2 \cdots q_m,$$

gdje je v invertibilan, a svaki q_i prost, tada je $m = n$ i postoji permutacija $\sigma \in S_n$, takva da je q_i asociran s $p_{\sigma(i)}$ za $1 \leq i \leq n$.

Dokaz. Prvo ćemo dokazati egzistenciju.
Neka je $a \neq 0 \in R$. U slučaju da je a prost ili je a invertibilan, egzistencija stoji. Uzmimo a koji nije prost i nije invertibilan. Tada a možemo zapisati kao $a = a_1 b_1$, gdje su a_1 i b_1 neinvertibilni elementi. Tada je $\langle a \rangle \subset \langle b_1 \rangle$. Ako je b_1 prost, stajemo. Inače, b_1 možemo zapisati kao $b_1 = a_2 b_2$, gdje su a_2 i b_2 neinvertibilni elementi i $\langle b_1 \rangle \subset \langle b_2 \rangle$. Na ovaj način možemo kreirati niz

$$\langle a \rangle \subset \langle b_1 \rangle \subset \langle b_2 \rangle \cdots$$

Budući da je R domena glavnih ideala, pa tako i Noetherin prsten, ovaj niz ideala mora stati na nekome $\langle b_n \rangle$. Tada je b_n prost i zaključujemo da za svaki neinvertibilni $a \neq 0$, $a \in R$ postoji prosti element koji dijeli a.
Neka je sada $a \neq 0$ neinvertiblni element. Tada a možemo zapisati kao $a = p_1 c_1$, gdje je p_1 prost. Također,

$$\langle a \rangle \subset \langle c_1 \rangle.$$

Ako je c_1 invertibilan, stajemo. Inače, c_1 možemo zapisati kao $c_1 = p_2 c_2$, gdje je p_2 prost i $\langle c_1 \rangle \subset \langle c_2 \rangle$. I tako redom možemo stvoriti niz

$$\langle a \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle \cdots .$$

Kako je R domena glavnih ideala, tada ovaj niz ideala ne može biti beskonačan te mora stati na nekom c_n koji je invertibilan. Tada je

$$a = p_1 p_2 \cdots p_n c_n = p_1 p_2 \cdots p_n u.$$

Dokažimo sada jedinstvenost.
Pretpostavimo da je

$$a = p_0 p_1 \cdots p_n = q_0 q_1 \cdots q_m,$$

gdje su $p_1, p_2, \ldots, p_n, q_1, q_2, \ldots, q_m$ prosti, a p_0 i q_0 invertibilni u R.
Jedinstvenost ćemo dokazati indukcijom po $k = \min\{m, n\}$.
Ako je $n = 0$, tada je a invertibilan, pa je a $= q_0$ te je $m = 0$.

Pretpostavimo da je $k > 0$ i pretpostavimo da je rezultat istinit za sve $b \in R$ koji se mogu faktorizirati na manje od k prostih elemenata. Tada

$$p_n | q_0 q_1 \cdots q_m$$

pa p_n dijeli neki q_i. Pretpostavimo da $p_n | q_m$. Kako je q_m prost, tada $q_m = p_n c$ povlači da je c invertibilan, a p_n i q_m su asocirani. Neka je

$$a' = \frac{a}{p_n} = p_0 p_1 \cdots p_{n-1} = (q_0 c) q_1 q_2 \cdots q_{m-1}.$$

Tada je a' faktoriziran na manje od k prostih elemenata, pa je po pretpostavci indukcije $n - 1 = m - 1$ i q_i je asociran s $p_{\sigma(i)}$ za neki $\sigma \in S_{n-1}$. □

Korolar 1.6.2. *Neka je R domena glavnih ideala i neka je $a \neq 0 \in R$. Tada je*

$$a = u p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k},$$

gdje su $p_1, p_2, \ldots, p_k$ različiti prosti elementi, a u je invertibilni element. Faktorizacija je jedinstvena.

1.7 Euklidska domena

Definicija 1.7.1. *Integralnu domenu R nazivamo euklidska domena ako postoji funkcija $v : R \setminus \{0\} \to \mathbb{Z}^+$ takva da:*

i) za svaki $a, b \in R \setminus \{0\}$, $v(a) \leq v(ab)$ i

ii) za dane $a, b \in R, a \neq 0$, postoje $q, r \in R$, $b = aq + r$ takvi da je $r = 0$ ili $v(r) < v(a)$.

Primjer 1.7.2. *Prsten cijelih brojeva $\mathbb{Z}$ uz funkciju $v(n) = |n|$ je euklidska domena.*

Teorem 1.7.3. *Neka je R euklidska domena. Tada je R domena glavnih ideala.*

Dokaz. Neka je $I \subseteq R$ nenul ideal i neka je

$$S = \{v(a) : a \in I \setminus \{0\}\} \subseteq \mathbb{Z}^+$$

Neka je n_0 najmanji element skupa S. Izaberimo $a \in I$ takav da je $v(a) = n_0$. Tvrdimo da je $I = \langle a \rangle$. Kako je $a \in I$, tada je $\langle a \rangle \in I$. Neka je $b \in I$. Tada je $b = aq + r$ za $q, r \in R$, gdje je $r = 0$ ili $v(r) < v(a)$. Kako je $r = b - aq \in I$, onda je $v(a) \leq v(r)$, ako je $r \neq 0$. Iz toga slijedi da r mora biti 0, pa je $b = aq \in \langle a \rangle$, $I = \langle a \rangle$, odnosno R je domena glavnih ideala. □

Euklidov algoritam za traženje najvećeg zajedničkog djelitelja dvaju prirodnih brojeva vrijedi i u euklidskoj domeni za traženje najvećeg zajedničkog djelitelja dvaju elemenata iz R. Algoritam je sljedeći:
Za dane elemente $a_1, a_2 \in R \setminus \{0\}$ napišimo

$$\begin{aligned}
a_1 &= a_2 q_1 + a_3, && \text{gdje je} \quad a_3 = 0 \quad \text{ili} \quad v(a_3) < v(a_2) \\
a_2 &= a_3 q_2 + a_4, && \text{gdje je} \quad a_4 = 0 \quad \text{ili} \quad v(a_4) < v(a_3) \\
a_3 &= a_4 q_3 + a_5, && \text{gdje je} \quad a_5 = 0 \quad \text{ili} \quad v(a_5) < v(a_4) \\
&\vdots
\end{aligned}$$

Budući da je $v(a_2) > v(a_3) > v(a_4) > \cdots$, algoritam mora stati nakon konačno mnogo koraka, odnosno $a_{n+1} = 0$ za neki n. Za taj n onda imamo

$$a_{n-1} = a_n q_{n-1} + 0.$$

Tvrdimo da je a_n najveći zajednički djelitelj od $\{a_1, a_2\}$. Dokažimo to.
Označimo najveći zajednički djelitelj od $a, b \in R$ s (a, b). Tada je, prema teoremu 1.4.2, (a, b) generator ideala generiranog s $\{a, b\}$. Tvrdimo da je

$$(a_i, a_{i+1}) = (a_{i+1}, a_{i+2})$$

za $1 \leq i \leq n - 1$. Kako je $a_i = a_{i+1} + q_i + a_{i+2}$, slijedi da je

$$\begin{aligned} xa_i + ya_{i+1} &= x(a_{i+1}q_i + a_{i+2}) + ya_{i+1} \\ &= (xq_i + y)a_{i+1} + xa_{i+2}. \end{aligned}$$

Tada je $\langle a_i, a_{i+1}\rangle \subseteq \langle a_{i+1}, a_{i+2}\rangle$.
Slično,

$$\begin{aligned} ra_{i+1} + sa_{i+2} &= ra_{i+1} + s(a_i - a_{i+1}q_i) \\ &= sa_i + (r - q_i)a_{i+1} \end{aligned}$$

pa je $\langle a_{i+1}, a_{i+2}\rangle \subseteq \langle a_i, a_{i+1}\rangle$, odnosno $\langle a_{i+1}, a_{i+2}\rangle = \langle a_i, a_{i+1}\rangle$ iz čega slijedi da je $(a_i, a_{i+1}) = (a_{i+1}, a_{i+2})$. Zaključujemo da je

$$(a_1, a_2) = (a_2, a_3) = \cdots = (a_{n-1}, a_n).$$

Kako $a_n | a_{n-1}$, to je $(a_{n-1}, a_n) = a_n$ pa je tvrdnja dokazana.

1.8 Polje kvocijenata

Definicija 1.8.1. *Ako je R komutativni prsten, za S podskup od R reći ćemo da je multiplikativni podskup ako je produkt bilo koja dva elementa u S, element u S.*

Definicija 1.8.2. *Neka je R komutativan prsten i neka je $S \subseteq R$, neprazan multiplikativni podskup u R koji nema djelitelja nule. Lokalizacija od R po S je komutativni prsten R_S s jedinicom i injektivni homomorfizam prstenova $\phi : R \to R_S$ takav da za sve $a \in R_S$ postoji $b \in R$ i $c \in S$ takav da je $\phi(c)$ invertibilan u R_S i $a = \phi(b)\phi(c)^{-1}$. Ako je R integralna domena i $S = R \setminus \{0\}$, onda R_S nazivamo polje kvocijenata.*

Teorem 1.8.3. *Neka je R komutativni prsten. Neka je $S \subseteq R$ neprazan multiplikativni podskup koji nema djelitelja nule. Tada postoji lokalizacija R_S po S i R_S je jedinstven do na ekvivalenciju.*

Dokaz. Definirajmo relaciju $\sim$ na $R \times S$

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Relacija $\sim$ je relacija ekvivalencije.
Neka je $R_S = R \times S/\sim$ skup svih klasa ekvivalencije relacije $\sim$. Klasu ekvivalencije (a, b) označit ćemo s $\frac{a}{b}$.
Za svaki $c \in S$, $(a, b) \sim (ac, bc)$, odnosno $\frac{a}{b} = \frac{ac}{bc}$ za svaki $c \in S$. Na R_S definirajmo operacije zbrajanja i množenja:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \tag{1.1}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \tag{1.2}$$

Jer je S multiplikativni podskup, $bd \in S$. Provjerimo sada da operacije ne ovise o izboru predstavnika klase ekvivalencije:
Neka je $\frac{a}{b} = \frac{a'}{b'}$ i neka je $\frac{c}{d} = \frac{c'}{d'}$. Tada je i $ab' = ba'$ te $cd' = dc'$, pa je i $acb'd' = bda'c'$, odnosno $\frac{ac}{bd} = \frac{a'c'}{b'd'}$ pa je operacija množenja (1.2) dobro definirana. Također, provjerimo da je operacija zbrajanja (1.1) dobro definirana:

$$\begin{aligned}(ad + bc)b'd' &= ab'dd' + bb'cd' \\ &= ba'dd' + bb'dc' \\ &= (a'd' + b'c')bd.\end{aligned}$$

Zaključujemo da je R_S komutativni prsten s jedinicom. Definirajmo sada $\phi : R \to R_S$. Neka je $s \in S$ i definirajmo $\phi_s : R \to R_s$, $\phi_s(a) = \frac{as}{s}$. Tvrdimo da ako je $s' \in S$, tada je $\phi_s = \phi_{s'}$. Kako je $\phi_s(a) = \frac{as}{s}$ i $\phi_{s'}(a) = \frac{as'}{s'}$, te $ass' = as's$, slijedi da je $\phi_s = \phi_{s'}$ i možemo definirati ϕ kao ϕ_s za bilo koji $s \in S$.

Pokažimo sada da je ϕ homomorfizam prstenova. Neka su $a, b \in R$ i $s \in S$.

$$\begin{aligned}\phi(ab) &= \frac{abs}{s} = \frac{abs^2}{s^2} \\ &= \frac{as}{s} \cdot \frac{bs}{s} = \phi(a)\phi(b)\end{aligned}$$

i

$$\begin{aligned}\phi(a+b) &= \frac{(a+b)s}{s} = \frac{as^2+bs^2}{s^2} \\ &= \frac{as}{s} + \frac{bs}{s} = \phi(a) + \phi(b).\end{aligned}$$

$\phi(1) = \frac{s}{s} = 1_{R_s}$, $\mathrm{Ker}(\phi) = \{a \in R : \frac{a}{s} = \frac{0}{s'}\} = \{0\}$.
Dakle, ϕ je injektivni homomorfizam prstenova.
Pretpostavimo da je $\frac{a}{b} \in R_s$, $a \in R, b \in S$. Tada je

$$\frac{a}{b} = \frac{as}{s} \cdot \frac{s}{bs} = \phi(a)(\phi(b))^{-1},$$

odnosno konstruirali smo lokalizaciju od R po S.
Provjerimo još jedinstvenost do na ekvivalenciju:
Pretpostavimo da su $\phi : R \to R_S$ i $\phi' : R \to R'_S$ dvije lokalizacije od R po S.
Definirajmo $\beta : R_S \to R'_S$:
Neka je $a \in R_S$. Tada a možemo napisati kao $a = \phi(b)(\phi(c))^{-1}$, gdje je $b \in R$ i $c \in S$, pa definirajmo $\beta(a) = \phi'(b)(\phi'(c))^{-1}$. Pokažimo da je β dobro definiran:
Ako je

$$\phi(b)(\phi(c))^{-1} = a = \phi(b')(\phi(c'))^{-1},$$

tada je $\phi(b)\phi(c') = \phi(b')\phi(c)$, odnosno $\phi(bc')) = \phi(b'c)$. Budući da je ϕ injektivan, to je $bc' = b'c$.
Jer je ϕ' homomorfizam, dobivamo da je

$$\phi'(b)(\phi'(c))^{-1} = \beta(a) = \phi'(b')(\phi'(c'))^{-1},$$

te je β dobro definirana funkcija.

Pokažimo sada da je β bijekcija. Definirajmo
$\gamma : R'_S \to R_S$, $\gamma(a') = \phi(b')(\phi(c'))^{-1}$ ako je $a' = \phi'(b')(\phi'(c'))^{-1}$ za neke $b' \in R, c' \in S$.
Kao i za β, pokaže se da je γ dobro definirana funkcija.
Za $a \in R_S$, napišimo $a = \phi(b)(\phi(c))^{-1}$ i izračunajmo

$$\begin{aligned}\gamma(\beta(a)) &= \gamma(\phi'(b)(\phi'(c))^{-1}) \\ &= \phi(b)(\phi(c))^{-1} \\ &= a\end{aligned}$$

Slično pokažemo da je $\beta(\gamma(a')) = a'$ pa je β bijektivna funkcija. Lako se još provjeri da je β homomorfizam, čime je teorem dokazan. □

Primjer 1.8.4. *Polje racionalnih brojeva nad integralnom domenom $\mathbb{Z}$ je polje kvocijenata.*

1.9 Prsten polinoma

Definicija 1.9.1. *Neka je R komutativni prsten s jedinicom. Označimo s $R[X]$ skup svih funkcija $f : \mathbb{Z}^+ \to R$ takvih da je $f(n) = 0$ za sve, osim za konačno mnogo nenegativnih brojeva n. Strukturu na skupu $R[X]$ zajedno s operacijama*

$$\begin{aligned}(f+g)(n) &= f(n) + g(n) \\ (fg)(n) &= \sum_{m=0}^{n} f(m)g(n-m)\end{aligned}$$

zovemo prsten polinoma u X s koeficijentima iz R.

Definirajmo $X \in R[X]$ s

$$X(n) = \begin{cases} 1, & \text{ako je } n = 1 \\ 0, & \text{ako je } n \neq 1. \end{cases}$$

Funkcija X^n je tada:

$$X^n(m) = \begin{cases} 1, & \text{ako je } m = n \\ 0, & \text{ako je } m \neq n \end{cases}$$

pa svaki $f \in R[X]$ možemo jedinstveno napisati kao

$$f = \sum_{n=0}^{\infty} a_n X^n,$$

gdje je $a_n = f(n)$. X^0 je jedinica u $R[X]$. Elemente u $R[X]$ zovemo polinomi i označavat ćemo ih s $f(X)$.
Definirajmo stupanj polinoma $f(X) = \sum_{n=0}^{\infty} a_n X^n \in R[X]$, $f(X) \neq 0$, u oznaci $\deg(f(X))$ s:

$$\deg(f(X)) = \max\{m : a_m \neq 0\}.$$

Ako je n stupanj polinoma $f(X) \in R[X]$, onda možemo pisati $f(X) = \sum_{i=0}^{n} a_n X^n$. Koeficijent a_n tada nazivamo vodeći koeficijent i označavat ćemo ga s $\mathrm{lc}(f(X))$. Ako je vodeći koeficijent polinoma $f(X)$ jednak 1, reći ćemo da je polinom $f(X)$ normiran. Dogovorno, stupanj nulpolinoma je $\deg(f(0)) = -\infty$.

Lema 1.9.2. *Neka je R komutativni prsten i neka su $f(X), g(X) \in R[X]$. Tada:*

(*i*) $\deg(f(X) + \deg(g(X)) \leq \max\{\deg(f(X)), \deg(g(X))\}$,

(*ii*) $\deg(f(X)g(X)) \leq \deg(f(X) + \deg(g(X)$,

(*iii*) *ako je R integralna domena, tada je* $\deg(f(X)g(X)) = \deg(f(X) + \deg(g(X)$.

Korolar 1.9.3. *Ako je R integralna domena, tada:*

(1) *$R[X]$ je integralna domena,*

(2) *invertibilni elementi u $R[X]$ su invertibilni u R.*

Dokaz. (1) Ako je $f(X) \neq 0, g(x) \neq 0$, tada je

$$\deg(f(X)g(X)) = \deg(f(X)) + \deg(g(X)) \geq 0 > -\infty,$$

pa je $f(X)g(X) \neq 0$.

(2) Ako je $f(X)g(X) = 1$, tada je $\deg(f(X)) + \deg(g(X)) = \deg(1) = 0$, što znači da su $f(X)$ i $g(X)$ polinomi stupnja 0, odnosno da su iz R.

□

Teorem 1.9.4 (Teorem o dijeljenju s ostatkom)**.** *Neka je R komutativan prsten s jedinicom, neka je $f(X) \in R[X]$ i neka je $g(X) \in R[X]$ normirani polinom. Tada postoje jedinstveni polinomi $q(X)$ i $r(X)$ u $R[X]$, $\deg(r(X)) < \deg(g(X))$ takvi da je*

$$f(X) = g(X)q(X) + r(X).$$

Dokaz. Dokažimo egzistenciju:
Neka je $f(X) = a_0 + a_1X + \cdots a_nX^n \in R[X]$ i neka je $g(X) = b_0 + b_1X + \cdots + b_{m-1}X^{m-1} + X^m$ normirani polinom u $R[X]$ stupnja $m \geq 1$. Ako je $n \geq m$, neka je $q_1(X) = a_nX^{n-m}$. Tada je $f_1(X) = f(X) - g(X)q_1(X)$ stupnja manjeg ili jednakog $n-1$. Ako je $\deg(f_1(X)) \geq m$, ponavljamo proces. Nakon konačno mnogo koraka, dobit ćemo polinom $f_s(X)$ stupnja manjeg od m.
Za $q(X) = q_1(X)+q_2(X)+\cdots+q_s(X)$ i $r(X) = f(X)-g(X)q(X)$ dobivamo jednakost

$$f(X) = g(X)q(X) + r(X), \tag{1.3}$$

gdje je $\deg(r(X)) < \deg(g(X))$.
Dokažimo sada jedinstvenost. Pretpostavimo da osim (1.3), postoji i $f(X) = g(X)q_1(X)+ r_1(X)$, $\deg(r_1(X)) < \deg(g(X))$.
Tada je

$$g(X)(q_1(X) - q(X)) = r(X) - r_1(X).$$

Kako je $g(X)$ normirani polinom, tada je

$$\deg(g(X)) + \deg(q_1(X) - q(X)) = \deg(r(X) - r_1(X)) < \deg(g(X)).$$

Iz toga slijedi da je $\deg(q_1(X) - q(X)) = -\infty$, odnosno $q_1(X) = q(X)$. To povlači da je $r_1(X) = r(X)$, čime smo dokazali jedinstvenost. □

Korolar 1.9.5. *Neka je R komutativan prsten s jedinicom i neka je $a \in R$. Tada je za svaki $f(X) \in R[X]$*

$$f(X) = (X - a)q(X) + f(a)$$

za neki $q(X) \in R[X]$.

Teorem 1.9.6. *Neka je F polje. Tada je $F[X]$ domena glavnih ideala.*

Dokaz. Neka je I ideal u $F[X]$.
Ako je $I = \{0\}$, tada je I glavni ideal. Pretpostavimo da je $I \neq \{0\}$. Uzmimo $g(X) \in I$ takav da $g(X) \neq 0$ i $\deg(g(X)) \leq \deg(f(X))$, za svaki $f(X) \in I \setminus \{0\}$. Tvrdimo: $I = \langle g(X) \rangle$. Kako je F polje, $g(X)$ možemo množiti s elementom iz F tako da dobijemo normirani polinom, koji je također u I. Zato možemo pretpostaviti da je $g(X)$ normirani polinom koji je također iz I.
Neka je $f(X) \in I$. Tada je, prema teoremu 1.9.4,

$$f(X) = g(X)q(X) + r(X), \ \deg(r(X)) < \deg(g(X)).$$

Ali, $r(X) = f(X) - g(X)q(X)$, pa zbog izbora $g(X)$, $r(X) = 0$. Znači, $f(X) = g(X)q(X) \in I$, $I = \langle g(X) \rangle$ pa je $F[X]$ domena glavnih ideala. □

Teorem 1.9.7 (Hilbertov teorem o bazi)**.** *Neka je R komutativni prsten s jedinicom u kojemu je svaki ideal konačno generiran. Tada je svaki ideal u prstenu polinoma $R[X]$ također konačno generiran.*

Dokaz. Uočimo da je $\langle 0 \rangle \subseteq R[X]$ konačno generiran pa neka je $I \subseteq R[X]$, $I \neq \langle 0 \rangle$. Prisjetimo se, s $\mathrm{lc}(f(X))$ označili smo vodeći koeficijent od $f(X) \in R[X], f(X) \neq 0$.
Neka je $f(X) \in R[X], f(X) \neq 0$. Za $n = 0, 1, 2, \ldots$ neka je

$$I_n = \{a \in R : \mathrm{lc}(f(X)) = a \text{ za neke } f(X) \in I \text{ stupnja } n\} \cup \{0\}.$$

Uočimo da je za svaki n, I_n ideal u R. Budući da je

$$\mathrm{lc}(f(X)) = \mathrm{lc}(X(f(X)),$$

slijedi da je $I_n \subseteq I_{n+1}$ za svaki n.
Neka je $J = \bigcup_{n=0}^{\infty} I_n$. Tada je J ideal u R i J je konačno generiran. Obzirom da J konačno generiran, $J = I_n$ za neki n.
Neka je $0 \leq m \leq n$ i neka skup $\{a_{m1}, a_{m2}, \ldots, a_{mk_m}\}$ generira I_m.
Izaberimo $f_{mj}(X) \in I$ takav da

$$\deg(f_{mj}(X)) = m \text{ i } \mathrm{lc}(f_{mj}(X)) = a_{mj},$$

za $0 \leq m \leq n$, $1 \leq j \leq k_m$.
Neka je

$$\hat{I} = \langle f_{mj}(X) : 0 \leq m \leq n, 1 \leq j \leq k_m \rangle.$$

Pokazat ćemo da je $\hat{I} = I$.
Pretpostavimo da je $f(X) \in I$.
Ako je $f(X) = 0$ ili $\deg(f(X)) = 0$, tada je $f(X) \in \hat{I}$ pa pretpostavimo da je $\deg(f(X)) = r > 0$ i dokažimo indukcijom po r da je $I \subseteq \hat{I}$.
Neka je a jednak vodećem koeficijentu od $f(X)$, odnosno $a = \mathrm{lc}(f(X))$.
Ako je $r \leq n$, tada je $a \in I_r$ pa možemo napisati

$$a = c_1 a_{r1} + c_2 a_{r2} + \cdots + c_{k_r} a_{rk_r}.$$

Tada je $\mathrm{lc}(\sum_{i=1}^{k_r} c_i f_{ri}(X)) = a$.
Budući da su $f(X)$ i $\sum_{i=1}^{k_r} c_i f_{ri}(X)$ istog stupnja i imaju jednak vodeći koeficijent, to je

$$\deg(f(X) - \sum_{i=1}^{k_r} c_i f_{ri}(X)) < r.$$

Indukcijom po r možemo zaključiti da je $f(X) - \sum_{i=1}^{k_r} c_i f_{ri}(X) \in \hat{I}$ pa je i $f(X) \in \hat{I}$, u slučaju $r \leq n$.
Ako je $r > n$, tada je $a \in I_r = I_n$, odnosno a možemo zapisati kao

$$a = c_1 a_{n1} + c_2 a_{n2} + \cdots + c_{k_n} a_{nk_n}.$$

Tada je, slično kao u prethodnom slučaju,

$$\deg(f(X) - \sum_{i=1}^{k_n} c_i X^{r-n} f_{ni}(X)) < r$$

te je, induktivno po r, $f(X) \in \hat{I}$.
Ovime smo dokazali da je $I \subseteq \hat{I}$. Jasno je da je $\hat{I} \subseteq I$ pa je $I = \hat{I}$.
Time smo dokazali da je I konačno generiran. □

Navedimo još ova dva rezultata koja direktno slijede iz Hilbertovog teorema o bazi:

Korolar 1.9.8. *Neka je R komutativan prsten s jedinicom u kojemu je svaki ideal konačno generiran. Tada je svaki ideal u $R[X_1, X_2, \ldots, X_n]$ konačno generiran.*

Korolar 1.9.9. *Neka je F polje. Tada je svaki ideal u prstenu polinoma $F[X_1, X_2, \ldots, X_n]$ konačno generiran.*

1.10 Domena jedinstvene faktorizacije

Proučavat ćemo domene jedinstvene faktorizacije. Domenu jedinstvene faktorizacije nazivamo još i faktorijalni prsten.

Definicija 1.10.1. *Integralnu domenu R nazivamo domena jedinstvene faktorizacije, ako svaki nenul element a iz R možemo jednoznačno napisati kao $a = up_1p_2 \cdots p_r$, gdje je u inveritibilni element, a svaki p_i je ireducibilni element u R. Rastav je jedinstven, odnosno, ako je $a = vq_1q_2 \cdots q_s$, gdje je v invertibilan, a svaki q_j ireducibilan, tada je $r = s$ i nakon permutiranja, (ukoliko je potrebno) q_i je asociran s p_j. Također, a možemo zapisati kao*

$$a = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t},$$

gdje p_i nije asociran s p_j za $i \neq j$. Za svaki p_i kažemo da je prosti faktor od a.

Lema 1.10.2. *Neka je R domena jedinstvene faktorizacije. Element $a \in R$ je ireducibilan ako i samo ako je prost.*

Dokaz. Pretpostavimo da je a ireducibilan i da $a|bc$. Tada je $ad = bc$ za neki $d \in R$. Kako je R domena jedinstvene faktorizacije, b, c možemo zapisati kao produkt:

$$au_1d_1d_2 \cdots d_r = u_2b_1b_2 \cdots b_su_3c_1c_2 \cdots c_t,$$

gdje su svaki b_i, c_j i d_k ireducibilni i svaki u_l je invertibilan. Kako je faktorizacija od bc jedinstvena, slijedi da je a asociran s nekim b_i ili c_j, što znači da $a|b$ ili $a|c$. □

Faktorizacija u prstenu polinoma

Pokazat ćemo da ako je R domena jedinstvene faktorizacije, tada je $R[X]$ također domena jedinstvene faktorizacije.

Definicija 1.10.3. *Neka je R domena jedinstvene faktorizacije i neka je $f(X) \in R[X]$, $f(X) \neq 0$. Najveći zajednički djelitelj koeficijenata od $f(X)$ nazivamo sadržaj od $f(X)$ i označavamo s* $\operatorname{cont}(f(X))$. *Polinom $f(X)$ nazivamo primitivni polinom ako je* $\operatorname{cont}(f(X)) = 1$.

Lema 1.10.4 (Gaussova lema)**.** *Neka je R domena jedinstvene faktorizacije i neka su $f(X)$, $g(X)$ nenul polinomi u $R[X]$. Tada je*

$$\operatorname{cont}(f(X)g(X)) = \operatorname{cont}(f(X)) \operatorname{cont}(g(X)).$$

Posebno, ako su $f(X)$ i $g(X)$ primitivni, onda je produkt $f(X)g(X)$ primitivan.

Dokaz. Napišimo $f(X) = \operatorname{cont}(f(X))f_1(X)$ i $g(X) = \operatorname{cont}(g(X))g_1(X)$, gdje su $f_1(X)$ i $g_1(X)$ primitivni polinomi. Tada je

$$f(X)g(X) = \operatorname{cont}(f(X)) \operatorname{cont}(g(X))f_1(X)g_1(X).$$

Pokazat ćemo da je produkt $f_1(X)g_1(X)$ primitivan.
Neka su

$$f_1(X) = a_0 + a_1X + \cdots + a_mX^m \text{ i}$$

$$g_1(X) = b_0 + b_1X + \cdots + b_nX^n,$$

i pretpostavimo da koeficijenti od $f_1(X)g_1(X)$ imaju zajednički djelitelj d koji nije invertibilan. Neka je p prosti djelitelj od d. Tada p mora dijeliti sve koeficijente od $f_1(X)g_1(X)$, ali budući da su $f_1(X)$ i $g_1(X)$ primitivni, p ne dijeli sve koeficijente od $f_1(X)$ i ne dijeli sve koeficijente od $g_1(X)$.
Neka je a_r prvi koeficijent od $f_1(X)$ kojeg p ne dijeli i neka je b_s prvi koeficijent od g_1 kojeg p ne dijeli. Promatrajmo onda koeficijente od X^{r+s} produkta $f_1(X)g_1(X)$. Ti koeficijenti su oblika

$$a_rb_s + (a_{r+1}b_{s-1} + a_{r+2}b_{s-2} + \cdots) + (a_{r-1}b_{s+1} + a_{r-2}b_{s+2} + \cdots).$$

Kako p dijeli ovu sumu i p dijeli svaki a_i, $i < r$ te p dijeli svaki b_j, $j < s$, dobijemo da $p|a_r b_s$, a kako je p prost, $p|a_r$ ili $p|b_s$, što je kontradikcija s pretpostavkom, odnosno produkt $f_1(X)g_1(X)$ je primitivan. □

Lema 1.10.5. *Neka je R domena jedinstvene faktorizacije s poljem kvocijenata F. Ako je $f(X) \in F[X]$, $f(X) \neq 0$, tada je $f(X) = \alpha f_1(X)$, gdje je $\alpha \in F$ i $f_1(X)$ je primitivni polinom u $R[X]$. Faktorizacija je jedinstvena do na množenje s invertibilnim elementom iz R.*

Dokaz. Napišimo $f(X) = \frac{1}{d}\tilde{f}(X)$, gdje je $\tilde{f}(X) \in R[X]$, a d zajednički nazivnik nenul koeficijenata od $f(X)$. Neka je $\alpha = \frac{\text{cont}(\tilde{f}(X))}{d} = \frac{c}{d} \in F$. Iz toga slijedi da je $f(X) = \alpha f_1(X)$, gdje je $f_1(X)$ primitivni polinom.
Dokažimo sada jedinstvenost.
Pretpostavimo da $f(X)$ možemo zapisati i kao $\beta f_2(X)$, gdje je $f_2(X)$ primitivni polinom u $R[X]$, a $\beta = \frac{a}{b}$. Tada

$$adf_2(X) = cbf_1(X) \Rightarrow ad = ucb \Rightarrow uf_2(X) = f_1(X),$$

gdje je $u \in R$ invertibilni element. □

Lema 1.10.6. *Pretpostavimo da je R domena jedinstvene faktorizacije s poljem kvocijenata F. Ako $f(X) \in R[X]$ pozitivnog stupnja i ireducibilan u $R[X]$, tada je $f(X)$ ireducibilan u $F[X]$.*

Dokaz. Ako je $f(X) \in R[X]$ pozitivnog stupnja i ireducibilan u $R[X]$, tada je $f(X)$ primitivan.
Pretpostavimo da je $f(X)$ reducibilan u $F[X]$. Tada je $f(X) = g_1(X)g_2(X)$, gdje su $g_i \in F[X]$ i $\deg(g_i(X_i)) > 0$, za $i = 1, 2$. Tada je $g_i(X) = \alpha_i f_i(X)$, gdje je $\alpha_i \in F$ i $f_i(X) \in R[X]$ je primitivan i

$$f(X) = \alpha_1\alpha_2 f_1(X)f_2(X).$$

Prema Gaussovoj lemi 1.10.4, $f_1(X)f_2(X)$ je primitivan, a prema lemi 1.10.5 $f(X)$ i $f_1(X)f_2(X)$ različiti su do na množenje invertibilnim elementom iz R, što je u

kontradikciji s ireducibilnošću $f(X)$ u $R[X]$. Zaključujemo da je $f(X)$ ireducibilan u $F[X]$. □

Teorem 1.10.7. *Ako je R domena jedinstvene faktorizacije, tada je i $R[X]$ domena jedinstvene faktorizacije.*

Dokaz. Neka je F polje kvocijenata od R i neka je $f(X) \in R[X]$, $f(X) \neq 0$. Kako je $F[X]$ domena jedinstvene faktorizacije, možemo napisati

$$f(X) = p_1(X)p_2(X)\cdots p_r(X),$$

gdje su $p_i \in F[X]$ ireducibilni polinomi za $1 \leq i \leq r$. Prema lemi 1.10.5, $p_i(X) = \alpha_i q_i(X)$, gdje je $\alpha_i \in F$ i $q_i(X) \in R[X]$ primitivni polinom.
Onda je

$$f(X) = cq_1(X)q_2(X)\cdots q_r(X),$$

gdje je $c = \alpha_1\alpha_2\cdots\alpha_r \in F$. Neka je $c = \frac{a}{b}$, $a, b \in R$. Tada, prema Gaussovoj lemi imamo

$$\operatorname{cont}(bf(X)) = \operatorname{cont}(aq_1(X)q_2(X)\cdots q_r(X)) = a,$$

odnosno $b\operatorname{cont}(f(X)) = a$ pa $b|a$ i $\operatorname{cont}(f(X)) = c \in R$.
Svaki $q_i(X)$ je ireducibilan u $F[X]$, pa je ireducibilan i u $R[X]$. Kako je R domena jedinstvene faktorizacije, napišimo $c = ud_1d_2\cdots d_s$, gdje je svaki d_i prost u R i $u \in R$ je invertibilan. Tada je

$$f(X) = ud_1d_2\cdots d_sq_1(X)q_2(X)\cdots q_r(X),$$

odnosno $f(X)$ je produkt ireducibilnih elemenata iz $R[X]$.
Trebamo još dokazati jedinstvenost faktorizacije. Pretpostavimo da je

$$f(X) = vb_1b_2\cdots b_tq_1'(X)q_2'(X)\cdots q_k'(X),$$

gdje je svaki q_i' primitivni polinom u $R[X]$, a svaki b_i ireducibilan u R. Kako je to faktorizacija i u $F[X]$, onda je $r = k$ i svaki q_i je asociran s q_i'. No kako su primitivni polinomi asocirani u $F[X]$, tada su asocirani i u $R[X]$. Nadalje,

$$\operatorname{cont}(f(X)) = vb_1b_2\cdots b_t = ud_1d_2\cdots d_s,$$

pa, jer je R domena jedinstvene faktorizacije, $s = t$ i b_i je asociran s d_i. □

Za kraj ovog poglavlja, dokazat ćemo Eisensteinov kriterij.

Teorem 1.10.8 (Eisensteinov kriterij)**.** *Neka je R domena jedinstvene faktorizacije s poljem kvocijenata F. Neka je $f(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$, $a_n \neq 0$ i pretpostavimo da je $p \in R$ prost element takav da*

(1) *p ne dijeli a_n,*

(2) *p dijeli a_i, za $0 \leq i \leq n-1$,*

(3) *p^2 ne dijeli a_0.*

Tada je $f(X)$ ireducibilan u $F[X]$.

Dokaz. Bez smanjenja općenitosti možemo pretpostaviti da je $f(x)$ primitivni polinom. Ukoliko postoji faktorizacija od $f(x)$ u faktore stupnja većeg ili jednakog 1 u $F[X]$, tada prema lemi 1.10.6 postoji faktorizacija u $R[X]$.
Pretpostavimo da možemo zapisati $f(X) = g(X)h(X)$, gdje su $g(X), h(X) \in R[X]$. Tada su, prema Gaussovoj lemi 1.10.4 $f(X)$ i $g(X)$ primitivni polinomi. Pretpostavimo da je

$$g(X) = b_0 + b_1X + \cdots + b_lX^l$$

$$h(X) = c_0 + c_1X + \cdots + c_mX^m$$

takvi da su $l, m \geq 1$, $b_lc_m \neq 0$ i $l + m = n$. Kako $p|a_0 = b_0c_0$, ali p^2 ne dijeli a_0, slijedi da $p|b_0$ ili $p|c_0$, ali ne dijeli oboje.
Pretpostavimo da $p|b_0$ i da p ne dijeli c_0. Kako je $g(X)$ primitivan, tada nisu svi koeficijenti od $g(X)$ djeljivi s p. Neka je b_i prvi koeficijent od $g(X)$ koji nije djeljiv s p, $0 < i \leq l < n$. Tada je

$$a_i = b_ic_0 + b_{i-1}c_1 + \cdots + b_0c_i.$$

Kako $p|a_i$ i $p|b_j$ za $j < i$, tada $p|b_ic_0$. Ali kako p ne dijeli b_i i p ne dijeli c_0, dolazimo do kontradikcije, i zaključujemo da je $f(X)$ ireducibilan u $F[X]$. □

Korolar 1.10.9. *Neka je p prost broj i neka je $f_p(X) \in \mathbb{Q}[X]$,*

$$f_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 = \frac{X^p - 1}{X - 1}.$$

Tada je $f_p(X)$ ireducibilan.

Dokaz. Budući da je preslikavanje $g(X) \mapsto g(X+1)$ izomorfizam prstenova $\mathbb{Q}[X] \to \mathbb{Q}[X]$, dovoljno je pokazati da je $f_p(X+1)$ ireducibilan. Lako se pokaže da p dijeli svaki binomni koeficijent $\binom{p}{k}$, za $1 \leq k < p$ pa je

$$f_p(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = X^{p-1} + pX^{p-2} + \cdots + p.$$

$f_p(X+1)$ zadovoljava Eisensteinov kriterij, čime smo dokazali korolar.

□

Poglavlje 2

Moduli

Pojam vektorskog prostora nad poljem poznat nam je iz linearne algebre. Module nad prstenovima možemo shvatiti kao generalizaciju vektorskih prostora nad poljem. U ovom poglavlju obradit ćemo osnovna svojstva vezana za module te posebno obraditi module koji imaju bazu, odnosno slobodne module.

2.1 Osnovne definicije i teoremi iz teorije modula

Definicije

Definicija 2.1.1. *Neka je R prsten s jedinicom.*

1. *Lijevi R-modul je Abelova grupa zajedno s operacijom skalarnog množenja $\cdot : R \times M \to M$, koja za sve elemente a, b iz R i m, n iz M zadovoljava sljedeće aksiome:*

   (i) $a(m+n) = am + an$

   (ii) $(a+b)m = am + bm$

   (iii) $(ab)m = a(bm)$

   (iv) $1m = m.$

2. *Desni R-modul je Abelova grupa zajedno s operacijom skalarnog množenja $\cdot : M \times R \to M$, koja za sve elemente a, b iz R i m, n iz M zadovoljava sljedeće aksiome:*

   (i) $(m+n)a = ma + na$

   (ii) $m(a+b) = ma + mb$

   (iii) $m(ab) = (ma)b$

   (iv) $m1 = m.$

U daljnjem tekstu, osim ako drugačije ne naznačimo, pisat ćemo i dokazivati tvrdnje za lijevi R-modul, pri tome ćemo pisati samo R-modul, a sve tvrdnje i dokazi vrijedit će i za desni R-modul.

Homomorfizmi modula, slično kao i kod prstenova, su korisna preslikavanja jer poštuju strukturu modula:

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

$$f(m_1 + m_2) = f(m_1) + f(m_2),\ m_1, m_2 \in M$$

i

$$f(am) = af(m),\ a \in R, m \in M.$$

Primjer 2.1.3. *Neka je G Abelova grupa i neka je $g \in G$. Za $n \in \mathbb{Z}$ definirajmo skalarno množenje ng s*

$$ng = \begin{cases} g + g + \cdots + g, & (n \text{ puta}) \text{ za } n > 0 \\ 0, & \text{ako je } n = 0 \\ (-g) + (-g) + \cdots + (-g), & (-n \text{ puta}) \text{ za } n < 0. \end{cases}$$

Uz ovakvo skalarno množenje, G je $\mathbb{Z}$-modul. Štoviše, ako su G i H Abelove grupe i $f : G \to H$ je homomorfizam grupa, tada je f homomorfizam $\mathbb{Z}$-modula (jer je $f(ng) = f(g + g + \cdots + g) = f(g) + f(g) + \cdots + f(g) = nf(g)$ i $f(-g) = -f(g)$.)

Primjer 2.1.4. *Neka je R prsten i $I \subseteq R$. Tada je kvocijentni prsten R/I lijevi R-modul i desni R-modul s preslikavanjima zadanima s*

$$R \times R/I \to R/I$$
$$(a, b + I) \mapsto ab + I$$

i

$$R/I \times R \to R/I$$
$$(a + I, b) \mapsto ab + I.$$

Definicija 2.1.5. *1. Neka je F polje. Tada F-modul V nazivamo vektorski prostor nad F.*

2. Ako su V i W vektorski prostori nad poljem F, tada je linearna transformacija s V u W homomorfizam F-modula s V u W.

Definicija 2.1.6. *Neka je R prsten i M R-modul. Za N podskup od M kažemo da je podmodul (ili R-podmodul) od M ako je N podgrupa aditivne grupe M s obzirom na istu operaciju skalarnog množenja na M.*

Neka je M R-modul i neka je $N \subseteq M$ podmodul. M/N je tada kvocijentna podgrupa. Definirajmo skalarno množenje na M/N s

$$a(m + N) = am + N,\ a \in R, m + N \in M/N.$$

Ako je $m + N = m' + N$, tada je $m - m' \in N$ pa je $am - am' = a(m - m') \in N$, odnosno $am + N = am' + N$.
Stoga je M/N R-modul i nazivamo ga kvocijentni modul M po podmodulu N.

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

Definicija 2.1.8. *Kažemo da je R-modul M konačno generiran ako je $M = \langle S \rangle$ za neki konačni podskup S od M. M je ciklički ako je $M = \langle m \rangle$ za neki element $m \in M$. Ako je M konačno generiran, označimo s $\mu(M)$ minimalni broj generatora od M. Ako M nije konačno generiran, definirajmo $\mu(M) = \infty$. $\mu(M)$ nazivamo dimenzija od M.*

Ako je R domena glavnih ideala, tada je svaki R-podmodul M od R ideal pa je $\mu(M) = 1$.

Definicija 2.1.9. *Ako je R prsten, M R-modul i X je podskup od M, tada anihilator od X, u oznaci* $\mathrm{Ann}(X)$*, definiramo s*

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

Lako se provjeri da je $\mathrm{Ann}(X)$ lijevi ideal u R, štoviše, ako je $X = N$ podmodul od M, tada je $\mathrm{Ann}(N)$ ideal u R. Ako je R komutativan i $N = \langle x \rangle$ ciklički podmodul od M s generatorom x, tada je anihilator elementa x jednak

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

Definicija 2.1.10. *Neka je R integralna domena i neka je M R-modul. Kažemo da je element $x \in M$ torzioni element ako je* $\mathrm{Ann}(x) \neq \{0\}$.

Element $x \in M$ je torzioni element ako i samo ako postoji $a \neq 0 \in R$ takav da je $ax = 0$.
Neka je M_τ skup svih torzionih elemenata od M. Za M ćemo reći da je torziono slobodan ako je $M_\tau = \{0\}$. M je torzioni modul ako je $M = M_\tau$.

Propozicija 2.1.11. *Neka je R integralna domena i neka je M R-modul.*

1. *M_τ je podmodul od M i nazivamo ga torzioni podmodul.*

2. *M/M_τ je torziono slobodan.*

Dokaz. 1. Neka su $x, y \in M_\tau$ i neka je $c, d \in R$. Tada postoje $a \neq 0, b \neq 0 \in R$ takvi da je $ax = 0$ i $by = 0$. Kako je R integralna domena, $ab \neq 0$. Onda je

$$ab(cx + dy) = (bc(ax) + ad(by) = 0$$

pa je $cx + dy \in M_\tau$.

2. Pretpostavimo da je $a \neq 0 \in R$ i $a(x + M_\tau) = 0 \in (M/M_\tau)_\tau$. Tada je $ax \in M_\tau$ a postoji $b \neq 0 \in R$ takav da je $(ba)x = b(ax) = 0$. Kako je $ba \neq 0$, slijedi da je $x \in M_\tau$, odnosno $x + M_\tau = 0 \in M/M_\tau$.

□

2.2 Teoremi o izomorfizmima modula

Teoreme o izomorfizmima modula navodima bez dokaza, koji se mogu pronaći u [1].

Teorem 2.2.1 (Prvi teorem o izomorfizmu modula)**.** *Neka su M, N R-moduli i neka je $f : M \to N$ homomorfizam R-modula. Tada je*

$$M/\operatorname{Ker}(f) \cong \operatorname{Im}(f).$$

Teorem 2.2.2 (Drugi teorem o izomorfizmu modula)**.** *Neka je M R-modul i neka su N, P podmoduli. Tada postoji izomorfizam R-modula*

$$(N + P)/P \cong N/(N \cap P).$$

Teorem 2.2.3 (Treći teorem o izomorfizmu modula)**.** *Neka je M R-modul i neka su N i P podmoduli od M takvi da je $P \subseteq N$. Tada je*

$$M/N \cong (M/P)/(N/P).$$

2.3 Slobodni moduli

Vektorski prostor nad poljem uvijek ima bazu. Za module to nije uvijek istinito. U ovom odjeljku proučavat ćemo module koji imaju bazu.

Definicija 2.3.1. *Neka je R prsten i neka je M R-modul. Za S podskup od M kažemo da je R-linearno zavisan ako postoje međusobno različiti $x_1, x_2, \ldots, x_n$ iz S i elementi $a_1, a_2, \ldots, a_n$ iz R, koji nisu svi jednaki 0, takvi da*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0.$$

Za skup koji nije R-linearno zavisan kažemo da je R-linearno nezavisan.

Definicija 2.3.2. *Neka je M R-modul. Podskup S od M je baza od M ako S generira M kao R-modul i ako je S R-linearno nezavisan.*

Drugim riječima, $S \subseteq M$ je baza ako i samo ako je

1. $M = \{0\}$ pa je $S = \emptyset$ baza; ili
2. $M \neq \{0\}$ pa je $S \subseteq M$ baza od M ako i samo ako svaki $x \in M$ možemo jedinstveno napisati kao $x = a_1x_1 + \cdots + a_nx_n$, $x_1, x_2, \ldots, x_n \in S$ i $a_1, a_2, \ldots, a_n \in R$.

Definicija 2.3.3. *R-modul M je slobodan R-modul ako ima bazu.*

Primjer 2.3.4. *$M_{m,n}(R)$ je slobodan R-modul s bazom*

$$S = \{E_{ij} : 1 \leq i \leq m, 1 \leq j \leq n\}.$$

Primjer 2.3.5. *Prsten $R[X]$ je slobodan R-modul s bazom $\{X^n : n \in \mathbb{Z}^+\}$. Također, $R[X]$ je slobodan $R[X]$-modul s bazom $\{1\}$.*

Propozicija 2.3.6. *Neka je R integralna domena i neka je M slobodan R-modul. Tada je M torziono slobodan.*

Dokaz. Neka je $S = \{x_j\}_{j\in J}$ baza od M i neka je $x \in M_\tau$. Tada je $ax = 0$ za neki $a \neq 0 \in R$. Napišimo $x = \sum_{j\in J} a_j x_j$. Tada je

$$0 = ax = \sum_{j\in J} (aa_j)x_j.$$

Budući da je S baza od M, $aa_j = 0$ za svaki $j \in J$, a jer je $a \neq 0$ i R integralna domena, zaključujemo da je $a_j = 0$ za svaki $j \in J$.
Iz toga slijedi da je $x = 0$ i $M_\tau = \langle 0 \rangle$ pa je M torziono slobodan. □

Teorem 2.3.7. *Neka je D prsten s dijeljenjem i neka je V D-modul. Tada je V slobodan D-modul. Posebno, svaki vektorski prostor V ima bazu.*

Dokaz. Neka je S generira V i neka je $B_0 \subseteq S$ linearno nezavisan skup od S. Neka je $\mathcal{T}$ parcijalno uređen skup svih linearno nezavisnih podskupova od S koji sadrže B_0, uređen skupovnom inkluzijom. Ako je $\{B_i\}$ niz u $\mathcal{T}$, tada je $\cup B_i$ linearno nezavisan podskup od S koji sadrži B_0, odnosno svaki niz u $\mathcal{T}$ ima gornju među. Prema Zornovoj lemi, postoji maksimalni element u $\mathcal{T}$. Neka je B maksimalni linearno nezavisni podskup od S koji sadrži B_0. Tvrdimo da je $S \subseteq \langle B \rangle$, takav da je $V = \langle S \rangle \subseteq \langle B \rangle$. Neka je $v \in S$. Kako je B maksimalan, tada je $V \cup \{v\}$ linearno zavisan pa je

$$\sum_{i=1}^{m} a_i v_i + bv = 0,$$

gdje su $v_1, v_2, \ldots, v_m$ međusobno različiti elementi u B i $a_1, a_2, \ldots a_m, b \in D$ nisu svi 0. Ako bi b bio jednak 0, slijedilo bi da je $\sum_{i=1}^{m} a_i v_i = 0$. Kako nisu svi $a_i = 0$, to je u kontradikciji s linearnom nezavisnošću od B, odnosno $b \neq 0$ i zaključujemo da je

$$v = b^{-1}(bv) = \sum_{i=1}^{m} (-b^{-1}a_i)v_i \in \langle B \rangle.$$

Tada je $S \subseteq \langle B \rangle$ što povlači da je B baza od V.

□

Bibliografija

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

[2] K. Horvatić, *Linearna algebra*, sv. I, Matematički odjel PMF-a, Sveučilište u Zagrebu, Zagreb, 1999.

[3] B. Širola, *Algebarske strukture*, `http://web.math.pmf.unizg.hr/nastava/alg/predavanja/ASpred.pdf`, lipanj 2014.

[4] H. Kraljević, *Algebra*, `http://web.math.pmf.unizg.hr/~hrk/nastava/2006-07/algebra_Osijek_2006_7.pdf`, lipanj 2014.

Sažetak

U ovom radu napravljen je pregled osnovnih koncepata komutativnih prstenova i modula.
Nakon definicija i osnovnih teorema iz teorije prstenova, u radu se baziramo na komutativne prstenove i definiramo domene glavnih ideala, euklidske domene, domene jedinstvene faktorizacije te dokazujemo teoreme iz tog područja. Poseban naglasak dan je na prstenu polinoma i njegovim svojstvima.
Drugi dio rada posvećen je modulima. Osim osnovnih definicija iz teorije modula, obrađujemo i slobodne module.

Summary

This paper presents an overview of basic concepts concerning commutative rings and modules.
Following definitions and basic theorems from ring theory, this paper is focused on commutative rings and definitions of principal ideal domains, Euclidean domains, unique factorization domains completed with proofs of said theorems. A particular emphasis is given to polynomial ring and its attributes.
Second part of this paper is dedicated to modules. Apart from basic definitions from module theory, focus is given to free modules.

Životopis

Autorica ovog rada rođena je 17. siječnja 1984. godine u Virovitici, gdje je završila Osnovnu školu Vladimira Nazora i prirodoslovno - matematički smjer Gimnazije Petra Preradovića. Na Prirodoslovno - matematičkom fakultetu, Matematičkom odsjeku u Zagrebu završila je preddiplomski studij edukacije matematike i upisala diplomski studij Matematika i informatika: smjer nastavnički.