Univerzitet u Beogradu
Matematički fakultet

Zoran S. Pucanović

PRSTENI SA JEDNOZNAČNOM FAKTORIZACIJOM

magistarski rad

Beograd
2002.

Sadržaj

Glava 0

Uvod i istorijski osvrt

Jednoznačna faktorizacija u prstenu $\mathbb{Z}$ je opštepoznata osobina koju često i nesvesno koristimo pri radu sa celim brojevima. Još je Euklid znao da se svaki ceo broj na jedinstven način predstavlja u obliku $up_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$, gde su p_i medjusobno različiti prosti brojevi i $u = 1$ ili $u = -1$. Ovo svojstvo rad sa celim brojevima čini udobnim i lakim. Dodajući prstenu celih brojeva rešenje jednačine $x^2 + 1 = 0$, Gauss je 1828. pokazao da ista osobina važi i u prstenu $\mathbb{Z}[i]$. Jednoznačna faktorizacija čini lakim račun u ovom prstenu kao i u prstenu $\mathbb{Z}$. Prirodno se dalje nametnulo pitanje da li će isto važiti i prstenu $\mathbb{Z}[\zeta]$, gde je ζ koren nekog polinoma iz $\mathbb{Z}[x]$. Ovo pitanje blisko je povezano sa rešavanjem Fermaove poslednje teoreme, naime neke njene specijalne slučajeve Kummer je rešio podrazumevajući jednoznačnu faktorizaciju u prstenu $\mathbb{Z}[\omega]$, gde je ω koren iz jedinice. Ključna stvar u dokazu je da se jednačina $x^n + y^n = z^n$, može, u tom slučaju, faktorisanjem leve strane, napisati u obliku:

$$(x + y)(x + \omega y)\dots(x + \omega^{n-1}y) = z^n\,,$$

pa se poredjenjem ovih faktorizacija može, relativno lako, dobiti željeni rezultat. Problem sa ovim dokazom je medjutim u tome što $\mathbb{Z}[\omega]$ ne mora imati jednoznačnu faktorizaciju, npr. za $n = 23$. Jednoznačna faktorizacija elemenata u proizvod ireducibilnih nije moguća ni u mnogim drugim prstenima ovog oblika, npr. u $\mathbb{Z}[\sqrt{10}\,]$, $\mathbb{Z}[\sqrt{-17}\,]$. Tražeći neku vrstu generalizacije jednoznačne faktorizacije koja će važiti u ovim prstenima Kummer uvodi pojam "idealnih brojeva". Rešavajući isti problem, Dedekind dolazi na ideju da umesto elementa a prstena R posmatra sve njegove umnoške $(a) = \{ar \mid r \in R\}$ i uvodi 1871. pojam ideala. Savremena algebra ne može se zamisliti bez ovog pojma, pa se može reći da je početak moderne algebre povezan upravo sa rešavanjem problema faktorijalnosti. Dedekind je dokazao da se da se u ovim prstenima svaki ideal može jednoznačno razložiti u proizvod prostih ideala i našao uslove pod kojima će dati prsten R imati ovu osobinu. U njegovu čast domeni u kojima se svaki ideal jednoznačno razlaže u proizvod prostih ideala, zovu se *Dedekindovi domeni.* Dalje je razvoj algebarske geometrije uslovio rad sa prstenima polinoma $k[x_1, x_2, \dots, x_n]$, gde je k algebarski zatvoreno polje. Kako ovi prsteni

nisu Dedekindovi za $n > 1$, za ideale ne važe prethodna tvrdjenja. Tražeći neku drugu vrstu razlaganja neophodno je proizvode zameniti presecima ideala. Ovo vodi u drugi tip generalizacije jednoznačne faktorizacije tzv. *primarnu dekompoziciju ideala*. Lasker je 1905. pokazao da je svaki ideal prstena polinoma sa više neodredjenih presek konačno mnogo primarnih ideala. Ova dekompozicija nije medjutim jednoznačna. Emmy Noether je 1920. uvela uslove kidanja lanaca i na taj način objedinila Laskerove i Dedekindove rezultate. Pri tome je Neterin domen faktorijalan akko su njegovi minimalni prosti ideali glavni.

Iako suštinski različita, jednoznačna faktorizacija elemenata u faktorijalnim domenima i ideala u Dedekindovim domenima ima dosta zajedničkih osobina. Dalja uopštenja ovih osobina vode ka važnoj klasi *Krulovih domena* koja sadrži obe ove klase. Ovi domeni čuvaju neke od bitnih osobina faktorijalnih domena, dok se provera faktorijalnosti Krulovog domena A svodi se na računanje njegove *grupe divizor klasa* $Cl(A)$. Pri tome je Krulov domen A faktorijalan akko je $Cl(A) = 0$. Osim grupe divizor klasa, koja se može pridružiti svakom Krulovom domenu, proizvoljnom domenu A može se takodje pridružiti jedna grupa pomoću koje se mogu dobiti neke informacije vezane za faktorizaciju elemenata; to je tzv. *grupa valuacija*, u oznaci $G(A)$. Pri tome je domen A faktorijalan akko je $G(A)$ slobodna Abelova grupa. Ovo predstavlja potpuno drugačiji pristup pitanju jednoznačne faktorizacije; umesto klasičnih provera da li svaki element ima atomično razlaganje i da li je ono jedinstveno, može se prosto odrediti grupa $G(A)$, odnosno $Cl(A)$, ako je A Krulov. Na taj način pitanje jednoznačne faktorizacije u prstenu svodi se na tehnike računanja ovih grupa. Sama provera faktorijalnosti nekog domena, kao i odredjivanje ovih grupa, često je netrivijalno pitanje, pa je osim ovih, poželjno imati i druge kriterijume za proveru faktorijalnosti, kakvi su npr. *Nagatina i teorema Kaplanskog*.

Jednoznačna faktorizacija ima i svoju vezu sa algebarskom geometrijom. Koordinatni prsten neke mnogostrukosti V dimenzije n biće faktorijalan akko je svaka podmnogostrukost dimenzije $n - 1$ generisana glavnim idealom. S druge strane, ako posmatramo fiksiranu tačku $x \in V$, onda funkcije definisane u x formiraju *lokalan prsten* $\mathfrak{o}_x$. Pitanja faktorijalnosti ovih prstena obično se rešavaju homološkim metodama. Ako je x prosta tačka mnogostrukosti, onda je $\mathfrak{o}_x$ *regularan lokalan prsten*, koji mora biti faktorijalan.

Iz svega rečenog može se videti da je jednoznačna faktorizacija bitno svojstvo prstena. Cilj ovog rada sastoji se u preciznom opisu faktorijalnih prstena i njihovih veza sa drugim značajnim klasama prstena, kao i u opisu kriterijuma za proveru faktorijalnosti i nekim uopštenjima pojma jednoznačne faktorizacije. Rad je neposredno inspirisan programom seminara za Algebru Matamatičkog fakulteta u Beogradu. Pojedini delovi u tekstu, a posebno glava 5, oslanjaju se na teme obradjene na seminaru.

Glava 1 sadrži početne definicije jednoznačne faktorizacije u prstenu kao i veze faktorijalnih domena sa klasičnim domenima: Euklidovim, Gausovim, Bezuovim i glavnim domenima. U Glavi 2 posmatra se ponašanje faktorizacije u raširenjima prstena. Posebno se razmatraju tipična raširenja kao što su cela raširenja, polinomi, formalni redovi, lokalizacija i uslovi pod kojima se jednoznačna faktorizacija prenosi sa prstena na njegovo raširenje. Glava 3 sadrži

neke delove teorije uredjenih Abelovih grupa i valuacionih domena, potrebnih za opis grupe valuacija. Ističe se nova karakterizacija faktorijalnosti u zavisnosti od ove grupe i opisuju se karakteristike valuacija u faktorijalnim domenima. Glava 4 posvećena je faktorizaciji u Neterinim domenima. Dat je kriterijum faktorijalnosti, kao i izvesna uopštenja: primarna dekompozicija i jednoznačna faktorizacija ideala. Glava 5 predstavlja sintezu prethodnih glava. Uvodi se pojam divizorskih ideala i Krulovih domena. Dat je pregled osnovnih osobina Krulovih domena, konstrukcija njegove grupe divizor klasa $Cl(A)$ i nova definicija faktorijalnog domena bazirana na ovoj grupi. Glava 6 vezana je za neke homološke metode pri proveri faktorijalnosti. Data je veza CM, regularnih i regularnih lokalnih prstena sa faktorijalnim domenima uz naglasak na primenama u algebarskoj geometriji i prstenima formalnih redova. U Glavi 7, koja se bazira na [6], posmatra se nekomutativan slučaj i potpuno je nezavisna od prethodnih glava. Razmatra se problem definisanja nekomutativnog faktorijalnog domena koji bi naravno trebalo da sadrži komutativan slučaj, i daje se kratak prikaz osnovnih rezultata iz ove oblasti.

Glava 1

Faktorizacija u klasičnim domenima

1.1 Osnovni pojmovi i oznake

Ako se ne naglasi drugačije domen A biće komutativan prsten sa jedinicom bez delitelja nule. Invertibilne elemente domena A označavaćemo sa A^*.

Definicija 1.1.1. *Elementi a, b domena A su asocirani ako $\exists u \in A^*$ tako da je $a = ub$.*

Definicija 1.1.2. *Ideal P domena A je prost ako:*

$$P \neq A \quad i \quad ab \in P \Rightarrow (a \in P \vee b \in P)$$

Ekvivalentno je reći da je faktorprsten A/P domen.

Kako je u domenu nula ideal uvek prost, proste ideale različite od nule zvaćemo *pravim prostim idealima.*

Definicija 1.1.3. *Ideal M domena A je maksimalan ako je*

$$M \neq A \quad i \quad M \subseteq I \subseteq A \Rightarrow (I = M \vee I = A)$$

Ekvivalentno je reći da je faktorprsten A/M polje.

Definicija 1.1.4. *Za element $p \neq 0$ domena A kažemo da je atom ili da je ireducibilan ako:*

$$p \notin A^* \quad i \quad p = ab \Rightarrow a \in A^* \vee b \in A^*.$$

Definicija 1.1.5. *Za element $p \neq 0$ domena A kažemo da je prost ako:*

$$p \notin A^* \quad i \quad p \mid ab \Rightarrow p \mid a \vee p \mid b.$$

Ekvivalentna karakterizacija može se dati pomoću ideala:
Element $p \in A$ je prost akko je glavni ideal (p) pravi prost ideal.
Element $p \in A$ je atom akko je (p) maksimalan medju svim pravim glavnim idealima u A.

Tvrdjenje 1.1.6. *Prost element u domenu je ireducibilan.*

Dokaz. Neka je $p \in A$ prost tj. ideal (p) je pravi prost ideal. Neka je $(p) \subseteq (q) \subsetneqq A$. Tada je $p = qr$, za neko $r \in A$, pa $p \mid q$ *ili* $p \mid r$. Ako $p \mid r$ onda je $r = ps$ za neko $s \in A$, pa je $p = qps$, tj. $qs = 1$, odakle je $q \in A^*$. Odavde je $(q) = A$. Ako $p \mid q$ onda je $(q) \subseteq (p)$, odakle je $(p) = (q)$. Dakle jedini glavni ideali u kojima je (p) sadržan su $A = (1)$ i sam ideal (p). Ideal (p) maksimalan je medju glavnim idealima domena A, pa je p atom. $\square$
Veza prostih i ireducibilnih elemenata bitna je za faktorizaciju. Obratna implikacija u prethodnom tvrdjenju ne mora da važi što se može videti iz sledećih primera.

Primer 1.1.7.

$$A = \mathbb{Z}\left[\sqrt{-17}\ \right] = \{a + b\sqrt{-17} \mid a, b \in \mathbb{Z}\}$$

Za element $\alpha \in A$ definiše se njegova norma $N(\alpha) = N(x + y\sqrt{-17}) = x^2 + 17y^2$. Invertibilni elementi u A su oni sa normom ± 1. Jedina celobrojna rešenja jednačine $x^2 + 17y^2 = \pm 1$ su $x = \pm 1, y = 0$ pa je $A^* = \{1, -1\}$. Broj 2 je atom u A koji nije prost; U domenu A nema elemenata sa normom 2 jer jednačina $x^2 + 17y^2 = 2$ nema celobrojnih rešenja. Jedini delitelji elementa 2 su dakle asocirani s njim, jer:

$$2 = \alpha\beta \Rightarrow 4 = N(\alpha)N(\beta)$$

Odavde je $N(\alpha) = \pm 1$ ili $N(\beta) = \pm 1$ pa je 2 asociran sa α ili sa β , odnosno 2 je atom. Element 2 medjutim nije prost jer npr.

$$2 \mid 18 = (1 + \sqrt{-17})(1 - \sqrt{-17})$$

$$2 \nmid (1 + \sqrt{-17})\ ,\ 2 \nmid (1 - \sqrt{-17})$$

Poslednje važi zbog toga što su $1 + \sqrt{-17}$, $1 - \sqrt{-17}$ ireducibilni što se može videti poredjenjem normi, naime, ako je $1+\sqrt{-17} = \alpha\beta$ onda je $18 = N(\alpha)N(\beta)$. Mogućnosti su dakle $(N(\alpha), N(\beta)) = (\pm 1, \pm 18)$, $(N(\alpha), N(\beta)) = (\pm 2, \pm 9)$, $(N(\alpha), N(\beta)) = (\pm 3, \pm 6)$ ili obrnuto ako α i β zamene mesta. Kako jednačine $x^2+17y^2 = 2$, $x^2+17y^2 = 3$ nemaju rešenja u skupu celih brojeva pa mora biti $N(\alpha) = \pm 1$, odnosno $1 + \sqrt{-17}$ je atom. Analogno vidimo da je i $1 - \sqrt{-17}$ atom. Primetimo da je broj 2 koji je prost u prstenu $\mathbb{Z}$ prelaskom u $\mathbb{Z}\left[\sqrt{-17}\ \right]$ izgubio to svojstvo. Primetimo takodje da faktorizacija u ovom prstenu nije jednoznačna: $(1+\sqrt{-17})(1-\sqrt{-17})$, $2 \cdot 3 \cdot 3$ su dve različite atomičke faktorizacije broja 18. ▼

Primer 1.1.8.

$$A = k[X, Y, Z, T]/(XY - ZT)$$

Ovde je k proizvoljno polje i $A = k[x, y, z, t]$, gde su sa x, y, z, t označene odgovarajuće homomorfne slike: $x = X + I$, $y = Y + I$, $z = Z + I$, $t = T + I$, $I = (XY - ZT)$. A je prsten generisan elementima x, y, z, t nad poljem k koji su povezani relacijom:

$$xy = zt$$

Element x ovog prstena je atom koji nije prost jer iz generišuće relacije: $x \mid zt$, $x \nmid z$, $x \nmid t$. ▼

Primer 1.1.9.

$$A = \mathbb{Z}\left[2X, 2X^2, 2X^3, \dots\right]$$

Na A možemo gledati kao na potprsten prstena polinoma $\mathbb{Z}[X]$ u kome su koeficijenti uz X, X^2, ... parni. Kako $X \notin A$, elementi $2X\,, 2X^2\,, \dots$ su atomi ovog prstena. Nijedan od njih medjutim nije i prost, npr.

$$2X \mid 4X^2 = 2 \cdot 2X^2 \quad \text{ali} \quad 2\mathrm{X} \nmid 2\ ,\ 2\mathrm{X} \nmid 2\mathrm{X}^2$$

$$2X^2 \mid 4X^2 = 2X \cdot 2X \quad \text{ali} \quad 2\mathrm{X}^2 \nmid 2\mathrm{X}\ ▼$$

Primer 1.1.10.

$$A = \mathbb{Z} + X\mathbb{Q}[X]$$

A je potprsten prstena polinoma $\mathbb{Q}[X]$ čiji su elementi polinomi sa celim konstantnim koeficijentima. Nasuprot prethodnim primerima ovde se ne može svaki element faktorisati u proizvod atoma. Sama neodredjena X nije atom u ovom prstenu i ne može se razložiti u proizvod atoma , npr:

$$X = 2 \cdot \frac{X}{2} = 2 \cdot 2 \cdot \frac{X}{4} = 2 \cdot 3 \cdot \frac{X}{6} = \dots\ ▼$$

Definicija 1.1.11. *Domen A je atomičan ako je svaki nenulti, neinvertibilni element proizvod atoma.*

Definicija 1.1.12. *Domen A je domen sa jednoznačnom faktorizacijom (faktorijalan, UFD) ako zadovoljava sledeće uslove:*
(**A1**) *A je atomičan.*
(**A2**) *Faktorizacija je jednoznačna u sledećem smislu: Dve atomičke faktorizacije istog elementa $a \in A$ jednake su do na redosled atoma u faktorizaciji i do na množenje invertibilnim elementima.*

Na taj način, ako je A UFD i $a \in A$ takav da je:

$$a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$$

gde su p_i, q_j atomi u A mora biti $n = m$ i odgovarajućom prenumeracijom p_i asociran je sa q_i tj. $p_i = u_i q_i$ za neko $u_i \in A^*$.

Tvrdjenje 1.1.13. *Neka je domen A UFD . Element $p \in A$ je atom akko je prost.*

Dokaz. Pretpostavimo da je $p \in A$ atom i neka $ab \in (p)$. Tada je $ab = pc$ za neko $c \in A$. S obzirom da je A UFD elementi a, b, c imaju atomičke faktorizacije, pa važi:

$$a_1 \dots a_k b_1 \dots b_m = pc_1 \dots c_n$$

gde su a_i,b_i,c_i ireducibilni. Iz jednoznačnosti gornje faktorizacije atom p mora biti asociran s nekim od atoma a_i odnosno b_i tj. $p \mid a$ ili $p \mid b$. Ovo poslednje ekvivalentno je sa $a \in (p)$ ili $b \in (p)$. Ideal (p) odavde je prost pa je takav i element p. Ovim je tvrdjenje dokazano jer prema tvrdjenju 1.1.6 obratno važi u svakom domenu. □

Iz prethodnog tvrdjenja vidimo da u faktorijalnim domenima ireducibilni elementi koji učestvuju u faktorizaciji imaju jače svojstvo: *oni su prosti*. Takodje, primenom ovog tvrdjenja možemo videti da nijedan od prstena iz prethodnih primera nije UFD; prva tri imaju atome koji nisu prosti, dok poslednji nije atomičan. U primenama ovog tvrdjenja ipak treba biti obazriv, npr. u prstenu $A = \mathbb{Z}\left[\sqrt{3}\,\right] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ važi $2 \cdot 11 = (5 + \sqrt{3})(5 - \sqrt{3})$ što navodi na pomisao da faktorizacija nije jednoznačna. Ipak, $\mathbb{Z}\left[\sqrt{3}\,\right]$jeste UFD. Ovo se naravno lako može objasniti; prosti celi brojevi 2 i 11 u prstenu $\mathbb{Z}\left[\sqrt{3}\,\right]$ nisu atomi, pa samim tim nisu ni prosti. Najpre, elementi $\alpha = 1 + \sqrt{3}$, $\beta = -1 + \sqrt{3}$ su ovde ireducibilni jer iz pretpostavke $\alpha = uv$ sledila bi jednakost normi $N(\alpha) = N(u)N(v)$, odnosno $-2 = N(u)N(v)$. Mora dakle biti $N(u) = \pm 1$ ili $N(v) = \pm 1$ pa su jedini delitelji broja α asocirani s njim, odnosno α je atom. Iz istih razloga β je atom. Na sličan način može se pokazati da su i elementi $\gamma = 1 + 2\sqrt{3}$, $\delta = -1 + 2\sqrt{3}$ ireducibilni u ovom prstenu. Ovde je naravno $5 + \sqrt{3} = \alpha\delta$, $5 - \sqrt{3} = \beta\gamma$. Jednakosti $2 = \alpha\beta$, $11 = \gamma\delta$ pokazuju da 2 i 11 nisu atomi. Dakle $2 \cdot 11$, $(5+\sqrt{3})(5-\sqrt{3})$, $(1+\sqrt{3})(-1+\sqrt{3})(1+2\sqrt{3})(1-2\sqrt{3})$ su različite "faktorizacije" broja 22 u ovom prstenu. Samo poslednja je medjutim atomička tj. faktorizacija u smislu naše definicije.

Vratimo se sada definiciji faktorijalnog domena, odnosno uslovima **A1** i **A2**. Ako u domenu A važi **A1** svaki element može se razložiti u proizvod atoma. Takva faktorizacija ne mora obavezno biti i jedinstvena. Ako u **A1** zahtevamo više, da se svaki element može razložiti u proizvod prostih elemenata, uslov **A2** postaje suvišan. S tim u vezi je i sledeće tvrdjenje.

Tvrdjenje 1.1.14. *Prosta faktorizacija elemenata domena uvek je jednoznačna.*

Dokaz. Neka je A domen i $a \in A$ element koji ima dve proste faktorizacije

$$a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$$

gde su p_i,q_i prosti. Iz gornje jednakosti imamo da $p_1 \mid q_1 q_2 \dots q_m$. Kako je p_1 prost, ovo znači da $p_1 \mid q_1 \vee \dots \vee p_1 \mid q_m$. Ne umanjujući opštost možemo pretpostaviti da $p_1 \mid q_1$. Kako su p_1 i q_1 prosti, pa dakle i atomi odavde je p_1 asociran sa q_1 tj. $q_1 = up_1$ za neko $u \in A^*$. Na taj način gornja faktorizacija može se "skratiti" sa p_1, pa dobijamo

$$p_2 \dots p_n = uq_2 \dots q_m$$

Dalje, indukcijom dobijamo da je $n = m$ i p_i je asociran sa q_i tj. faktorizacija je jednoznačna u smislu **A2**. $\square$
Kombinujući prethodna tvrdjenja, vidimo da se uslovi **A1** i **A2** mogu zameniti ekvivalentnim uslovom:

(**A3**) *Svaki ne-nula, neinvertibilan element domena ima prostu faktorizaciju.*

U skladu sa tim dajemo i novu definiciju faktorijalnog domena.

Definicija 1.1.15. *Domen A je UFD ako zadovoljava uslov* (**A3**).

Definicija 1.1.16. *Neka je $S \subseteq A$. Za podskup S kažemo da je multiplikativno zatvoren ako zadovoljava uslov: $a, b \in S \Rightarrow ab \in S$. Ako važi obratna implikacija podskup S je multiplikativno zasićen.*

Lako se može pokazati da je skup S svih elemenata domena A koji imaju prostu faktorizaciju multiplikativno zatvoren i zasićen. Multiplikativno zatvoreni skupovi značajni su, izmedju ostalog, i zbog konstrukcije prostih ideala; ako imamo multiplikativno zatvoren podskup S, svaki ideal $I \lhd A$ takav da je $I \cap S = \emptyset$ možemo primenom Zorn-ove leme raširiti do maksimalnog ideala J takvog da $J \supseteq I$, $J \cap S = \emptyset$. Ideal J je prost. Na taj način, uz pomoć multiplikativno zatvorenog skupa S uvek možemo konstruisati prost ideal disjunktan s njim. Ova činjenica koristi se pri dokazu sledećeg veoma praktičnog kriterijuma za proveru faktorijalnosti domena.

Teorema 1.1.17 (Kaplansky)**.** *Za domen A sledeći uslovi su ekvivalentni:*
(i) A je UFD.
(ii) Svaki pravi prost ideal u A sadrži prost element.

Dokaz.
$(i) \Rightarrow (ii)$: Neka je A UFD i $P \lhd A$ prost ideal, $P \neq 0$. Tada postoji $p \in P$, $p \neq 0$, $p \notin A^*$. Kako je A faktorijalan p ima neku prostu faktorizaciju $p = p_1 p_2 \dots p_k$. Kako je P prost, bar jedan od $p_i \in P$, i to je traženi prost element.
$(ii) \Rightarrow (i)$: Pretpostavimo sada da svaki pravi prost ideal u A sadrži prost element. Neka je S skup svih elemenata domena A koji imaju prostu faktorizaciju, i $a \in A$ proizvoljan element, takav da je $a \neq 0$, $a \notin A^*$. Dovoljno je pokazati da $a \in S$, jer će u tom slučaju biti ispunjen uslov (**A3**), pa je A UFD. Pretpostavimo suprotno, da $a \notin S$. Tada je $(a) \cap S = \emptyset$ jer u suprotnom bi postojao neki element $c \in (a) \cap S$, pa je $c = ab = p_1 p_2 \dots p_k \in S$. Skup S je medjutim multiplikativno zasićen, pa dobijamo da $a \in S$, što je u kontradikciji sa pretpostavkom da $a \notin S$. Glavni ideal (a) možemo sada raširiti do maksimalnog ideala P disjunktnog sa S. On je prost, pa prema pretpostaci sadrži prost element p. Medjutim $p \in S$ prema definiciji skupa S, pa opet dobijamo kontradikciju $P \cap S \neq \emptyset$. Dakle $a \in S$, pa je A UFD. $\square$

Primer 1.1.18.

$$A = \mathbb{Z}\left[2X, 2X^2, 2X^3, \dots\right]$$

Ideal $P = \left(2X, 2X^2, 2X^3, \dots\right)$ je prost u ovom prstenu jer je faktorprsten

$$\mathbb{Z}\left[2X, 2X^2, 2X^3, \dots\right] / \left(2X, 2X^2, 2X^3, \dots\right) \cong \mathbb{Z}$$

domen. Ideal P ne sadrži medjutim nijedan prost element (videli smo već da su $2X, 2X^2, 2X^3, \dots$ atomi koji nisu prosti). Domen A prema prethodnoj teoremi nije UFD. ▼

Definicija 1.1.19. *Prost ideal P je visine ili ranga n, u oznaci* $\mathrm{ht(P) = n}$*, ako postoji lanac prostih ideala $P = P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_n$ i nema dužih lanaca. Proste ideale visine 1 zovemo minimalnim prostim idealima. Skup svih minimalnih prostih ideala domena A označavaćemo sa $\mathcal{P}(A)$.*

Teorema 1.1.20. *Pravi prosti glavni ideali u faktorijalnom domenu su minimalni.*

Dokaz. Neka je A UFD, $P = (p)$ pravi prost ideal u A, tj. p je prost, dakle atom, i neka je $Q \subseteq P$, gde je Q pravi prost ideal. Tada prema teoremi 1.1.17, Q sadrži prost element q, pa je $(q) \subseteq (p)$, odnosno $p \mid q$. Odavde, s obzirom da su p i q atomi, oni moraju biti asocirani pa generišu isti ideal $(p) = (q)$ tj. $Q = P$, pa je P minimalan. □

Teorema 1.1.21. *Neka je A domen sa jednoznačnom faktorizacijom. Minimalni prosti ideali su onda glavni.*

Dokaz. Neka je $P \in \mathcal{P}(A)$. Postoji $p \in P$, $p \neq 0$, $p \notin A^*$. Kako je A UFD p ima prostu faktorizaciju $p = p_1 p_2 \dots p_k$. Medjutim, to znači da $p_1 p_2 \dots p_k \in P$ odakle, s obzirom da je P prost ideal, $p_1 \in P \vee \cdots \vee p_k \in P$. Neka npr. $p_1 \in P$. Tada imamo lanac prostih ideala $P \supseteq (p_1) \supseteq (0)$. Medjutim $\mathrm{ht(P)} = 1$, odakle mora biti $P = (p_1)$ tj. P je glavni. □
Primedba. Obrat ove teoreme važi u Neterinim domenima.

Primer 1.1.22.

$$A = \mathbb{Z}[X, \sqrt{2X}]$$

Neka je $P = (X, \sqrt{2X})$ ideal nekonstantnih članova. P je prost jer je $\mathbb{Z}[X, \sqrt{2X}]/(X, \sqrt{2X}) \cong \mathbb{Z}$ domen. Neka je dalje $Q \subseteq P$ pravi prost ideal sadržan u P. Mogući su sledeći slučajevi:
(i) $X \in Q$, $\sqrt{2X} \notin Q$. Tada je i $2X = \sqrt{2X}\sqrt{2X} \in Q$. S obzirom da je Q prost dobija se da $\sqrt{2X} \in Q$ što je kontradikcija.
(ii) $\sqrt{2X} \in Q$, $X \notin Q$. Tada je i $\sqrt{2X}\sqrt{2X} = 2X \in Q$. S obzirom da je Q prost i da $X \notin Q$ dobija se da $2 \in Q$. Odavde je medjutim i $2 \in P$ što je kontradikcija sa pretpostavkom da je P ideal koji ne sadrži konstantne članove različite od nule.
(iii) $X \notin Q$, $\sqrt{2X} \notin Q$. Tada ni $X\sqrt{2X} \notin Q$ pa Q mora sadržati konstantni član q. S obzirom da je $Q \subseteq P$ jedina mogućnost je $q = 0$. Odavde je $Q = 0$ što je u kontrdikciji sa pretpostavkom da je Q pravi prost ideal.
Ostaje dakle jedino mogućnost $X \in Q$, $\sqrt{2X} \in Q$ i u tom slučaju je $Q = P$. Dakle P je minimalan prost ideal u A koji nije glavni. Prema prethodnoj teoremi A nije UFD. ▼

1.2 Faktorizacija u klasičnim domenima

Definicija 1.2.1. *Neka su $a, b \in A$, $a, b \neq 0$. Element $d \in A$ je najveći zajednički delitelj elemenata a i b, u oznaci $d = \text{nzd}\,[a, b]$, ako važi:*
(i) $d \mid a\ ,\ d \mid b$
(ii) $d' \mid a\ ,\ d' \mid b \Rightarrow d' \mid d$

Definicija 1.2.2. *Neka su $a, b \in A$. Element $m \in A$ je najmanji zajednički sadržalac elemenata a i b, u oznaci $m = \text{nzs}\,[a, b]$, ako važi:*
(i) $a \mid m\ ,\ b \mid m$
(ii) $a \mid m'\ ,\ b \mid m' \Rightarrow m \mid m'$

Naravno, za par elemenata $a, b \in A$, najveći zajednički delitelj, odnosno najmanji zajednički sadržalac ne moraju postojati, a ako postoje ne moraju biti jedinstveni. Oni su odredjeni jednoznačno do na množenje invertibilnim faktorom. Za elemente a, b kažemo da su *koprosti* ako je $\text{nzd}\,[a, b] = 1$. Primetimo ovde da iz definicije najmanjeg zajedničkog sadržaoca neposredno sledi:

$$m = \text{nzs}\,[a, b] \Leftrightarrow (m) = (a) \cap (b)$$

Egzistencija najmanjeg zajedničkog sadržaoca za par elemenata $a, b \in A$ ekvivalentna je dakle sa uslovom da je presek glavnih ideala $(a) \cap (b)$, glavni ideal generisan upravo nzs-om tih elemenata.

Tvrdjenje 1.2.3. *Neka su a, b elementi domena A za koje postoji* $\text{nzs}\,[a, b]$. *Tada postoji i* $\text{nzd}\,[a, b]$.

Dokaz. Neka je $m = \text{nzs}\,[a, b]$ tj. $(m) = (a) \cap (b)$. Tada je $(ab) \subseteq (a) \cap (b) = (m)$, pa $(\exists c \in A)$ t.d. je $ab = cm$. Pokazaćemo da je $c = \text{nzd}\,[a, b]$. Kako $m \in (a) \cap (b)$ imamo da je $m = ad_1 = bd_2$ odakle je $ab = cad_1 = cbd_2$. Iz poslednjih jednakosti dobijamo $b = cd_1\ ,\ a = cd_2$ pa $c \mid a\ ,\ c \mid b$. Neka sada $z \mid a\ ,\ z \mid b$. Tada je $a = ze\ ,\ b = zf$ odakle $a \mid zef$, $b \mid zef$ pa je zef zajednički sadržalac za a i b. Kako je $m = \text{nzs}\,[a, b]$ važiće $m \mid zef$, pa je $cm = ab = zzef = zmg$ odakle $c = zg$, tj. $z \mid c$. $\square$

Primer 1.2.4. *Neka je $A = \mathbb{Z}\left[\sqrt{-17}\ \right]$. U jednom od prethodnih primera videli smo da je 2 atom ovog prstena koji nije prost. Označimo sa α i β elemente ovog prstena $\alpha = 1+\sqrt{-17}\ ,\ \beta = 1-\sqrt{-17}$. Važi $18 = \alpha\beta \in (2)$ dok $\alpha, \beta \notin (2)$. Kako su 2 , α atomi ovog prstena* $\text{nzd}\,[\alpha, 2] = 1$. *S druge strane $18 = \alpha\beta \in (2) \cap (\alpha)$ medjutim $18 = \alpha\beta \notin (2\alpha)$ pa* $\text{nzs}\,[\alpha, 2]$ *ne postoji.* ▼

Iz prethodnog tvrdjenja i primera vidimo da egzistencija najmanjeg zajedničkog sadržaoca elemenata a i b povlači za sobom i egzistenciju najvećeg zajedničkog delitelja za isti taj par elemenata, kao i da obratno ne mora uvek da važi. Medjutim, ako za svaki par elemenata a,b postoji $\text{nzd}\,[a, b]$ dolazi se do pravilnosti; onda svaki par elemenata ima i nzs. Domeni u kojima ovo važi čine široku klasu klasičnih domena. Sledeća dva tvrdjenja odnose se na ove domene i biće posledica osobina grupe valuacija domena A pa ih ovde nećemo posebno dokazivati.

Tvrdjenje 1.2.5. *U domenu A sledeći uslovi su ekvivalentni:*
(1) $(\forall x, y \in A)\ \exists \mathrm{nzd}\,[\,x, y\,]$.
(2) $(\forall x, y \in A)\ \exists \mathrm{nzs}\,[\,x, y\,]$.
(3) *Presek dva glavna ideala domena A je glavni ideal.* □

Definicija 1.2.6. *Domen koji zadovoljava ekvivalentne uslove prethodnog tvrdjenja zovemo Gausovim (pseudo-Bezuovim, GCD) domenom.*

Tvrdjenje 1.2.7. *U GCD domenu važi:*
(1) $\mathrm{nzd}\,[\,ab, ac\,] = a \cdot \mathrm{nzd}\,[\,b, c\,]$.
(2) $\mathrm{nzd}\,[\,a, b\,] = d \Rightarrow \mathrm{nzd}\,[\,\frac{a}{d}, \frac{b}{d}\,] = 1$.
(3) $\mathrm{nzd}\,[\,a, b\,] = \mathrm{nzd}\,[\,a, c\,] = 1 \Rightarrow \mathrm{nzd}\,[\,a, bc\,] = 1$.
(4) $\mathrm{nzd}\,[\,a, b\,] \cdot \mathrm{nzs}\,[\,a, b\,] = ab$. □

Neka je sada A domen sa jednoznačnom faktorizacijom i $a, b \in A$ nenulti, neinvertibilni elementi. Tada oni imaju neke faktorizacije:
$a = \prod p_i^{\alpha_i}$, $b = \prod p_i^{\beta_i}$ pa je $\mathrm{nzd}\,[\,a, b\,] = \prod p_i^{\gamma_i}$, $\mathrm{nzs}\,[\,a, b\,] = \prod p_i^{\delta_i}$, gde je $\gamma_i = min\{\alpha_i, \beta_i\}$, $\delta_i = max\{\alpha_i, \beta_i\}$. Odavde očigledno svaka dva elementa u faktorijalnom domenu imaju nzd i nzs pa je ovim dokazano sledeće tvrdjenje:

Tvrdjenje 1.2.8. *Svaki UFD je Gausov domen.* □

Tvrdjenje 1.2.9. *U Gausovom domenu ireducibilan element je prost.*

Dokaz. Neka je A Gausov domen i $p \in A$ ireducibilan, takav da $p \mid ab$. Pretpostavimo suprotno, da $p \nmid a,\ p \nmid b$. Tada će, s obzirom da je p atom, važiti: $\mathrm{nzd}\,[\,a, p\,] = \mathrm{nzd}\,[\,b, p\,] = 1$. Odavde je medjutim $\mathrm{nzd}\,[\,p, ab\,] = 1$. Kako $p \mid ab$ dobijamo da $p \mid 1$ tj. $p \in A^*$, što je u kontradikciji sa pretpostavkom da je p atom. □

Teorema 1.2.10. *Za domen A sledeći uslovi su ekvivalentni:*
(1) *A je UFD.*
(2) *A je atomičan i za svaka dva elementa* $a,\ b \in A$ *postoji* $\mathrm{nzd}\,[\,a, b\,]$.
(3) *A je atomičan i za svaka dva elementa* $a,\ b \in A$ *postoji* $\mathrm{nzs}\,[\,a, b\,]$.
(4) *A je atomičan i presek dva glavna ideala je glavni ideal.*
(5) *A je atomičan i svaki atom je prost.*

Dokaz.
$1 \Rightarrow 2$: Tvrdjenje 1.2.8.
$2 \Leftrightarrow 3 \Leftrightarrow 4$: Tvrdjenje 1.2.5.
$2 \Rightarrow 5$: Tvrdjenje 1.2.9.
$5 \Rightarrow 1$: Iz atomičnosti svaki nenulti neinvertibilni element ima $a \in A$ ima faktorizaciju $a = p_1 p_2 \dots p_k$. Kako je svaki od atoma koji učestvuju u faktorizaciji prost, ova faktorizacija je jednoznačna prema tvrdjenju 1.14. □
Sada se možemo vratiti na početnu definiciju faktorijalnog domena i istaknute uslove **(A1), (A2)**. Prethodna teorema daje nam, uz pretpostaku da važi atomičnost, neke ekvivalentne uslove za **(A2)**:
(**A2′**) Svaki atom je prost.
(**A2″**) Svaka dva elementa u A imaju nzd.

(**A2'''**) Svaka dva elementa u A imaju nzs.
(**A2''''**) Presek svaka dva glavna ideala u A je glavni ideal.
Pogledajmo sada šta su dovoljni uslovi za **(A1)**; neka postoji $a \in A$, $a \notin A^*$ koji nema atomičnu dekompoziciju. Tada a nije atom jer u suprotnom bi $a = a \cdot 1$ bilo atomičko razlaganje. Dakle postoje elementi $b, c \in A$, $b, c \notin A^*$ takvi da je $a = bc$. Ako bi b i c imali atomičku dekompoziciju onda bi je imao i a. Možemo dakle pretpostaviti da jedan od njih, npr. b nema atomičko razlaganje. Tako dobijamo:

$$a = bc \Rightarrow b \mid a \Rightarrow (a) \subsetneqq (b)$$

Važi stroga inkluzija $(a) \neq (b)$ jer $c \notin A^*$. Ovaj postupak sada se može nastaviti jer b nema dekompoziciju. Na taj način, svakom elementu $a \in A$ koji se ne može rastaviti u proizvod atoma možemo pridružiti strogo rastući lanac glavnih ideala:

$\mathcal{L}$: $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots$ Dovoljan uslov za atomičnost domena biće dakle uslov kidanja ovakvih lanaca. Skraćeno ćemo taj uslov označiti sa ACC_1 a njegov ekvivalent sa $(ACC_1)'$

(**ACC**$_1$) Svaki strogo rastući lanac glavnih ideala u A je konačan tj. za svaki lanac $\mathcal{L}$: $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots$ $(\exists n)$ t.d. je $(a_n) = (a_{n+1}) = \ldots$

(**ACC**$_1$)$'$ Svaka neprazna familija glavnih ideala u A ima maksimalan element u odnosu na inkluziju.

Posledica 1.2.11. *Domen A je faktorijalan akko je Gausov domen u kome važi uslov ACC_1.* □

Na osnovu prethodnog vidimo da se mogu dati i druge, ekvivalentne definicije faktorijalnog domena. U nekim slučajevima ovi uslovi pokazuju se pogodnijim, npr. ako je iz nekog razloga pogodnije raditi sa idealima možemo dati sledeću definiciju:

Definicija 1.2.12. *Domen A je UFD ako je svaki strogo rastući niz glavnih ideala u A konačan i presek dva glavna ideala u A je glavni ideal.*

Tvrdjenje 1.2.13. *Svaki glavni domen je UFD.*

Dokaz. Kako su svi ideali glavni, to je i presek glavnih ideala glavni ideal, pa je dovoljno pokazati da važi uslov ACC_1. Neka je: $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots$ strogo rastući lanac glavnih ideala. Kako je u pitanju lanac, to je i $\bigcup\limits_{n \in N} (a_n) = I$ ideal i to glavni, npr. $I = (a)$. Kako $a \in \bigcup\limits_{n \in N} (a_n)$ to je $a \in (a_m)$ za neko $m \in N$. Odavde je $I = (a) \subseteq (a_m)$. Iz obratne inkluzije $(a_m) \subseteq I = \bigcup\limits_{n \in N} (a_n)$ dobijamo da je $I = (a_m)$ pa $(\exists m \in N)$ takvo da je $(a_m) = (a_{m+1}) = \ldots$ odnosno važi uslov kidanja lanaca ACC_1. □

Primer 1.2.14.

$$A = \mathbb{Z}\left[X^2, X^3\right]$$

Domen A nije Gausov pa samim tim nije ni UFD. S obzirom da $X^2 \nmid X^3$ jer $X \notin A$ biće $\operatorname{nzd}[X^2, X^3] = 1$. S druge strane $\operatorname{nzs}[X^2, X^3]$ ne postoji jer ako bi postojao, to bi morao biti element X^5. Ovo nije moguće jer X^6 je zajednički sadržaoc ovih elemenata ($X^6 = X^2X^4$, $X^6 = X^3X^3$), a $X^5 \nmid X^6$. Drugim rečima presek glavnih ideala $(X^2) \cap (X^3)$ nije glavni, pa A nije UFD. Primetimo da u ovom prstenu elementi X^5, X^6 nemaju nzd , pa samim tim ni nzs. Ovde su naime $1, X^2, X^3$ njihovi zajednički delitelji. Nijedan od njih medjutim ne ispunjava uslov definicije najvećeg zajedničkog delitelja: X^3 nije nzd jer je X^2 zajednički delitelj i $X^2 \nmid X^3$; X^2 nije nzd jer je X^3 zajednički delitelj i $X^3 \nmid X^2$; Najzad X^5, X^6 očigledno nisu koprosti pa ni 1 nije nzd. ▼

Primer 1.2.15.

$$A = \{\, a_0 + 3a_1X + a_2X^2 + \cdots + a_nX^n \;\mid\; a_i \in \mathbb{Z},\ n \in \mathbb{N} \,\}$$

Na A možemo gledati kao na potprsten prstena polinoma $\mathbb{Z}[X]$, u kome su koeficijenti uz X deljivi sa 3. Slično kao i u prethodnom primeru možemo posmatrati elemente $a = 3X, b = 3X^2$. Ovde naravno $3X \nmid 3X^2$, jer $X \notin A$. Samim tim je i $\operatorname{nzd}[\,3X, 3X^2\,] = 1$, dok nzs i ovde ne postoji. Kako je

$$9X^2 = 3X \cdot 3X,\ 9X^2 = 3 \cdot 3X^2\,,$$

jedini "kandidat" za nzs je $9X^2$. Medjutim, ako postoji, $\operatorname{nzs}[\,a, b\,]$ bi svakako morao da deli proizvod ab što ovde nije slučaj jer $9X^2 \nmid 9X^3$. Presek glavnih ideala $(3X) \cap (3X^2)$ nije glavni ideal, pa A nije UFD. ▼

Videli smo da u faktorijalnom domenu svaka dva elementa imaju nzd i kako se on može odrediti ako znamo faktorizacije tih elemenata. Ove faktorizacije u nekim slučajevima medjutim nije lako odrediti. Za odredjene klase domena postoji još jedan način za računanje najvećeg zajedničkog delitelja, poznatiji kao Euklidov algoritam.

Definicija 1.2.16. *Domen A je Euklidov ako postoji funkcija* $\varphi : A\backslash\{0\} \to \mathbb{Z}^+$ *sa osobinama:*

$$ab \neq 0 \Rightarrow \varphi(ab) \geq \varphi(a) \tag{1.1}$$

$$(\forall a, b \in A,\ b \neq 0)(\exists q, r \in A) \quad a = bq + r \quad \varphi(r) < \varphi(b) \tag{1.2}$$

Funkciju φ iz prethodne definicije zovemo Euklidskim algoritmom. Euklidski algoritam ne mora postojati, a i ako postoji, ne mora biti odredjen jednoznačno. Možemo naći više funkcija koje zadovoljavaju gornje uslove, npr. ako je φ Euklidski algoritam onda je to i funkcija $\varphi + 1$ pa se može govoriti o familiji algoritama φ_i. Koristeći definiciju Euklidske funkcije φ može se pokazati da je $\varphi(0) = 0$ kao i da je $\varphi(a) = 1 \Leftrightarrow a \in A^*$. Sama definicija Euklidovog domena zahteva dakle spoljnu funkciju te je stoga često nepogodna za korišćenje. Unutrašnja karakteristika ovih prstena je da u njima važi algoritam "deljenja sa ostatkom". Elemente q i r iz definicije funkcije φ zovemo Euklidskim količnikom i ostatkom. Euklidovi prsteni su npr. prsten celih brojeva $\mathbb{Z}$ sa Euklidskom funkcijom $\varphi(n) = |n|$, prsten polinoma $k[X]$ nad poljem k sa odgovarajućom

funkcijom $\varphi(f) = 2^{deg(f)}$, kao i takozvani Gausov prsten $\mathbb{Z}[i]$ sa funkcijom $\varphi(a+bi) = a^2+b^2$. U sva tri slučaja radi se o glavnoidealskim domenima. Važi sledeće tvrdjenje.

Tvrdjenje 1.2.17. *Euklidov domen je glavni (pa samim tim i UFD).*

Dokaz. Neka je A Euklidov domen i $I \lhd A$ proizvoljan ideal. Možemo pretpostaviti da postoji $a \in I$, $a \neq 0$ jer je u suprotnom $I = (0)$ očigledno glavni ideal. Skup $\{\varphi(a) \mid a \in I, a \neq 0\}$ je dakle neprazan podskup skupa prirodnih brojeva $\mathbf{N}$ pa kao takav ima najmanji element npr. $\varphi(b) = m$. Neka je $a \in I$. Iz algoritma deljenja, postoje elementi q i r takvi da je $a = bq + r$ i $\varphi(r) < m$. Kako je i $r \in I$, mora biti $r = 0$ tj. $a = bq$. Odavde je $I \subseteq (b)$. Obratna inkluzija $b \subseteq (I)$ je očigledna jer $b \in I$ pa je dakle $I = (b)$ glavni ideal. $\square$
Iz prethodnog tvrdjenja vidimo da se neprijatno pitanje egzistencije Euklidove funkcije φ za dati domen A, može značajno redukovati, jer je dovoljno posmatrati samo glavne domene. Npr. u prsten polinoma $\mathbb{Z}[X]$ ne može se uvesti Euklidova funkcija. Naime, $\mathbb{Z}[X]$ nije glavni domen, pa nije ni Euklidov; u njemu ne važi algoritam deljenja sa ostatkom. Neka je sada A Euklidov domen, φ odgovarajuća funkcija i $a, b \in A$, $b \neq 0$. Tada se prema (1.2) može generisati sistem jednačina:

$$r_{i-2} = r_{i-1}q_i + r_i \ , \ \varphi(r_i) < \varphi(r_{i-1}) \ , \ i = 1, 2 \ldots \tag{1.3}$$

$$r_{-1} = a \ , \ r_0 = b \ , \ q_1 = q \ , \ r_1 = r$$

Ovaj proces prekida se kada je $r_{k+1} = 0$ i može se pokazati da je tada r_k upravo $\text{nzd}\,[a, b]$ i više, da je on njihova linearna kombinacija. Ovo se može formulisati u obliku sledećeg tvrdjenja:

Tvrdjenje 1.2.18. *U Euklidovom domenu za svaka dva elementa $a, b \in A$ postoji* $\text{nzd}\,[a, b]$ *i važi*

$$\text{nzd}\,[a, b] = \alpha a + \beta b \qquad za\ neke\ \alpha\ , \beta \in A \tag{1.4}$$

Naravno može se dati i direktan dokaz da je Euklidov prsten faktorijalan, ne koristeći tvrdjenje 1.2.17.

Tvrdjenje 1.2.19. *Euklidov domen je UFD.*

Dokaz. Proverimo najpre atomičnost. Neka su $(a), (b)$ glavni ideali Euklidovog domena A takvi da je $(a) \subsetneq (b)$. Tada je $a = bc$, $c \notin A^*$ odakle je $\varphi(a) = \varphi(bc) > \varphi(b)$. Drugim rečima važi: $(a) \subsetneq (b) \Rightarrow \varphi(a) > \varphi(b)$. Odavde se svakom strogo rastućem lancu glavnih ideala:

$$\mathcal{L}_1 : \qquad (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \ldots$$

može pridružiti lanac prirodnih brojeva:

$$\mathcal{L}_2 : \qquad \varphi(a_1) > \varphi(a_2) > \varphi(a_3) > \ldots$$

Kako je lanac $\mathcal{L}_2$ konačan, to je i $\mathcal{L}_1$ konačan pa važi uslov ACC_1 tj. A je atomičan. Dokažimo sada da važi i uslov **A2**, tj. neki od njegovih ekvivalenata npr. **A2′**. Neka je $p \in A$ ireducibilan. Dovoljno je pokazati da je p prost. Zato pretpostavimo da $p \mid ab$ i da $p \nmid a$. Osim toga ni $a \nmid p$, jer je p atom, pa je $\text{nzd}\,[a, p\,] = 1$. To znači da postoje elementi $\lambda, \mu \in A$ takvi da je:

$$a\lambda + p\mu = 1$$

Ako poslednju jednakost pomnožimo sa b dobijamo $ab\lambda + pb\mu = b$. Kako je $ps = ab$, jer $p \mid ab$, dobijamo $b = p(s\lambda + b\mu)$ pa $p \mid b$, odakle je p prost. □

Prsten algebarskih celih.

Neka je $d \in \mathbb{Z}$ bezkvadratan, tj. oblika $d = \pm p_1 p_2 \dots p_k$, gde su $p_i \neq p_j$ prosti brojevi. Posmatramo kvadratno raširenje $\mathbb{Q}[\sqrt{d}\,] = \{u + v\sqrt{d} \mid u\,, v \in \mathbb{Q}\}$ polja racionalnih brojeva $\mathbb{Q}$. Element $\alpha \in \mathbb{Q}[\sqrt{d}\,]$ je *ceo* nad $\mathbb{Z}$ ako je koren nekog moničnog polinoma iz $\mathbb{Z}[X]$. Ako su α, β celi može se pokazati da su i $\alpha + \beta\,, \alpha\beta$ celi, pa svi celi elementi obrazuju jedan prsten koji ćemo označiti sa

$$\mathbb{Q}(d) = \{u + v\sqrt{d} \mid u + v\sqrt{d} \text{ ceo nad } \mathbb{Z}\}$$

i zvaćemo ga *prstenom algebarskih celih*. U vezi sa ovim prstenima može se postaviti niz zanimljivih pitanja kojima se bavi algebarska teorija brojeva, npr: Kakvog su oblika ireducibilni i prosti elementi ovih prstena i u kakvoj su vezi sa prostim brojevima iz $\mathbb{Z}$? Šta su inverzibilni elementi u ovim prstenima? Za koje d je $\mathbb{Q}(d)$ glavni? Da li u njima važi Euklidov algoritam? Šta se može reći o faktorizaciji u njima? Može se lako pokazati da je:

$$\mathbb{Q}(d) = \mathbb{Z}[\sqrt{d}\,] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} \quad \text{ako je} \quad d \equiv 2 \pmod 4\,, d \equiv 3 \pmod 4$$

$$\mathbb{Q}(d) = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{\frac{a}{2} + \frac{b}{2}\sqrt{d} \mid a, b \in \mathbb{Z} \text{ iste parnosti}\right\} \text{ ako je } d \equiv 1 \pmod 4$$

Za element $\alpha = u + v\sqrt{d} \in A$, gde je $A = Q(d)$, definiše se ceo broj, njegova *norma*, $N(\alpha) = u^2 - dv^2$. Za ovako definisanu normu važi:

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

$$\alpha \in \mathbb{Q}(d)^* \Leftrightarrow N(\alpha) = \pm 1$$

Može se pokazati da prsteni algebarskih celih u slučaju $d < 0$ imaju konačno mnogo inverzibilnih elemenata i da su oni zadati nulama polinoma $x^2 - 1$, $x^4 - 1$, $x^6 - 1$, dok u slučaju $d > 0$ prsteni $Q(d)$ sadrže beskonačno mnogo inverzibilnih elemenata. Ovo se može dobiti kao specijalan slučaj poznate Dirihleove teoreme o jedinicama. U prstenu algebarskih celih možemo definisati norma-funkciju sa:

$$\varphi(\alpha) = |N(\alpha)| \quad \text{ili sa} \quad N(\alpha) = |A/\alpha A|\,, \alpha \neq 0$$

Mogu se postaviti sledeća pitanja:
Za koje d je $\mathbb{Q}(d)$ Euklidov odnosno kada je norma-funkcija Euklidski algoritam?
Za koje d će prsten $\mathbb{Q}(d)$ biti UFD?
Oba pitanja imaju veoma dugu istoriju u algebarskoj teoriji brojeva. Prvo pitanje u potpunosti je rešeno (Chatland, Davenport 1950). Oni su dokazali da medju prstenima $\mathbb{Q}(d)$ ima svega 21 Euklidovih.

Teorema 1.2.20. *$\mathbb{Q}(d)$ je Euklidov akko*

$$d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$$

Drugo pitanje rešeno je samo delimično, za $d < 0$. Dokazano je naime, (Baker, Stark 1966), da za $d < 0$ ima tačno 9 UFD prstena. Preciznije, važi sledeća teorema:

Teorema 1.2.21. *Za $d < 0$ prsten $\mathbb{Q}(d)$ je UFD akko*

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$$

U dokazu, koji nije algebarskog karaktera, koristi se teorija eliptičkih modularnih krivih i transcendentna teorija. Za $d > 0$ problem nije u potpunosti rešen. Mada se za manje vrednosti, npr. za $d < 100$ znaju svi UFD-ovi ne zna se da li je njihov broj konačan. Istaknimo ovu nedokazanu hipotezu:

(H) *Za $d > 0$ beskonačno mnogo prstena $\mathbb{Q}(d)$ ima jednoznačnu faktorizaciju.*

Takodje se ne zna da li je broj glavnih prstena $\mathbb{Q}(d)$ konačan ili ne. Kasnije ćemo medjutim videti da su ova dva pitanja za prsten algebarskih celih ekvivalentna tj. da je $\mathbb{Q}(d)$ glavni akko je UFD. Ovde se mogu dati i primeri glavnih prstena algebarskih celih koji nisu Euklidovi. Takvi su npr. prsteni $\mathbb{Q}(-19) = \mathbb{Z}\left[(1+\sqrt{-19})/2\right]$ i $\mathbb{Q}(-43) = \mathbb{Z}\left[(1+\sqrt{-43})/2\right]$.

Videli smo da u Euklidovom domenu A za proizvoljna dva elementa a, b postoji najveći zajednički delitelj d i da je on njihova linearna kombinacija, $d = \alpha a + \beta b$ za neke $\alpha, \beta \in A$. Ovo zapravo znači da je zbir glavnih ideala (a) i (b), glavni ideal $(a) + (b) = (d)$. Indukcijom je onda i $(a_1) + (a_2) + \cdots + (a_n)$ glavni ideal. Sledeći uslovi su dakle ekvivalentni:

(i) $(\forall a, b \in A)(\exists d \in A)\ d = \text{nzd}\,[a, b]$ i $d = \alpha a + \beta b$ za neke $\alpha, \beta \in A$
(ii) $(a, b) = (d)$ (zbir glavnih ideala u A je glavni ideal)
(iii) $(a_1, a_2, \ldots, a_n) = (d)$ (svaki konačno generisan ideal u A je glavni)

Definicija 1.2.22. *Domen A je Bezuov ako zadovoljava jedan, a time i svaki od uslova (i), (ii), (iii).*

U Bezuovim domenima svaka dva elementa imaju nzd , pa prema prethodnom i nzs tj. u ovim domenima je presek i zbir glavnih ideala glavni ideal. Posebno ovo znači da je u Bezuovim domenima ispunjen uslov **A2** tj. u njima je su svi atomi prosti. Da bi Bezuov domen bio UFD dovoljno je dakle da bude

atomičan. Neposredno iz definicije Bezuovog domena sledi da je svaki glavni domen i Bezuov, kao i da je svaki Bezuov domen i Gausov. Da obratno ne mora da važi može se videti iz sledećih primera.

Primer 1.2.23. *Neka je $A = \mathbb{Z}[X]$. A je UFD pa je stoga i Gausov domen. On medjutim nije i Bezuov. Npr. ideal $(2, X)$ nije glavni pa ne važi uslov (ii).*

Primer 1.2.24. *Neka je*

$$A = \mathbb{Z} + X\mathbb{Q}\,[X]$$

prsten iz primera 1.1.10. A je Bezuov domen koji nije glavni.

Neka su $f, g \in A$. A je potprsten Euklidovog prstena $\mathbb{Q}\,[X]$ pa za polinome f, g postoji $d = \mathrm{nzd}\,[f, g]$, $d \in \mathbb{Q}\,[X]$ i

$$d = qf + rg \tag{1.5}$$

za neke polinome $q, r \in \mathbb{Q}\,[X]$. Kako je najveći zajednički delitelj odredjen do na asociranost važi:

$$\mathrm{nzd}\,[\,f, g\,] = \{\, sd \mid s \in \mathbb{Q}\ ,\ s \neq 0 \,\} \tag{1.6}$$

pa možemo smatrati da su polinomi d, q, r u (1.5) iz potprstena A. Dakle (1.5) je Bezuova relacija u A. Uočimo sada strogo rastući lanac glavnih ideala

$$\mathcal{L}:\ \left(\frac{X}{2}\right) \subsetneq \left(\frac{X}{4}\right) \subsetneq \left(\frac{X}{8}\right) \subsetneq \dots$$

Ovaj lanac se ne prekida, pa nije ispunjen uslov kidanja lanaca koji mora da važi u glavnim domenima. A dakle nije glavni domen jer ideal $\left(X/2, X/2^2, X/2^3, \dots\right)$ nije glavni. ▼

Iz prethodnog primera možemo videti da se Bezuovi i glavni domeni razlikuju u uslovima konačnosti. Preciznu formulaciju, kao i vezu Bezuovih i faktorijalnih domena, daje nam sledeća teorema.

Teorema 1.2.25. *Za domen A sledeći uslovi su ekvivalentni:*
(1) *A je glavni.*
(2) *A je Bezuov i atomičan.*
(3) *A je Bezuov i UFD.*

Dokaz.
(1)⇒(2): Neka je A glavni domen. Tada važi uslov ACC_1 pa je A atomičan. Svi ideali u A su glavni pa je i svaki konačno generisan glavni. A je dakle i Bezuov.
(2)⇒(3): Ako je A Bezuov i atomičan uslovi **(A1)** i **(A2)** očigledno važe pa je A i UFD.
(3)⇒(1): Neka je $I \lhd A$, $I \neq 0$. Tada postoji $a \in I$, $a \neq 0$ i glavni ideal $(a) \subseteq I$. A je UFD pa a ima faktorizaciju $a = p_1 p_2 \dots p_k$ dužine k. Možemo pretpostaviti da smo odabrali $a \in I$ sa najmanjom dužinom faktorizacije. Pretpostavimo dalje da je $(a) \neq I$. Tada postoji $b \in I \setminus (a)$, pa je $(a) \subsetneq (a, b)$. Kako je A Bezuov (a, b) je glavni ideal pa važi:

$$(a) \subsetneq (a, b) = (d) \quad , \quad d = ax + by \in I$$

Iz $(a) \subsetneq (d)$ dobijamo da $d \mid a$, $d \neq ua$, $u \in A^*$. Odavde je dužina faktorizacije elementa $d \in I$ manja od k što je kontradikcija sa izborom elementa a. Dakle $I = (a)$. Proizvoljan ideal $I \lhd A$ je glavni pa je i A glavni domen. $\square$
Na osnovu prethodnih tvrdjenja i primera vidimo da medju klasičnim domenima važe sledeći odnosi:

$$Euklidovi \Rightarrow Glavnoidealski \Rightarrow Bezuovi \Rightarrow Gausovi$$

$$Euklidovi \Rightarrow Glavnoidealski \Rightarrow Faktorijalni$$

kao i da važi: $Faktorijalni \cap Bezuovi = Glavnoidealski$

Glava 2

Faktorizacija u raširenjima prstena

2.1 Raširenja prstena

Neka je A potprsten prstena B koji ćemo još zvati i *raširenjem* prstena A. Zanimaju nas zajedničke osobine ovih prstena tj. da li neka uočena osobina prstena A, u ovom slučaju faktorijalnost, važi i u B i obratno. Pogledajmo neke od prethodnih primera.

Primer 2.1.1. $A = \mathbb{Z}\left[2X, 2X^2, 2X^3, \dots\right]$, $B = \mathbb{Z}[X]$. A nije, dok B jeste UFD.

Primer 2.1.2. $A = \mathbb{Z}$, $B = \mathbb{Z}\left[\sqrt{-17}\,\right]$. A je UFD. B nije UFD.

Primer 2.1.3. $A = \mathbb{Z}$, $B = \mathbb{Z}[i\,]$. A je UFD. B je UFD.

Već iz ovih primera vidimo da se osobina koja nas ovde zanima - jednoznačna faktorizacija, dosta loše ponaša u raširenjima. Potprsten UFD-a ne mora biti UFD, takodje ni raširenje UFD-a ne mora biti UFD. Ipak, u nekim raširenjima, faktorijalnost se čuva. Cilj će nam biti da opišemo ta raširenja. Od posebnog interesa biće veza medju prostim idealima ovih prstena. Ako je $\overline{P} \lhd B$ prost ideal u B, onda je $\overline{P} \cap A = P$ prost ideal u A koji zovemo i *kontrakcijom* ideala $\overline{P}$. Ako je P prost ideal u A onda ideal $PB \lhd B$ zovemo i *ekstenzijom* ideala P. Za razliku od kontrakcije, ekstenzija prostog ideala ne mora biti prost ideal. Postavlja se pitanje kada je svaki prost ideal u A kontrakcija prostog ideala iz B, odnosno kada je svaki prost ideal u B ekstenzija prostog ideala iz A. Odgovor na ovo pitanje zavisi naravno od vrste raširenja. Univerzalne osobine koje su od interesa u svakom raširenju su: LO (lying-over, natkrivanje), GU (going-up, rast), GD (going-down, opadanje) i INC (incomparability, neuporedivost).

Definicija 2.1.4. *Neka je B raširenje prstena A. Označimo sa P i Q proste ideale u A i sa $\overline{P}$ i $\overline{Q}$ proste ideale u B. Par (A,B) zadovoljava redom* LO, GU, GD, INC ako je ispunjeno:

(LO) $\forall P\ \exists \overline{P}$ tako da je $\overline{P} \cap A = P$.
(GU) $\forall P\ \forall Q\ \forall \overline{P}\ (P \subseteq Q\ ,\ \overline{P} \cap A = P)(\exists \overline{Q})$ *tako da* $\overline{P} \subseteq \overline{Q}\ ,\ \overline{Q} \cap A = Q$.
(GD) $\forall P\ \forall Q\ \forall \overline{Q}\ (P \subseteq Q\ ,\ \overline{Q} \cap A = Q)(\exists \overline{P})$ *tako da* $\overline{P} \subseteq \overline{Q}\ ,\ \overline{P} \cap A = P$.
(INC) $\forall \overline{P}\ \forall \overline{Q}\quad \overline{P} \cap A = \overline{Q} \cap A\ \Rightarrow\ \overline{P} = \overline{Q}$.

U vezi sa ovim osobinama važe sledeća tvrdjenja [15]:

Tvrdjenje 2.1.5.
(1) *Ako za par (A,B) važi* GU onda važi i LO.
(2) Ako za par (A,B) važi INC i ako je $\overline{P} \cap A = P$ onda je ht($\overline{\mathrm{P}}$) $\leq$ ht(P).
(3) Neka za par (A,B) važi GU i neka je $P \lhd A$, ht(P) = n. Tada postoji $\overline{P} \lhd B$, $\overline{P} \cap A = P$ *i* ht($\overline{\mathrm{P}}$) $\geq$ n. Ako uz to važi i INC onda je ht($\overline{\mathrm{P}}$) = n.
(4) Ako za par (A,B) važi GU i INC onda je dim(A) = dim(B). $\square$

Tipična raširenja prstena A sa kojima radimo su: lokalizacija A_S, cela raširenja A', prsten polinoma $A[X]$ i prsten formalnih redova $A[[X]]$. Za ova raširenja važi:
Par (A, A_S) zadovoljava GD, INC. Par (A, A') zadovoljava GU, LO, INC.
Par $(A, A[X])$ zadovoljava GD, LO . Par $(A, A[[X]])$ zadovoljava GD, LO .

2.2 Lokalizacija i faktorizacija

Neka je A prsten, $S \subseteq A$ multiplikativno zatvoren podskup, $0 \notin S$. Na $A \times S$ definišemo relaciju ekvivalencije:

$$(a, s) \backsim (b, t) \Leftrightarrow (\exists\, u \in S) \quad u(at - bs) = 0 \tag{2.1}$$

Specijalno, ako je A domen relacija (2.1) svodi se na:

$$(a, s) \backsim (b, t)\ \Leftrightarrow\ (at - bs) = 0 \tag{2.2}$$

Klasu ekvivalencije elementa (a, s) označavaćemo formalnim razlomkom a/s. Na skupu svih klasa ekvivalencije, u oznaci A_S ili $S^{-1}A$, definišemo sabiranje i množenje klasa sa:

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} \qquad \frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$

Sa ovako definisanim operacijama $(A_S, +, \cdot)$ je prsten, koji zovemo *lokalizacijom* prstena A. Na taj način pomoću prstena A i njegovog multiplikativno zatvorenog skupa S dobija se novi prsten u kome svi elementi iz S postaju inverzibilni. Pri tome postoji i kanonski homomorfizam $\varphi_S : A \to A_S$ definisan sa $\varphi_S(x) = x/1$. Njegovo jezgro $Ker\varphi_S = \{\, x \in A \mid sx = 0\ ,\ za\ neko\ s \in S \,\}$ je trivijalno akko S ne sadrži delitelje nule prstena A i u tom slučaju φ_S je utapanje. Naravno, ovo važi uvek ako je A domen, pa je lokalizacija A_S raširenje domena A. Par (A, A_S) u tom slučaju zadovoljava GD i INC ali ne i LO pa samim tim ni GU. U opštem slučaju je dim($\mathrm{A_S}$) $\leq$ dim(A).

Neka je sada A domen. Tada je njegov podskup $S = A \setminus \{0\}$ multiplikativno zatvoren. Ako lokalizujemo po ovom skupu S svi ne-nula elementi domena A postaju inverzibilni, pa je

$$A_S = \left\{ \frac{a}{s} \mid a, s \in A \ , \ s \neq 0 \right\}$$

jedno polje. Ovako dobijeno polje je *polje razlomaka* ili *količničko polje* domena A, u oznaci $k = Frac(A)$. Primetimo da je ovde S najširi podskup po kome se može lokalizovati. Sužavanjem skupa S odgovarajuće lokalizacije $S^{-1}A$ biće potprsteni količničkog polja k pa na lokalizacije domena možemo gledati kao na potprstene njegovog polja razlomaka. Veza medju idealima u A i A_S potpuno je odredjena sledećom teoremom.

Teorema 2.2.1 (teorema o korespodenciji)**.** *Neka je A domen, $S \subseteq A$ multiplikativno zatvoren podskup i A_S odgovarajuća lokalizacija prstena A.*
(i) Svi ideali u A_S su ekstenzije ideala iz A tj. oblika IA_S za neki ideal $I \lhd A$. Preciznije, $J = (J \cap A)A_S$ za svaki ideal $J \lhd A_S$ i preslikavanje $J \mapsto J \cap A$ je rastuća injekcija uredjenog skupa svih ideala u A_S u uredjen skup svih ideala u A.
(ii) Prosti ideali u A_S su u uzajamno jednoznačnoj korespodenciji sa prostim idealima u A disjunktnim sa S. Preciznije, ako je $\overline{P} \lhd A_S$ prost preslikavanje: $\overline{P} \mapsto \overline{P} \cap A$ skupa svih prostih ideala u A_S u skup prostih ideala u A disjunktnih sa S je bijektivno i čuva uredjenje.

Dokaz. (i). Dokažimo najpre da za ideal $J \lhd A_S$ važi $(J \cap A)A_S = J$. Neka $x = \frac{a}{s} \in J \ , \ a \in A \ , \ s \in S$. Tada $sx = a \in J$ pa $a \in J \cap A$. Odavde je

$$x = \frac{1}{s} \cdot a \in (J \cap A)A_S \ \text{ pa je dakle } \ J \subseteq (J \cap A)A_S$$

Sdruge strane, kako je $J \cap A \subseteq J$ biće i $(J \cap A)A_S \subseteq JA_S = J$odakle je $J = (J \cap A)A_S$. Neka su sada I, J ideali u A_S sa istim kontrakcijama:

$$J \cap A = I \cap A \ \Rightarrow \ (J \cap A)A_S = (I \cap A)A_S \ \Rightarrow \ J = I \tag{2.3}$$

Preslikavanje $J \to J \cap A$ je prema tome injektivno. Specijalno odavde sledi i da za par (A, A_S) važi INC.
(ii). Neka je sada $\overline{P}$ prost ideal u A_S i $\overline{P} \cap A = P$. Ideal P je prost i prema *(i)* je $PA_S = \overline{P}$. Kako je $\overline{P}$ prost on ne sadrži invertibilne elemente (u suprotnom dobijamo kontradikciju $\overline{P} = A_S$), odakle je $P \cap S = \emptyset$. Obratno, neka je sada P prost ideal u A disjunktan sa S. Treba pokazti da je PA_S prost ideal u A_S. Neka je

$$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} \in PA_S \ \Rightarrow \ \frac{a_1 a_2}{s_1 s_2} = \frac{p}{s_3} \ \text{ za neke } \ p \in P \ , \ s \in S \tag{$*$}$$

Iz poslednje jednakosti biće $ps_1s_2 = s_3a_1a_2 \in P$. Kako $s_3 \notin P$ mora biti

$$a_1 \in P \ \vee \ a_2 \in P \ \Rightarrow \ \frac{a_1}{s_1} \in PA_S \ \vee \ \frac{a_2}{s_2} \in PA_S \tag{$**$}$$

Kako je PA_S pravi ideal u A_S, jer u suprotnom $PA_S = A_S$ pa $1 = p/s \in PA_S$ odakle je $s = p \in P \cap S$ što je kontradikcija sa pretpostavkom $P \cap S = \emptyset$, prema (*) i (**) on je prost. Ako sa $\overline{\mathcal{P}}$ označimo proste ideale u A_S i sa $\mathcal{P}'$ proste u A disjunktne sa S možemo definisati preslikavanja:

$$\phi : \overline{\mathcal{P}} \to \mathcal{P}' \qquad \psi : \mathcal{P}' \to \overline{\mathcal{P}}$$

$$\phi(\overline{P}) = \overline{P} \cap A \qquad \psi(P) = PA_S$$

Ova preslikavanja daju uzajamno jednoznačnu vezu izmedju $\overline{\mathcal{P}}$ i $\mathcal{P}'$. $\square$

Multiplikativno zatvoreni skupovi po kojima lokalizujemo mogu biti različiti a najčešće ćemo koristiti sledeća dva podskupa:
(i) $S = \{\, 1, f, f^2, \dots \}$ gde je $f \in A$ nenilpotentan element. Za lokalizaciju A_S u tom slučaju koristimo oznaku A_f. Prema 2.2.1 prosti ideali u A_f su u korespodenciji sa prostim idealima u A koji ne sadrže f.
(ii) $S = A \setminus P$ komplement prostog ideala $P \lhd A$. Za lokalizaciju A_S uobičajena oznaka je A_P umesto $A_{A \setminus P}$. Elementi prstena A_P su formalni razlomci:

$$A_P = \left\{ \frac{a}{b} \;\mid\; a, b \in A \;,\; b \notin P \right\}$$

dok su njegovi invertibilni elementi:

$$A_P^* = \left\{ \frac{a}{b} \;\mid\; a \notin P \;,\; b \notin P \right\}$$

Dobijeni prsten A_P ima lepu osobinu - on ima tačno jedan maksimalan ideal, u oznaci P_P ili PA_P, u kome se nalaze svi neinvertibilni elementi domena A:

$$P_P = \left\{ \frac{a}{b} \;\mid\; a \in P \;,\; b \notin P \right\}$$

Drugim rečima A_P je *kvazilokalan*[1] domen. Prema 2.2.1 prosti ideli prstena A_P u korespodenciji su sa prostim idealima u A koji su sadržani u P, pa važi $\dim(\mathrm{A_P}) = \mathrm{ht(P)}$.

Teorema 2.2.2.
Neka je A domen sa jednoznačnom faktorizacijom i $S \subseteq A$ multiplikativno zatvoren podskup. Tada je i A_S faktorijalan domen, tj. lokalizacija UFD-a je UFD.

Dokaz. Iskoristimo teoremu Kaplanskog: Domen je UFD akko svaki pravi prost ideal sadrži prost element. Neka je zato $\overline{P} \lhd A_S$ pravi prost ideal. Prema 2.2.1 njemu u korespodenciji odgovara $\overline{P} \cap A = P$ pravi prost ideal u A takav da je

[1] Domen A je kvazilokalan ako zadovoljava jedan od sledećih ekvivalentnih uslova:
(i) A ima tačno jedan maksimalan ideal.
(ii) Svi neinvertibilni elementi domena A sadržani su u nekom pravom idealu.
(iii) Skup svih neinvertibilnih elemenata domena A je jedan ideal.

$P \cap S = \emptyset$. A je po pretpostavci UFD pa ideal $P \lhd A$ sadrži neki prost element p. To znači da je glavni ideal $(p) = pA$ prost. Tada je:

$$(p) \subseteq P \quad \text{pa} \quad P \cap S = \emptyset \;\Rightarrow\; (p) \cap S = \emptyset$$

Sada se opet može primeniti teorema o korespodenciji: prostom idealu $(p) \lhd A$ odgovara prost ideal $(p)A_S \lhd A_S$ tj. element p ostaje prost i u A_S. Kako je $P = \overline{P} \cap A$ to je i $p \in \overline{P}$, pa je p traženi prost element. $\square$

***Veza faktorizacije u* $\mathbf{A}$ *i u* $\mathbf{A_S}$**

Prema prethodnom prost element $p \in A$ postaje invertibilan u A_S ako $p \mid s$ za neko $s \in S$. U suprotnom p ostaje prost i u A_S. Neka je sada A UFD (a samim tim i A_S) i neka je $x \in A_S$. Označimo sa $\mathcal{P}$ skup atoma u A. Element x je oblika $x = a/s = a \cdot 1/s$, $a \in A$, $s \in S$. Dalje je s invertibilan u A_S pa možemo uvesti oznaku $1/s = u \in A_S^*$. Kako je A UFD i $a \in A$ postoji jednoznačna faktorizacija elementa a:

$$a = \prod_{p \in \mathcal{P}} p^{n_p} \tag{1}$$

Ako neki od atoma $p \in \mathcal{P}$ pripada i S, tačnije ako $p \mid s$ za neko $s \in S$, on je invertibilan u A_S jer:

$$p \mid s \;\Rightarrow\; ap = s \;,\; a \in A \;\Rightarrow\; 1/p = a/s \in A_S$$

Takve elemente možemo dakle isključiti iz gornje faktorizacije tj. skup $\mathcal{P}$ možemo redukovati tako što izbacimo skup

$$\mathcal{P}' = \{\, p \in \mathcal{P} \;\mid\; p \mid s \;,\; \textit{za neko } s \in S \,\}$$

Faktorizacija proizvoljnog elementa $x \in A_S$ imaće dakle sledeći oblik:

$$x = u \prod_{p \in \mathcal{P} \setminus \mathcal{P}'} p^{n_p} \qquad u \in A_S^* \tag{2}$$

Ova faktorizacija je jednoznačna prema 2.2.2. Može se reći da su generalno faktorizacije u lokalizaciji "kraće" što je i očekivano jer su neki od atoma postali invertibilni.

Primer 2.2.3.

$$A = k[X, Y]/(XY - 1)$$

k je proizvoljno polje. Ako sa x, y označimo odgovarajuće slike elemenata X, Y pri kanonskom homomorfizmu $k[X, Y] \mapsto A \quad x = X + (XY - 1)$, $y = Y + (XY - 1)$, tada je A generisan elementima x, y nad poljem k sa definišućom relacijom $xy = 1$, pa je

$$A = k[x, y] = k[x, 1/x] = k[x][1/x] = k[x]_S$$

gde je $S = \{\, 1, x, x^2, \dots \}$. Kako je $k[x]$ UFD (glavnoidealski) to je prema 2.2.2 i $A = k[x]_S$ UFD. ▼

Primer 2.2.4.

$$A = \mathbb{C}[X, Y]/(X^2 + Y^2 - 1)$$

$\mathbb{C}$ je polje kompleksnih brojeva. Uz iste oznake kao i u prethodnom primeru imamo da je $A = \mathbb{C}[x, y]$, $x^2 + y^2 = 1$. Ako transformišemo definišuću relaciju na sledeći način:

$$1 = x^2 + y^2 = (x + iy)(x - iy) = uv \qquad x = (u + v)/2 \ , \ y = u - v/2i$$

dobijamo da je $A = \mathbb{C}[u, v]$ sa definišućom relacijom $uv = 1$. Prema prethodnom primeru $\mathbb{C}[U, V]/(UV - 1)$ je UFD, pa je i A UFD. ▼

Primedba. $\mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$ nije UFD.

Može se pokazati npr. da je x atom koji nije prost jer iz jednakosti:

$$x^2 = 1 - y^2 = (1 - y)(1 + y)$$

sledi da $x \mid (1 - y)(1 + y)$. Dalje se pokazuje da $x \nmid 1 - y$, $x \nmid 1 + y$.

Primer 2.2.5.

$$A = \mathbb{Z}[\sqrt{-5}\,] \ , \ P = (3, 2 + \sqrt{-5})$$

A nije UFD dok lokalizacija A_P jeste. Iz ovog primera vidi se da obrat teoreme 2.2.2 u opštem slučaju ne važi. Dodatne uslove pod kojima će to važiti daje poznata Nagatina teorema. ▼

2.3 Nagatina teorema

Teorema 2.3.1 (Nagata)**.** *Neka je A domen koji zadovoljava uslov ACC_1 i $S \subseteq A$ multiplikativno zatvoren podskup generisan prostim elementima. Ako je A_S UFD onda je i A UFD.*

Dokaz. Neka je S generisan prostim elementima $\{ p_i \mid i \in I \}$ i neka je Q pravi prost ideal u A. Dovoljno je pokazati da Q sadrži neki prost element. Ako je $Q \cap S \neq \emptyset$ onda $s = p_1 p_2 \dots p_k \in Q \cap S$ gde su p_i generatori skupa S. Kako je Q prost ideal mora biti $p_1 \in Q \vee \dots \vee p_k \in Q$ pa Q sadrži prost element.
Može se dakle pretpostaviti da nijedan od generatora p_i nije u Q tj. da je $Q \cap S = \emptyset$. Prema 2.2.1 prostom idealu $Q \lhd A$ u korespodenciji odgovara pravi prost ideal $QA_S = \overline{Q} \lhd A_S$. Kako je A_S UFD ideal $\overline{Q}$ sadrži neki element q koji je prost u A_S. Dalje se može pretpostaviti da je $q \in Q$ jer:

$$q = \frac{a}{s} \in \overline{Q} \ , \ a \in Q \ , \ s \in S \ \Rightarrow \ sq = a \in Q$$

$$Q \cap S = \emptyset \ \Rightarrow \ s \notin Q \ \Rightarrow \ q \in Q$$

Takodje se može pretpostaviti da nijedan od generatora p_i skupa S ne deli q jer ako npr. $p_1 \mid q$ onda:

$$\frac{q}{p_1} \in \overline{Q} \cap A = Q \quad \text{i} \quad \frac{q}{p_1} \mid q \ \Rightarrow \ (q) \subsetneq \left(\frac{q}{p_1} \right)$$

$$\frac{q}{p_1p_2} \mid \frac{q}{p_1} \;\Rightarrow\; \left(\frac{q}{p_1}\right) \subsetneq \left(\frac{q}{p_1p_2}\right)$$

Na taj način dobija se lanac $\mathcal{L}$ glavnih ideala u A,

$$\mathcal{L}: \qquad (q) \subsetneq \left(\frac{q}{p_1}\right) \subsetneq \left(\frac{q}{p_1p_2}\right) \subsetneq \left(\frac{q}{p_1p_2p_3}\right) \subsetneq \dots$$

Medjutim u A važi uslov ACC_1 pa se lanac $\mathcal{L}$ mora zaustaviti, tj.

$$(\exists\, m) \quad \text{tako da je} \quad \left(\frac{q}{p_1p_2\dots p_m}\right) = \left(\frac{q}{p_1p_2\dots p_mp_{m+1}}\right)$$

Odavde je $p_{m+1} \in A^*$, što je besmisleno jer su p_i prosti. Ostalo je još da se pokaže da je q prost element u A tj. da je (q) prost ideal u A. Pretpostavimo zato da $ab \in (q)$. Prelaskom u A_S gde je $(q)A_S$ prost dobija se da $a \in (q)A_S$ ili $b \in (q)A_S$. Neka npr. $a \in (q)A_S$. Tada je:

$$a = \frac{c}{s}\, q\ , \quad \text{za neko} \quad s = p_1 \dots p_k \in S$$

$$\text{odavde je} \quad sa = cq \quad \text{tj.} \quad p_1 \dots p_k a = cq \tag{i}$$

Iz poslednje jednačine dobija se da elementi $p_1, \dots, p_k$ dele cq. Kako su p_i prosti elementi koji ne dele q, to znači da $p_i \mid c\ ,\ i = 1, \dots, k$. Odavde je $c = p_1 \dots p_k c'$ pa jednakost (i) postaje:

$$p_1 \dots p_k a = p_1 \dots p_k c' q$$

Odavde je $a = c'q$ pa $q \mid a$ tj. $a \in (q)$. Prema tome (q) je prost ideal u A odnosno q je prost element koji pripada Q što je i trebalo pokazati. $\square$

Nagatina teorema jedno je od najkorisnijih tvrdjenja u teoriji faktorijalnih domena. Njena primena obično daje elegantna rešenja u raznim problemima vezanim za faktorizaciju. Npr. uobičajen način kojim se dokazuje da se faktorijalnost prenosi sa prstena A na prsten polinoma $A[X]$ je primena Gausove leme i može se naći u standardnim udžbenicima komutativne algebre. Ako na raspolaganju imamo Nagatinu teoremu dokaz je znatno kraći.

Teorema 2.3.2.

$$A \text{ UFD} \;\Rightarrow\; \text{A[X] UFD.}$$

Dokaz. Neka je $k = Frac(A)$ količničko polje domena A. Neka je $S = A \setminus \{0\}$. Kako je A prema pretpostavci UFD svaki element $s \in S$ ima prostu faktorizaciju pa je multiplikativno zatvoren podskup $S \subseteq A$ generisan prostim elementima u A. Iz utapanja $A \hookrightarrow A[X]$ možemo smatrati da je S multiplikativno zatvoren podskup u $A[X]$. Kao takav on je takodje generisan prostim elementima. Ovo važi jer ako je p prost element u A onda je:

$$A[X]/pA[X] = (A/pA)\,[X]$$

domen, odnosno glavni ideal $(p) = pA[X] \lhd A[X]$ je prost pa element p ostaje prost i u $A[X]$. Neka je dalje $\mathcal{L}'$ lanac glavnih ideala u $A[X]$.

$\mathcal{L}' : \ (f_1) \subseteq (f_2) \subseteq (f_3) \subseteq \dots$

Neka su $a_i \in A$ vodeći koeficijenti polinoma $f_i \in A[X]$. Tada:

$$(f_1) \subseteq (f_2) \ \Rightarrow \ f_2 \mid f_1 \ \Rightarrow \ a_2 \mid a_1 \ \Rightarrow \ (a_1) \subseteq (a_2)$$

pa se lancu $\mathcal{L}'$ može pridružiti lanac $\mathcal{L}''$ glavnih ideala (a_i) u A generisanih vodećim koeficijentima polinoma f_i.

$\mathcal{L}'' : (a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$

Kako je A UFD lanac $\mathcal{L}''$ se kida, pa se kida i $\mathcal{L}'$ tj. u $A[X]$ važi uslov ACC_1. Kako je $A[X]_S = k[X]$ Euklidov prsten, pa samim tim i UFD ispunjeni su svi uslovi teoreme 2.3.1 pa je $A[X]$ UFD. $\square$
Kako je $A[X, Y] = A[X][Y]$ indukcijom se ova teorema može proširiti na polinome sa više neodredjenih.

Posledica 2.3.3.

$$A \text{ UFD } \Rightarrow \text{ A[X}_1, \text{X}_2, \dots, \text{X}_\text{n} \text{] UFD. } \square$$

Posledica 2.3.4 (Klajn - Nagatina teorema)**.**
Neka je k algebarski zatvoreno polje, $Char(k) \neq 2$ i neka je $F \in k[X_1, \dots, X_n]$ nedegenerisana kvadratna forma, gde je $n \geq 5$. Tada je $A_F = k[X_1, \dots, X_n]/(F)$ UFD.

Dokaz. Može se pretpostaviti da je $F = X_1X_2 + G(X_3, \dots, X_n)$. Polje k je algebarski zatvoreno i $n \geq 5$ pa je polinom $G(X_3, \dots, X_n)$ ireducibilan. Ako sa x_i označimo homomorfne slike $x_i = X_i + (F)$, $i = 1, \dots, n$ dobijamo da je:

$$A_F/x_1A_F \cong k[X_2, \dots, X_n]/(G)$$

pa je A_F/x_1A_F domen tj. x_1 je prost u A_F. Multiplikativno zatvoren podskup $S \subseteq A_F$, $S = \{ 1, x_1, x_1^2, \dots \}$ tada zadovoljava uslove teoreme 2.3.1 jer je generisan prostim elementom x_1 pa je dovoljno dokazati da je odgovarajuća lokalizacija $(A_F)_S = A_F[x_1^{-1}]$ UFD. Kako u A_F važi:

$$0 = F(x_1, x_2, \dots, x_n) = x_1x_2 + G(x_3, \dots, x_n)$$

dobija se: $\quad x_2 = -G(x_3, \dots, x_n)x_1^{-1} \in k[x_3, \dots, x_n, x_1^{-1}]$

pa je: $\quad A_F[x_1^{-1}] = k[x_1, x_2, \dots, x_n][x_1^{-1}] = k[x_1, x_3, \dots, x_n][x_1^{-1}]$

Elementi $x_1, x_3, \dots, x_n$ sada su algebarski nezavisni pa je $k[x_1, x_3, \dots, x_n]$ izomorfan prstenu polinoma sa $n-1$ neodredjenih nad poljem k koji je prema 2.3.3 UFD. Prema 2.2.2 i njegova lokalizacija $(A_F)_S = A_F[x_1^{-1}]$ je UFD što je i trebalo dokazati. $\square$

Primer 2.3.5 (Samuel)**.**

$$A = k[X, Y, Z]/(X^2 + Y^2 + Z^2 - 1)$$

A je UFD ako je k polje, $Char(k) \neq 2$ tako da $i \notin k$.

Dokaz. Označimo sa x, y, z slike pri kanonskom homomorfizmu. Pri ovim oznakama $A = k[x, y, z]$ gde je $x^2 + y^2 + z^2 = 1$ odnosno $x^2 + y^2 = (1 - z)(1 + z)$

$$A/(z-1) = k[x, y, z]/(z-1) = k[X, Y, Z]/F \;/\; (F, 1-Z)/F = k[X, Y, Z]/(F, 1-Z)$$

$$= k[X, Y, Z]/(1 - Z) \;/\; (F, 1 - Z)/(1 - Z) = k[X, Y]/(X^2 + Y^2)$$

gde je sa F označen ideal $F = (X^2 + Y^2 + Z^2 - 1)$. Kako je $Char(k) \neq 2$ i $i \notin k$, polinom $X^2 + Y^2$ je ireducibilan pa je ideal $(X^2 + Y^2)$ prost, odakle je $A/(z - 1)$ domen, tj. $(z - 1)$ je prost u A. Neka je $S = \{\, 1, z - 1, (z - 1)^2, \dots \}$ i $t = (z - 1)^{-1}$.

$$x^2 + y^2 = -(z - 1)(z + 1) \;\Rightarrow\; z + 1 = -t(x^2 + y^2) \;\Rightarrow\; z \in k[x, y, t]$$

odakle je: $$A[t] = k[x, y, z, t] = k[x, y, t]$$

Kako je $1/t = z - 1 = -t(x^2 + y^2) - 2 \in k[x, y, t]$ važi inkluzija $k[tx, ty, 1/t] \subseteq k[x, y, t]$. Sdruge strane je:

$$(tx)^2 + (ty)^2 = t^2(1 - z^2) = t^2(1 - (1/t + 1)^2) = t^2(-2/t - 1/t^2) = -2t - 1$$

odakle je $t = -1/2((tx)^2 + (ty)^2 + 1) \in k[tx, ty]$, $x = (tx) \cdot 1/t$, $y = (ty) \cdot 1/t$ pa $x, y \in k[tx, ty, 1/t]$. Važi dakle i obratna inkluzija $k[x, y, t] \subseteq k[tx, ty, 1/t]$ pa je:

$$k[x, y, t] = k[tx, ty, 1/t] = k[tx, ty][1/t] = k[tx, ty]_T$$

gde je T multiplikativno zatvoren podskup $T = \{\, 1, t, t^2, \dots \}$. $k[tx, ty]$ je prsten polinoma sa dve neodredjene pa je UFD a ujedno je to i $k[tx, ty]_T = A[t]$ kao njegova lokalizacija. Medjutim $A[t] = A_S$ gde je S generisan prostim elementom $z - 1$ pa je i A UFD prema Nagatinoj teoremi. □

Na sličan način može se pokazati da je $k[X, Y, Z]/(X^r + Y^s + Z^t)$ UFD ako su r, s, t uzajamno prosti i k proizvoljno polje [24].

2.4 Faktorizacija u integralnim raširenjima

Definicija 2.4.1. *Neka je A potprsten prstena B. Element $\alpha \in B$ je ceo nad A ako postoji moničan polinom $g \in A[X]$ takav da je $g(\alpha) = 0$.*

Može se pokazati da je α ceo akko je $A[\alpha]$ konačno generisan A-modul. Skup svih celih elemenata $A' = \{\, \alpha \in B \mid \alpha \text{ ceo nad } A \,\}$ je tada jedan potprsten prstena B koji zovemo *integralnim zatvorenjem* prstena A u B. Specijalno, ako je $A' = B$ kažemo da je B *celo raširenje prstena* A, a ako je $A' = A$ kažemo da je A *integralno zatvoren* u B.

Definicija 2.4.2. *Neka je A domen i $k = Frac(A)$ njegovo polje razlomaka. Domen A je integralno zatvoren ako je integralno zatvoren u k.*

Neke od osobina celih raširenja i integralno zatvorenih domena dajemo u obliku sledećeg tvrdjenja. Dokazi se mogu naći u [15].

Tvrdjenje 2.4.3. *Neka je A' celo raširenje prstena A. Tada važe sledeće osobine:*
(1) *Ako je A' domen onda je i A domen.*
(2) *Ako je A' domen onda je A' polje akko A je polje.*
(3) *Ako je $S \subseteq A$ multiplikativan onda je A'_S celo raširenje od A_S.*
(4) *Par (A, A') zadovoljava GU, LO, INC.*
(5) *Par (A, A') zadovoljava i GD ako je A' domen i A integralno zatvoren.*
(6) $\dim(\mathrm{A}) = \dim(\mathrm{A}')$.
(7) *Ako je A' kvazilokalan onda je i A kvazilokalan.*
(8) *Presek $\bigcap_{i \in I} A_i$ familije integralno zatvorenih domena A_i je integralno zatvoren.*
(9) *Lokalizacija integralno zatvorenog domena je integralno zatvoren domen.*

Integralna raširenja ne čuvaju faktorijalnost što se može videti u brojnim primerima prstena algebarskih celih $\mathbb{Q}(d)$. Svi ovi prsteni su cela raširenja faktorijalnog domena $\mathbb{Z}$. Kao što smo već videli u mnogima od njih faktorizacija nije jednoznačna. Sledeći primer pokazuje da je moguć i obratan slučaj; u celom raširenju A' faktorizacija je jednoznačna dok u A nije.

Primer 2.4.4.

$$A = \mathbb{Z}[\sqrt{-3}\,] = \{\, m + n\sqrt{-3} \;\mid\; m, n \in \mathbb{Z} \,\}$$

Lako se može videti da A nije faktorijalan. Npr. 2 je atom ovog prstena koji nije prost. Jednačina $m^2 + 3n^2 = 2$ nema celobrojnih rešenja pa su elementi $1+\sqrt{-3}, 1-\sqrt{-3}$ ireducibilni i $2 \mid (1+\sqrt{-3})(1-\sqrt{-3})$, $2 \nmid 1+\sqrt{-3}$, $2 \nmid 1-\sqrt{-3}$ S druge strane njegovo celo raširenje:

$$\mathbb{Q}(-3) = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] \qquad \text{je glavni domen pa je UFD. } \blacktriangledown$$

Već iz ovih primera vidimo da u opštem slučaju cela raširenja nisu zanimljiva sa stanovišta faktorizacije. Faktorijalni domeni pripadaju medjutim širokoj klasi integralno zatvorenih domena.

Teorema 2.4.5. *Gausov domen A je integralno zatvoren.*

Dokaz. Neka je $k = Frac(A)$ i $\alpha \in k$ ceo nad A. Tada postoji moničan polinom $g \in A[X]$ takav da je $g(\alpha) = 0$. Neka je:

$$g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \quad , \; a_0, a_1, \ldots a_{n-1} \in A$$

Za element $\alpha = u/v \in k$ može se pretpostaviti da je "neskrativ razlomak" tj. $\mathrm{nzd}[u, v] = 1$. Ovo važi jer je domen A prema pretpostavci Gausov, pa

u suprotnom možemo podeliti u i v njihovim najvećim zajedničkim deliteljem. Kako je $g(\alpha) = 0$, na taj način dobijamo:

$$\left(\frac{u}{v}\right)^n + a_{n-1}\left(\frac{u}{v}\right)^{n-1} + \cdots + a_1\left(\frac{u}{v}\right) + a_0 = 0$$

Množenjem gornje jednakosti sa v^n dobijamo:

$$u^n + a_{n-1}vu^{n-1} + \cdots + a_1v^{n-1}u + a_0v^n = 0$$

odnosno: $$u^n = v(-a_{n-1}u^{n-1} - \cdots - a_1v^{n-2} - a_0v^{n-1})$$

Odavde dobijamo da $v \mid u^n$. Medjutim nzd$[u, v] = 1$ pa mora biti $v \in A^*$ tj. $\alpha = u/v \in A$. □

Posledica 2.4.6. *Svaki UFD je integralno zatvoren.* □

Primer 2.4.7.

$$A = \{\, a + 2bi \mid a, b \in \mathbb{Z} \,\}$$

A je potprsten Gausovog prstena $B = \mathbb{Z}[i]$, pa je $Frac(A) \subseteq Frac(B) = \mathbb{Q}[i]$. Neka je $u \in Frac(A)$ ceo nad A. Tada postoji moničan polinom $f \in A[X]$ takav da je $f(u) = 0$. S obzirom da je tada $f \in B[X]$ i $u \in Frac(B)$ iz jednakosti $f(u) = 0$ dobijamo da je u ceo nad B. Kako je B UFD on je i integralno zatvoren, pa $u \in B$. Odavde je $A' \subseteq B$.
Neka je sada $\alpha \in B$, $\alpha = a + bi$ $a, b \in Z$. Tada je $(\alpha - a)^2 = -b^2$, odnosno $\alpha^2 - 2a\alpha + a^2 + b^2 = 0$. Postoji dakle moničan polinom $p \in \mathbb{Z}[X] \subseteq A[X]$ koji α poništava:

$$p(x) = x^2 - 2ax + a^2 + b^2 \quad , \quad p(\alpha) = 0$$

Odavde je α ceo nad A tj. $B \subseteq A'$. Integralno zatvorenje domena A je dakle $A' = B \neq A$ pa A nije integralno zatvoren. Prema prethodnoj posledici A nije UFD. ▼
Postoje naravno integralno zatvoreni domeni u kojima faktorizacija nije jednoznačna. Takav je npr. domen $A = \mathbb{Z}[\sqrt{-5}\,]$. Odavde vidimo da obratno u posledici 2.4.6 ne mora da važi.

2.5 Jednoznačna faktorizacija u kompletno integralno zatvorenim domenima

Definicija 2.5.1. *Neka je A domen i $k = Frac(A)$. A-podmodul I polja k je razlomljen ideal ako postoji $d \in A \setminus \{0\}$ tako da je $dI \subseteq A$.*

Obični ideali domena A su prema ovoj definiciji razlomljeni i njih zovemo celim idealima. Razlomljen ideal je pravi razlomljen ideal ako je različit od nule. Skup svih pravih razlomljenih ideala označavamo sa $I(A)$. Ako $P, Q \in I(A)$ onda i $P : Q \in I(A)$, gde je $P : Q = \{\, x \in k \mid xQ \subseteq P \,\}$.

Definicija 2.5.2. *Element $x \in k$ je skoro ceo nad A ako je ideal $A[x] = \sum_{k=0}^{\infty} Ax^k$ razlomljen.*

Prema ovoj definiciji element x je skoro ceo ako postoji $d \in A$, $d \neq 0$ takav da je $dA[x] \subseteq A$ tj. svi njegovi stepeni imaju isti imenilac: $x^n = a_n/d$, $a_n \in A$, $n \in \mathbb{N}$. Svi celi elementi su naravno i skoro celi. Može se dati karakterizacija skoro celih elemenata preko razlomljenih ideala: $x \in k$ je skoro ceo akko postoji $P \in I(A)$ takav da je $x \in P : P$. Može se takodje pokazati da je skup:

$$\widetilde{A} = \{\ x \in k \mid x \text{ skoro ceo nad } A\ \}$$

jedan potprsten polja k koji zovemo kompletnim integralnim zatvorenjem domena A.

Definicija 2.5.3. *Domen A je kompletno integralno zatvoren ako je $A = \widetilde{A}$.*

Ako je A kompletno integralno zatvoren domen onda je svaki skoro ceo $x \in k$ u A. Kako je svaki ceo i skoro ceo onda su i svi celi u A tj. A je i integralno zatvoren. Odavde je dakle svaki kompletno integralno zatvoren domen i integralno zatvoren, uz napomenu da u Neterinim domenima važi i obratno. Takodje je i presek familije kompletno integralno zatvorenih domena kompletno integralno zatvoren. Preko razlomljenih ideala može se dati sledeća karakterizacija: domen A je kompletno integralno zatvoren akko $A = P : P$ za svaki razlomljen ideal $P \in I(A)$. Da bi utvrdili vezu faktorijalnih i kompletno integralno zatvorenih domena potrebno je nekoliko pomoćnih tvrdjenja.

Lema 2.5.4. *Presek familije glavnih ideala u faktorijalnom domenu A je glavni ideal.*

Dokaz. Neka je $(a_i)_{i\in I}$ familija glavnih ideala u A. Svaki od elemenata a_i ima jednoznačnu faktorizaciju:

$$a_i = u_i \prod_{p_k \in \mathcal{P}} p_k^{\alpha_{ik}} \quad , \quad u_i \in A^*$$

U slučaju trivijalnog preseka $\bigcap_{i\in I}(a_i) = (0)$ je očigledno glavni ideal. U slučaju da je presek različit od nule biće:

$$\bigcap_{i\in I}(a_i) = (d) \quad \text{gde je} \quad d = \prod_{p_k \in \mathcal{P}} p_k^{max\{\alpha_{ik}|i\in I\}} \qquad \square$$

Lema 2.5.5. *Neka je A UFD i $p \in A$, $p \notin A^*$. Tada je $\bigcap_{n\in\mathbb{N}}(p^n) = (0)$.*

Dokaz. Pretpostavimo suprotno, da je

$$\bigcap_{n\in\mathbb{N}}(p^n) \neq (0)$$

Prema prethodnoj lemi presek je neki glavni ideal (q) , $q \neq 0$. Tada:

$$\bigcap_{n\in\mathbb{N}} (p^n) = (q) \;\Rightarrow\; (q) \subseteq (p^n) \;,\; \forall\, n \;\Rightarrow\; \forall\, n \;\; q = a_n p^n \text{ za neko } a_n \in A$$

$$\Rightarrow\; qp^{-1} = a_n p^{n-1} \in (p^{n-1}) \;,\; \forall\, n \;,\; n > 1 \text{ pa: } qp^{-1} \in \bigcap_{n>1} (p^n) = (q)$$

$$\text{jer je } (p^k) \subseteq (p) \;,\; k > 1. \text{ Odavde je } qp^{-1} = aq \text{ tj. } q(ap-1) = 0$$

Kako je $q \neq 0$ mora biti $ap = 1$ tj. $p \in A^*$ što je kontradikcija. □

Teorema 2.5.6. *Domen A sa jednoznačnom faktorizacijom je kompletno integralno zatvoren.*

Dokaz. Neka je A UFD, $k = Frac(A)$ i $x = u/v \in k$ skoro ceo nad A. Može se pretpostaviti da je $\text{nzd}[u, v] = 1$. Kako je x skoro ceo nad A postoji $d \in A \setminus \{0\}$ tako da je $dx^n \in A$,$\forall\, n \in \mathbb{N}$. Odavde je:

$$d\frac{u^n}{v^n} \in A \;,\; \forall\, n \;\Rightarrow\; v^n \mid du^n \;,\; \forall\, n$$

$$\text{nzd}[u^n, v^n] = 1 \;\Rightarrow\; v^n \mid d \;,\; \forall\, n$$

$$\Rightarrow\; (d) \subseteq (v^n) \;,\; \forall\, n \;\Rightarrow\; (d) \subseteq \bigcap_{n\in\mathbb{N}} (v^n) = (0) \qquad \text{prema lemi 2.5.5}$$

Odavde je dakle $d = 0$ što je kontradikcija. Mora dakle biti $v \in A^*$, odakle $x = u/v \in A$. □

Primer 2.5.7.

$$A = k[X, XY, XY^2, \dots] \;,\; k \text{ polje}$$

$Y = XY/X$ pa $Y \in Frac(A)$. Kako $XY^n \in A$, Y je skoro ceo nad A. Na taj način vidimo da A nije kompletno integralno zatvoren jer $Y \notin A$. Prema prethodnoj teoremi A nije UFD. ▼

Postoje kompletno integralno zatvoreni domeni koji nisu faktorijalni. Takvi su npr. svi prsteni algebarskih celih u kojima faktorizacija nije jednoznačna. Obrat prethodne teoreme prema tome ne važi.

2.6 Faktorizacija u prstenu polinoma i prstenu formalnih redova

Faktorizacija u prstenu polinoma potpuno je odredjena teoremom 2.3.3. Ako je A domen sa jednoznačnom faktorizacijom takvi su i $A[X]$, $A[X_1, X_2, \dots, X_n]$. Prsten formalnih redova ne mora medjutim imati ovu osobinu mada se kontraprimer ne može baš lako naći. Jedan od načina konstrukcije faktorijalnog domena A pri čemu $A[[X]]$ nije UFD dat je sledećim tvrdjenjem. Detalji ove konstrukcije mogu se naći u [24].

Tvrdjenje 2.6.1. *Neka je A Neterin domen $x, y, z \in A$ i $m, n, p \in \mathbb{N}$ takvi da su ispunjeni sledeći uslovi:*
(i) $mnp \geq mn + np + pm$
(ii) y *prost*
(iii) $z \notin (y)$
(iv) $x^{m-1} \notin (y, z)$, $x^m \in (y^p, z^n)$
Tada $A[[X]]$ *nije UFD.* $\square$

Primer 2.6.2.

$$A = k[X, Y, Z]/(Z^p - X^{p+1} - Y^{2p+1})$$

gde je k polje, $Char(k) = p \geq 3$. Može se pokazati da je A UFD koji zadovoljava uslove prethodnog tvrdjenja pa $A[[T]]$ nije UFD. ▼

Formalni redovi u opštem slučaju dakle ne čuvaju faktorijalnost. Da bi se faktorijalnost prenela sa A na $A[[X]]$ potreban je, kao što ćemo videti u poglavlju o Krulovim domenima, dodatni uslov: regularnost prstena. Što se ostalih osobina tiče istaknimo da se kompletna integralna zatvorenost prenosi sa domena A na $A[X]$ kao i na $A[[X]]$. S druge strane integralna zatvorenost domena A prenosi se na prsten polinoma dok to nije slučaj i sa formalnim redovima.

Glava 3

Grupa valuacija faktorijalnog domena

Promenom pristupa proučavanju jednoznačne faktorizacije u domenima, tako što umesto prstena A posmatramo samo njegov monoid $(A \setminus \{0\}, \cdot)$, dobija se nova karakterizacija faktorijalnosti kao i mnogi drugi zanimljivi rezultati. Jednoznačna faktorizacija je naime multiplikativno svojstvo prstena, pa zato ima smisla posmatrati ove monoide.
Na proizvoljnom monoidu sa kraćenjem[1] M relacija deljivosti

$$a \mid b \Leftrightarrow b = ac \quad \text{za neko } c \in M \tag{i}$$

predstavlja očigledno jedno preduredjenje. Sada iz $a \mid b$ i $b \mid a$ dobijamo $a = bc$, $b = ad$ tj. $a = adc$. S obzirom da je M monoid sa kraćenjem, mora biti $dc = 1$ gde je sa 1 označen neutralni element monoida M. Odavde su d i c invertibilni, odnosno a i b su asocirani elementi. To posebno znači da je $a = b$, odnosno (i) je parcijalno uredjenje na M, akko je 1 jedini invertibilan element u M. Takve monoide zovemo *koničnim.* Od proizvoljnog monoida M može se naravno konstruisati koničan M/U, gde je sa U označena njegova podgrupa jedinica, što posebno znači da se svaki monoid sa kraćenjem može urediti na opisani način. Cohn u [6] daje sledeću definiciju UF-monoida;

Definicija 3.0.3. *Komutativan monoid sa kraćenjem M je UF-monoid ako je njegov asocirani koničan monoid M/U slobodan komutativan.*

Na taj način priča o domenima sa jednoznačnom faktorizacijom postaje priča o UF-monoidima; domen A je naime UFD akko njegovi nenulti elementi formiraju UF-monoid u odnosu na množenje. Osobine monoida $(A \setminus \{0\}, \cdot)$ koji nas ovde interesuje operativnije je proučavati ako ga posmatramo kao podmonoid pozitivnih elemenata grupe valuacija $G(A)$. Naredno poglavlje posvećeno je stoga uredjenim grupama i posebno grupi valuacija.

[1] Posebno, ako je A domen, onda njegovi elementi različiti od nule formiraju monoid sa kraćenjem.

3.1 Osnovne osobine valuacionih domena

Definicija 3.1.1. *Neka je A domen i $k = Frac(A)$. A je valuacioni domen ako zadovoljava jedan od ekvivalentnih uslova:*
(1) $\forall a, b \in A \quad a \mid b \ \vee \ b \mid a$
(2) $\forall a, b \in A \quad (a) \subseteq (b) \ \vee \ (b) \subseteq (a)$
(3) $\forall x \in k \qquad x \in A \ \vee \ x^{-1} \in A \ \ tj. \ \ A \cup A^{-1} = k$

Neka su I, J proizvoljni ideali valuacionog domena A takvi da $I \nsubseteq J$ tj. postoji $x \in I$, $x \notin J$ i neka je $y \neq 0$ proizvoljan element iz J. Tada $y \nmid x$ jer bi u suprotnom $x = ya \in J$. To znači da $x \mid y$ tj. $y/x \in A$. Odavde je $y = x(y/x) \in I$ pa je $J \subseteq I$. Odavde vidimo da ideali u valuacionom domenu obrazuju linearno uredjen skup u odnosu na inkluziju. To posebno znači da je svaki valuacioni domen i kvazilokalan. Ako odgovarajući maksimalan ideal označimo sa $\mathfrak{m}$ prema uslovu (3) je $k \setminus A = \{x \in k^* \mid x^{-1} \in \mathfrak{m}\}$. Na taj način prsten A potpuno je odredjen svojim maksimalnim idealom $\mathfrak{m}$ i poljem k. Osim toga, iz uslova (1) sledi da za svaki par elemenata a, b valuacionog domena A postoji nzd$[a, b]$ (koji je jednak a ili b) tj. A je Bezuov pa dakle i Gausov domen. To nam posebno govori da su atomični valuacioni domeni i faktorijalni. Sada su prema teoremi 2.4.5 valuacioni domeni i integralno zatvoreni. Može se pokazati da važi sledeća teorema koja povezuje valuacione i integralno zatvorene domene [15]:

Teorema 3.1.2. *Domen A je integralno zatvoren akko $A = \bigcap_\alpha V_\alpha$ gde su V_α valuacioni domeni, $A \subseteq V_\alpha \subseteq k$, $k = Frac(A)$.* $\square$

Kako je svaki UFD integralno zatvoren, prema ovoj teoremi svaki UFD je presek nekih valuacionih domena, pa je zbog toga ova klasa domena zanimljiva za pitanja faktorijalnosti.

3.2 Grupa valuacija

Definicija 3.2.1. *Neka je A domen, $k = Frac(A)$ njegovo polje razlomaka, k^* multiplikativna grupa polja k i A^* podgrupa invertibilnih elemenata iz A. Grupa valuacija $G(A)$ domena A je faktorgrupa k^*/A^*.*

Za $x, y \in k^*$ može se definisati relacija $\leq$ na sledeći način:

$$x \leq y \overset{\text{def}}{\Leftrightarrow} x \mid y \text{ (u A)} \Leftrightarrow yx^{-1} \in A \Leftrightarrow Ax \supseteq Ay$$

Ovako definisana relacija očigledno je refleksivna i tranzitivna pa predstavlja jedno preduredjenje na k^*. Ako za $x, y \in k^*$ stavimo,

$$x \sim y \Leftrightarrow x \mid y \, , \, y \mid x \Leftrightarrow Ax = Ay \Leftrightarrow y = xa \, , \, a \in A^* \Leftrightarrow y \in xA^*,$$

$G(A) = k^*/A^*$ postaje uredjena grupa. Ako sa $x^* = xA^*$, $y^* = yA^*$ označimo slike elemenata $x, y \in k^*$ pri kanonskom homomorfizmu $k^* \to k^*/A^*$, onda je uredjenje na $G(A)$ dato sa:

$$x^* \leq y^* \Leftrightarrow x \mid y \text{ (u A)} \Leftrightarrow Ax \supseteq Ay \tag{1}$$

Ovako uvedeno uredjenje saglasno je sa operacijom, tj. važi

$$x \mid y \Rightarrow xz \mid yz \quad \forall z \in k^* \tag{2}$$

Ako je poznata struktura grupe valuacija $G(A)$ onda se mogu dobiti značajne informacije o samom domenu, naime neke od unutrašnjih osobina domena mogu se formulasati u ovim terminima. To će posebno važiti i za jednoznačnu faktorizaciju; Za domen A važi:

(1) A je UFD akko je $G(A) \cong \mathbb{Z}^{(I)}$ (teorema 3.2.16).
(2) A je valuacioni akko je $G(A)$ linearno uredjena.
(3) A je Gausov akko je $G(A)$ mrežasto uredjena.
(4) A je DVR akko je $G(A) \cong \mathbb{Z}$.
(5) A je Krulov akko je $G(A) \cong H$, gde je H neka podgrupa grupe $\mathbb{Z}^{(I)}$.

Ove ekvivalencije govore o značaju i bliskoj povezanosti grupe valuacija nekog domena i njegovih karakteristika. Za poredjenje služi grupa $\mathbb{Z}^{(I)}$, sa komponentnim uredjenjem:

$$(a_i)_{i\in I} \leq (b_i)_{i\in I} \overset{\text{def}}{\Longleftrightarrow} a_i \leq b_i \quad \forall i \in I \tag{3}$$

Primetimo da (1) predstavlja suštinski novu karakterizaciju faktorijalnih domena. Sam dokaz zahteva poznavanje nekih osobina uredjenih grupa koje ćemo ukratko izložiti. Detaljnije o teoriji uredjenih grupa, potrebnoj za dokaze ostalih tvrdjenja, može se naći u [4].

Uredjene grupe. Grupa $(G, \cdot)$ na kojoj je zadato uredjenje " $\leq$ " je uredjena ako je uvedeno uredjenje saglasno sa operacijom grupe, tj. ako je za svako $a, b \in G$ ispunjen uslov: $a \leq b \Rightarrow xa \leq xb$, $ax \leq bx$, $\forall x \in G$. Iz ove osobine i tranzitivnosti relacije " $\leq$ " dobija se da u svakoj uredjenoj grupi važi:

$$a \leq b\,,\, c \leq d \Rightarrow ac \leq bd \tag{4}$$

Element $a \in G$ je *pozitivan* ako je $1 \leq a$. Ako sa $P = \{\, x \in G \mid 1 \leq x \,\}$, označimo skup svih pozitivnih elemenata uredjene grupe G, dobijeni skup P je prema (4) multiplikativan, pa predstavlja jednu podpolugrupu grupe G. Pritom za $a, b \in G$ važi: $a \leq b \Leftrightarrow 1 \leq ba^{-1} \Leftrightarrow ba^{-1} \in P$, pa je polugrupom pozitivnih elemenata P, uredjenje " $\leq$ " potpuno odredjeno.

Lema 3.2.2 ([17]). *Neka je G grupa i P njena podpolugrupa. Tada na G postoji uredjenje u odnosu na koje je P polugrupa pozitivnih elemenata akko su ispunjeni sledeći uslovi:*
(a) $1 \in P$.
(b) $a \in P\,,\, a^{-1} \in P \Rightarrow a = 1$.
(c) $a \in P\,,\, x \in G \Rightarrow x^{-1}ax \in P$. $\square$

Ako je uz to grupa G linearno uredjena i $a \notin P$, odnosno $a < 1$, onda je $1 = aa^{-1} < a^{-1}$ pa $a^{-1} \in P$. S druge strane, ako uz uslove prethodne leme važi

i uslov,

$$(d) \qquad \forall a \in G \quad a \in P \vee a^{-1} \in P$$

neposredno se može proveriti da je onda formulom:

$$a \leq b \overset{\text{def}}{\iff} ba^{-1} \in P \tag{5}$$

definisano jedno linearno uredjenje grupe G. Na taj način dobija se sledeća lema.

Lema 3.2.3. *Polugrupa P pozitivnih elemenata grupe G definiše linearno uredjenje na G akko uz uslove prethodne leme važi i uslov (d).* □

Definicija 3.2.4. *Uredjena grupa G generisana polugrupom svojih pozitivnih elemenata, $G = PP^{-1}$, naziva se usmerenom (filterskom) grupom*[2].

Definicija 3.2.5. *Grupa G je mrežasto uredjena ako svaki konačan podskup*[3] *elemenata ima supremum i infimum.*

Može se pokazati da je mrežasto uredjenje i filtersko uz napomenu da ne mora da važi i obratno. Podgrupa mrežasto uredjene grupe ne mora biti mrežasto uredjena. Proizvod $\prod_{i\in I} G_i$, familije uredjenih grupa $(G_i)_{i\in I}$, je uredjena grupa ako se uvede komponentno uredjenje: $(x_i)_{i\in I} \leq (y_i)_{i\in I}$ akko $x_i \leq y_i\,,\ \forall i \in I$. Pri tome je proizvod mrežasto uredjenih grupa takodje mrežasto uredjena. Posebno je odavde i $\mathbb{Z}^{(I)} = \{\,(x_i)_{i\in I} \mid x_i \in \mathbb{Z}\,,\ x_i \neq 0$ samo za konačno mnogo $i \in I\,\}$ mrežasto uredjena grupa. Zbog rada sa Abelovim grupama ovde je pogodnije koristiti aditivnu notaciju. Ako grupu označimo aditivno sa $(G,+)$ a sa $P = \{\,x \in G \mid x \geq 0\,\}$ polugrupu pozitvnih elemenata onda uslovi $(a),(b)$ leme 3.2.2 postaju:
(a') $0 \in P$.
(b') $a \in P\,,\ -a \in P \Rightarrow a = 0$ tj. $P \cap (-P) = \{0\}$.
dok je uslov (c) suvišan u komutativnom slučaju. Uslov (d) i relacija (5) su ovde: (d') $P \cup (-P) = G$ odnosno $(5')$ $a \leq b \Leftrightarrow b - a \in P$. Za mrežasto uredjene grupe važi sledeće tvrdjenje ([4]).

Tvrdjenje 3.2.6. *Neka je G uredjena grupa i P polugrupa njenih pozitivnih elemenata. Grupa G je mrežasto uredjena akko su ispunjeni sledeći uslovi:*
1) *G je filterska ($G = P - P$).*
2) $(\forall x, y \in P)(\exists^4 \sup_P(x,y))$. □

Ovi rezultati mogu se sada primeniti na grupu valuacija, odnosno na njoj izomorfnu grupu glavnih razlomljenih ideala $\mathcal{P}^*$.

Grupa $\mathcal{P}^*$. Neka je A domen, $k = Frac(A)$ polje razlomaka, $G(A) = k^*/A^*$

[2]Ovaj uslov ekvivalentan je uslovu $(\forall a, b \in G)(\exists c \in G)\, a \leq c\,,\ b \leq c$.
[3]Dovoljno je raći: svaki par elemenata.
[4]Ovaj uslov može se zameniti ekvivalentnim: $(\forall x, y \in P)(\exists \inf_P(x,y))$.

grupa valuacija i $\mathcal{P}^* = \{ Ax \mid x \in k^* \}$ grupa glavnih razlomljenih ideala (operacija je proizvod razlomljenih ideala $AxAy = Axy$). Tada je preslikavanjem $xA^* \mapsto xA$ očigledno definisan izomorfizam $G(A) \cong \mathcal{P}^*$. Ako grupu $\mathcal{P}^*$ uredimo inkluzijom ovaj izomorfizam menja poredak, tj. važi $x^* \leq y^* \Leftrightarrow Ax \supseteq Ay$. Iz tog razloga uredjenje " $\leq$ " na $\mathcal{P}^*$ definišemo suprotno inkluziji: $Ax \leq Ay \overset{\text{def}}{\Leftrightarrow} Ax \supseteq Ay$. Na taj način izomorfizam $\varphi : G(A) \to \mathcal{P}^*$, definisan sa $\varphi(x^*) = Ax$, čuva poredak, tj. važi $x^* \leq y^* \Leftrightarrow Ax \leq Ay$. Sada je: $x^* \geq 1^* \Leftrightarrow Ax \geq A \Leftrightarrow Ax \subseteq A$, pa su pozitivni elementi grupe $\mathcal{P}^*$ upravo celi ideali domena A, dok su pozitivni elementi grupe valuacija svi nenulti elementi domena A ($x^* \geq 1^* \Leftrightarrow 1 \mid x \Leftrightarrow x \in A\,,\, x \neq 0$). Kako je $P \cap P^{-1} = A^*$ i $1 \in P$, to je prema lemi 3.2.2 $G(A)$ uredjena grupa. Ona će biti i linearno uredjena akko je $P \cup P^{-1} = k$ tj. akko $(\forall x \in k)\, x \in A \vee x^{-1} \in A$. Poslednje upravo znači da je A valuacioni domen. Takodje je $\mathcal{P}^*$, odnosno $G(A)$ filterska grupa jer je $k = Frac(A)$ pa je svaki $x \in k$ oblika $x = a/b = ab^{-1}\,,\, a, b \in A\,,\, b \neq 0$. Neka su sada $x, y \in k^*$. Grupa $\mathcal{P}^*$ obično je uredjena inkluzijom, dok je $Ax \leq Ay \Leftrightarrow Ax \supseteq Ay$ u cilju čuvanja poretka. Ovde može doći do zabune koja se može izbeći isticanjem uredjenja koje posmatramo:

$$\inf(x, y) = d = \operatorname{nzd}[x, y] \Leftrightarrow \sup{}_{\subset}(Ax, Ay) = Ad = \inf{}_{\leq}(Ax, Ay) \qquad (6)$$

$$\sup(x, y) = m = \operatorname{nzs}[x, y] \Leftrightarrow \inf{}_{\subset}(Ax, Ay) = Am = \sup{}_{\leq}(Ax, Ay) \qquad (7)$$

Infimum i supremum naravno ne moraju postojati, a ako postoje odredjeni su do na množenje invertibilnim elementima iz A^*. U jednakostima (6) i (7) prepoznaju se uslovi iz definicije Gausovog domena. Važi: A je Gausov domen akko je grupa valuacija $G(A)$ mrežasto uredjena. Sada se, koristeći osobine supremuma i infimuma, može pokazati da svaki element x mrežasto uredjene grupe G ima reprezentaciju $x = x^+ - x^-$, gde je $x^+ = \sup(x, 0)\,,\, x^- = \sup(-x, 0)$ i važi $\inf(x^+, x^-) = 0$. Preformulacija na grupu valuacija, odnosno na $\mathcal{P}^*$ je poznata osobina Gausovih domena; ako je $\mathcal{P}^*$ mrežasto uredjena, odnosno ako je A Gausov domen, onda se svaki element $x \in k^*$ može predstaviti u obliku "neskrativog razlomka" $x = u/v$, gde su $u, v \in A$ koprosti, tj. $\inf(u, v) = \operatorname{nzd}[u, v] = 1$. Elementi x, y mrežasto uredjene grupe G su *nezavisni* ako je $\inf(x, y) = 0$[5]. Prema tome, x, y biće nezavisni u $G(A)$ akko su koprosti. S druge strane, (celi) ideali Ax, Ay su nezavisni u $\mathcal{P}^*$ akko $\sup{}_{\subset}(Ax, Ay) = A$ tj. akko je $\inf{}_{\leq}(Ax, Ay) = A$. Osnovne osobine mrežasto uredjenih grupa date su sledećim tvrdjenjem (dokaz [4]).

Tvrdjenje 3.2.7. *U mrežasto uredjenoj grupi G važi:*
(1) $\inf(x - z, y - z) = 0 \Leftrightarrow \inf(x, y) = z$.
(2) $\inf(x, y) = 0\,,\, z \geq 0 \Rightarrow \inf(x, z) = \inf(x, y + z)$.
(3) $\inf(x, y) = 0\,,\, z \geq 0\,,\, x \leq y + z \Rightarrow x \leq z$.
(4) $\inf(x, y) = \inf(x, z) = 0 \Rightarrow \inf(x, y + z) = 0$.
(5) $\inf(x_i, y_j) = 0 \Rightarrow \inf(x_1 + \cdots + x_n, y_1 + \cdots + y_m) = 0$.
(6) $\inf(x_i, x_j) = 0\,,\, i \neq j\,,\, i, j = 1, \ldots, n \Rightarrow \sup(x_1, \ldots, x_n) = x_1 + \ldots x_n$. □

[5]Primetimo da su nezavisni elementi prema definiciji pozitivni.

Ako je A Gausov domen preformulacija ovog tvrdjenja na grupu valuacija $G(A)$ predstavlja uobičajena pravila za rad sa nzd-om i nzs-om;
$(1')$ $x/z, y/z$ su koprosti $\Leftrightarrow z = \operatorname{nzd}[x, y]$.
$(2')$ $\operatorname{nzd}[x, y] = 1\,,\ z \in A \setminus \{0\} \Rightarrow \operatorname{nzd}[x, z] = \operatorname{nzd}[x, yz]$.
$(3')$ $\operatorname{nzd}[x, y] = 1\,,\ z \in A \setminus \{0\}\,,\ x \mid yz \Rightarrow x \mid z$.
$(4')$ $\operatorname{nzd}[x, y] = \operatorname{nzd}[x, z] = 1 \Rightarrow \operatorname{nzd}[x, yz] = 1$.
$(5')$ $\operatorname{nzd}[x_i, y_j] = 1 \Rightarrow \operatorname{nzd}[x_1 \dots x_n, y_1 \dots y_m] = 1$.
$(6')$ $\operatorname{nzd}[x_i, x_j] = 1\,,\ i \neq j \Rightarrow \operatorname{nzs}[x_1, \dots, x_n] = x_1 \dots x_n$.
Ako se za uredjenje grupe $\mathcal{P}^*$ uzme "$\leq$", onda tvrdjenje 3.2.7 ima sledeću formulaciju:
$(1'')$ $\inf(Ax/z, Ay/z) = A \Leftrightarrow \inf(Ax, Ay) = Az$.
$(2'')$ $\inf(Ax, Ay) = A\,,\ Az \subseteq A \Rightarrow \inf(Ax, Ay) = \inf(Ax, Ayz)$.
$(3'')$ $\inf(Ax, Ay) = A\,,\ Az \subseteq A\,,\ Ayz \subseteq Ax \Rightarrow Az \subseteq Ax$.
$(4'')$ $\inf(Ax, Ay) = \inf(Ax, Az) = A \Rightarrow \inf(Ax, Ayz) = A$.
$(5'')$ $\inf(Ax_i, Ay_j) = A \Rightarrow \inf(Ax_1 \dots x_n, Ay_1 \dots y_m) = A$.
$(6'')$ $\inf(Ax_i, Ax_j) = A\,,\ i \neq j \Rightarrow \sup(Ax_1, \dots, Ax_n) = Ax_1 \dots x_n$.

Ekstremalni elementi uredjene grupe.

Definicija 3.2.8. *Element uredjene grupe je ekstremalan ako je minimalan u skupu njenih strogo pozitivnih elemenata.*

Neka je $(G, +)$ uredjena grupa, $x \in G$ njen ekstremalni element i $y \geq 0$ proizvoljan pozitivan element. Tada je moguć jedan od sledećih slučajeva:
(i) $\inf(x, y)$ ne postoji.
(ii) $\inf(x, y) = x$.
(iii) $\inf(x, y) = 0$.
Ako je uredjenje mrežasto uslov (i) otpada, pa je svaki pozitivan element ili veći od ekstremalnog elementa p ili nezavisan s njim. To posebno znači da su svaka dva ekstremalna elementa u mrežasto uredjenoj grupi nezavisna. U grupi $\mathcal{P}^*$ ovo će značiti da je glavni ideal pA ekstremalan akko je maksimalan (u odnosu na inkluziju) medju glavnim idealima u A. U grupi valuacija $G(A)$, $p \in A$ je ekstremalan ako je atom.

Teorema 3.2.9. *Element $x > 0$ uredjene grupe G koji zadovoljava uslov:*

$$(\mathbf{P}) \qquad x \leq y + z\,,\ y \geq 0\,,\ z \geq 0 \Rightarrow x \leq y \ \vee\ x \leq z.$$

je ekstremalan. Obratno, ako je G mrežasto uredjena, onda za ekstremalne elemente važi uslov $\mathbf{P}$.

Dokaz. ($\Rightarrow$:) Neka za x važi uslov $\mathbf{P}$ i neka je $0 \leq y \leq x$. Tada postoji $z \geq 0$ tako da je $x = y + z$. Iz uslova $\mathbf{P}$ mora biti $x \leq y$ ili $x \leq z$. Ako je $x \leq y$ onda iz $y \leq x$ mora biti $x = y$. Ako je $x \leq z$, onda iz $z = x - y$, važi $x \leq x - y$ tj. $y \leq 0$ pa je $y = 0$. Element x je prema tome ekstremalan.
($\Leftarrow$:) Neka je sada G mrežasto uredjena grupa, $x \in G$ ekstremalan i $y, z \in G$ pozitivni elementi. Tada je $\inf(x, y) = 0$ ili $\inf(x, y) = x$. U prvom slučaju x i y su nezavisni pa prema 3.2.7(3) mora biti $x \leq z$. U drugom slučaju je

$\inf(x,y) = x$ pa je $x \leq y$. $\square$
Preformulacija ove teoreme na grupu $G(A)$ daje poznato tvrdjenje: prost element domena je ireducibilan, dok u Gausovom domenu važi i obratno.

Teorema 3.2.10. *Neka je G mrežasto uredjena grupa i G' njena podgrupa generisana ekstremalnim, medjusobno različitim elementima $(p_i)_{i\in I}$. Tada za element $x = \sum_{i\in I} n_i p_i$, $n_i \in \mathbb{Z}$ podgrupe G' važi: x je pozitivan akko $n_i \geq 0$, $\forall i$.*

Dokaz. Neka je $x = \sum_I n_i p_i \geq 0$, $I' = \{i \in I \mid n_i \geq 0\}$, $I'' = \{i \in I \mid n_i \leq 0\}$. Tada

$$x = \sum_{I'} n_i p_i + \sum_{I''} n_j p_j \geq 0 \Rightarrow \sum_{I'} n_i p_i \geq \sum_{I''} \underbrace{(-n_j)}_{\geq 0} p_j \geq p_k \,,$$

za fiksirano $k \in I''$. Prema tome važi: $p_k \leq n_i p_i = p_i + \ldots p_i$, pa je prema uslovu **P**, $p_k \leq p_i$ odakle se dobija kontradikcija $p_k = p_i$. Dalje $I'' = \emptyset$, pa je $I = I' \Rightarrow n_i \geq 0$, $\forall i$. Obratno očigledno važi, jer $n_i \geq 0 \Rightarrow x = \sum n_i p_i \geq 0$, pa je ovim teorema dokazana. $\square$
Primedba. Neka je sada $x = \sum_I n_i p_i = 0$. Tada je $x \geq 0$ i $-x \geq 0$, pa je prema prethodnoj teoremi $n_i \geq 0$ i $-n_i \geq 0$, $\forall i$, odnosno $n_i = 0$, $\forall i$. Ako sada sa $\mathcal{P}(A)$ označimo skup ekstremalnih elemenata uredjene grupe G i sa I skup iste kardinalnosti $Card(I) = Card(\mathcal{P}(A))$, onda je pod uslovima teoreme 3.2.10 sa:

$$(n_i)_{i\in I} \mapsto \sum_{i\in I} n_i p_i \tag{8}$$

definisan izomorfizam grupe $\mathbb{Z}^{(I)}$ i podgrupe G' generisane ekstremalnim elementima. Uslov izomorfizma $G \cong \mathbb{Z}^{(I)}$, je dakle pored mrežaste uredjenosti grupe G i to da je G generisana svojim ekstremalnim elementima. Poslednji uslov može se zameniti ekvivalentnim uslovom:
(**M**) *Svaki neprazan podskup pozitivnih elemenata grupe G sadrži minimalan element.*
Ovde se mogu prepoznati poznati uslovi iz definicije faktorijalnog domena. Uslov **M** je zapravo uslov (**A1**), dok je uslov mrežaste uredjenosti uslov (**A2**).

Teorema 3.2.11. *$\mathbb{Z}^{(I)}$ je mrežasto uredjena grupa u kojoj važi uslov* **M**.

Dokaz. $Z^{(I)}$ je mrežasto uredjena, kao proizvod mrežasto uredjenih grupa. Neka je P' neprazan podskup pozitivnih elemenata u $\mathbb{Z}^{(I)}$ i neka je $x \in P'$. Tada je x oblika $x = \sum n_i e_i$, $n_i \geq 0$, gde je (e_i) standardna baza za $\mathbb{Z}^{(I)}$. Ima konačno mnogo pozitivnih elemenata manjih od x (njihov broj je $\prod(n_i + 1)$), pa je i podskup $P'' \subseteq P'$, pozitivnih iz P' manjih od x konačan. Odavde P'' sadrži minimalan element, koji je minimalan i u P'. $\square$

Primer 3.2.12.

$$G(\mathbb{Z}) = \mathbb{Z}^{(I)} = \sum_{p\in\mathcal{P}} \mathbb{Z} \,,$$

gde je sa $\mathcal{P}$ označen skup prostih brojeva i sa I skup iste kardinalnosti. ▼

Teorema 3.2.13. *Neka je G uredjena grupa u kojoj je ispunjen uslov* **M** *i neka je $\mathcal{P}$ podskup ekstremalnih elemenata u G. Tada:*

$$(\forall x > 0)\,(\exists p \in \mathcal{P})\ \textit{tako da}\ p \leq x\,.$$

Dokaz. Neka je $\mathcal{P}' = \{\, y \in \mathcal{P} \mid 0 < y \leq x \,\}$. Kako je $\mathcal{P}'$ neprazan ($x \in \mathcal{P}'$), iz uslova **M**, u $\mathcal{P}'$ postoji minimalan element p. On je ekstremalan prema definiciji ekstremalnog elementa. □

Teorema 3.2.14. *Ako u uredjenoj filterskoj grupi G važi uslov* **M** *i za svaki ekstremalan element važi uslov* **P**, *G je generisana ekstremalnim elementima.*

Dokaz. Neka je P podskup pozitivnih elemenata u G. Tada je G, s obzirom da je filterska, generisana pozitivnim elementima, $G = P - P$. Dovoljno je zato pokazati da je svaki pozitivan element $x > 0$ suma ekstremalnih. Posmatramo zato skup

$$E = \{\, y \in G \mid y \geq 0\,,\ y = x - (p_1 + \cdots + p_n)\,,\ p_i \in \mathcal{P}\}$$

Kako je $x > 0$, prema teoremi 3.2.13 postoji ekstremalan element $p \in \mathcal{P}$ takav da je $p \leq x$ tj. $y = x - p \geq 0$. Skup E je dakle neprazan, pa iz uslova **M** on ima minimalan element q. Ako pretpostavimo da je $q \neq 0$, onda iz 3.2.13 postoji ekstremalan element p takav da:

$$p \leq q \Rightarrow y = q - p \geq 0 \Rightarrow q - p \in E\ \text{ i }\ q - p < q\,,$$

što je u kontradikciji sa minimalnošću q u E. To znači da je $q = 0$, tj. proizvoljan element $x > 0$ je suma ekstremalnih. □

Teorema 3.2.15. *U uredjenoj filterskoj grupi G sledeći uslovi su ekvivalentni:*
(1) $G \cong \mathbb{Z}^{(I)}$.
(2) *G je mrežasto uredjena grupa u kojoj važi uslov* **M**.
(3) *G zadovoljava uslov* **M** *i za svaki ekstremalan element ispunjen je uslov* **P**.
(4) *G je generisana ekstremalnim elementima i za svaki od njih važi uslov* **P**.

Dokaz.
(1) ⇒ (2) : Teorema 3.2.11.
(2) ⇒ (3) : Teorema 3.2.9.
(3) ⇒ (4) : Teorema 3.2.14.
(4) ⇒ (1) : Teorema 3.2.10 (primedba). □
Neka je sada A domen i $G = G(A)$ njegova grupa valuacija. Uslov **M** je ovde zapravo uslov ACC_1, uslov **P** znači da je element prost, dok uslov mrežaste uredjenosti znači da je A Gausov domen. U tom smislu, uslovi (2),(3) i (4) su poznati ekvivalentni uslovi za faktorijalnost domena, dok je uslov (1) suštinski nov. Formulišemo zato teoremu 3.2.15 za (uredjenu, filtersku) grupu valuacija $G(A) = k^*/A^*$;

Teorema 3.2.16. *Za domen A sledeći uslovi su ekvivalentni:*
(1) $G(A) \cong \mathbb{Z}^{(I)}$.
(2) *A je Gausov domen i ispunjen je uslov ACC_1.*
(3) *U domenu A važi uslov ACC_1 i svaki atom je prost.*
(4) *A je atomičan i svaki atom je prost.*
(5) *A je UFD.* $\square$

Ako uredjena filterska grupa zadovoljava ekvivalentne uslove teoreme 3.2.15, onda postoji familija $\mathcal{P}$ pozitivnih elemenata u G, takva da se svaki pozitivan element $x \in G$ na jedinstven način može predstaviti u obliku:

$$(i) \quad x = \sum_{p \in \mathcal{P}} x(p)p \ , \ x(p) \geq 0 \ , \ x(p) \neq 0 \ \text{ samo za konačno mnogo } p \in \mathcal{P}$$

Formulom (i) data je "faktorizacija" pozitivnih elemenata grupe G pomoću ekstremalnih. Kako je $G = P - P$, gde je P skup pozitivnih elemenata grupe G, svaki element $z \in G$ ima reprezentaciju $z = x - y$, $x, y \in P$. Ako sada predjemo na domen A i multiplikativnu grupu $G(A)$, formula (i) postaje:

$$(ii) \quad x = u \prod_{p \in \mathcal{P}} p^{v_p(x)} \ , \ v_p(x) \geq 0 \ , \ v_p(x) \neq 0 \ \text{ samo za konačno mnogo } p \in \mathcal{P},$$

gde je $u \in A^*$ invertibilan element. Pozitivni su ovde upravo svi elementi domena A različiti od nule, dok se svaki $z \in G(A)$ može predstaviti u obliku $z = x/y$, $x, y \in A \setminus \{0\}$. To posebno znači da se u formuli (ii) mogu dopustiti i negativni eksponenti $v_p(x)$.

Teorema 3.2.17. *Ako uredjena grupa G zadovoljava ekvivalentne uslove teoreme* 3.2.15*, onda je familija $\mathcal{P} \subseteq G$ odredjena jednoznačno. To su upravo ekstremalni elementi grupe G.*

Dokaz. Neka je $\mathcal{P}'$ skup svih ekstremalnih elemenata u G.

$\mathcal{P}' \subseteq \mathcal{P}$: Neka je $x \in \mathcal{P}'$. Tada je $x > 0$, pa x prema (i) ima reprezentaciju $x = \sum_{p \in \mathcal{P}} x(p)p$. To znači da postoji $p \in \mathcal{P}$ takav da je $x(p) > 0$, odakle je $p \leq x$. Kako je x ekstremalan mora biti $x = p$ tj. $\mathcal{P}' \subseteq \mathcal{P}$.

$\mathcal{P} \subseteq \mathcal{P}'$: Neka je sada $x \in \mathcal{P}$. Onda je $x > 0$ pa prema 3.2.13 postoji $p \in \mathcal{P}'$ takav da je $p \leq x$. Medjutim $p > 0$, pa ima jednoznačnu faktorizaciju $p = \sum_{y \in \mathcal{P}} p\,(y)\, y$. Dalje, kako je $p \leq x$ tj. $x - p \geq 0$ imamo da je $x - p = \sum_{y \in \mathcal{P}} q\,(y)\, y$. Odavde je:

$$x = \sum_{y \in \mathcal{P}} (\, p\,(y) + q\,(y)\,)\, y$$

Kako je $x \in \mathcal{P}$, iz jednoznačnosti faktorizacije važiće $p\,(y) + q\,(y) = 0$, za $y \neq x$ i $p\,(x) + q\,(x) = 1$, pa se može uzeti $p\,(y) = 0$ za $y \neq x$ i $p\,(x) = 1$. Sada se iz početne reprezentacije za p, $p = \sum_{y \in \mathcal{P}} p\,(y)\, y$, dobija $p = x$ tj. $x \in \mathcal{P}'$. $\square$

Primedba. Iz ovog tvrdjenja vidi se da pri definisanju faktorijalnog domena nije neophodno isticati ekstremalnost elemenata familije $\mathcal{P}$. Na taj način može se dati sledeća, na prvi pogled opštija, definicija faktorijalnog domena.

Definicija 3.2.18. *Domen A je UFD ako postoji podskup $\mathcal{P} \subseteq A$ takav da se svaki nenulti element $x \in A$ na jedinstven način može predstaviti u obliku*

$$x = u \prod_{p \in \mathcal{P}} p^{v_p(x)}\,, \tag{9}$$

gde je $u \in A^*$, $v_p(x) \geq 0$, $v_p(x) \neq 0$ samo za konačno mnogo $p \in \mathcal{P}$.

3.3 Valuacije i njihova veza sa faktorizacijom

Definicija 3.3.1. *Neka je $(G, +)$ linearno uredjena Abelova grupa i k neko polje. Preslikavanje $v : k \to G \cup \{\infty\}$ je valuacija polja k ako zadovoljava sledeće uslove:*
(v_1) $v(xy) = v(x) + v(y)$
(v_2) $v(x + y) \geq \min\{v(x), v(y)\}$
(v_3) $v(x) = \infty \;\Leftrightarrow\; x = 0$

Iz (v_1) vidimo da valuacija polja k definiše jedan homomorfizam $v : k^* \to G$ multiplikativne grupe polja k u grupu G. Slika $v(k^*)$ je podgrupa grupe G koju zovemo grupom valuacija za v. Obično je A domen i $k = Frac(A)$. Tada je dovoljno da restrikcija $v : A \to G$ zadovoljava uslove (v_1) i (v_2). Ovo preslikavanje može se u tom slučaju proširiti na k ako stavimo $v(a/b) = v(a) - v(b)$. Iz definicije se neposredno dobijaju sledeće osobine valuacija:

(1) $v(a^{-1}) = -v(a)$
(2) $v(1) = 0$
(3) $v(-a) = v(a)$
(4) $v(a) < v(b) \;\Rightarrow\; v(a + b) = v(a)$

Ako je v valuacija iz osobina $(v_1), (v_2)$ skup:

$$A_v = \{x \in k \mid v(x) \geq 0\}$$

je prsten. Kako je $v(a^{-1}) = -v(a)$ za svako $a \in k$ važiće $a \in A_v$ ili $a^{-1} \in A_v$ pa je prsten A_v valuacioni. Prsten A_v zovemo valuacionim prstenom koji odgovara valuaciji v. On je naravno i kvazilokalan sa maksimalnim idealom:

$$\mathfrak{m}_v = \{x \in k \mid v(x) > 0\}$$

Iz ovoga se vidi da svaka valuacija polja k definiše jedan valuacioni domen.

Obratno, ako je dat valuacioni domen A, grupa $G(A)$, odnosno grupa $\mathcal{P}^*$, je linearno uredjena pa za grupu G možemo uzeti upravo $\mathcal{P}^* = G = \{Ax \mid x \in k^*\}$, samo što je ona sada multiplikativna. Sada se može definisati preslikavanje $v : k \to G \cup \{\infty\}$ sa $v(x) = Ax$, $x \in k^*$, $v(0) = \infty$. Grupu $\mathcal{P}^*$ uredili smo stavljajući $Ax \leq Ay \;\Leftrightarrow\; Ax \supseteq Ay$ pa će ovde važiti:

$$v(x) \leq v(y) \;\Leftrightarrow\; Ax \supseteq Ay$$

Za ovako definisano preslikavanje ispunjeni su uslovi $(v_1), (v_2), (v_3)$ pa je v jedna valuacija polja k sa valuacionim prstenom $A_v = A$. Pri tome valuacija koja odgovara valuacionom domenu A nije odredjena jednoznačno ali su svake dve takve valuacije ekvivalentne (valuacije $v_1 : k^* \to G_1$, $v_2 : k^* \to G_2$ su ekvivalentne ako postoji izomorfizam $\varphi : G_1 \to G_2$ takav da je $\varphi \circ v_1 = v_2$). Iz svega rečenog sledi da valuacioni domeni i aditivne valuacije opisiju istu stvar tj. važi sledeće tvrdjenje.

Tvrdjenje 3.3.2. *Za svako polje k postoji bijekcija izmedju valuacionih prstena polja k i klasa ekvivalentnih valuacija na k. U toj bijekciji prstenu A odgovara valuacija v akko je A valuacioni prsten za v.* □

Posebno važan slučaj je kada je grupa valuacija k^*/A^* ciklična. Odgovarajući valuacioni prsten tada zovemo diskretnim valuacionim prstenom, ili kraće DVR. To posebno važi ako za grupu G uzmemo aditivnu grupu celih brojeva $(\mathbb{Z}, +)$. Netrivijalne valuacije sa kodomenom $\mathbb{Z}$ zovemo i glavnim valuacijama (valuacija je trivijalna ako je $v(x) = 0$, $x \in k^*$ i $v(0) = \infty$). Ako je v glavna valuacija onda je $v(k^*)$ podgrupa grupe $\mathbb{Z}$ pa je ciklična, $v(k^*) = n\mathbb{Z}$. Pomoću valuacije v možemo dobiti novu valuaciju $v' = (1/n)v$ (normiranje glavne valuacije) i dobijamo da je grupa valuacija upravo $\mathbb{Z}$. Za valuaciju v' kažemo da je diskretna, ranga 1. Diskretni valuacioni prsteni imaju veoma prostu strukturu. To su glavni domeni sa tačno jednim prostim idealom, dok su svi ostali ideali njegovi stepeni. Potpun opis diskretnih valuacionih prstena daje sledeća teorema.

Teorema 3.3.3. *Neka je v valuacija polja k i A_v odgovarajući valuacioni prsten. Tada je v glavna valuacija akko je A_v glavni. Važi i više: postoji $p \in k$ takav da je $k^* = (p)A_v^*$. Element $p \in k$ je prost element valuacije v. Odredjen je jednoznačno do na invertibilan faktor.*

Dokaz. Neka je v glavna valuacija i $A_v = \{x \in k \mid v(x) \geq 0\}$. Normiranjem možemo naći $p \in A_v$ tako da je $v(p) = 1$. Neka je sada $x \in k$ proizvoljan element takav da je $v(x) > 0$ tj. $v(x) = n$, za neko $n \in \mathbb{N}$. Tada je:

$$v(xp^{-n}) = v(x) + v(p^{-n}) = n - n = 0$$

Odavde je $xp^{-n} = \alpha \in A_v^*$ tj. $x = \alpha p^n$, $\alpha \in A_v^*$. Ako bi postojala i druga reprezentacija $x = \beta p^n$, $\beta \in A_v^*$ onda bi važilo $0 = v(\alpha/\beta) = v(p^{m-n}) = m-n$. Odavde je $m = n$ pa je reprezentacija $x = \alpha p^n$ jednoznačna do na množenje invertibilnim elementom. Ako je $I \lhd A_v$ ideal, $I \neq A_v$, tada je $v(x) > 0$ za svako $x \in I$, pa postoji $m = \min\{v(x) \mid x \in I\}$. Odavde je $I = (p^m)$ tj. I je glavni ideal. Kako to važi za proizvoljan ideal A_v je glavni.
Obratno, neka je sada A_v glavni valuacioni prsten i $\mathfrak{m} \lhd A_v$ maksimalan ideal. I on je naravno glavni npr. $\mathfrak{m} = (p)$. Kako je A_v glavni pa prema tome i UFD iz leme 2.5.5 imamo da je $\bigcap_{n\in\mathbb{N}}(p^n) = (0)$. Dakle za element $a \in A_v$, $a \neq 0$ važi $a \notin \bigcap_{n\in\mathbb{N}}(p^n)$, pa postoji i najmanje n tako da je $a \in (p^n)$, $a \notin (p^{n+1})$. Odavde je $a = up^n$, $u \in A_v$. Treba još pokazti da je u invertibilan u A_v. Ako pretpostavimo suprotno, da $u \notin A_v^*$, mora biti $u \in \mathfrak{m} = (p)$ pa je $u = vp$. Dolazi se do kontradikcije $a = uvp^{n+1} \in (p^{n+1})$. Reprezentacija:

$$a = up^n \ , \ u \in A_v^* \ , \ n \in \mathbb{N} \tag{1}$$

je jednoznačna. Prema (1) može se definisati valuacija stavljajući $v(a) \stackrel{\text{def}}{=} n$. Definicija se može proširiti na polje k sa $v(a/b) = v(a) - v(b)$. Za $x \in k^*$ imamo $x = a/b = up^n/vp^m = (u/v)p^{n-m} = wp^k$ tj.

$$x = wp^k \ , \ w \in A_v^* \ , \ k \in \mathbb{Z} \tag{2}$$

Iz (2) se dobija $k^* = (p)A_v^*$. $\square$

Teorema 3.3.4. *Neka je A valuacioni domen. A je UFD akko A je DVR.*

Dokaz. Očigledno, ako je A DVR, on je glavni pa je zato i UFD. S druge strane, ako je A faktorijalan domen, on ima najviše jedan ireducibilan element p. Ako pretpostavimo suprotno, da postoje dva različita atoma p i q, s obzirom da je A valuacioni, važi $p \mid q \ \vee \ q \mid p$. To znači da su p i q asocirani pa ih možemo identifikovati. Svaki element x domena A ima dakle jednoznačnu reprezentaciju $x = up^n \ , \ u \in A^* \ , \ n \geq 0$. Prema prethodnom A je DVR. $\square$

Primer 3.3.5. *$k[[X]]$ je UFD ako je k proizvoljno polje.*

Formalni red

$$f = a_0 + a_1X + a_2X^2 + \cdots \in A[[X]]$$

je invertibilan u $A[[X]]$ akko je a_0 invertibilan u A. To posebno znači da je za $A = k$ formalni red f invertibilan akko je $a_0 \neq 0$. Neinvertibilni elementi ovog prstena su dakle oblika:

$$g = a_1X + a_2X^2 + \cdots = X(a_1 + a_2X + \dots) = Xh$$

Drugim rečima $k[[X]]$ je kvazilokalan domen sa maksimalnim idealom (X). Proizvoljan element $f \in k[[X]] \, , \, f \neq 0$ ima reprezentaciju $f = gX^n$ gde je $g \in k[[X]]^* \, , \, n \geq 0$ pa je $k[[X]]$ DVR dakle i UFD. ▼

Primer 3.3.6. *Neka je $k = \mathbb{Q}$ polje racionalnih brojeva i $p \in \mathbb{Z}$ fiksiran prost broj. Svako $x \in k$ može se na jedinstven način predstaviti u obliku:*

$$x = \alpha p^n \ , \ \alpha = u/v \ , \ nzd\,[\,u, v\,] = nzd\,[\,u, p\,] = nzd\,[\,v, p\,] = 1 \ , \ n \in \mathbb{Z}$$

Definišemo $v_p(x) \stackrel{\text{def}}{=} n$. Lako se vidi da su za ovako definisano preslikavanje v_p zadovoljeni uslovi (v_1) i (v_2) pa je v_p jedna valuacija polja $\mathbb{Q}$ pridružena prostom broju $p \in \mathbb{Z}$. Ovako odredjene valuacije zovu se p-adične valuacije. Može se dokazati da su sve netrivijalne valuacije polja $\mathbb{Q}$ upravo p-adične.

Primer 3.3.7. *Ako za polje k uzmemo polje racionalnih funkcija $k = K(X)$, gde je K proizvoljno polje, možemo postupiti na isti način kao u prethodnom primeru fiksirajući ireducibilan polinom $p \in K[X]$. Osim p-adičnih valuacija v_p za ireducibilan polinom p, može se pokazati da polje $K(X)$ ima još jednu netrivijalnu valuaciju v definisanu sa $v(f/g) = deg(g) - deg(f)$.*

Iz ovih primera vidimo da se na poljima $\mathbb{Q} = Frac(\mathbb{Z})$ i $K(X) = Frac(K[X])$ može definisati familija p-adičnih valuacija indukovana atomima ovih prstena. Videćemo sada da važi i opštije: u svakom faktorijalnom domenu može se definisati familija $(v_p)_{p\in\mathcal{P}}$ p-adičnih valuacija.
Neka je A UFD i $a \in A\ ,\ a \notin A^*\ ,\ a \neq 0$. Neka je $\mathcal{P} \subseteq A$ skup ekstremalnih elemenata grupe $G(A)$ tj. skup atoma u A. Tada a ima jednoznačnu faktorizaciju:

$$a = u \prod_{p\in\mathcal{P}} p^{v_p(a)} \quad , \quad v_p(a) \geq 0 \tag{3}$$

pri čemu je $v_p(a) \neq 0$ samo za konačno mnogo $p \in \mathcal{P}$. Faktorizacija (3) za fiksirano $p \in \mathcal{P}$ definiše preslikavanje $A \mapsto \mathbb{Z}$ dato sa: $a \mapsto v_p(a)$. Neka su $a, b \in A$ elementi domena A sa faktorizacijama $a = u\prod p^{v_p(a)}\ ,\ b = v\prod p^{v_p(b)}$ gde su $v_p(a), v_p(b) \geq 0$. Tada je:

$$ab = uv \prod p^{v_p(a)+v_p(b)} \ \Rightarrow\ v_p(ab) = v_p(a) + v_p(b) \tag{4}$$

$$a + b = u\prod p^{v_p(a)} + v\prod p^{v_p(b)} = \underbrace{\prod p^{m_p}}_{x}\left(\underbrace{u\prod p^{a_p} + v\prod p^{b_p}}_{y}\right) = xy$$

gde je:
$$m_p = \min\{v_p(a), v_p(b)\}$$
$$v_p(a) = m_p + a_p\ , a_p \geq 0$$
$$v_p(b) = m_p + b_p\ ,\ b_p \geq 0$$
$$y \in A\ \Rightarrow\ y = w\prod p^{v_p(y)}\ ,\ v_p(y) \geq 0 \tag{5}$$

Sada iz (4) i (5) dobijamo:

$$v_p(a+b) = v_p(xy) = v_p(x) + v_p(y) = m_p + v_p(y) \geq m_p$$

odakle je:
$$v_p(a+b) \geq \min\{v_p(a), v_p(b)\} \tag{6}$$

Iz (4) i (6) vidimo da za preslikavanje v_p važe uslovi $(v_1), (v_2)$ tj. v_p je jedna valuacija koju standardno širimo na polje $k = Frac(A)$. Za $x \in k$ imamo reprezentaciju:

$$x = \frac{u}{v}p^m\ ,\ m \in \mathbb{Z}\ ,\ \text{nzd}\,[\,u, p\,] = \text{nzd}\,[\,v, p\,] = 1 \tag{7}$$

pa definišemo $v_p(x) \stackrel{\text{def}}{=} m$. Na taj način fiksiran atom p odredjuje jednu p-adičnu valuaciju, pa se u svakom faktorijalnom domenu A može govoriti o familiji $(v_p)_{p\in\mathcal{P}}$ takvih valuacija. Sve ove valuacije su diskretne, ranga 1, pa su odgovarajući valuacioni prsteni A_{v_p} diskretni. Kako je za $x \in k$, prema reprezentaciji (7) $v_p(x) \geq 0\ \Leftrightarrow\ m \geq 0\,,$ dobijamo da je:

$$A_{v_p} = \{x \in k\ \mid\ v_p(x) \geq 0\} = A_{(p)}$$

$$M_{v_p} = \{x \in k \mid v_p(x) > 0\} = (p)A_{(p)}$$

Odgovarajući valuacioni prsten A_{v_p} je upravo lokalizacija po glavnom idealu (p) sa maksimalnim idealom $(p)A_{(p)}$. Dalje je:

$$x \in A \Leftrightarrow x = u\prod_{p\in\mathcal{P}} p^{v_p(x)}\ ,\ v_p(x) \geq 0 \Leftrightarrow x \in A_{v_p}\ ,\ \forall p \in \mathcal{P} \Leftrightarrow x \in \bigcap_{p\in\mathcal{P}} A_{v_p}$$

Pa je sam domen A jednak preseku odgovarajućih lokalizacija:

$$A = \bigcap_{p\in\mathcal{P}} A_{v_p} \tag{8}$$

Dalje, za svako $a \in A\ ,\ a \neq 0$, važi $v_p(a) \neq 0$ samo za konačno mnogo valuacija familije $(v_p)_{p\in\mathcal{P}}$, jer iz jednoznačnosti faktorizacije imamo:

$$a = up_1^{v_{p_1}(a)} \dots p_m^{v_{p_m}(a)} \qquad v_{p_1}(a) > 0, \dots, v_{p_m}(a) > 0$$

$$\Rightarrow\ a \in M_{v_{p_1}}, \dots, a \in M_{v_{p_m}}$$

dok u ostalim valuacionim domenima $A_{v_{p_i}}$ važi $v_{p_i}(a) = 0$ tj. a je inverzibilan u njima. Na ovaj način dokazana je sledeća teorema koja u suštini kaže da je svaki UFD Krulov domen.

Teorema 3.3.8. *Neka je A UFD, $k = Frac(A)$ i $(\mathcal{F}_p)$ familija svih p-adičnih valuacija indukovanih atomima u A. Tada ova familija zadovoljava sledeće uslove:*
(i) Svaka valuacija familije $(\mathcal{F}_p)$ je diskretna ranga 1.
(ii) Presek svih valuacionih prstena je sam prsten A, $A = \bigcap_{v\in\mathcal{F}_p} A_v$.
(iii) $\forall a \in A\ ,\ a \neq 0\,$, važi $v(a) = 0$ za gotovo sve valuacije familije $(\mathcal{F}_p)$. □

3.4 Invertibilni ideali u faktorijalnom domenu

Za razlomljen ideal $I \in I(A)$ definiše se njegov inverzni I^{-1} sa:

$$I^{-1} = A : I = \{x \in k \mid xI \subseteq A\}$$

Očigledno uvek važi $II^{-1} \subseteq A$. Invertibilni ideali biće oni kod kojih važi i obratna inkluzija.

Definicija 3.4.1. *Razlomljen ideal I je invertibilan ako je $II^{-1} = A$.*

Neka je $II^{-1} = A$. Tada je

$$1 = a_1b_1 + \dots + a_nb_n \tag{1}$$

za neke $a_i \in I, b_i \in I^{-1}$. Množenjem poslednje jednakosti sa x, gde je $x \in I$ dobija se:

$$x = (b_1x)a_1 + \dots + (b_nx)a_n \quad \forall x \in I$$

Kako su $b_i x \in A$ ideal I je konačno generisan $I = (a_1, \ldots, a_n)$. Ako je domen A još i kvazilokalan onda bar jedan od elemenata $a_j b_j$ u jednakosti (1) mora biti invertibilan. U suprotnom bi naime svi bili u maksimalnom idealu $M \lhd A$ odakle prema (1) dobijamo kontradikciju $1 \in M$. Neka je npr. $a_1 b_1$ invertibilan i $x \in I$. Tada za neko $c_1 \in A$ važi:

$$1 = a_1 b_1 c_1 \;\Rightarrow\; x = (b_1 c_1 x) a_1 \;\Rightarrow\; I = (a_1) \quad \text{jer} \;\; b_1 c_1 x \in A$$

Na taj način dokazana su sledeća tvrdjenja u vezi sa invertibilnim idealima;
(i) Svaki invertibilan ideal je konačno generisan.
(ii) Svaki invertibilan ideal u kvazilokalnom domenu je glavni.
Može se pokazati i da se invertibilnost ideala čuva lokalizacijom: ako je I invertibilan ideal u A onda je i I_S invertibilan ideal u A_S, gde je $S \subseteq A$ multiplikativno zatvoren podskup.

Teorema 3.4.2. *Invertibilni ideali u faktorijalnom domenu su glavni.*

Dokaz. Neka je A UFD, $k = Frac(A)$ i $I \in I(A)$ invertibilan ideal.

$$I^{-1} = A : I = \{x \in k \;\mid\; xI \subseteq A\} = \{x \in k \;\mid\; I \subseteq Ax^{-1}\}$$

$II^{-1} = A \;\Rightarrow\; a_1 b_1 + \cdots + a_n b_n = 1 \quad$ za neke $\; a_i \in I, b_i \in I^{-1}$

$b_i \in I^{-1} \;\Rightarrow\; b_i I \subseteq A \;\Rightarrow\; I \subseteq b_i^{-1} A \;\Rightarrow\; I \subseteq \bigcap_{i=1}^{n} A b_i^{-1}$

Neka je sada $x \in \bigcap_{i=1}^{n} A b_i^{-1}$. Tada je $b_1 x \in A, \ldots, b_n x \in A$ pa važi:

$$x = a_1(x b_1) + \cdots + a_n(x b_n) \in I$$

odakle je $\bigcap_{i=1}^{n} A b_i^{-1} \subseteq I$. Iz ove i prethodne inkluzije sledi da je $I = \bigcap_{i=1}^{n} A b_i^{-1}$. S obzirom da je A UFD, prema 2.5.4 I je glavni ideal. $\square$

Kako je svaki glavni ideal (a), gde je $a \neq 0$, invertibilan, u kvazilokalnim domenima invertibilni i glavni ideali se poklapaju. Svaki konačno generisani ideal ne mora medjutim biti i invertibilan. Klasu domena u kojima je svaki konačno generisan ideal invertibilan zovemo *Prüferovim* domenima. Prema definiciji Bezuovog domena svaki konačno generisan ideal je glavni, dakle i invertibilan, pa je svaki Bezuov domen i *Prüferov*. S druge strane, svaki valuacioni domen je i Bezuov, pa imamo sledeće inkluzije:

$$Valuacioni\ domeni \;\subseteq\; Bezuovi\ domeni \;\subseteq\; Prüferovi\ domeni \qquad (2)$$

Može se pokazati da u vezi sa ovim domenima važe sledeća tvrdjenja [15], na koja ćemo se kasnije pozivati.

Teorema 3.4.3. *Neka je A domen i I konačno generisan ideal. I je invertibilan akko I_M je glavni ideal za svaki maksimalan ideal $M \lhd A$.* $\square$

Teorema 3.4.4. *Kvazilokalan domen je valuacioni akko je Bezuov.* $\square$

Teorema 3.4.5. *Za domen A sledeća tvrdjenja su ekvivalentna:*
(i) A je $Prüferov$ domen.
(ii) A_P je valuacioni domen za svaki prost ideal $P \lhd A$.
(iii) A_M je valuacioni domen za svaki maksimalan ideal $M \lhd A$. $\square$

Teorema 3.4.6. *Neka je A $Prüferov$ domen, $k = Frac(A)$ i V valuacioni domen: $A \subseteq V \subseteq k$. Tada je V lokalizacija po prostom idealu, tj. V mora biti oblika A_P, za neki prost ideal $P \lhd A$.* $\square$

Glava 4

Neterini prsteni i generalizacija jednoznačne faktorizacije

Različite klase komutativnih prstena u algebarskoj teoriji brojeva i algebarskoj geometriji nisu faktorijalni domeni. Ipak, neki od njih poseduju nešto slabija svojstva koja možemo smatrati i nekom vrstom generalizacije jednoznačne faktorizacije. Umesto faktorizacije elemenata, u Neterinim prstenima posmatra se "faktorizacija" ideala. Jednoznačna dekompozicija elemenata u proizvod atoma u UFD-u, u Neterinim prstenima može se zameniti primarnom dekompozicijom ideala (teorema 4.3.3), dok se u Dedekindovim domenima, posebnoj klasi Neterinih domena, može zameniti jednoznačnom "faktorizacijom" ideala u proizvod prostih ideala (teorema 4.4.4).

4.1 Definicija i osnovne osobine Neterinih prstena

Definicija 4.1.1. *Komutativan prsten R je Neterin ako zadovoljava neki od ekvivalentnih uslova:*
- Svaki rastući lanac ideala u R je konačan. (ACC)
- Svaki neprazan skup ideala u R ima maksimalan element u odnosu na inkluziju.
- Svaki ideal[1] *prstena R je konačno generisan.*

Neterini prsteni čine široku i po svojim specifičnostima značajnu klasu prstena, pa se kao takvi često posebno razmatraju. Za faktorizaciju su posebno zanimljivi Dedekindovi i glavni domeni kao posebne klase Neterinih domena. Iz obilja materijala vezanih za ove prstene biće spomenute samo neke od teorema značajnih sa stanovišta faktorizacije. Detaljnija analiza ovih prstena, kao i dokazi svih tvrdjenja mogu se naći u [3, 15, 21]. Jedna od najvažnijih teorema vezana za ove prstene je Krulova glavnoidealska teorema.

[1] Dovoljno je ograničiti se na proste ideale.

Teorema 4.1.2 (Krulova glavnoidealska teorema)**.**
Neka je prsten R Neterin , $x \in R$, $x \notin R^*$ i $\mathfrak{p}$ minimalan prost ideal prstena R koji sadrži glavni ideal (x). Tada je $\mathrm{ht}(\mathfrak{p}) \leq 1$.[2] □

Teorema 4.1.3 (Generalizacija Krulove glavnoidealske teoreme)**.**
Neka je R Neterin prsten i $I = (a_1, \ldots, a_n)$ ideal prstena R, $I \neq R$. Ako je $\mathfrak{p}$ minimalan prost ideal nad I onda je $\mathrm{ht}(\mathfrak{p}) \leq \mathrm{n}$. □

Posledica 4.1.4. *Prosti ideali u Neterinom prstenu su konačne visine.* □

Teorema 4.1.5 ([21])**.** *Za valuacioni domen R sledeći uslovi su ekvivalentni:*
(1) *R je DVR.*
(2) *R je glavni.*
(3) *R je Neterin.* □

Teorema 4.1.6 ([21])**.** *Za prsten R sledeći uslovi su ekvivalentni:*
(1) *R je DVR.*
(2) *R je kvazilokalan, glavni i nije polje.*
(3) *R je lokalan*[3] *, $dim(R) > 0$ i maksimalan ideal M je glavni.*
(4) *R je lokalan, integralno zatvoren i $dim(R) = 1$.* □

Teorema 4.1.7 ([15])**.**
Neka je R Neterin integralno zatvoren domen i $\mathcal{P}(R) = \{\, \mathfrak{p} \lhd R \mid \mathrm{ht}(\mathfrak{p}) = 1 \,\}$. Tada je $R_\mathfrak{p}$ DVR za svaki minimalan prost ideal $\mathfrak{p} \in \mathcal{P}(R)$ i

$$R = \bigcap_{\mathfrak{p} \in \mathcal{P}(R)} R_\mathfrak{p}$$ □

Za raširenja Neterinih prstena važe sledeća tvrdjenja:

Teorema 4.1.8 (Hilbert)**.** *Ako je R Neterin prsten onda je i prsten polinoma $R[X]$ Neterin.* □

Teorema 4.1.9. *Ako je R Neterin prsten i $S \subseteq R$ multiplikativno zatvoren podskup onda je i R_S Neterin.* □

Teorema 4.1.10. *Ako je R Neterin prsten onda je i prsten formalnih redova $R[[X]]$ Neterin.* □

4.2 Jednoznačna faktorizacija u Neterinim domenima

U Neterinim domenima svaki rastući lanac ideala:

$$I_1 \subseteq I_2 \subseteq I_3 \ldots$$

je konačan. To posebno znači da je i svaki rastući lanac glavnih ideala:

$$(a_1) \subseteq (a_2) \subseteq (a_3) \ldots$$

[2] Ako x nije delitelj nule onda je ovde $\mathrm{ht}(\mathfrak{p}) = 1$. To specijalno važi ako je R domen.
[3] Neterin kvazilokalan.

konačan, tj. važi uslov ACC_1 pa je svaki Neterin domen atomičan. Neterin domen je dakle i UFD ako zadovoljava uslov (**A2**) ili neki od njegovih ekvivalenata. To posebno znači da je Neterin Gausov domen UFD. Ovo se može formulisati i u obliku sledećeg tvrdjenja.

Tvrdjenje 4.2.1. *Neterin domen R je UFD ako zadovoljava jedan od sledećih uslova:*
(1) *Svaki atom u R je prost.*
(2) *Presek glavnih ideala u R je glavni ideal.* □

Pored ovoga primenom Krulove glavnoidealske teoreme može se pokazati da u Neterinim domenima važi i obrat teoreme 1.1.21.

Teorema 4.2.2. *Neterin domen R je UFD akko je svaki minimalan prost ideal $\mathfrak{p} \in \mathcal{P}(R)$ glavni.*

Dokaz. Minimalni prosti ideali u svakom faktorijalnom domenu su glavni pa je dovoljno dokazati jednu implikaciju. Pretpostavimo da je R Neterin domen i da su svi ideali u $\mathcal{P}(R)$ glavni. Prema prethodnom tvrdjenju dovoljno je pokazati da je svaki atom prost. Neka je zato $p \in R$ atom i $\mathfrak{p} \lhd R$ minimalan prost ideal koji sadrži (p). Onda prema teoremi 4.1.2 važi $\mathrm{ht}(\mathfrak{p}) = 1$ tj. $\mathfrak{p} \in \mathcal{P}(R)$. Prema pretpostavci $\mathfrak{p}$ je onda glavni ideal, $\mathfrak{p} = (q)$, $q \notin R^*$. Tada je:

$$(p) \subseteq (q) \;\Rightarrow\; p = qr \;,\; r \in R \tag{1}$$

Kako je p ireducibilan mora biti $r \in R^*$ pa su prema (1) elementi p i q asocirani, odnosno $(p) = (q) = \mathfrak{p}$. Odavde je (p) prost ideal tj. p je prost element. □

Teorema 4.2.3. *Neka je A glavni domen. Tada je $A[[X]]$ UFD.*

Dokaz. S obzirom da je A glavni domen, dakle Neterin to je i $A[[X]]$ Neterin pa možemo primeniti prethodnu teoremu. Neka je $\mathfrak{p}$ minimalan prost ideal u $A[[X]]$; $\mathfrak{p}$ je konačno generisan pa postoje formalni redovi $f_1, \ldots, f_n$ takvi da je $\mathfrak{p} = (f_1, \ldots, f_n)$. Neka su $a_i \in A$ slobodni koeficijenti ovih formalnih redova,

$$f_i = a_i + Xg_i \;,\; g_i \in A[[X]] \;,\; i = 1, \ldots, n \tag{2}$$

Tada je $(a_1, \ldots, a_n)$ ideal u A. Kako je A prema pretpostavci glavni domen, postoji $a \in A$ tako da je $(a_1, \ldots, a_n) = (a)$. Postoje dakle elementi $b_i \in A$ takvi da je $a_i = ab_i$, $i = 1, \ldots, n$. Tada je prema (2) :

$$f_i = ab_i + Xg_i \;,\; g_i \in A[[X]] \;,\; i = 1, \ldots, n \tag{3}$$

Kako $X \notin \mathfrak{p}$, jer bi u suprotnom imali $(X) \subseteq \mathfrak{p}$, što je u kontradikciji sa pretpostavkom da je $\mathfrak{p}$ minimalan prost ideal, iz (2) i (3) ideal $\mathfrak{p}$ generisan je formalnim redom:

$$f = a + Xg \;,\; g \in A[[X]] \tag{4}$$

Odavde $\mathfrak{p} = (f)$ je glavni ideal i $A[[X]]$ je prema prethodnoj teoremi UFD. □

Primer 4.2.4.

$$\mathbf{Z}[[X]]\ ,\ k[[X]]\ ,\ k[X][[T]]\ ,\ \mathbf{Z}[i][[X]]\ ,\ \mathbf{Z}[\sqrt{3}][[X]]$$

su faktorijalni domeni. ▼

4.3 Primarna dekompozicija ideala u Neterinim prstenima

Kao motivacija za uvodjenje pojma primarnog ideala i primarne dekompozicije može poslužiti prsten celih brojeva $\mathbb{Z}$, ili bilo koji glavni domen A. Neka je zato A glavni domen, dakle i UFD, i $a \in A$ nenulti, neinvertibilni element domena A. Tada a ima prostu faktorizaciju:

$$a = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} \qquad (i)$$

U terminima ideala, ovo znači da svaki pravi ideal $(a) \lhd A$ ima jednoznačnu "faktorizaciju":

$$(a) = (p_1)^{n_1}(p_2)^{n_2} \dots (p_k)^{n_k} = (p_1)^{n_1} \cap (p_2)^{n_2} \cap \dots \cap (p_k)^{n_k} \qquad (ii)$$

gde su p_i prosti elementi, $n_i > 0$ i $(p_i)^{n_i} = (p_i^{n_i})$. Iz ovih osobina, aritmetika glavnih domena slična je aritmetici prstena celih brojeva, što ih čini udobnim za rad. Lako se pokazuje da ideali $(p_i)^{n_i}$ u dekompoziciji (ii) imaju osobinu: $bc \in (p_i)^{n_i}$, $b \notin (p_i)^{n_i} \Rightarrow c \in (p_i)^{n_i}$, tj. oni su primarni. Na taj način, svaki ideal glavnog domena može se na jedinstven način razložiti u presek primarnih. U glavnim domenima je $(p^k) = (p)^k$, pa je svaki primaran ideal stepen prostog ideala. Ovo medjutim ne važi u prozvoljnom Neterinom domenu, npr. u prstenu polinoma $k[X, Y]$ nad poljem k ideal (X, Y^2) je primaran i nije stepen prostog. Struktura ideala u prstenu polinoma sa više neodredjenih nad poljem bitna je u algebarskoj geometriji. Da bi se dobila neka vrsta generalizacije jednoznačne faktorizacije ideala u ovim prstenima, motivisani primerom glavnog domena, proizvod menjamo presekom ideala, dok stepen prostog menjamo primarnim idealom. Daćemo kraći prikaz ovog razlaganja uz napomenu da se svi dokazi tvrdjenja vezanih za primarne ideale, kao i dokaz teoreme 4.3.3, mogu naći npr. u [13].

Definicija 4.3.1. *Ideal $I \lhd R$ je primaran ako: $ab \in I \Rightarrow a \in I \vee b^k \in I$ za neko $k > 0$. Ideal I je ireducibilan ako $I = J \cap K \Rightarrow I = J \vee I = K$, za sve ideale J, K prstena R za koje je $I \subseteq J$ i $I \subseteq K$.*

Može se pokazati da je u komutativnim Neterinim prstenima svaki ireducibilan ideal primaran. Prema ovoj definiciji prosti ideali su i primarni dok obratno ne mora da važi. Takodje stepen prostog ideala ne mora biti primaran, niti primaran mora biti stepen prostog[4]. Svakom primarnom idealu $\mathfrak{q}$ možemo medjutim pridružiti jedan prost ideal, njegov *radikal*:

$$\mathfrak{p} = \sqrt{\mathfrak{q}} = \{x \in R \mid x^k \in \mathfrak{q} \text{ za neko } k > 0\} = \bigcap_{J \supseteq \mathfrak{q},\ J\ prost} J \qquad (1)$$

[4]Stepeni maksimalnih ideala su primarni.

U tom slučaju kažemo da je $\mathfrak{q}$ $\mathfrak{p}$-*primaran* ili da je $\mathfrak{p}$ *asociran prost ideal* za $\mathfrak{q}$. Za primaran ideal $\mathfrak{q}$, ideal $\mathfrak{p} = \sqrt{\mathfrak{q}}$ odredjen je jednoznačno, medjutim ideal $\mathfrak{p}$ može biti asociran i za druge primarne ideale, npr. u prstenu $\mathbb{Z}$ primarni ideali $(p^2), (p^3), \ldots$ imaju isti asociran prost ideal (p). Kako je, $\sqrt{\mathfrak{q}_1 \ldots \mathfrak{q}_n} = \sqrt{\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n} = \sqrt{\mathfrak{q}_1} \cap \cdots \cap \sqrt{\mathfrak{q}_n}$, to je za $\mathfrak{p}$-primarne ideale $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$, ideal $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ takodje $\mathfrak{p}$-primaran. Svaki ideal sadržan je očigledno u svom radikalu. Ideale koji su jednaki svom radikalu zovemo *radikalnim* idealima. Svaki prost ideal je prema tome i radikalan. Ako je I radikalan ideal onda je:

$$I = \sqrt{I} = \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p} \tag{2}$$

pa je radikalan ideal presek familije prostih ideala koji ga sadrže. U ovom preseku možemo se naravno ograničiti samo na minimalne proste ideale nad I. U Neterinom prstenu takvih je konačno mnogo pa je svaki radikalan ideal Neterinog prstena presek konačno mnogo prostih. Ova lepa osobina radikalnih ideala ne prenosi se medjutim na sve ideale Neterinog prstena.

Definicija 4.3.2. *Ideal $I \triangleleft R$ ima primarnu dekompoziciju ako postoje primarni ideali $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ takvi da je $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$. Ova dekompozicija je redukovana ako nijedan od ideala $\mathfrak{q}_i$ ne sadrži presek ostalih i ako su asocirani prosti ideali $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ medjusobno različiti.*

Uslov kidanja lanaca u Neterinim prstenima dovoljan je da bi se svaki ideal predstavio kao konačan presek ireducibilnih. Ako to ne bilo ispunjeno, s obzirom da je prsten Neterin, postojao bi maksimalan ideal I sa tom osobinom. Taj ideal nije ireducibilan, pa je presek dva ideala $I = J \cap K$. Medjutim J i K su prema pretpostavci konačni preseci ireducibilnih ideala, što je kontradikcija. Svaki ideal I Neterinog prstena R ima dakle konačnu dekompoziciju:

$$I = J_1 \cap J_2 \cap \cdots \cap J_n \quad \text{gde su } J_i \text{ ireducibilni.} \tag{3}$$

Jednoznačnost ove dekompozicije, koja nas ovde zanima, nije medjutim ispunjena i može se narušiti na razne načine. Najpre, kako su J_i ireducibilni, oni su i $\mathfrak{p}_i$-primarni, gde je $\mathfrak{p}_i = \sqrt{J_i}$. Može se desiti da medju $\mathfrak{p}_i$-ovima ima jednakih, npr. $\mathfrak{p}_1 = \cdots = \mathfrak{p}_k = \mathfrak{p}$. U tom slučaju je $\sqrt{J_1 \cap \cdots \cap J_k} = \mathfrak{p}$, pa $J_1 \cap \cdots \cap J_k$ posmatramo kao jednu komponentu[5]. Na taj način, može se smatrati da je (3) primarna dekompozicija u kojoj su asocirani prosti ideali $\mathfrak{p}_i$ različiti. Takodje, ako neki od ideala J_i sadrži presek preostalih on se može izostaviti, pa se može govoriti o redukovanoj primarnoj dekompoziciji. Ovo se može formulisati na sledeći način; u Neterinom domenu R svaki ideal I ima konačnu dekompoziciju:

$$I = K_1 \cap K_2 \cap \cdots \cap K_n \quad \text{gde su } K_i \text{ primarni t.d.} \tag{4}$$

(i) K_i su $\mathfrak{p}_i$-primarni[6].
(ii) Prosti ideali $\mathfrak{p}_i$ su medjusobno različiti, tj. dekompozicija (4) je redukovana.

[5] Ovim se medjutim gubi ireducibilnost komponenata.
[6] $\mathfrak{p}_i$ su možda reducibilni.

I ovde se medjutim mogu javiti problemi, naime ideal I može imati više različitih redukovanih dekompozicija. Komponenta K_i jednoznačno je odredjena ako je $\mathfrak{p}_i$ minimalan prost ideal nad I. Sam ideal $\mathfrak{p}_i$ u tom slučaju zovemo *izolovanim* prostim idealom. Nasuprot tome, ako je za neko $j \neq i$ ispunjeno $\mathfrak{p}_i \supseteq \mathfrak{p}_j$, onda je $\mathfrak{p}_i$ *utapajući* ideal. Za utapajući ideal $\mathfrak{p}_i$ komponenta K_i ne mora biti jednoznačno odredjena pa su ovi ideali uzrok "nejednoznačnosti faktorizacije" (4). Ipak, komponente $\mathfrak{p}_i$, kao i broj n, u dekompoziciji (4) odredjeni su jednoznačno, što je rezultat sledeće teoreme o dekompoziciji.

Teorema 4.3.3 (Lasker-Noether)**.** *Neka je R komutativan Neterin prsten i I ideal u R. Tada postoje primarni ideali $Q_1, \ldots, Q_n$ takvi da je:*

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_n \,.$$

Ideali Q_i imaju različite asocirane proste ideale $\mathfrak{p}_i$ i nijedan od njih ne sadrži presek ostalih. U svakoj drugoj primarnoj dekompoziciji za I mora biti n ideala, i skup asociranih prostih je isti. □

Primedba. Asocirani prosti ideali $\mathfrak{p}_i = \sqrt{Q_i}$ prema ovoj teoremi jednoznačno su odredjeni idealom I, i potpuno su nezavisni od izbora primarnih komponenata Q_i. Na taj način svakom idealu I Neterinog prstena R možemo pridružiti jednoznačno odredjen prirodan broj n i konačan skup prostih ideala

$$Ass(I) = \{\, \mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n \}\,.$$

Neka je sada A Neterin domen, $S \subseteq A$ multiplikativan podskup, P ideal u A i U ideal u A_S. Ako sa $P^e = PA_S$ označimo ekstenziju ideala P u A_S, i sa $U^c = U \cap A$ kontrakciju ideala U u A, može se pokazati da onda važi $(\sqrt{U}\,)^c = \sqrt{U^c}$, $(\sqrt{P}\,)^e \subseteq \sqrt{P^e}$. Takodje se može pokazati da za P-primaran ideal Q u A, takav da je $Q \cap S = \emptyset$ važi $P \cap S = \emptyset$, Q^e je primaran i $P^e = \sqrt{Q^e}$. Ideal $(Q^n)^{ec} = Q^n A_S \cap A$ zovemo *n-tim simboličkim stepenom* ideala Q, u oznaci $Q^{(n)}$. Stepen Q^n primarnog ideala Q ne mora i sam biti primaran ali $Q^{(n)}$ je primaran ideal koji sadrži Q^n. Posebno, ako je i Q^n primaran, onda je $Q^n = Q^{(n)}$. Važi sledeće tvrdjenje.

Tvrdjenje 4.3.4. *Neka je $\mathfrak{q}$ $\mathfrak{p}$-primaran, tj. $\mathfrak{p} = \sqrt{\mathfrak{q}}$, i neka je $n \in \mathbb{N}$. Tada:*
(i) $\mathfrak{q}^{(n)}$ je $\mathfrak{p}$-primaran.
(ii) Ako je $\mathfrak{q}^n$ konačan presek primarnih ideala, tada je $\mathfrak{p}$ jedini izolovan ideal, $\mathfrak{q}^n = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \Rightarrow \sqrt{\mathfrak{q}_i} = \mathfrak{p}$ i odgovarajuća primarna komponenta je $\mathfrak{q}^{(n)}$. □

4.4 Jednoznačna faktorizacija ideala u Dedekindovim domenima

Istorijski, pojam Dedekindovog domena potiče iz algebarske teorije brojeva i vezan je za prstene algebarskih celih. Zapravo, savremena komutativna algebra svoje početke duguje rešavanju problema faktorizacije u ovim prstenima. Tražeći neku vrstu analogije jednoznačne faktorizacije koja će važiti u svim prstenima

algebarskih celih, Dedekind (1871) uvodi pojam idela. Radi motivacije može se pogledati sledeći primer.

Primer 4.4.1. $A = \mathbb{Z}[\sqrt{-5}\,]$

Domen A nije UFD. U njemu nalazimo dve različite atomične faktorizacije broja 6:

$$2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) \qquad (i)$$

Elementi 2 i 3 su atomi ovog prstena koji nisu prosti. Ako pogledamo ideale $\langle\, 2\,\rangle, \langle\, 3\,\rangle$ koje oni generišu, može se pokazati da je $\langle\, 2\,\rangle = P_1^2, \langle\, 3\,\rangle = P_2P_3$, gde je $P_1 = \langle\, 2, 1 + \sqrt{-5}\,\rangle$, $P_2 = \langle\, 3, 1 + \sqrt{-5}\,\rangle$, $P_3 = \langle\, 3, 1 - \sqrt{-5}\,\rangle$. Dalje se pokazuje da su P_1, P_2, P_3 maksimalni, dakle prosti ideali domena A, kao i da važi: $\langle\, 1 + \sqrt{-5}\,\rangle = P_1P_2\,, \langle\, 1 - \sqrt{-5}\,\rangle = P_1P_3$. Sada se faktorizacija (i) zameni faktorizacijom ideala:

$$\langle\, 2\,\rangle\langle\, 3\,\rangle = \langle\, 1 + \sqrt{-5}\,\rangle\langle\, 1 - \sqrt{-5}\,\rangle \qquad (ii)$$

Koristeći gornje jednakosti, (ii) postaje: $P_1^2P_2P_3 = P_1P_2P_1P_3$. Zamenom elemenata idealima koji oni generišu, od nejednoznačne faktorizacije (i), dobija se dakle jednoznačna "faktorizacija" (ii). ▼

Ovu osobinu prstena algebarskih celih prvi je uočio i dokazao Dedekind, pa se domeni u kojima se svaki ideal jednoznačno faktoriše u proizvod prostih ideala zovu Dedekindovi domeni. Ova osobina očigledno je ispunjena u glavnim domenima. Za razliku od ideala, faktorizacija elemenata Dedekindovog domena ne mora medjutim biti jednoznačna, pa se na Dedekindove domene može gledati kao na generalizaciju glavnih domena. Vremenom se došlo do puno ekvivalentnih karakterizacija ovih domena, pa se zato Dedekindovi domeni mogu definisati na različite (ekvivalentne) načine. Uobičajena je sledeća definicija.

Definicija 4.4.2. *Domen R je Dedekindov ako je Neterin, integralno zatvoren i svaki pravi prost ideal u R je maksimalan.*

Sledeća teorema ([15],[t.96]) daje novu, pogodnu karakterizaciju Dedekindovog domena.

Teorema 4.4.3. *Za domen R sledeći uslovi su ekvivalentni:*
(1) *R je Dedekindov.*
(2) *Svaki nenulti ideal u R je invertibilan.*
(3) *R je Neterin i $R_{\mathfrak{m}}$ je DVR za svaki maksimalan ideal $\mathfrak{m}$ u R.* □

Teorema 4.4.4. *U Dedekindovom domenu R svaki nenulti ideal jednoznačno se faktoriše u proizvod prostih ideala.*

Dokaz. Egzistencija: Neka je $I \neq 0$ proizvoljan ideal u R. Ako je I prost nema se šta dokazivati. Ako I nije prost, on je sadržan u nekom maksimalnom, dakle prostom idealu P. Sada je, prema uslovu (2) prethodne teoreme, ideal P invertibilan, $PP^{-1} = R$, pa dobijamo faktorizaciju:

$$I = IR = (IP^{-1})P \quad , \quad I \subsetneqq IP^{-1} \qquad (i)$$

U (i) važi stroga inkluzija jer bi u suprotnom, iz $IP^{-1} = I$, množenjem sa P dobili $I = IP$. Medjutim i ideal I je invertibilan, pa se množenjem poslednje jednakosti sa I^{-1} dolazi do kontradikcije, $P = R$. Ako je IP^{-1} prost, dokaz je završen. Ako nije, onda postoji prost ideal Q koji ga sadrži i važi:

$$IP^{-1} = IR = (IP^{-1}Q^{-1})Q \quad , \quad IP^{-1} \subsetneqq IP^{-1}Q^{-1} \qquad (ii)$$

Ovaj proces se dalje na isti način nastavlja sve do tražene proste faktorizacije. Proces se mora zaustaviti jer je R Neterin pa se lanac $I \subsetneqq IP^{-1} \subsetneqq IP^{-1}Q^{-1} \dots$ prekida.
Jednoznačnost: Neka su

$$P_1P_2 \dots P_n = Q_1Q_2 \dots Q_m \qquad (iii)$$

dve različite faktorizacije, gde su P_i , Q_j prosti ideali u R. Ovde je $P_1P_2 \dots P_n \subseteq Q_1$ i Q_1 je prost, pa se bez ograničenja opštosti može pretpostaviti da je npr. $P_1 \subseteq Q_1$. Medjutim R je Dedekindov, dakle dimR ≤ 1, pa lanci dužine 2 ne postoje u R. Odavde mora biti $P_1 = Q_1$. Množenjem jednakosti (iii) sa P^{-1} dobija se $P_2 \dots P_n = Q_2 \dots Q_m$. Dalje se indukcijom po n dobija $m = n$ i odgovarajućom prenumeracijom $P_i = Q_i$. $\square$
Primedba. U knjigama iz oblasti algebarske teorije brojeva mogu se naći i druge ekvivalentne karakterizacije Dedekindovih domena, izmedju ostalih i obrat teoreme 4.4.4. Istaknimo neke od tih karakterizacija u obliku sledećeg tvrdjenja, uz napomenu da se dokazi svih ekvivalencija mogu naći u [3, 20, 23, 13].

Tvrdjenje 4.4.5. *Za domen R sledeći uslovi su ekvivalentni:*
(1) *Svaki pravi ideal u R jednoznačno se faktoriše u proizvod prostih ideala.*
(2) *Svaki pravi ideal u R faktoriše se u proizvod prostih ideala.*
(3) *Svaki pravi ideal u R je invertibilan.*
(4) *Svaki razlomljeni ideal je invertibilan.*
(5) *$(I(R), \cdot)$ je grupa.*
(6) *R je Neterin, integralno zatvoren i* $\dim(\mathrm{R}) = 1$.
(7) *R je Neterin i $R_{\mathfrak{m}}$ je DVR za svaki maksimalan ideal $\mathfrak{m}$ u R.*
(8) *R je Neterin i $R_{\mathfrak{p}}$ je DVR za svaki prost ideal $\mathfrak{p}$ u R.*
(9) *R je Neterin i Prüferov.* $\square$

Jednoznačna faktorizacija ideala, kao što se može videti iz primera 4.4.1, ne povlači za sobom jednoznačnu faktrizaciju elemenata. Takodje ne mora da važi ni obratno, npr. prsten polinoma $k[X, Y]$ nad poljem k je UFD ali nije Dedekindov jer je dimenzije 2. Precizan odnos faktorizacije elemenata i ideala dat je sledećom teoremom.

Teorema 4.4.6. *Dedekindov domen R je UFD akko je glavni.*

Dokaz. Neka je R Dedekindov, faktorijalan domen, $\mathfrak{p}$ proizvoljan prost ideal u R i $a \in \mathfrak{p}$. Kako je R UFD, a ima jednoznačnu faktorizaciju $a = p_1^{\alpha_1}p_2^{\alpha_2} \dots p_k^{\alpha_k}$, gde su p_i prosti elementi u R. Dalje, kako je $a \in \mathfrak{p}$ i $\mathfrak{p}$ je prost, neki od elemenata $p_1, \dots, p_k$ pripada $\mathfrak{p}$. Neka npr. p_1 pripada $\mathfrak{p}$ tj. $(p_1) \subseteq \mathfrak{p}$. Kako je $\mathrm{ht}(\mathfrak{p}) = 1$,

jer je domen R Dedekindov, i (p_1) je prost ideal sadržan u $\mathfrak{p}$, mora biti $(p_1) = \mathfrak{p}$, odnosno $\mathfrak{p}$ je glavni. Neka je sada I proizvoljan ideal u R. Ideal I ima prostu faktorizaciju, a pokazano je da su prosti ideali glavni, pa je I glavni ideal, tj. R je glavni domen. Kako obratno očigledno važi, ovim je teorema dokazana. □

Teorema 4.4.6 karakteriše glavne domene kao Dedekindove UFD domene i ima česte primene u algebarskoj geometriji; da bi dokazali da je normalan domen glavni dovoljno je dokazati da je dimenzije ≤ 1 i da je faktorijalan. Na taj način vidimo da su UFD domeni dimenzije 1 upravo glavni domeni, kao i da su lokalni UFD domeni dimenzije 1 diskretni valuacioni prsteni. U algebarskoj teoriji brojeva ova teorema ima primenu u prstenima algebarskih celih. Ovi prsteni su integralno zatvoreni, Neterini, dimenzije 1 pa dakle i Dedekindovi. Pitanje faktorijalnosti ovih prstena teoremom 4.4.6 redukovano je na pitanje koji od ovih prstena je glavni. U algebarskoj teoriji brojeva postoji metod kojim se, primenom teoreme Minkovskog ([1, 23, 20]), direktnim računanjem može proveriti da li je dati domen glavni tj. da li je faktorijalan.
Ako sa $\mathfrak{D}$ označimo klasu Dedekindovih domena, sa $\mathfrak{U}$ klasu faktorijalnih domena i sa $\mathfrak{G}$ klasu glavnih domena, onda važi $\mathfrak{D} \cap \mathfrak{U} = \mathfrak{G}$. Odstupanje Dedekindovog domena od faktorijalnosti može se dakle "izmeriti" njegovim odstupanjem od glavnog domena. Ako sa $F(R)$ označimo grupu svih glavnih razlomljenih ideala Dedekindovog domena R, onda je $F(R)$ podgrupa grupe svih nenultih razlomljenih ideala $I(R)$, dok je je odgovarajuća grupa koja meri odstupanje od glavnog, odnosno UFD domena, faktorgrupa:

$$C(R) = I(R)/F(R) \tag{1}$$

Grupa $C(R)$ zove se još i *grupa klasa ideala*. Ona je u stvari specijalan slučaj grupe divizor klasa Krulovog domena. Pri tome je Dedekindov domen R UFD akko je grupa $C(R)$ trivijalna, tj. akko je *klasni razred*[7] $|C(R)| = 1$. Može se pokazati da je da je za sve prstene algebabarskih celih klasni razred konačan broj. Za $d < 0$ poznati su svi prsteni algebarskih celih $\mathbb{Q}(d)$ klasnog razreda 1. Ima ih ukupno 9, (teorema 1.2.21). Mada se za $d > 0$ klasni razredi mogu izračunati (tablice za $d < 500$ mogu se naći npr. u [2]), kao što je već rečeno, još uvek nije dokazana Gausova hipoteza da ima beskonačno mnogo prstena $\mathbb{Q}(d)$ klasnog razreda 1.
Razmotrimo sada bliže faktorizaciju na proste ideale i odgovarajuće veze sa valuacijama. Neka je R Dedekindov domen i $\mathcal{P}$ skup svih prostih ideala u R različitih od 0. Svaki razlomljeni ideal $I \in I(R)$ može se na jedinstven način predstaviti u obliku:

$$I = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{n_{\mathfrak{p}}(I)} \text{ , gde je samo konačno mnogo } n_{\mathfrak{p}}(I) \in \mathbb{Z} \text{ različito od 0.} \tag{2}$$

Očigledno je iz (2) $I \subseteq R$ ceo ideal akko su svi eksponenti $n_{\mathfrak{p}}(I) \geq 0$. Ako su

[7] Class number

sada $I, J \in I(R)$ razlomljeni ideali, $I = \prod \mathfrak{p}^{n_\mathfrak{p}(I)}$, $J = \prod \mathfrak{p}^{n_\mathfrak{p}(J)}$, onda važi:

$$IJ = \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{n_\mathfrak{p}(I)+n_\mathfrak{p}(J)} \quad , \quad I + J = \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{\inf(n_\mathfrak{p}(I),n_\mathfrak{p}(J))}$$

$$I \cap J = \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{\sup(n_\mathfrak{p}(I),n_\mathfrak{p}(J))} \quad , \quad I : J = \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{n_\mathfrak{p}(I)-n_\mathfrak{p}(J)}$$

Odavde imamo sledeće osobine:
(a) $I \subseteq R \Leftrightarrow n_\mathfrak{p}(I) \geq 0 \ \forall \mathfrak{p} \in \mathcal{P}$
(b) $I \subseteq J \Leftrightarrow n_\mathfrak{p}(I) \geq n_\mathfrak{p}(J)$
(c) $n_\mathfrak{p}(IJ) = n_\mathfrak{p}(I) + n_\mathfrak{p}(J)$
(d) $n_\mathfrak{p}(I + J) = \inf(n_\mathfrak{p}(I), n_\mathfrak{p}(J))$
(e) $n_\mathfrak{p}(I \cap J) = \sup(n_\mathfrak{p}(I), n_\mathfrak{p}(J))$
Neka je sada $a \in R$ proizvoljan element različit od nule. Tada se glavni ideal (a) jednoznačno faktoriše u proizvod:

$$(a) = \mathfrak{p}_1^{n_{\mathfrak{p}_1}} \mathfrak{p}_2^{n_{\mathfrak{p}_2}} \dots \mathfrak{p}_k^{n_{\mathfrak{p}_k}} = \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{v_\mathfrak{p}(a)} \quad , \quad v_{\mathfrak{p}_i}(a) = n_{\mathfrak{p}_i} \tag{3}$$

pa elementu $a \in R$ možemo pridružiti preslikavanja $v_{\mathfrak{p}_1}, \dots, v_{\mathfrak{p}_k} : R \to \mathbb{Z}$. Prema (c) i (d) za ova preslikavanja važe uslovi $v1$, $v2$, pa ih sa $v_\mathfrak{p}(a/b) = v_\mathfrak{p}(a) - v_\mathfrak{p}(b)$ možemo proširiti do valuacija na polju razlomaka $k = Frac(R)$. Na taj način dolazi se do familije valuacija $(v_\mathfrak{p})_{\mathfrak{p}\in\mathcal{P}}$ pridruženih Dedekindovom domenu R. Odgovarajući valuacioni prsteni su, slično kao kod faktorijalnih domena, lokalizacije po prostim idealima $\mathfrak{p} \in \mathcal{P}$ tj.

$$R_{v_\mathfrak{p}} = \{\, x \in k \mid v_\mathfrak{p}(x) \geq 0 \,\} = R_\mathfrak{p} \,,$$

sa maksimalnim idealom $\mathfrak{m}_{v_\mathfrak{p}} = \mathfrak{p}R_\mathfrak{p}$. Oni su naravno diskretni valuacioni prsteni (R je Dedekindov), $v_\mathfrak{p}(x) \neq 0$ samo za konačno mnogo $\mathfrak{p} \in \mathcal{P}$ (samo za one proste ideale koji učestvuju u faktorizaciji glavnog ideala Rx) i sam domen R jednak je preseku svojih lokalizacija $R = \cap_{\mathfrak{p}\in\mathcal{P}} R_\mathfrak{p}$. Ovo upravo znači da je svaki Dedekindov domen Krulov. Familija valuacija sa ovim osobinama može se, prema teoremi 3.3.8, pridružiti i svakom faktorijalnom domenu, pa se oni mogu u široj klasi Krulovih domena razmatrati sa istog stanovišta. Upravo iz toga vidi se i značaj Krulovih domena, kao univerzalnog koncepta za ispitivanje zajedničkih osobina Dedekindovih i faktorijalnih domena tj. faktorizacije, kako elemenata, tako i ideala.

Glava 5

Grupa klasa divizora Krulovog domena

5.1 Divizori

Neka je A domen, $k = Frac(A)$ i $I(A)$ skup svih razlomljenih ideala različitih od nule. Za $\mathfrak{p}, \mathfrak{q} \in I(A)$ definišemo relaciju $\mathfrak{p}$ "ispred" $\mathfrak{q}$ sa:

$$\mathfrak{p} \prec \mathfrak{q} \overset{\text{def}}{\iff} \forall x \in k^* \ (Ax \supseteq \mathfrak{p} \ \Rightarrow \ Ax \supseteq \mathfrak{q}) \tag{1}$$

Ovako definisana relacija suprotna je relaciji inkluzije medju razlmljenim idealima jer $\mathfrak{p} \supseteq \mathfrak{q} \ \Rightarrow \ \mathfrak{p} \prec \mathfrak{q}$. Očigledno je prema (1) relacija "ispred" refleksivna i tranzitivna, pa predstavlja jedno preduredjenje na $I(A)$. Ako stavimo:

$$\mathfrak{p} \sim \mathfrak{q} \ \Leftrightarrow \ \mathfrak{p} \prec \mathfrak{q} \ , \ \mathfrak{q} \prec \mathfrak{p} \tag{2}$$

relacija "ispred" postaje uredjenje na količničkom skupu $I(A)/\sim$ koji ćemo označiti sa $D(A)$. Elementi skupa $D(A)$ su klase ekvivalencije razlomljenih ideala, u oznaci $\mathrm{div}(\mathfrak{p})$, za $\mathfrak{p} \in I(A)$ i zovemo ih *divizorima* prstena A. Pri tome je:

$$\mathrm{div}\,\mathfrak{p} \leq \mathrm{div}\,\mathfrak{q}^{1} \ \Leftrightarrow \ \mathfrak{p} \prec \mathfrak{q} \tag{3}$$

$$\mathrm{div}\,\mathfrak{p} = \mathrm{div}\,\mathfrak{q} \ \Leftrightarrow \ \mathfrak{p} \sim \mathfrak{q} \tag{4}$$

Divizori glavnih razlomljenih ideala $\mathrm{div}\,(\mathrm{Ax})$, $\mathrm{x} \in \mathrm{k}^*$ zovu se *glavni divizori*, u oznaci $\mathrm{div(x)}$, $\mathrm{x} \in \mathrm{k}^*$. Prema (4) dva divizora su jednaka ako odgovarajući ideali imaju iste familije glavnih ideala nad sobom. Ako je $\mathfrak{p} \in I(A)$ onda postoji $d \in A$, $d \neq 0$ tako da je $d\,\mathfrak{p} \subseteq A$ tj. $\mathfrak{p} \subseteq Ad^{-1}$. Prema definiciji je dakle razlomljen ideal sadržan u nekom glavnom razlomljenom idealu, pa ima smisla posmatrati presek:

$$\widehat{\mathfrak{p}} = \bigcap_{Ax \supseteq \mathfrak{p}} Ax \ , \ \mathfrak{p} \in I(A) \tag{5}$$

[1] Koristi se i oznaka $P \leq Q$, pri čemu se podrazumevaju divizori.

Prema ovoj definiciji je $\widehat{\mathfrak{p}} \subseteq Ad^{-1}$, odnosno $d\widehat{\mathfrak{p}} \subseteq A$. Takodje je $\widehat{\mathfrak{p}} \neq 0$, jer $\widehat{\mathfrak{p}} \supseteq \mathfrak{p} \neq 0$, pa je $\widehat{\mathfrak{p}} \in I(A)$ razlomljen ideal. Pri tome važi:

$$\operatorname{div}\mathfrak{p} \leq \operatorname{div}\mathfrak{q} \;\Leftrightarrow\; \mathfrak{p} \prec \mathfrak{q} \;\Leftrightarrow\; \widehat{\mathfrak{p}} \supseteq \widehat{\mathfrak{q}} \tag{3'}$$

$$\operatorname{div}\mathfrak{p} = \operatorname{div}\mathfrak{q} \;\Leftrightarrow\; \mathfrak{p} \sim \mathfrak{q} \;\Leftrightarrow\; \widehat{\mathfrak{p}} = \widehat{\mathfrak{q}} \tag{4'}$$

Definicija 5.1.1. *Razlomljen ideal $\mathfrak{p} \in I(A)$ je divizorski ako je $\mathfrak{p} = \widehat{\mathfrak{p}}$.*

Prema ovoj definiciji divizorski ideali biće nenulti preseci nepraznih familija glavnih razlomljenih ideala. Iz toga neposredno važe sledeće osobine:

- Glavni ideali kao i nenulti preseci glavnih ideala su divizorski ideali.
- Nenulti presek familije divizorskih ideala je divizorski ideal.
- Ako je $\mathfrak{p}$ divizorski ideal onda je i $\mathfrak{p}x$ divizorski ideal, $x \in k^*$.

Kako je $\widehat{\widehat{\mathfrak{p}}} = \widehat{\mathfrak{p}}$, ideal $\widehat{\mathfrak{p}}$ je divizorski i $\mathfrak{p} \sim \widehat{\mathfrak{p}}$ pa je $\widehat{\mathfrak{p}}$ najmanji divizorski ideal koji sadrži $\mathfrak{p}$. Taj ideal jedinstven je u klasi $\operatorname{div}\mathfrak{p}$. Ako je i $\mathfrak{q}$ divizorski ideal u toj klasi, onda je $\operatorname{div}\mathfrak{q} = \operatorname{div}\mathfrak{p}$ pa je $\widehat{\mathfrak{q}} = \widehat{\mathfrak{p}}$. Kako je $\mathfrak{q}$ divizorski $\widehat{\mathfrak{q}} = \mathfrak{q}$, pa je $\mathfrak{q} = \widehat{\mathfrak{p}}$ odakle sledi jedinstvenost ovog ideala.
Neka su sada $\mathfrak{p}, \mathfrak{q} \in I(A)$ i neka je $\mathfrak{q} : \mathfrak{p} = \{x \in k \mid x\mathfrak{p} \subseteq \mathfrak{q}\}$. Može se pokazati da je onda i ideal $\mathfrak{q} : \mathfrak{p} \in I(A)$. Važi:

$$y \in \mathfrak{q} : \mathfrak{p} \;\Leftrightarrow\; yx \in \mathfrak{q}\ ,\ x \in \mathfrak{p} \;\Leftrightarrow\; y \in \mathfrak{q}x^{-1}\ ,\ x \in \mathfrak{p} \setminus \{0\} \;\Leftrightarrow\; y \in \bigcap_{x \in \mathfrak{p}\setminus\{0\}} \mathfrak{q}x^{-1}$$

Odakle je:
$$\mathfrak{q} : \mathfrak{p} = \bigcap_{x \in \mathfrak{p}\setminus\{0\}} \mathfrak{q}x^{-1}$$

Ako je $\mathfrak{q}$ divizorski ideal, onda su divizorski i ideali $\mathfrak{q}x^{-1}$, $x \in \mathfrak{p}$, $x \neq 0$ pa je takav i njihov presek, odosno ideal $\mathfrak{q} : \mathfrak{p}$ je divizorski. U vezi sa divizorskim idealima važi sledeće tvrdjenje [3].

Tvrdjenje 5.1.2. *Neka su $\mathfrak{p}, \mathfrak{q} \in I(A)$. Tada važi:*
(1) *Ako je $\mathfrak{q}$ divizorski ideal onda je i $\mathfrak{q} : \mathfrak{p}$ divizorski ideal.*
(2) $\operatorname{div}\mathfrak{p} = \operatorname{div}\mathfrak{q} \;\Leftrightarrow\; \mathrm{A} : \mathfrak{p} = \mathrm{A} : \mathfrak{q}$.
(3) $\widehat{\mathfrak{p}} = A : (A : \mathfrak{p})$. □

Prema ovom tvrdjenju ideal $\mathfrak{p} \in I(A)$ je divizorski akko je $\mathfrak{p} = A : (A : \mathfrak{p})$ tj. ako je $(\mathfrak{p}^{-1})^{-1} = \mathfrak{p}$. Specijalno, ako je I invertibilan ideal onda je $II^{-1} = A$ pa je $(I^{-1})^{-1} = I$. Kao posledicu dobijamo sledeće tvrdjenje.

Tvrdjenje 5.1.3. *Svaki invertibilan ideal je divizorski.* □

Teorema 5.1.4 ([3])**.**
(i) Svaki odozgo (odozdo) ograničen podskup u $D(A)$ ima supremum (infimum). Ako je $(\mathfrak{p}_i)_{i\in I}$ familija elemenata iz $I(A)$ ograničena odozgo (odozdo) onda je

$$\sup\left(\operatorname{div}\mathfrak{p}_{\mathrm{i}}\right) = \operatorname{div}\left(\bigcap \widehat{\mathfrak{p}}_{\mathrm{i}}\right) \quad , \quad \inf\left(\operatorname{div}\mathfrak{p}_{\mathrm{i}}\right) = \operatorname{div}\left(\sum \mathfrak{p}_{\mathrm{i}}\right) \tag{5}$$

(ii) $(D(A), \leq)$ je mreža. □

Prema ovom tvrdjenju za $\mathfrak{p},\mathfrak{q} \in I(A)$ skup $\{\mathfrak{p},\mathfrak{q}\}$ ograničen odozgo u $D(A)$ sa $\mathfrak{p}\cap\mathfrak{q}$, i odozdo sa $\mathfrak{p}+\mathfrak{q}$ ima supremum i infimum.

$$\sup(\mathfrak{p},\mathfrak{q}) = \operatorname{div}(\widehat{\mathfrak{p}}\cap\widehat{\mathfrak{q}}) \quad , \quad \inf(\mathfrak{p},\mathfrak{q}) = \operatorname{div}(\mathfrak{p}+\mathfrak{q}) \tag{6}$$

Posebno, ako su $x, y \in k^*$ onda:
$A(x+y) \subseteq Ax + Ay \;\Rightarrow\; \operatorname{div} \mathrm{A}(\mathrm{x}+\mathrm{y}) \geq \operatorname{div}(\mathrm{Ax}+\mathrm{Ay}) = \inf(\operatorname{div}\mathrm{Ax}, \operatorname{div}\mathrm{Ay})$
pa za glavne divizore važi:

$$\operatorname{div}(\mathrm{x}+\mathrm{y}) \geq \inf(\operatorname{div}(\mathrm{x}), \operatorname{div}(\mathrm{y})) \tag{7}$$

Lema 5.1.5. *Neka su* $\mathfrak{p},\mathfrak{q},\mathfrak{r} \in I(A)$ *i* $\mathfrak{p} \prec \mathfrak{q}$. *Tada je i* $\mathfrak{pr} \prec \mathfrak{qr}$.

Dokaz. $Ax \supseteq \mathfrak{pr} \;\Rightarrow\; Ax \supseteq \mathfrak{p}y \;\; (\forall y \in \mathfrak{r}) \;\Rightarrow\; Axy^{-1} \supseteq \mathfrak{p} \;\; (\forall y \in \mathfrak{r})$
$Axy^{-1} \supseteq \mathfrak{q} \;\; (\forall y \in \mathfrak{r}) \;\Rightarrow\; Ax \supseteq \mathfrak{q}y \;\; (\forall y \in \mathfrak{r}) \;\Rightarrow\; Ax \supseteq \mathfrak{qr}$

Svaki glavni ideal koji sadrži $\mathfrak{pr}$ sadrži i $\mathfrak{qr}$ pa je prema definiciji relacije " $\prec$ " ispunjeno $\mathfrak{pr} \prec \mathfrak{qr}$. $\square$
U mrežasto uredjenom skupu $D(A)$ može se definisati binarna operacija " $+$ " na sledeći način:

$$\operatorname{div}\mathfrak{p} + \operatorname{div}\mathfrak{q} \overset{\text{def}}{=} \operatorname{div}\mathfrak{pq} \tag{8}$$

Dobra definisanost: Neka je $\operatorname{div}\mathfrak{p} = \operatorname{div}\mathfrak{p}'$, $\operatorname{div}\mathfrak{q} = \operatorname{div}\mathfrak{q}'$. To znači da je $\mathfrak{p} \sim \mathfrak{p}'$, $\mathfrak{q} \sim \mathfrak{q}'$ tj. $\mathfrak{p} \prec \mathfrak{p}'$, $\mathfrak{p}' \prec \mathfrak{p}$, $\mathfrak{q} \prec \mathfrak{q}'$, $\mathfrak{q}' \prec \mathfrak{q}$. Primenom prethodne leme i tranzitivnosti relacije " $\prec$ " dobija se: $\mathfrak{pq} \prec \mathfrak{p}'\mathfrak{q} \prec \mathfrak{p}'\mathfrak{q}'$, $\mathfrak{p}'\mathfrak{q}' \prec \mathfrak{p}'\mathfrak{q} \prec \mathfrak{pq}$. Odavde je $\mathfrak{pq} \sim \mathfrak{p}'\mathfrak{q}'$, odnosno $\operatorname{div}(\mathfrak{pq}) = \operatorname{div}(\mathfrak{p}'\mathfrak{q}')$, iz čega sledi dobra definisanost operacije "+".

Saglasnost sa uredjenjem: Ako je $\operatorname{div}\mathfrak{p} \leq \operatorname{div}\mathfrak{q}$ prema lemi 5.1.5 je onda i $\operatorname{div}(\mathfrak{pr}) \leq \operatorname{div}(\mathfrak{qr})$. Prema definiciji operacije "+" onda je i $\operatorname{div}\mathfrak{p} + \operatorname{div}\mathfrak{r} \leq \operatorname{div}\mathfrak{q} + \operatorname{div}\mathfrak{r}$ tj. "+" je saglasno sa uredjenjem.

Neutralni element: Kako je $A\mathfrak{p} = \mathfrak{p}$, za svako $\mathfrak{p} \in I(A)$ važi:

$$\operatorname{div}\mathfrak{p} = \operatorname{div}\mathrm{A}\mathfrak{p} = \operatorname{div}\mathfrak{p} + \operatorname{div}\mathrm{A}$$

pa je neutralni element $0 = \operatorname{div}\mathrm{A} = \operatorname{div}(1)$.

Asocijativnost i komutativnost:

$$(\mathfrak{pq})\mathfrak{r} = \mathfrak{p}(\mathfrak{qr}) \;\Rightarrow\; (\operatorname{div}\mathfrak{p} + \operatorname{div}\mathfrak{q}) + \operatorname{div}\mathfrak{r} = \operatorname{div}\mathfrak{p} + (\operatorname{div}\mathfrak{q} + \operatorname{div}\mathfrak{r})$$

$$\mathfrak{pq} = \mathfrak{qp} \;\Rightarrow\; \operatorname{div}\mathfrak{p} + \operatorname{div}\mathfrak{q} = \operatorname{div}\mathfrak{q} + \operatorname{div}\mathfrak{p}$$

Iz ovih osobina dobija se:

Teorema 5.1.6. $(D(A), +)$ *je uredjen komutativan monoid.* $\square$

Neka je $\mathfrak{p} \in I(A)$ razlomljen ideal. Tada je prema definiciji uredjenja na $D(A)$:

$$\operatorname{div}\mathfrak{p} \geq 0 \;\Leftrightarrow\; \operatorname{div}\mathfrak{p} \geq \operatorname{div}\mathrm{A} \;\Leftrightarrow\; \mathfrak{p} \subseteq \mathrm{A}$$

Pozitivni elementi u $D(A)$ su prema tome celi ideali u A. Naravno, važno pitanje ovde je odrediti uslove pod kojima će $(D(A), +)$ biti grupa. To posebno važi ako se ograničimo na glavne divizore; neka je zato $F(A) = \{\, \operatorname{div}(\mathrm{x}) \mid \mathrm{x} \in \mathrm{k}^* \,\}$. Tada za $x, y \in k^*$ važi:

$$\operatorname{div}(\mathrm{x}) = \operatorname{div}(\mathrm{y}) \;\Leftrightarrow\; \widehat{\mathrm{Ax}} = \widehat{\mathrm{Ay}} \;\Leftrightarrow\; \mathrm{Ax} = \mathrm{Ay} \tag{9}$$

$$\operatorname{div}(\mathrm{x}) \leq \operatorname{div}(\mathrm{y}) \;\Leftrightarrow\; \mathrm{Ax} \leq \mathrm{Ay} \;\Leftrightarrow\; \mathrm{Ax} \supseteq \mathrm{Ay} \tag{10}$$

$$Ax \cdot Ax^{-1} = A \;\Rightarrow\; \operatorname{div}(\mathrm{x}) + \operatorname{div}(\mathrm{x}^{-1}) = 0 \tag{11}$$

Iz ovih osobina dobija se:

Teorema 5.1.7. *$(F(A), +)$ je uredjena Abelova grupa sa uredjenjem indukovanim uredjenjem " $\leq$ " na $D(A)$. Takodje je $F(A) \cong \mathcal{P}^*$, gde je $(\mathcal{P}^*, \cdot)$ multiplikativna grupa glavnih razlomljenih ideala uredjena inkluzijom.* $\square$

Za $P, Q \in D(A)$ definišemo relaciju:

$$P \approx Q \;\overset{\text{def}}{\Longleftrightarrow}\; P = Q + \operatorname{div}(\mathrm{x}) \quad \text{za neko } \mathrm{x} \in \mathrm{k}^* \tag{12}$$

Uvedena relacija " $\approx$ " je relacija ekvivalencije na $D(A)$. Elemente $P, Q \in D(A)$ takve da je $P \approx Q$ zovemo *ekvivalentnim divizorima.* Iz definicije (12) vidi se da su za divizorske ideale $\mathfrak{p}, \mathfrak{q}$ divizori $\operatorname{div}\mathfrak{p}, \operatorname{div}\mathfrak{q}$ ekvivalentni akko $\mathfrak{p} = \mathfrak{q}x$ za neko $x \in k^*$, kao i da je relacija " $\approx$ " saglasna sa " $+$ ". $D(A)/\approx$ odnosno $D(A)/F(A)$ je komutativan monoid koji zovemo *monoidom divizor klasa* na A. Neka je $J(A) = \{J \in I(A) \mid JJ^{-1} = A\}$ skup invertibilnih ideala u A i neka su $\mathfrak{p}, \mathfrak{q} \in J(A)$. Tada i $\mathfrak{pq} \in J(A)$ jer $\mathfrak{pp}^{-1} = \mathfrak{qq}^{-1} = A \;\Rightarrow\; \mathfrak{pq}(\mathfrak{pq})^{-1} = A$. Takodje je $\operatorname{div}\mathfrak{p} + \operatorname{div}\mathfrak{p}^{-1} = 0$, pa je i $J(A)$ jedna podgrupa monoida $D(A)$. Kako je svaki glavni ideal invertibilan važe sledeće inkluzije:

$$F(A) \;\subseteq\; J(A) \;\subseteq\; D(A)$$

Može se posmatrati monoid $D(A)/J(A)$, kao i faktorgrupa $J(A)/F(A)$. Faktorgrupu $J(A)/F(A)$ zovemo još i *Pikarovom grupom* domena A, u oznaci $Pic(A)$.

Lema 5.1.8. *Neka su $\mathfrak{p}, \mathfrak{q} \in J(A)$ takvi da je $\operatorname{div}\mathfrak{p} = \operatorname{div}\mathfrak{q}$. Tada je $\mathfrak{p} = \mathfrak{q}$.*

Dokaz. Neka $\mathfrak{r} \in J(A)$, $\operatorname{div}\mathfrak{r} = 0$. Tada iz $\mathfrak{r} \subseteq A$ i $\mathfrak{r}^{-1} = A$, sledi da je $\operatorname{div}\mathfrak{r} + \operatorname{div}\mathfrak{r}^{-1} = 0$ odnosno $\operatorname{div}\mathfrak{r}^{-1} = 0$. To znači da su $\mathfrak{r}, \mathfrak{r}^{-1} \subseteq A$ tj. $\mathfrak{r}, A : \mathfrak{r} \subseteq A$ odakle je $A \subseteq A : (A : \mathfrak{r}) = \mathfrak{r}$. Sada $\mathfrak{r} \subseteq A$ i $A \subseteq \mathfrak{r}$ daje $A = \mathfrak{r}$ tj. jedini invertibilan ideal $\mathfrak{r}$ takav da je $\operatorname{div}\mathfrak{r} = 0$ je sam domen A. Ako su sada $\mathfrak{p}, \mathfrak{q} \in J(A)$ invertibilni ideali za koje je $\operatorname{div}\mathfrak{p} = \operatorname{div}\mathfrak{q}$ onda je $\operatorname{div}\mathfrak{p} - \operatorname{div}\mathfrak{q} = 0$ odnosno $\operatorname{div}\mathfrak{pq}^{-1} = 0$. Kako je $\mathfrak{pq}^{-1}$ invertibilan, jer je $\mathfrak{pq}^{-1}(\mathfrak{pq}^{-1})^{-1} = A$, prema prethodnom mora biti $\mathfrak{pq}^{-1} = A$ tj. $\mathfrak{p} = \mathfrak{q}$. $\square$

Teorema 5.1.9. *Monoid $D(A)$ je grupa akko je A kompletno integralno zatvoren.*

Dokaz. ($\Rightarrow$:) Neka je $x \in k$ skoro ceo nad A tj. $A[x] \in I(A)$. Tada je:

$$xA[x] \subseteq A[x] \;\Rightarrow\; \mathrm{div(xA[x])} \geq \mathrm{divA[x]} \;\Rightarrow\; \mathrm{div(x)} + \mathrm{div\,A[x]} \geq \mathrm{div\,A[x]}$$

Kako je $D(A)$ uredjena grupa, iz poslednje relacije biće $\mathrm{div(x)} \geq 0$, odnosno $Ax \subseteq A$, pa je $x \in A$.
($\Leftarrow$:) Neka je sada A kompletno integralno zatvoren domen tj. $A = I : I$ za svaki razlomljeni ideal $I \in I(A)$. Neka je $\mathfrak{p} \in I(A)$ proizvoljan razlomljen ideal. Dovoljno je naći inverzan element u $D(A)$ za $\mathrm{div}\,\mathfrak{p}$. Koristeći osbinu razlomljenih ideala $I : JK = (I : J) : K$ za $I, J, K \in I(A)$ i kompletnu integralnu zatvorenost domena A dobija se sledeća jednakost:

$$A : \mathfrak{p}(A : \mathfrak{p}) = (A : \mathfrak{p}) : (A : \mathfrak{p}) = A$$

Odakle je
$$A : (A : \mathfrak{p}(A : \mathfrak{p})) = A : A = A$$

$$\mathrm{div}(\mathfrak{p}(\mathrm{A} : \mathfrak{p})) = \mathrm{div\,A} \;\Rightarrow\; \mathrm{div}\,\mathfrak{p} + \mathrm{div(A} : \mathfrak{p}) = 0$$

Iz poslednje jednakosti $A : \mathfrak{p}$ je traženi inverzni element. □

Definicija 5.1.10. *U slučaju kompletno integralno zatvorenog domena A faktorgrupu $D(A)/F(A)$ zovemo grupom klasa divizora ili grupom divizor klasa domena A, u oznaci*

$$Cl(A) = D(A)/F(A)$$

Primedba. Grupa divizor klasa ne mora se definisati ovim putem. Jedan od mogućih načina za dobijanje grupe $Cl(A)$ je sledeći [10]; Za $D(A)$ uzmemo skup svih divizorskih ideala sa operacijom " $\cdot$ " :

$$\mathfrak{p} \cdot \mathfrak{q} \stackrel{\mathrm{def}}{=} A : (A : \mathfrak{pq}\,) \tag{13}$$

Desna strana ove jednakosti je prema 5.1.2 takodje divizorski ideal. Na ovaj način umesto sa klasama $\mathrm{div}\,\mathfrak{p}$ radimo sa reprezentima tih klasa - divizorskim idealima. Računanjem se može pokazati da je ovako uvedena operacija asocijativna i komutativna sa neutralnim elementom A, pa je $(D(A), \cdot\,)$ komutativan monoid. Uredjenje na $D(A)$ dato je sa:

$$\mathfrak{p} \leq \mathfrak{q} \;\Leftrightarrow\; A : \mathfrak{p} \supseteq A : \mathfrak{q} \tag{14}$$

Ako je A kompletno integralno zatvoren $D(A)$ postaje uredjena Abelova grupa. Dobijena grupa $Cl(A) = D(A)/F(A)$ je ista kao i grupa dobijena definicijom (8), pa su (8) i (13) ekvivalentne definicije.

5.2 Krulovi domeni

Definicija 5.2.1. *Domen A je Krulov ako postoji familija $(V_i)_{i \in I}$ valuacionih prstena, $A \subseteq V_i \subseteq k$, $k = Frac(A)$ takva da su ispunjena sledeća tri uslova:*

(K_1) *V_i su glavni valuacioni (DVR).*
(K_2) $A = \bigcap_{i\in I} V_i$. (1)
(K_3) *Ako je $a \in A$, $a \neq 0$ onda se a nalazi u najviše konačno mnogo maksimalnih ideala M_i domena V_i, tj. invertibilan je skoro u svakom V_i.*

Osobina (K_3) je osobina tzv. *lokalne konačnosti preseka* (1). Ako je potrebno naglasiti valuacijski pristup prethodna definicija može se dati i u sledećem ekvivalentnom obliku;

Definicija 5.2.2. *Domen A je Krulov ako postoji familija $(v_i)_{i\in I}$ valuacija njegovog polja razlomaka k za koje su ispunjeni sledeći uslovi:*
(K_1') *Valuacije v_i su diskretne.*
(K_2') $A = \bigcap_{i\in I} A_{v_i}$. (2)
(K_3') *Presek* (2) *je lokalno konačan; ako je $a \in A$, $a \neq 0$ onda je $v_i(a) \neq 0$ samo za konačno mnogo $i \in I$.*

Beskonačna familija diskretnih valuacionih prstena $(V_i)_{i\in I}$ koji definišu Krulov domen u 5.2.1 ne mora biti jednoznačna. Ako sa $\mathcal{P}(A)$ označimo skup minimalnih prostih ideala u A, može se pokazati da za svaki minimalan prost ideal $\mathfrak{p} \in \mathcal{P}(A)$, $A_\mathfrak{p}$ pripada familiji $(V_i)_{i\in I}$ kao i da je $A = \bigcap\limits_{\mathfrak{p}\in\mathcal{P}(A)} A_\mathfrak{p}$ [15, 21]. Na taj način familija $(A_\mathfrak{p})_{\mathfrak{p}\in\mathcal{P}(A)}$ je minimalna familija koja definiše Krulov domen A. Zbog toga se definicija Krulovog domena često daje i u sledećem obliku:

Definicija 5.2.3. *Domen A je Krulov ako su ispunjeni sledeći uslovi:*
(K_1'') *$A_\mathfrak{p}$ je DVR za svaki minimalan prost ideal $\mathfrak{p}$.*
(K_2'') $A = \bigcap_{\mathfrak{p}\in\mathcal{P}(A)} A_\mathfrak{p}$. (3)
(K_3'') *Presek* (3) *je lokalno konačan; ako je $a \in A$, $a \neq 0$ onda a leži u najviše konačno mnogo $\mathfrak{p} \in \mathcal{P}(A)$.*

Sledeće dve teoreme su neposredna posledica definicije Krulovog domena, teoreme 3.3.8 i osobina familije valuacija koje se mogu pridružiti svakom Dedekindovom domenu.

Teorema 5.2.4. *UFD je Krulov domen.* □

Teorema 5.2.5. *Dedekindov domen je Krulov.* □

Kako postoje Dedekindovi domeni sa nejednoznačnom faktorizacijom, kao i faktorijalni domeni koji nisu Dedekindovi iz prethodnih teorema vidi se i značaj Krulovih domena kao šire, objedinjujuće klase u okviru koje se mogu ispitivati njihova zajednička svojstva. Teorema 5.2.5 može se dobiti i kao posledica sledeće teoreme iz koje vidimo da klasa Krulovih domena sadrži i široku klasu normalnih[2] domena.

Teorema 5.2.6. *Neterin integralno zatvoren domen je Krulov.*

[2]Neterini integralno zatvoreni domeni.

Dokaz. Neka je A normalan domen i $\mathcal{P}(A) = \{\, \mathfrak{p} \lhd A \mid \mathrm{ht}(\mathfrak{p}) = 1\}$. Prema 4.1.7 $A_{\mathfrak{p}}$ je DVR za svako $\mathfrak{p} \in \mathcal{P}(A)$ i $A = \bigcap_{\mathfrak{p}\in\mathcal{P}(A)} A_{\mathfrak{p}}$ pa je dovoljno pokazati lokalnu konačnost ovog preseka. Neka je $a \in A$, $a \neq 0$. Glavni ideal aA ima konačnu primarnu dekompoziciju:

$$aA = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \ ; \ Ass(aA) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \ , \ \mathfrak{p}_i = \sqrt{\mathfrak{q}_i} \tag{4}$$

Iz primarnog razlaganja (4) sledi da ima samo konačno mnogo minimalnih prostih ideala koji sarže glavni ideal aA pa a leži u najviše konačno mnogo $\mathfrak{p} \in \mathcal{P}(A)$. □

Svaki Krulov domen je i integralno zatvoren kao presek valuacionih domena koji su integralno zatvoreni. Svaki Krulov domen nije medjutim i Neterin. Npr. $k[X_1, X_2, \ldots]$ prsten polinoma sa beskonačno mnogo promenljivih nad poljem k je UFD pa je Krulov i očigledno nije Neterin pa obrat teoreme 5.2.6 ne mora da važi. Mogu se takodje naći primeri Neterinih ili integralno zatvorenih domena koji nisu Krulovi.

Teorema 5.2.7. *Svaki Krulov domen je kompletno integralno zatvoren.*

Dokaz. Kako je Krulov domen lokalno konačan presek diskretnih valuacionih prstena dovoljno je dokazati da je svaki diskretni valuacioni prsten kompletno integralno zatvoren. DVR je prema 3.3.4 UFD, pa je prema teoremi 2.5.6 kompletno integralno zatvoren. □

Ako imamo familiju Krulovih domena $(A_i)_{i\in I}$ sadržanih u istom polju k i sa $(v_{ij})_{j\in J}$ označimo familiju diskretnih valuacija koje definišu A_i onda i familija $(w_{ij})_{j\in J}$, gde su w_{ij} restrikcije valuacija v_{ij} na količničko polje domena $\bigcap_{i\in I} A_i$, zadovoljava uslove definicije 5.2.2. Iz toga se dobija sledeće tvrdjenje.

Lema 5.2.8. *Neka je $(A_i)_{i\in I}$ familija Krulovih domena sadržanih u istom polju k čiji je presek lokalno konačan. Tada je i $A = \bigcap_{i\in I} A_i$ Krulov domen.* □

Posledica 5.2.9. *Ako je A Krulov domen, $k = Frac(A)$ i k' potpolje polja k onda je i $A \cap k'$ Krulov domen.* □

Posledica 5.2.10. *Neka je $A = \bigcap_{i\in I} V_i$ Krulov domen. Tada je i podpresek $A' = \bigcap_{j\in J} V_j$, gde je $J \subseteq I$, takodje Krulov.*

Dokaz. Svaki diskretni valuacioni prsten V_j je Neterin i integralno zatvoren dakle Krulov. Kako je $A \subseteq V_j \subseteq k$, za svako $j \in J$, prema lemi 5.2.8 i $\bigcap_{j\in J} V_j$ je onda Krulov. □

5.3 Raširenja Krulovih domena

Teorema 5.3.1. *Lokalizacija Krulovog domena je Krulov domen. Preciznije, ako je $A = \bigcap_{i\in I} A_{v_i}$ Krulov domen i $S \subseteq A$ multiplikativan podskup, onda je $A_S = \bigcap_{j\in J} A_{v_j}$, gde je:*

$$J = \{\, j \in I \mid v_j(s) = 0 \ , \ s \in S \,\} = \{\, j \in I \mid A_S \subseteq A_{v_j} \,\} \tag{5}$$

Dokaz. Najpre se pokazuje da je $v_j \mid_{\mathrm{s}} = 0 \Leftrightarrow A_S \subseteq A_{v_j}$. Neka je zato $v_j \mid_{\mathrm{s}} = 0$ i $a/s \in A_S$, $a \in A$, $s \in S$. Tada je

$$v_j(a/s) = v_j(a) - v_j(s) = v_j(a) \geq 0$$

jer je $A \subseteq A_{v_j}$. Odavde je $a/s \in A_{v_j}$ pa imamo inkluziju $A_S \subseteq A_{v_j}$. Obratno, ako je $A_S \subseteq A_{v_j}$ i $s \in S$ proizvoljan element, onda $1/s \in A_{v_j}$, odakle je

$$v_j(1/s) = v_j(1) - v_j(s) = -v_j(s) \geq 0$$

Kako je $S \subseteq A$, važi i $v_j(s) \geq 0$, pa mora biti $v_j(s) = 0$, odnosno $v_j \mid_{\mathrm{s}} = 0$. Posebno, odavde imamo i inkluziju $A_S \subseteq \bigcap_{j \in J} A_{v_j}$.

Neka sada $x \in \bigcap_{j \in J} A_{v_j}$. A je Krulov domen pa je iz uslova (K_3') skup indeksa $\{\, i \in I \mid v_i(x) \neq 0 \,\}$ konačan. Specijalno je onda konačan i njegov podskup $J' = \{\, t \in I \mid v_t(x) < 0 \,\}$. Dakle za $t \in J'$ važi $x \notin A_{v_t}$ pa $t \notin J$. Postoji dakle element $s_t \in S$ takav da je $v_t(s_t) > 0$ npr. $v_t(s_t) = m_t$. Tada je:

$$v_t(s_t^{n_t} x) = n_t m_t + v_t(x)$$

Biramo n_t tako da je $v_t(s_t^{n_t} x) \geq 0$. Ako za konačan skup indeksa J' stavimo $s = \prod_{t \in J'} s_t^{n_t}$ važiće $v_t(sx) \geq 0$, za svako $t \in I$. Odavde je $sx \in A$ tj. $x \in A_S$, pa je ovim dokazana i obratna inkluzija, dakle $A_S = \bigcap_{j \in J} A_{v_j}$. Sada je A_S Krulov prema 5.2.10. $\square$

Primedba. Obrat ove teoreme važi pod uslovima Nagatine teoreme [11]: ako je A domen u kome važi uslov ACC_1 i $S \subseteq A$ multiplikativan podskup generisan familijom prostih elemenata takav da je A_S Krulov domen, onda je i A Krulov.

Teorema 5.3.2. *A Krulov $\Rightarrow$ $A[X]$ Krulov.*

Dokaz. Neka je $A = \bigcap_{v \in F} A_v$, gde je F-familija diskretnih valuacija koja definiše Krulov domen A i neka je $k = Frac(A)$. $k[X]$ je glavni domen, dakle i Krulov, pa je $k[X] = \bigcap_{v_f \in G} A_{v_f}$, gde je G-familija p-adičnih valuacija indukovanih atomima $f \in k[X]$. Svaka glavna valuacija $v \in F$, $v : k \to \mathbb{Z}$, može se produžiti do valuacije $w : k(X) \to \mathbb{Z}$, na sledeći način; za polinom $p\,(X) = a_0 + a_1 X + \cdots + a_n X^n$ iz $k[X]$ definišemo: $w(\,p\,(X)) \stackrel{\text{def}}{=} \min\{v(a_i)\}$. Za ovako definisano preslikavanje važe uslovi $(v_1), (v_2)$ pa se može produžiti do valuacije na $k(X)$ stavljajući $w(\,p\,(X)/q\,(X)\,) = w(\,p\,(X)) - w(\,q\,(X))$. Neka je F'-familija ovako dobijenih valuacija. Sve valuacije $v_f \in G$, $w \in F'$ su diskretne i ako je $p \in k[X]$ onda je $v_f(p) \neq 0$, $w(p) \neq 0$ samo za konačno mnogo $v_f \in G$, $w \in F'$. Dovoljno je pokazati da je tada:

$$A[X] = \bigcap_{v_f \in G} A[X]_{v_f} \cap \Big(\bigcap_{w \in F'} A[X]_w \Big) = k[X] \cap \Big(\bigcap_{w \in F'} A[X]_w \Big) \qquad (6)$$

Neka je $p = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$. Kako je $A \subseteq A_v$, $\forall v \in F$ to je i $v(a_i) \geq 0$, $i = 0, \ldots, n$ odakle je i $w(p) = \min\{v(a_i)\} \geq 0$. To znači da $p \in A[X]_w$, tj. $A[X] \subseteq A[X]_w$, $\forall w \in F'$. Kako je $A[X] \subseteq k[X]$ time je dokazana

inkluzija $A[X] \subseteq k[X] \cap (\cap A[X]_w)$. Neka sada polinom $p \in k[X]$ pripada i preseku $\bigcap_{w \in F'} A[X]_w$. To znači da je $w(p) \geq 0\,, \forall w$, odnosno $\min\{v(a_i)\} \geq 0\,, \forall v$. Odavde:

$$v(a_i) \geq 0 \;\; \forall v\,, \forall i \;\Rightarrow\; a_i \in A_v \;\; \forall v\,, \forall i \;\Rightarrow\; a_i \in \bigcap_{v \in F} A_v = A$$

Odavde $p \in A[X]\,$, čime je dokazana jednakost (6). $\square$

Indukcijom se odavde dobija da je i prsten polinoma $A[X_1, \ldots, X_n]$ Krulov ako je A Krulov. Može se takodje pokazati da je onda i $A[X_1, X_2, \ldots]$ Krulov. Koristeći jednakost (6) može se pokazati da su minimalni prosti ideali prstena polinoma $A[X]$ oblika $\mathfrak{p}A[X]$, gde je $\mathfrak{p} \in \mathcal{P}(A)$, ili oblika $(f) \cap A[X]$, gde je $f \in k[X]$ ireducibilan polinom.

Teorema 5.3.3. *A Krulov $\Rightarrow$ $A[[X]]$ Krulov.*

Dokaz. Neka je $A = \bigcap_{i \in I} A_i\,$, gde su A_i diskretni valuacioni prsteni. To posebno znači i da su A_i kompletno integralno zatvoreni pa je takav i svaki od prstena $A_i[[X]]\,, i \in I$. Kako je svaki od njih i Neterin, prema 5.2.6 $A_i[[X]]\,, i \in I$ su Krulovi domeni. Ako je $k = Frac(A)$ onda je $k[[x]]$ DVR, pa je Krulov i $A_i[[X]] \subseteq k[[X]]\,, \forall i$, pa je

$$A[[X]] = \bigcap_{i \in I} A_i[[X]] \tag{7}$$

presek unutar $k[[X]]$. Presek (7) nije medjutim i lokalno konačan jer element X nije invertibilan u $A_i[[X]]$ za gotovo sve $i \in I$. Da bi dobili lokalnu konačnost preseka proširimo $A_i[[X]]$ stavljajući $B_i = A_i[[X]][X^{-1}]$. B_i su Krulovi kao lokalizacije Krulovih i

$$A[[X]] = k[[X]] \cap \big(\bigcap_{i \in I} B_i\big) \tag{8}$$

Neka je $f \in A[[X]]\,, f \neq 0$

$$f = a_n X^n + a_{n+1} X^{n+1} + \ldots\,, a_n \neq 0\,, a_i \in A$$

$$X^{-n} f = a_n + a_{n+1} X + \cdots \in k[[X]] \cap \big(\bigcap_{i \in I} B_i\big)$$

Odavde je f neinvertibilan u B_i akko je a_n neinvertibilan u A_i. Takvih i-ova je medjutim samo konačno mnogo jer je presek $\bigcap_{i \in I} A_i$ lokalno konačan. Sada je $A[[X]]$ Krulov prema 5.2.8. $\square$

5.4 Divizori u Krulovim domenima

Neka je sada A Krulov domen sa odgovarajućom familijom diskretnih valuacija $(v_i)_{i \in I}$. Prema 5.2.7 A je kompletno integralno zatvoren pa je monoid divizor

klasa, $(D(A)\,,+)$, uredjena grupa prema 5.1.9. Za razlomljen ideal $\mathfrak{p} \in I(A)$ definiše se:

$$v_i(\mathfrak{p}) \stackrel{\text{def}}{=} \sup_{Ax \supseteq \mathfrak{p}} (v_i(x)) \tag{9}$$

Familija celih brojeva $\{\, v_i(x) \mid Ax \supseteq \mathfrak{p} \,\}$ je ograničena jer za proizvoljan element $a \in \mathfrak{p}\,,\ a \neq 0$ važi $aA \subseteq xA \ \Rightarrow\ v_i(a) \geq v_i(x)$. Neka je sada $\mathfrak{p}$ divizorski ideal, $\mathfrak{p} = \bigcap_{Ax \supseteq \mathfrak{p}} Ax$. Tada $y \in \mathfrak{p}$ akko $y \in Ax$ kad god $Ax \supseteq \mathfrak{p}$. Odavde je $v_i(y) \geq v_i(x)\,,\ \forall i$ pa je $v_i(y) \geq v_i(\mathfrak{p})\,,\ \forall i$. S druge strane, ako je $v_i(y) \geq v_i(\mathfrak{p})\,,\ \forall i$, onda je $v_i(y) \geq v_i(x)$ kad god je $\mathfrak{p} \subseteq Ax$. Odavde je sada $v_i(y/x) \geq 0$ pa $y/x \in A$ kad god $Ax \supseteq \mathfrak{p}$ tj. $y \in \bigcap_{Ax \supseteq \mathfrak{p}} Ax = \mathfrak{p}$. Iz ovoga imamo sledeću karakterizaciju divizorskih ideala $\mathfrak{p}, \mathfrak{q}$ u Krulovom domenu A :

$(a)\ \ y \in \mathfrak{p} \ \Leftrightarrow\ v_i(y) \geq v_i(\mathfrak{p})\,,\ \forall i.$
$(b)\ \ \mathfrak{p} \subseteq \mathfrak{q} \ \Leftrightarrow\ v_i(\mathfrak{p}) \geq v_i(\mathfrak{q})\,,\ \forall i.$
$(c)\ \ v_i(x) = v_i(Ax)\ ,\ \forall x \in k^*.$

Neka je sada $\mathfrak{p} \in I(A)$ proizvoljan razlomljen ideal. Tada postoje $x, y \in k^*$ takvi da je $Ax \subseteq \mathfrak{p} \subseteq Ay$. Tada je $v_i(x) \geq v_i(\mathfrak{p}) \geq v_i(y)\,,\ \forall i$. Kako je A Krulov domen, biće $v_i(x) \neq 0\,,\ v_i(y) \neq 0$ samo za konačno mnogo $i \in I$, odakle je i $v_i(\mathfrak{p}) \neq 0$ za konačno mnogo $i \in I$, pa za razlomljene ideale važi:

$(d)\ \ \forall\, \mathfrak{p} \in I(A)\ v_i(\mathfrak{p}) \neq 0\ $ samo za konačno mnogo $i \in I$.

Prema (d) može se posmatrati preslikavanje:

$$\mathfrak{p} \mapsto (v_i(\mathfrak{p}))_{i \in I} \tag{10}$$

skupa divizorskih ideala Krulovog domena u mrežasto uredjenu grupu $\mathbb{Z}^{(I)}$. Ako se ograničimo samo na cele divizorske ideale onda $\mathfrak{p} \subseteq A \ \Rightarrow\ v_i(\mathfrak{p}) \geq v_i(A)$ tj. $v_i(\mathfrak{p}) \geq 0\,,\ \forall i \in I$. Ovim je definisano preslikavanje skupa celih divizorskih ideala u skup pozitivnih elemenata uredjene grupe $\mathbb{Z}^{(I)}$. Pri tome važi:

$$\mathfrak{p} \subseteq \mathfrak{q} \ \Rightarrow\ v_i(\mathfrak{p}) \geq v_i(\mathfrak{q})\,,\ \forall i \ \Rightarrow\ (v_i(\mathfrak{p}))_{i \in I} \geq (v_i(\mathfrak{q}))_{i \in I}$$

$$(v_i(\mathfrak{p}))_{i \in I} = (v_i(\mathfrak{q}))_{i \in I} \ \Leftrightarrow\ v_i(\mathfrak{p}) = v_i(\mathfrak{q})\,,\ \forall i \ \Leftrightarrow\ \mathfrak{p} = \mathfrak{q}$$

pa je ovo preslikavanje injektivno i opadajuće. Ove osobine mogu se formulisati u obliku sledeće leme.

Lema 5.4.1. *Neka je A Krulov domen odredjen familijom valuacija $(v_i)_{i \in I}$. Tada je preslikavanjem $\mathfrak{p} \mapsto (v_i(\mathfrak{p}))_{i \in I}$ uspostavljena monotona injekcija skupa celih divizorskih ideala u skup pozitivnih elemenata uredjene grupe $\mathbb{Z}^{(I)}$.* □

Kako u uredjenoj grupi $\mathbb{Z}^{(I)}$ svaki neprazan podskup pozitivnih elemenata ima minimalan element, neposredno se dobija sledeća posledica.

Posledica 5.4.2. *Svaka neprazna familija celih divizorskih ideala Krulovog domena ima maksimalan element u odnosu na inkluziju.* □

Teorema 5.4.3. *Domen A je Krulov akko A je kompletno integralno zatvoren i zadovoljava uslov ACC na divizorskim idealima.*

Važi i više: Ako sa $\mathcal{P}(A)$ označimo skup ekstremalnih elemenata grupe $D(A)$, onda je $\mathcal{P}(A)$ baza $\mathbb{Z}$-modula $D(A)$. Pozitivni elementi grupe $D(A)$ su linearne kombinacije elemenata iz $\mathcal{P}(A)$ sa koeficijentima ≥ 0.

Dokaz. Ako je A Krulov on je kompletno integralno zatvoren prema 5.2.7, dok uslov ACC na divizorskim idealima važi prema 5.4.2. Obratno, neka je sada domen A kompletno integralno zatvoren i ispunjava uslov kidanja lanaca divizorskih ideala. $D(A)$ je tada mrežasto uredjena grupa prema 5.1.4 i 5.1.9. Ako divizor $\operatorname{div}\mathfrak{p}$ pridružen razlomljenom idealu $\mathfrak{p} \in I(A)$ shvatimo kao divizorski ideal, (iz klase $\operatorname{div}\mathfrak{p}$ odaberemo predstavnika $\widehat{\mathfrak{p}}$), onda uslov ACC na divizorskim idealima znači da svaki neprazan podskup iz $D(A)$ ima minimalan element. Sada je, prema 3.2.15 $D(A) \cong \mathbb{Z}^{(I)}$, $\mathcal{P}(A)$ generiše grupu $D(A)$ i pozitivni elementi su kombinacije elemenata iz $\mathcal{P}(A)$ sa koficijentima ≥ 0. Neka je $x \in k^*$ proizvoljan element, $\mathrm{div(x)} = \mathrm{div\,Ax}$. $\mathrm{div\,Ax} \in \mathrm{D(A)}$ pa su jednoznačno odredjeni koeficijenti $v_P(x) \in \mathbb{Z}$, takvi da je:

$$\mathrm{div(x)} = \sum_{\mathrm{P}\in\mathcal{P}(\mathrm{A})} \mathrm{v_P(x)P} \tag{11}$$

Svakom elementu $x \in k^*$, prema formuli (11), može se pridružiti familija celih brojeva $(v_P(x))_{P\in I}$ iz $\mathbb{Z}^{(I)}$, gde je $I = \mathcal{P}(A)$. Na taj način, ako definišemo $v_P(0) \overset{\text{def}}{=} \infty$, dolazimo do familije preslikavanja $v_P : k \mapsto \mathbb{Z}$, $P \in \mathcal{P}(A)$. Iz osobina glavnih divizora dobija se:

$$\mathrm{div(xy)} = \mathrm{div(x)} + \mathrm{div(y)} \;\Rightarrow\; \sum \mathrm{v_P(xy)P} = \sum(\mathrm{v_P(x)} + \mathrm{v_P(y)})\mathrm{P}$$

$$\mathrm{div(x+y)} \geq \inf\,(\mathrm{div(x)}, \mathrm{div(y)}) \;\Rightarrow\; \sum \mathrm{v_P(x+y)P} \geq \inf\left(\sum \mathrm{v_P(x)P}, \sum \mathrm{v_P(y)P}\right)$$

Prelaskom u grupu $\mathbb{Z}^{(I)}$ dobija se:

$$v_P(xy) = v_P(x) + v_P(y)\,,\; v_P(x+y) \geq \inf(v_P(x), v_P(y))$$

pa su za familiju preslikavanja (v_P) ispunjeni uslovi v_1, v_2. Na taj način familija $(v_P)_{P\in\mathcal{P}(A)}$, je familija diskretnih valuacija pridružena domenu A. Sam domen A je presek odgovarajućih valuacionih prstena, $A = \bigcap_{P\in\mathcal{P}(A)} A_{v_P}$, jer je:

$$x \in A \;\Leftrightarrow\; Ax \subseteq A \;\Leftrightarrow\; \mathrm{div(x)} \geq 0 \;\Leftrightarrow\; \sum_{\mathrm{P}\in\mathcal{P}(\mathrm{A})} \mathrm{v_P(x)P} \geq 0 \;\Leftrightarrow\; \mathrm{v_P(x)} \geq 0\,,\, \forall \mathrm{P} \in \mathcal{P}(\mathrm{A})$$

$$\Leftrightarrow\; x \in A_{v_P}\,,\, \forall P \in \mathcal{P}(A) \;\Leftrightarrow\; x \in \bigcap_{P\in\mathcal{P}(A)} A_{v_P}$$

Iz izomorfizma $D(A) \cong \mathbb{Z}^{(I)}$, na familiju $(v_P)_{P\in\mathcal{P}(A)}$ može se gledati kao na element grupe $\mathbb{Z}^{(\mathcal{P}(A))}$. Zato je $v_P(x) \neq 0$ samo za konačno mnogo elemenata $P \in \mathcal{P}(A)$. Ispunjeni su svi uslovi definicije 5.2.2 pa je domen A Krulov. $\square$

Definicija 5.4.4. *Valuacije odredjene formulom* (11) *su esencijalne valuacije Krulovog domena.*

Neka je $\mathfrak{u} \in I(A)$ proizvoljan razlomljen ideal i $\operatorname{div}\mathfrak{u} \in \mathrm{D(A)}$ odgovarajući divizor. Prema 5.4.3

$$\operatorname{div}\mathfrak{u} = \sum_{\mathrm{P}\in\mathcal{P}(\mathrm{A})} \mathrm{n_P}(\mathfrak{u})\mathrm{P} \tag{12}$$

S druge strane $\mathfrak{u} = \sum\limits_{x\in\mathfrak{u}} Ax$, pa je:

$$\operatorname{div}\mathfrak{u} = \operatorname{div}\sum_{\mathrm{x}\in\mathfrak{u}} \mathrm{Ax} = \inf_{\mathrm{x}\in\mathfrak{u}} (\operatorname{div}\mathrm{Ax}) = \inf_{\mathrm{x}\in\mathfrak{u}} \Big(\sum_{\mathrm{P}\in\mathcal{P}(\mathrm{A})} \mathrm{v_P(x)P} \Big) = \sum_{\mathrm{P}\in\mathcal{P}(\mathrm{A})} (\inf_{\mathrm{x}\in\mathfrak{u}} \mathrm{v_P(x)})\mathrm{P}$$

Iz poslednje jednakosti dobijamo koeficijente uz ekstremalne divizorske ideale $P \in \mathcal{P}(A)$ u jednakosti (12) ; $n_P(\mathfrak{u}) = \inf\limits_{x\in\mathfrak{u}} v_P(x)$, gde su v_P esencijalne valuacije. Ako se u klasi $\operatorname{div}\mathfrak{u}$ odabere divizorski ideal $\mathfrak{u}$ čiji je divizor dat formulom (12), onda: $x \in \mathfrak{u} \Leftrightarrow Ax \subseteq \mathfrak{u} \Leftrightarrow \widehat{Ax} \subseteq \widehat{\mathfrak{u}} \Leftrightarrow \operatorname{div}(\mathrm{x}) \geq \operatorname{div}\mathfrak{u} \Leftrightarrow \sum \mathrm{v_P(x)P} \geq \sum \mathrm{n_P}(\mathfrak{u})\mathrm{P} \Leftrightarrow \mathrm{v_P(x)} \geq \mathrm{n_P}(\mathfrak{u})\,, \forall \mathrm{P} \in \mathcal{P}(\mathrm{A})$. Na taj način divizoru (12) odgovara divizorski ideal:

$$\mathfrak{u} = \{\, x \in k \mid v_P(x) \geq n_P\,, \forall P \in \mathcal{P}(A)\} \tag{13}$$

gde su v_P esencijalne valuacije Krulovog domena A. Sledeća tvrdjenja u vezi sa divizorima Krulovih domena, kao i svi dokazi mogu se naći u [3] ili u [10].

Teorema 5.4.5. *Neka je P ekstremalni divizor Krulovog domena A i $\mathfrak{p}$ divizorski ideal koji mu odgovara. Tada je $\mathfrak{p}$ prost i valuacioni prsten A_{v_P} je lokalizacija $A_{\mathfrak{p}}$, odnosno $A_{\mathfrak{p}}$ je DVR.* □

Teorema 5.4.6. *Neka je A Krulov domen i $\mathfrak{p}$ ceo ideal u A. Tada je $\mathfrak{p}$ divizorski ideal koji odgovara ekstremalnom divizoru P akko je $\mathfrak{p}$ minimalan prost ideal u A.* □

Primedba. Prema ovoj teoremi može se uspostaviti bijekcija medju minimalnim prostim idealima Krulovog domena i maksimalnim[3] divizorskim idealima. To je i razlog zašto ove ideale identifikujemo i koristimo istu oznaku $\mathcal{P}(A)$. Grupa $D(A)$ Krulovog domena A generisana je prema 5.4.3 ekstremalnim divizorima. Ravnopravno je zato reći da je ona generisana maksimalnim divizorskim idealima, (ako iz svake klase za predstavnika odaberemo divizorski ideal), odnosno, prema poslednjoj teoremi, minimalnim prostim idealima u A. U Krulovim domenima od interesa su dakle samo minimalni prosti ideali (prema 5.4.7 divizori ostalih prostih ideala jednaki nuli u $D(A)$). Dokazi narednih teorema mogu se naći u [3, 10].

Teorema 5.4.7. *U Krulovom domenu svaki pravi prost ideal $\mathfrak{q}$ sadrži prost ideal $\mathfrak{p}$, $\operatorname{ht}(\mathfrak{p}) = 1$. Ako je $\operatorname{ht}(\mathfrak{q}) > 1$ onda je $\operatorname{div}\mathfrak{q} = 0$ i $A : \mathfrak{q} = A$.* □

Teorema 5.4.8. *Neka je A Krulov domen, v valuacija polja $k = Frac(A)$ takva da je $v(a) \geq 0\,,\ a \in A$ i $\mathfrak{p} = \{\, x \in A \mid v(x) > 0\,\}$. Ako je $\operatorname{ht}(\mathfrak{p}) = 1$ onda je v esencijalna valuacija.* □

[3] U odnosu na inkluziju.

Teorema 5.4.9 (teorema o aproksimaciji)**.** *Neka su $v_1, \ldots, v_k$ medjusobno različite esencijalne valuacije Krulovog domena i $n_1, \ldots, n_k$ celi brojevi. Postoji $x \in k$ takav da je $v_i(x) = n_i$, $i = 1, \ldots, k$ i $v(x) \geq 0$ za svaku esencijalnu valuaciju v različitu od $v_1, \ldots, v_k$.* □

Lema 5.4.10. *Ako su $\mathfrak{p}, \mathfrak{q}$ i $\mathfrak{r}$ divizorski ideali Krulovog domena i $\mathfrak{p} \subseteq \mathfrak{q}$ onda postoji $x \in k$ takav da je $\mathfrak{p} = \mathfrak{q} \cap \mathfrak{r}x$.* □

Neka je sada $\mathfrak{p} \in I(A)$ divizorski ideal. Tada postoji $d \neq 0$ tako da je $\mathfrak{p} \subseteq Ad$. Ad je glavni ideal pa samim tim i divizorski. Ako sa $\mathfrak{q}$ i $\mathfrak{r}$ označimo divizorske ideale Ad i A, onda se primenom prethodne leme dobija da postoji $x \in k$ takav da je $\mathfrak{p} = Ad \cap Ax$, pa je $\mathfrak{p}$ presek glavnih ideala. Obratno naravno važi uvek prema definiciji divizorskih ideala pa imamo sledeću karakterizaciju divizorskih ideala u Krulovim domenima.

Teorema 5.4.11. *Razlomljen ideal $\mathfrak{p} \in I(A)$ Krulovog domena A je divizorski akko je presek dva glavna razlomljena ideala.* □

Teorema 5.4.12. *Neka je A Neterin integralno zatvoren domen. Tada važi:*
(1) *Ako je P ekstremalni divizor i $\mathfrak{p}$ odgovarajući divizorski ideal onda je n-ti simbolički stepen $\mathfrak{p}^{(n)} = \mathfrak{p}^n A_{\mathfrak{p}} \cap A$ divizorski ideal i $\mathfrak{p}^{(n)} = \{\, x \in A \mid v_{\mathfrak{p}}(x) \geq n \,\}$.*
(2) *Ako je $\mathfrak{u}$ ceo divizorski ideal,* $\operatorname{div}\mathfrak{u} = \sum_{i=1}^{k} n_i P_i$ *njegov divizor i $\mathfrak{p}_i$ divizorski ideali koji odgovaraju ekstremalnim divizorima P_i, onda je $\mathfrak{u} = \bigcap_{i=1}^{k} \mathfrak{p}_i^{(n_i)}$ jedinstveno primarno razlaganje ideala $\mathfrak{u}$ i ideali $\mathfrak{p}_i$ su izolovani.* □

Neka je A Krulov domen. Prema prethodnim tvrdjenjima familiju ekstremalnih divizora, $T = \mathcal{P}(A)$, koji generišu uredjenu grupu $D(A)$, možemo identifikovati sa familijom minimalnih prostih ideala u A tako što ekstremalnom divizoru $P \in D(A)$ pridružimo divizorski ideal $\mathfrak{p}$. Neka je $(v_{\mathfrak{p}})_{\mathfrak{p} \in T}$ familija esencijalnih valuacija odredjenih formulom (11) i $\mathfrak{u} \in I(A)$ proizvoljan razlomljen ideal. Prema prethodnom važi:

$$\operatorname{div}\mathfrak{u} = \sum_{\mathfrak{p} \in \mathcal{P}(A)} v_{\mathfrak{p}}(\mathfrak{u}) \operatorname{div}\mathfrak{p} \quad , \quad v_{\mathfrak{p}}(\mathfrak{u}) = \inf_{x \in \mathfrak{u}} v_{\mathfrak{p}}(x) \tag{14}$$

Sada se može definisati preslikavanje:

$$T \overset{\operatorname{div}\mathfrak{u}}{\longmapsto} \mathbb{Z} \quad , \quad \operatorname{div}\mathfrak{u}(\mathfrak{p}) \overset{\text{def}}{=} v_{\mathfrak{p}}(\mathfrak{u}) \tag{15}$$

Kako je $v_{\mathfrak{p}}(\mathfrak{u}) \neq 0$ samo za konačno mnogo $\mathfrak{p} \in T$, svakom razlomljenom idealu $\mathfrak{u} \in I(A)$ može se pridružiti familija $(v_{\mathfrak{p}}(\mathfrak{u}))_{\mathfrak{p} \in T}$ iz $\mathbb{Z}^{(T)}$. Na taj način dolazi se do preslikavanja:

$$I(A) \overset{\operatorname{div}}{\longmapsto} \mathbb{Z}^{(T)} \quad , \quad \operatorname{div}\mathfrak{u} \overset{\text{def}}{=} (v_{\mathfrak{p}}(\mathfrak{u}))_{\mathfrak{p} \in T} \tag{16}$$

Kako za $\mathfrak{a}, \mathfrak{b} \in I(A)$ važi: $\operatorname{div}\mathfrak{ab} = \operatorname{div}\mathfrak{a} + \operatorname{div}\mathfrak{b}$, preslikavanje div je homomorfizam sa sledećim osobinama:

(1) $\mathrm{div}\,(\mathrm{A} : \mathfrak{a}) = -\mathrm{div}\,\mathfrak{a}$
(2) $\mathrm{div}\,(\mathrm{A} : (\mathrm{A} : \mathfrak{a})) = \mathrm{div}\,\mathfrak{a}$
(3) $\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow \mathrm{div}\,\mathfrak{a} \geq \mathrm{div}\,\mathfrak{b}$
(4) $\mathrm{div}\,(\mathfrak{a} + \mathfrak{b}) = \inf\{\mathrm{div}\,\mathfrak{a}, \mathrm{div}\,\mathfrak{b}\}$
(5) $\mathrm{div}\,(\widehat{\mathfrak{a}} \cap \widehat{\mathfrak{b}}) = \sup\{\mathrm{div}\,\mathfrak{a}, \mathrm{div}\,\mathfrak{b}\}$
(6) Restrikcija na divizorske ideale[4] $D(A) \overset{\mathrm{div}}{\longmapsto} \mathbb{Z}^{(T)}$ je izomorfizam koji čuva poredak.

Iz poslednjeg izomorfizma, rad sa divizorima u Krulovom domenu A možemo zameniti udobnijim radom sa uredjenom grupom $\mathbb{Z}^{(T)}$. Elementi grupe $D(A)$ sada su formalne sume $\sum_{\mathfrak{p}\in T} n_{\mathfrak{p}}\mathfrak{p}$, gde je samo konačno mnogo $n_{\mathfrak{p}} \in \mathbb{Z}$ različito od nule, dok je sabiranje formalnih suma dato sa:

$$\sum_{\mathfrak{p}\in T} n_{\mathfrak{p}}\mathfrak{p} + \sum_{\mathfrak{p}\in T} m_{\mathfrak{p}}\mathfrak{p} = \sum_{\mathfrak{p}\in T} (n_{\mathfrak{p}} + m_{\mathfrak{p}})\mathfrak{p} \tag{17}$$

Za $x \in k^*$ sada je prema (11): $\mathrm{div(x)} = \sum \mathrm{v}_{\mathfrak{p}}(\mathrm{x})\mathfrak{p}$ gde su $v_{\mathfrak{p}}$ esencijalne valuacije. Kako je za $x, y \in k^*$ ispunjeno $\mathrm{div(xy)} = \mathrm{div(x)} + \mathrm{div(y)}$, preslikavanje $k^* \overset{\mathrm{div}}{\longmapsto} D(A)$ je homomorfizam. Slika $\mathrm{Im}(k^*)$ pri ovom homomorfizmu je podgrupa $F(A)$ glavnih divizora Krulovog domena. Ova razmatranja daju novu mogućnost za definisanje grupe divizor klasa Krulovog domena; ako sa $D(A)$ označimo skup svih formalnih suma

$$D(A) = \{ \sum_{\mathfrak{p}\in T} n_{\mathfrak{p}}\mathfrak{p} \mid n_{\mathfrak{p}} \neq 0 \text{ samo za konačno mnogo } \mathfrak{p} \in T \}$$

i sabiranje definišemo sa (17), onda je grupa divizor klasa $Cl(A) \overset{\mathrm{def}}{=} D(A)/F(A)$, gde je $F(A) = \mathrm{Im}(k^*)$.

5.5 Grupa divizor klasa Krulovog domena

Neka su A i B Krulovi domeni, $A \subseteq B$ i $\mathcal{P}(A), \mathcal{P}(B)$ minimalni prosti ideali ovih domena. Neka je $\mathfrak{q} \in \mathcal{P}(B)$ takav da je $\mathfrak{q} \cap A = \mathfrak{p} \in \mathcal{P}(A)$. Kako je $B_{\mathfrak{q}}$ DVR njegovi ideali su oblika $\mathfrak{q}^n B_{\mathfrak{q}}$ za neko n. Posebno je i $(\mathfrak{q} \cap A)B_{\mathfrak{q}} = \mathfrak{p}B_{\mathfrak{q}}$ ovog oblika tj. postoji jednoznačno odredjen broj e takav da je $\mathfrak{p}B_{\mathfrak{q}} = \mathfrak{q}^e B_{\mathfrak{q}}$.

Definicija 5.5.1. *Broj e odredjen na ovaj način zovemo indeksom grananja $\mathfrak{p}$ u $\mathfrak{q}$, u oznaci $e = e(\mathfrak{q}/\mathfrak{p})$.*

Za Krulove domene A i B, $A \subseteq B$ od posebnog značaja su uslovi pod kojima će kontrakcija minimalnog prostog ideala iz B biti minimalan prost ideal u A. Zbog toga se ističe uslov NBU[5]:

(NBU) $$\mathfrak{q} \in \mathcal{P}(B) \Rightarrow \mathrm{ht}(\mathfrak{q} \cap A) \leq 1$$

[4]Ovde se divizor P identifikuje sa svojim divizorskim idealom $\mathfrak{p}$.
[5]No Blowing Up

Ako je ovaj uslov ispunjen može se definisati homomorfizam grupa $D(A)$ i $D(B)$ koji čuva uredjenje. Važi sledeća teorema [3]:

Teorema 5.5.2. *Neka Krulovi domeni A i B, $A \subseteq B$ zadovoljavaju uslov* (NBU). *Tada važi:*
(1) *Skup $R^{\mathfrak{p}} = \{\, \mathfrak{q} \in \mathcal{P}(B) \mid \mathfrak{q} \cap A = \mathfrak{p} \,\}$ je konačan za svako $\mathfrak{p} \in \mathcal{P}(A)$.*
(2) *Preslikavanjem $i : \mathcal{P}(A) \to D(B)$ definisanim sa:*

$$i(\,\mathfrak{p}\,) = \sum_{\mathfrak{q} \,\in\, R^{\mathfrak{p}}} e(\mathfrak{q}/\mathfrak{p})\,\mathfrak{q} \tag{18}$$

odredjen je rastući homomorfizam grupe $D(A)$ u grupu $D(B)$ koji čuva glavne divizore i supremum. Ako je $x \in Frac(A)$, $x \neq 0$ i $U, V \in D(A)$ onda je:

$$i\,(\mathrm{div_A} x) = \mathrm{div_B} x \tag{3}$$

$$i\,(\sup(\,U, V\,)) = \sup(\,i\,(U), i\,(V)\,)\quad \square \tag{4}$$

Homomorfizam $i : D(A) \to D(B)$ indukuje homomorfizam:

$$\bar{\imath} : Cl(A) \to Cl(B) \tag{19}$$

za koji se takodje koristi oznaka i. Sa stanovišta faktorijalnosti posebno je bitno kada su ove grupe izomorfne, tj. kada je homomorfizam i 1-1 i na. Injektivnost i surjektivnost ovog homomorfizma zavisiće pre svega od vrste raširenja.

Definicija 5.5.3. *Neka je A domen, $k = Frac(A)$ i $A \subseteq B \subseteq k$ gde je B prsten sadržan u k. B je ravan A-modul (ravna A-algebra) ako za svaki maksimalan ideal $\mathfrak{m} \lhd B$ važi $B_{\mathfrak{m}} = A_{\mathfrak{m} \cap A}$.*

Ravno raširenje $B \supseteq A$ ima sledeću osobinu: ako su $\mathfrak{p}, \mathfrak{q}$ proizvoljni ideali u A onda je

$$(\mathfrak{p} \cap \mathfrak{q})B = \mathfrak{p}B \cap \mathfrak{q}B \tag{20}$$

Važan primer ravnog raširenja domena A je lokalizacija A_S, ako A_S posmatramo kao A-modul. Osim ravnih, od interesa su cela raširenja, kao i podpreseci. Može se pokazati da važi sledeće tvrdjenje ([10]), koje kaže da je u tim slučajevima ispunjen uslov NBU.

Tvrdjenje 5.5.4. *Neka je A domen i $B \supseteq A$ A-algebra. Uslov* NBU *ispunjen je u sledećim slučajevima:*
(*a*) *B je ravan A-modul.*
(*b*) *B je podpresek.*
(*c*) *B je celo nad A.* $\square$

Za celo raširenje $B \supseteq A$, minimalan prost ideal $\mathfrak{p} \in \mathcal{P}(A)$ je kontrakcija minimalnog prostog ideala $\overline{\mathfrak{p}} \in \mathcal{P}(B)$. Kako za par (A, B) važi uslov INC, ideal $\overline{\mathfrak{p}}$ je jedinstven ideal sa tom osobinom tj. $R^{\mathfrak{p}} = \{\, \overline{\mathfrak{p}} \,\}$. Sada je prema (18)

$$i(\,\mathfrak{p}\,) = e(\overline{\mathfrak{p}}/\mathfrak{p})\,\overline{\mathfrak{p}}$$

Odavde je $\ker i = 0$, pa je homomorfizam i u slučaju celih raširenja injektivan. Za ravna raširenja važi sledeća lema.

Lema 5.5.5. *Neka su A, B Krulovi domeni i neka je B ravna A-algebra. Tada su ekstenzije divizorskih ideala divizorski ideali tj. ako je $\mathfrak{u}$ divizorski ideal u A onda je $\mathfrak{u}B$ divizorski ideal u B i njegov divizor je slika divizora $\mathfrak{u}$:*

$$\mathrm{div_B}(\mathfrak{u}\mathrm{B}) = \mathrm{i}(\mathrm{div_A}\,\mathfrak{u}) \tag{21}$$

Dokaz. Prema 5.4.11 $\mathfrak{u} = Ax \cap Ay$ za neke $x, y \in k^*$. Ideal $\mathfrak{u}$ može se predstaviti i u obliku $\mathfrak{u} = d^{-1}(Aa \cap Ab)$, gde su $a, b, d \in A \setminus \{0\}$. Kako je B ravan A-modul, prema (20) je $B\mathfrak{u} = d^{-1}(Ba \cap Bb)$. Iz poslednje jednakosti $B\mathfrak{u}$ je divizorski ideal kao presek glavnih ideala Krulovog domena B. Ispunjen je uslov NBU pa je i homomorfizam koji, prema 5.5.2, čuva glavne divizore i supremum. Koristeći ove osobine dobija se:
$\mathrm{div_B}(\mathfrak{u}\mathrm{B}) = \mathrm{div}(\mathrm{B}a \cap \mathrm{B}b)d^{-1} = \sup(\mathrm{div_B}\,a, \mathrm{div_B}\,b) - \mathrm{div_B}\,d$
$= \sup(i(\mathrm{div_A}\,a), i(\mathrm{div_A}\,b)) - i(\mathrm{div_A}\,d) = i(\sup(\mathrm{div_A}\,a, \mathrm{div_A}\,b)) - i(\mathrm{div_A}\,d)$
$= i(\mathrm{div_A}(\mathrm{A}a \cap \mathrm{A}b)) - i(\mathrm{div_A}\,d) = i(\mathrm{div_A}(d^{-1}(\mathrm{A}a \cap \mathrm{A}b))) = i(\mathrm{div_A}\mathfrak{u})$ $\square$

Neka je sada A Krulov domen, $S \subseteq A$ multiplikativan podskup ($0 \notin S$), $\mathcal{P}(A)$ skup minimalnih prostih ideala u A i $A = \bigcap_{\mathfrak{p}_i \in \mathcal{P}(A)} A_{\mathfrak{p}_i}$. Kako za $\mathfrak{q} \in \mathcal{P}(A)$ važi $A_S \subseteq A_{\mathfrak{q}} \Leftrightarrow \mathfrak{q} \cap S = \emptyset$, prema teoremi 5.3.1 važiće $A_S = \bigcap_{\mathfrak{q}_i \in T} A_{\mathfrak{q}_i}$ gde je:

$$T = \{\, \mathfrak{q}_i \in \mathcal{P}(A) \mid A_S \subseteq A_{\mathfrak{q}_i} \,\} = \{\, \mathfrak{q}_i \in \mathcal{P}(A) \mid \mathfrak{q}_i \cap S = \emptyset \,\}$$

$D(A)$ je prema 5.4.3 slobodna Abelova grupa (izomorfna sa $\mathbb{Z}^{\mathcal{P}(A)}$) generisana ekstremalnim divizorima:

$$D(A) = \langle\, \mathrm{div}\,\mathfrak{p}_\mathrm{i} \mid \mathfrak{p}_\mathrm{i} \in \mathcal{P}(\mathrm{A}) \,\rangle \tag{23}$$

$D(A_S)$ je takodje slobodna Abelova grupa generisana sa:

$$D(A_S) = \langle\, \mathrm{div}\,\mathfrak{p}_\mathrm{i} \mid \mathfrak{p}_\mathrm{i} \in \mathcal{P}(\mathrm{A})\,,\ \mathfrak{p}_\mathrm{i} \cap \mathrm{S} = \emptyset \,\rangle \tag{24}$$

Ako sa G označimo grupu generisanu skupom $\{\, \mathrm{div}\,\mathfrak{p}_\mathrm{i} \mid \mathfrak{p}_\mathrm{i} \in \mathcal{P}(\mathrm{A})\,,\ \mathfrak{p}_\mathrm{i} \cap \mathrm{S} \neq \emptyset \,\}$ dobija se:

$$D(A) = D(A_S) \oplus G \tag{25}$$

Odavde je $D(A_S) \cong D(A)/G$, pa je za homomorfizam $i : D(A) \to D(A_S)$, jezgro $\ker i \cong G$. Homomorfizam i u ovom slučaju očigledno je surjektivan, pa je surjektivan i odgovarajući homomorfizam $\bar{\imath} : Cl(A) \to Cl(A_S)$, definisan sa:

$$\bar{\imath}\,(\mathrm{div_A}\mathfrak{u} + \mathrm{F(A)}) \stackrel{\mathrm{def}}{=} i(\mathrm{div_A}\mathfrak{u}) + \mathrm{F(A_S)} \tag{26}$$

Teorema 5.5.6. *Homomorfizam $\bar{\imath} : Cl(A) \to Cl(A_S)$ je surjektivan i uz prethodno uvedene oznake važi:*

$$\ker(\bar{\imath}) = (G + F(A))/F(A) = G/(G \cap F(A)) \tag{27}$$

Dokaz. Kako je lokalizacija A_S ravan A-modul, za $\mathfrak{p} \in \mathcal{P}(A)\,,\ \mathfrak{p} \cap S = \emptyset$, važi:

(i) $$\mathrm{div_{A_S}}(\,\mathfrak{p}\mathrm{A_S}) = i(\mathrm{div_A}\mathfrak{p})$$

Dok za $x \in A$, $s \in S$ važi: $\mathrm{div}_{\mathrm{A_S}}(x/s) = i(\mathrm{div}_{\mathrm{A}} x)$. Proizvoljan element $\mathrm{div}\,\mathfrak{u} + \mathrm{F(A)} \in \mathrm{Cl(A)}$, pripada jezgru $\ker(\bar{\imath})$ akko je $i(\mathrm{div}\,\mathfrak{u} + \mathrm{F(A)}) \in \mathrm{F(A_S)}$ tj.

$$i(\mathrm{div}\,\mathfrak{u}) + \mathrm{F(A_S)} = \mathrm{div}_{\mathrm{A_S}}(x/s) = i(\mathrm{div}_{\mathrm{A}} x)$$

Odavde je $i(\mathrm{div}\,\mathfrak{u} - \mathrm{div}_{\mathrm{A}} x) = 0$ u $D(A_S)$, pa je $\mathrm{div}\,\mathfrak{u} - \mathrm{div}_{\mathrm{A}} x \in \ker(i) = \mathrm{G}$. To znači da $\mathrm{div}\,\mathfrak{u} \in \mathrm{G} + \mathrm{F(A)}$, odakle je $\ker(\bar{\imath}) = (G + F(A))/F(A)$. Druga jednakost sledi iz teoreme o izomorfizmu. □

Teorema 5.5.7. *Neka je, uz prethodno uvedene oznake, S generisan familijom prostih elemenata. Tada je $Cl(A) \cong Cl(A_S)$.*

Dokaz. Neka je $\mathfrak{p} \in \mathcal{P}(A)$, $\mathfrak{p} \cap S \neq \emptyset$. Tada postoji $s = p_1^{\alpha_1} \dots p_k^{\alpha_k} \in \mathfrak{p} \cap S$. Ideal $\mathfrak{p}$ je prost, pa se može pretpostaviti da npr. $p_1 \in \mathfrak{p}$, odakle je $Ap_1 \subseteq \mathfrak{p}$. Kako je $\mathrm{ht}(\mathfrak{p}) = 1$, dobija se $\mathfrak{p} = Ap_1$ tj. $\mathfrak{p}$ je glavni ideal pa je $G \subseteq F(A)$. Prema prethodnom tvrdjenju, jezgro $\ker(\bar{\imath})$ je trivijalno pa je $\bar{\imath}$ injektivno. Kako je $\bar{\imath}$ i surjektivno, grupe $Cl(A)$ i $Cl(A_S)$ su izomorfne. □
Osobine grupe $Cl(A)$ i homomorfizma i opširno su opisane u [10]. Neke od tih osobina date su sledećim tvrdjenjima.

Teorema 5.5.8 ([10])**.** *Za Krulov domen A sledeća tvrdjenja su ekvivalentna:*
(1) *$Cl(A)$ je torziona grupa.*
(2) *Svaki podpresek domena A je lokalizacija.*
(3) $(\forall f, g \in A)$ $(\exists n = n(f,g))$ *tako da je $Af^n \cap Ag^n$ glavni ideal.*
(4) $(\forall \mathfrak{p} \in \mathcal{P}(A))$ $\mathfrak{p}^{(n)}$ *je glavni za neko $n > 0$.* □

Teorema 5.5.9 ([10])**.** *Ako je A Krulov domen onda je $Cl(A) \to Cl(A[X])$ izomorfizam.* □

Teorema 5.5.10 ([10])**.** *Ako je A Neterin integralno zatvoren domen onda je $Cl(A) \to Cl(A[[X]])$ monomorfizam.* □

5.6 Grupa Cl(A) i faktorizacija

Značaj grupe divizor klasa $Cl(A)$ Krulovog domena A pri ispitivanju faktorijalnosti ogleda se u tome što se njenim računanjem može, ne samo utvrditi da li je A UFD, već se u suprotnom na neki način može i "izmeriti njegova nefaktorijalnost". Pri definisanju faktorijalnog domena A kod nekih autora, ([3],[10]) koristi se grupa divizor klasa; faktorijalan domen A definiše se kao Krulov domen sa trivijalnom grupom divizor klasa. Razlog tome je sledeća teorema.

Teorema 5.6.1. *Neka je A domen, $k = Frac(A)$ i $\mathcal{P}^* = \{Ax \mid x \in k^*\}$. Tada su sledeći uslovi ekvivalentni:*
(1) *A je Krulov domen i $Cl(A) = 0$.*
(2) *$\mathcal{P}^* \cong \mathbb{Z}^{(I)}$ i izomorfizam čuva uredjenje.*
(3) *A je Krulov domen i svaki minimalan prost ideal $\mathfrak{p} \in \mathcal{P}(A)$ je glavni.* □

Dokaz. (1) $\Rightarrow$ (2) : Kako je domen A Krulov prema 5.4.3 je $D(A) \cong \mathbb{Z}^{(I)}$, gde je $I = \mathcal{P}(A)$. S druge strane, $Cl(A) = 0$ pa je $D(A) \cong F(A) = \mathcal{P}^*$ odakle sledi tvrdjenje.

(2) $\Rightarrow$ (3) : Neka je $\mathbb{Z}^{(I)} \cong \mathcal{P}^*$ i $Ax \overset{f}{\mapsto} (v_i(x))_{i\in I}$ odgovarajući izomorfizam koji glavnom idealu Ax , $x \in k^*$ pridružuje element $(v_i(x))_{i\in I}$ iz $\mathbb{Z}^{(I)}$. Ako fiksiramo i preslikavanje $x \mapsto v_i(x)$ je jedna valuacija polja k; f je homomorfizam pa je $f(Ax\, Ay) = f(Axy) = f(Ax) + f(Ay)$, odnosno:

$$(v_i(xy))_{i\in I} = (v_i(x) + v_i(y))_{i\in I}$$

Odavde se neposredno dobija osobina $(v_1) : v_i(xy) = v_i(x) + v_i(y)$. Iz mrežaste uredjenosti grupe $\mathbb{Z}^{(I)}$ i izomorfizma $\mathcal{P}^* \cong \mathbb{Z}^{(I)}$, za svako $x, y \in k^*$ postoji $\inf(Ax, Ay) = Az$, gde je $z = \operatorname{nzd}(x, y)$. Odavde je $\inf(v_i(x), v_i(y)) = v_i(z)$. S druge strane, $Ax, Ay \geq Az \Rightarrow Ax, Ay \subseteq Az \Rightarrow A(x + y) \subseteq Ax + Ay \subseteq Az$. To znači da je $A(x + y) \geq Az$, pa je $v_i(x + y) \geq v_i(z) = \inf(v_i(x), v_i(y))$ tj. ispunjena je i osobina $(v_2) : v_i(x + y) \geq \inf(v_i(x), v_i(y))$. Za fiksirano i, preslikavanje $v_i : k^* \to \mathbb{Z}$ je dakle jedna diskretna valuacija. Na taj način, posredstvom izomorfizma f, dobijena je familija $(v_i)_{i\in I}$, diskretnih valuacija polja $k = Frac(A)$ sa odgovarajućim diskretnim valuacionim prstenima,

$$A_{v_i} = \{\, x \in k^* \mid v_i(x) \geq 0 \,\}.$$

Ako je sada $x \in A$, onda je $Ax \subseteq A$ tj. $Ax \geq A$ odakle je $v_i(x) \geq 0$, $\forall i \in I$. To znači da je $x \in A_{v_i}$, $\forall i$ tj. $x \in \bigcap_{i\in I} A_{v_i}$. Ovim je dokazana inkluzija $A \subseteq \bigcap_{i\in I} A_{v_i}$. Ovde važi i obratna inkluzija, jer za $x \in \bigcap A_{v_i}$ važi $v_i(x) \geq 0$, $\forall i$, odakle je $(v_i(x))_{i\in I} \geq 0$. S obzirom da f čuva uredjenje, prelaskom u grupu $\mathcal{P}^*$ dobija se $Ax \geq A$. Odavde je $Ax \subseteq A$ pa $x \in A$, odnosno $\bigcap_{i\in I} A_{v_i} \subseteq A$. Odavde je:

$$\bigcap_{i\in I} A_{v_i} = A$$

Ovaj presek je i lokalno konačan, jer $(v_i(x))_{i\in I} \in \mathbb{Z}^{(I)}$, pa je $v_i(x) \neq 0$ samo za konačno mnogo $i \in I$. Ispunjeni su svi uslovi definicije 5.2.2 pa je domen A Krulov. Neka je $\mathfrak{q} \in \mathcal{P}(A)$ proizvoljan minimalan prost ideal. Tada u $\mathfrak{q}$ postoji neinvertibilan element $a \in A$, $a \neq 0$. Grupa $\mathbb{Z}^{(I)}$, odnosno $\mathcal{P}^*$, generisana je ekstremalnim elementima, pa je i a proizvod ekstremalnih elemenata. Medjutim $a \in \mathfrak{q}$ i $\mathfrak{q}$ je prost, pa bar jedan od ekstremalnih, npr. $p_\alpha \in \mathfrak{q}$. Kako su ekstremalni elementi u $\mathbb{Z}^{(I)}$, odnosno $\mathcal{P}^*$, prosti, to $\mathfrak{q}$ sadrži prost ideal Ap_α. Sada se iz $\mathfrak{q} \supseteq A_{p_\alpha}$ i $\operatorname{ht}(\mathfrak{q}) = 1$ dobija $\mathfrak{q} = Ap_\alpha$, pa je svaki minimalan prost ideal glavni.

(3) $\Rightarrow$ (1) : Neka je sada ispunjen uslov (3). Grupa $D(A)$ generisana je tada glavnim divizorima, pa za proizvoljan divizor $\operatorname{div}\mathfrak{u} \in \mathrm{D(A)}$ važi:

$$\operatorname{div}\mathfrak{u} = n_1 \operatorname{div}\mathfrak{p}_1 + \cdots + n_k \operatorname{div}\mathfrak{p}_k \quad \mathfrak{p}_\mathrm{i} \in \mathcal{P}(\mathrm{A}) \,,\, \mathfrak{p}_\mathrm{i} = Ap_i$$

tj. $\operatorname{div}\mathfrak{u} = \operatorname{div}(Ap_1)^{n_1} + \cdots + \operatorname{div}(Ap_k)^{n_k} = \operatorname{div}(Ap_1^{n_1} \dots p_k^{n_k}) = \operatorname{div}(Ax)$, gde je $x = p_1^{n_1} \dots p_k^{n_k}$. Odavde je $\operatorname{div}\mathfrak{u} \in \mathrm{F(A)}$ glavni divizor. Kako to važi za

proizvoljan divizor, dobija se da je $D(A) = F(A)$ tj. $Cl(A) = 0$. $\square$

Prema 3.2.16 domen A je UFD akko je $\mathcal{P}^* \cong \mathbb{Z}^{(I)}$. Sada se prema poslednjoj teoremi može dati nova definicija faktorijalnog domena.

Definicija 5.6.2. *A je domen sa jednoznačnom faktorizacijom ako je Krulov i $Cl(A) = 0$.*

Posledica 5.6.3 (Nagatina teorema)**.**

Dokaz. Pod pretpostavkama Nagatine teoreme, prema teoremi 5.5.7 ispunjeno je $Cl(A) \cong Cl(A_S)$. Prema poslednjoj definiciji to znači da je A UFD akko je A_S UFD. $\square$

Posledica 5.6.4. *Krulov domen A je UFD akko je $A[X]$ UFD.*

Dokaz. Prema 5.3.2 $A[X]$ je Krulov domen, dok je prema 5.5.9 $Cl(A) \cong Cl(A[X])$, odakle sledi tvrdjenje. $\square$

Tvrdjenje 5.6.5 ([3])**.**
(i) Neka je A domen i $a, b \in A$ takvi da je $Aa \cap Ab = Aab$. Tada je $(aX + b)$ prost ideal prstena polinoma $A[X]$.
(ii) Neka je sada domen A Krulov i $a, b \in A$ elementi za koje su Aa i $Aa + Ab$ različiti prosti ideali. Tada je $A[X]/(aX + b)$ Krulov domen i

$$Cl(A[X]/(aX + b)) \cong Cl(A)$$

Dokaz. (i) Neka je $k = Frac(A)$. Označimo sa φ homomorfizam $A[X] \mapsto k$ definisan sa $\varphi(f) = f(-b/a)$. Ako $f \in (aX+b)$, onda je očigledno $f(-b/a) = 0$, pa $f \in \mathrm{Ker}\,(\varphi)$. Odavde se dobija inkluzija $(aX + b) \subseteq \mathrm{Ker}\,(\varphi)$. Neka je sada $f(X) = a_0 + a_1X + \cdots + a_nX^n$ polinom koji pripada jezgru. Tada je

$$f(-b/a) = a_0 + a_1(-b/a) + \cdots + a_n(-b/a)^n = 0$$

$$0 = a^n f(-b/a) = a_0a^n - a_1a^{n-1}b + \cdots + (-1)^n a_n b^n$$

$$a^n f(X) - a^n f(-b/a) = \cdots = (aX + b)\,(b_0 + b_1X + \cdots + b_{n-1}X^{n-1})$$

S obzirom da je $a^n f(-b/a) = 0$, poslednju jednakost možemo pisati u obliku

$$a^n f(X) = (aX + b)g(X)\ ,$$

gde je $g(X) = b_0 + b_1X + \cdots + b_{n-1}X^{n-1}$. U razvijenom obliku imamo

$$a_0a^n + a_1a^nX + \cdots + a_na^nX^n = bb_0 + (bb_1 + ab_0)X + \cdots + ab_{n-1}X^n$$

Prema uslovu $Aa \cap Ab = Aab$, elementi a i b su koprosti, pa iz $a^n a_0 = bb_0$ imamo da je $bb_0 \in Aa^n \cap Ab = Aa^n b$, odakle $a^n \mid b_0$. Slično se iz uslova $a^n a_1 = bb_1 + b_0 a$ dobija da $a^n \mid b_1$. Nastavljajući ovaj postupak vidimo da a^n deli sve koeficijente polinoma $g(X)$, odakle $aX + b \mid f(X)$, tj. $f \in (aX + b)$. Na ovaj način dobija se i obratna inkluzija $\mathrm{Ker}\,(\varphi) \subseteq (aX + b)$, pa je $\mathrm{Ker}\,(\varphi) = (aX + b)$. Posebno je

onda i $A[X]/(aX+b) \cong Im(\varphi) = A[b/a]$, odakle sledi traženo tvrdjenje.

(ii) Pokažimo najpre da su ispunjene pretpostavke prvog dela tvrdjenja. Neka je $f \in Aa \cap Ab$, tj.

$$f = ax = by \quad , \text{ za neke } \quad x, y \in A$$

S obzirom da je a prost element kao i da $a \nmid b$, jer bi u suprotnom došli do kontradikcije $Aa + Ab = Aa$, iz $a \mid by$ dobijamo da $a \mid y$ tj. $y = az$, za neko $z \in A$. Odavde je $f = baz \in Aab$, pa je $Aa \cap Ab \subseteq Aab$. Kako obratna inkluzija važi uvek, ispunjene su pretpostavke iz (i) pa je $(aX+b)$ prost ideal u $A[X]$ i važi:

$$A[X]/(aX+b) \cong A[b/a] = B$$

Dalje pokazujemo da prost element $a \in A$ prelaskom u prsten B čuva ovu osobinu. Ovo važi jer je:

$$B/Ba = A[X]/(aX+b)/aA[X]/(aX+b) = A[X]/aA[X] = (A/aA)[X]$$

A/aA je domen pa je takav i $(A/aA)[X]$, odnosno B/Ba. Odavde je Ba prost ideal prstena B tj. element a je prost i u B. Sada uzimamo multiplikativan poskup $S = \{1, a, a^2, \dots\}$ generisan prostim elementom a i odgovarajuće lokalizacije $A_S = A[a^{-1}]$ i $B_S = B[a^{-1}]$. Iz $A \subseteq B$ biće i $A[a^{-1}] \subseteq B[a^{-1}]$. S druge strane jasno je da je $B[a^{-1}] = A[b/a][a^{-1}] \subseteq A[a^{-1}]$, pa su lokalizacije ovih prstena iste $A[a^{-1}] = B[a^{-1}]$. Sada je $B_S = B[a^{-1}] = A[a^{-1}]$ Krulov kao lokalizacija Krulovog domena A. Multiplikativan podskup $S \subseteq B$ generisan je prostim elementom a pa je prema primedbi teoreme 5.3.1 B Krulov domen. Dalje, uzastopna primena Nagatine teoreme daje:

$$Cl(A) = Cl(A[a^{-1}]) = Cl(B[a^{-1}]) = Cl(B) = Cl(A[X]/(aX+b))$$

što je i trebalo pokazati. $\square$

Prethodno tvrdjenje može se iskoristiti za konstrukciju različitih primera UFD domena čiju faktorijalnost nije lako ispitati neposredno. Evo jednog takvog primera.

Primer 5.6.6. *Za glavni domen $A = \mathbb{Z}[[X]]$ i njegove formalne redove $a = X$, $b = 2 + X + X^2 + \dots$ ispunjeni su uslovi prethodnog tvrdjenja.*

Dokaz. Najpre, ideal $(a) = (X)$ je prost jer je $\mathbb{Z}[[X]]/(X) \cong \mathbb{Z}$ domen. Ideal $(a, b) = (X, 2 + X + X^2 + \dots)$ je takodje prost što se može utvrditi neposredno. Neka $fg \in (X, b)$. Tada je

$$fg = X\alpha + b\beta \quad \text{za neke} \quad \alpha, \beta \in \mathbb{Z}[[X]]$$

$$(f_0 + f_1X + \dots)(g_0 + g_1X + \dots) = X(\alpha_0 + \alpha_1X + \dots) + (2 + X + \dots)(\beta_0 + \beta_1X + \dots)$$

$$f_0g_0 + (f_0g_1 + f_1g_0)X + \dots = 2\beta_0 + (\alpha_0 + \beta_0 + 2\beta_1)X + \dots$$

Kako je $f_0g_0 = 2\beta_0$ biće $f_0g_0 \in 2\mathbb{Z}$, odnosno $f_0 \in 2\mathbb{Z}$ ili $g_0 \in 2\mathbb{Z}$ jer je $2\mathbb{Z}$ prost ideal u $\mathbb{Z}$. Ovo znači da je $f \in (X, b)$ ili $g \in (X, b)$ tj. (X, b) je prost ideal u

$\mathbb{Z}[[X]]$. Očigledno je $(X) \neq (X, b)$ pa primenom prethodnog primera dobijamo da je:

$$Cl(\mathbb{Z}[[X]][\,T\,]\,/\,(XT+b)\,) \cong Cl(\,\mathbb{Z}[[X]]\,)$$

Kako je $Cl(\,\mathbb{Z}[[X]]\,) = 0$, to posebno znači da je

$$\mathbb{Z}[[X]][\,T\,]\,/\,(XT+b) \text{ UFD. } \blacktriangledown$$

Primer 5.6.7. *Neka je k algebarski zatvoreno polje, $A = k\,[X,Y,Z]$ prsten polinoma, $F = X^2+Y^2+Z^2$ i $A_F = k\,[X,Y,Z]\,/(X^2+Y^2+Z^2)$. Tada A_F nije UFD. Za njegovu grupu divizor klasa važi:*

$$Cl(A_F) \cong \mathbb{Z}/2\mathbb{Z}$$

Dokaz. Transformacijom $U = X+iY$, $V = X-iY$ kvadratnu formu F možemo predstaviti u obliku $F = UV + Z^2$, pa je

$$A_F = k\,[U,V,Z\,]\,/(UV+Z^2) = k\,[u,v,z] \quad , \quad uv+z^2 = 0 \qquad (i)$$

gde su malim slovima označene odgovarajuće slike pri kanonskom homomorfizmu $A \to A_F$. Ako se sada A_F lokalizuje po multiplikativnim podskupu $S = \{1, v, v^2, \dots\}$, dobija se:

$$(A_F)_S = A_F[v^{-1}] = k\,[u,v,z,v^{-1}] = k\,[z,v,v^{-1}]$$

Poslednja jednakost je ispunjena jer je prema (i) $u = -z^2v^{-1} \in k\,[z,v,v^{-1}]$. Sada je $(A_F)_S = k\,[z,v][v^{-1}] = k\,[z,v]_S$. Kako su z i v algebarski nezavisni, $k\,[z,v]$ je prsten polinoma nad poljem, dakle UFD. Odavde je to i $(A_F)_S$ kao lokalizacija UFD-a, pa je $Cl((A_F)_S) = 0$. Homomorfizam

$$\bar{\imath} : Cl(A_F) \to Cl((A_F)_S$$

je surjektivan prema teoremi 5.5.6 pa je $Cl(A_F)/\ker\bar{\imath} \cong Cl((A_F)_S)$, odakle je

$$Cl(A_F) \cong \ker\bar{\imath} \qquad (ii)$$

Jezgro je generisano divizorskim idealima koji seku S, odnosno sadrže v. Takvi ideali su zapravo ideali prstena $k\,[u,v,z\,]\,/(v)$.

$$k\,[\,u,v,z\,]\,/(v) = k\,[\,U,V,Z\,]\,/(F)\big/(F,V)/(F) = k\,[\,U,V,Z\,]\,/(F,V) =$$

$$k\,[\,U,V,Z\,]\,/(V)\big/(F,V)/(V) = k\,[\,U,Z\,]\,\big/(UV+Z^2,V)/(V) = k\,[\,U,Z\,]\,/(Z^2)$$

Minimalni prosti ideali ovog prstena, osim toga što sadrže v, odavde moraju biti generisani slikom od Z. Jedini takav ideal u A_F je ideal $\mathfrak{p} = (v,z)$. Tada je $\mathfrak{p}^2 = (v^2, vz, z^2) = (v^2, vz, -uv) = v(v,z,u)$, odakle je $\mathfrak{p}^{(2)} = (v)$ glavni ideal, pa je $2\mathrm{div}\,\mathfrak{p} = 0$. Sam ideal $\mathfrak{p}$ nije glavni, što se može videti poredjenjem homogenosti članova. Prema tome, jezgro epimorfizma $\bar{\imath}$ generisano je elementom reda dva, i iz (ii) je $Cl(A_F)$ ciklična grupa reda dva, odakle sledi tvrdjenje.$\blacktriangledown$

Primer 5.6.8. *Neka je k polje, $Char(k) = 0$, $A = k[X, Y, Z]$, $F = XY - Z^n$, $n > 1$ i $A_F = k[X, Y, Z]/(F)$. Tada je:*

$$Cl(A_F) \cong \mathbb{Z}/n\mathbb{Z}$$

Dokaz. Uz iste oznake i slično kao i u prethodnom primeru, može se videti da je:

$$A_F/(x, z) \cong k[X, Y, Z]/(X, Z) \cong k[Y]$$

odakle je $\mathfrak{p} = (x, z)$ minimalan prost ideal u A_F tj. $\mathfrak{p} \in \mathcal{P}(A_F)$. Može se takodje pokazati da je on i jedini generator grupe $Cl(A_F)$. Medjutim, iz relacije $xy = z^n$ sledi da je:

$$\mathfrak{p}^n = (x^n, x^{n-1}z, \ldots, xz^{n-1}, z^n) = (x^n, x^{n-1}z, \ldots, xy) = x(x^{n-1}, \ldots, y)$$

Odavde je $\mathfrak{p}^{(n)} = (x)$ glavni ideal, pa u $D(A_F)$ važi $\operatorname{div} x = n \operatorname{div} \mathfrak{p}$. Prelaskom u $Cl(A_F)$ dobija se $n \operatorname{div} \mathfrak{p} = 0$, odakle sledi tvrdjenje.▼

Primer 5.6.9 ([10])**.** *$A = k[X, Y, Z, T]$, $F = XY - ZT$, $A_F = A/F$. Tada je*

$$Cl(A_F) \cong \mathbb{Z}$$ ▼

Primer 5.6.10. *Neka je k algebarski zatvoreno polje, $A = k[X, Y, Z, T]$ i $F = X^2 + Y^2 + Z^2 + T^2$. Tada $A_F = A/(F)$ nije UFD.*

Dokaz.

$$F = (X + iY)(X - iY) + (Z + iT)(Z - iT)$$

Ako se ova forma transformiše, stavljajući $X + iY = U, X - iY = V, Z + iT = W, Z - iT = S$, dobija se da je $F = UV + WS$, odakle je

$$A_F = k[U, V, W, S]/(UV + WS).$$

Prema prethodnom primeru je $Cl(A_F) = \mathbb{Z}$ pa A_F nije UFD.▼
Primeri 5.6.7 i 5.6.10 pokazuju da Klajn-Nagatina teorema ne važi u slučaju $n < 5$. Za cikličnu grupu G proizvoljnog reda može se, prema 5.6.8 i 5.6.9 naći Krulov domen A tako da je $G \cong Cl(A)$. Zanimljivo je da važi i opštije: svaka Abelova grupa izomorfna je grupi divizor klasa nekog Dedekindovog (a samim tim i Krulovog) domena. Sam dokaz ove teoreme izvodi se u nekoliko koraka koji se mogu ukratko izložiti.
Najpre se za Krulov domen A konstruiše ravno raširenje B koje je Dedekindov domen i još je $Cl(A) \to Cl(B)$ bijekcija. Za podgrupu H u $Cl(A)$, u sledećem koraku konstruiše se Krulov domen B takav da je $Cl(B) = Cl(A)/H$. Kako se svaka Abelova grupa G može predstaviti kao faktorgrupa neke slobodne Abelove grupe, $G = \mathbb{Z}^{(I)}/H$, u sledećem koraku konstruiše se Krulov domen čija je grupa divizor klasa izomorfna sa $\mathbb{Z}^{(I)}$. Pokazuje se da je dovoljno uzeti I kopija afinog koordinatnog prstena $k[X, Y, Z, T]/(XY - ZT)$, iz primera 5.6.9. Detalji ovih konstrukcija mogu se naći u [10], poglavlje 14. Iz ovih konstrukcija dobija se sledeći rezultat.

Teorema 5.6.11 (Claborn)**.** *Neka je G proizvoljna komutativna grupa. Tada postoji Dedekindov domen A takav da je $Cl(A) \cong G$.* $\square$

Definicija 5.6.2 suštinski je različita od ranijih definicija faktorijalnog domena. Ovom definicijom problem jednoznačne faktorizacije u Krulovom domenu A svodi se na tehnike računanja[6] njegove grupe divizor klasa $Cl(A)$. Grupa $Cl(A)$ daje i odgovor na pitanje koliko je neki Krulov domen sa nejednoznačnom faktorizacijom "daleko" od UFD-a. S tim u vezi Krulovi domeni sa torzionom grupom divizor klasa zovu se i *skoro faktorijalni domeni.* Krulovi domeni čija je grupa $Cl(A)$ torziona opisani su teoremom 5.5.8. Svi prsteni algebarskih celih su primeri skoro faktorijalnih prstena. Kod njih je naime, $Cl(A) = I(A)/F(A)$ grupa klasa ideala, koja je uvek konačna.
Faktorijalnost Krulovog domena A ekvivalentna je trivijalnosti grupe $Cl(A)$, odnosno uslovu da je svaki divizorski ideal u A glavni. Ako se ovaj uslov malo oslabi, tj. ako se zameni uslovom da je svaki divizorski ideal invertibilan, A ne mora biti UFD ali u tom slučaju važi sledeća teorema.

Teorema 5.6.12. *Neka je A Krulov domen. Tada važi:*
(a) Ako je svaki divizorski ideal u A invertibilan, onda je za svaki maksimalan ideal $\mathfrak{m}$ u A, $A_\mathfrak{m}$ UFD.
(b) Obratno, ako je $A_\mathfrak{m}$ UFD za svaki maksimalan ideal $\mathfrak{m}$ u A, i ako su divizorski ideali konačno generisani[7], onda je svaki divizorski ideal invertibilan.

Dokaz. (*a*) Neka je $\mathfrak{U}$ divizorski ideal u $A_\mathfrak{m}$. $A_\mathfrak{m}$ je Krulov pa je prema 5.4.11 $\mathfrak{U}$ presek dva glavna razlomljena ideala u $A_\mathfrak{m}$:

$$\mathfrak{U} = xA_\mathfrak{m} \cap yA_\mathfrak{m}$$

Kako za ideale I, J u A i proizvoljan multiplikativan podskup $S \subseteq A$, važi $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$, ako se za S uzme multiplikativin podskup $A \setminus \mathfrak{m}$, dobija se:

$$\mathfrak{U} = (Ax \cap Ay)_\mathfrak{m}$$

Kako je A Krulov domen, ponovnom primenom teoreme 5.4.11, dobija se da je ideal,

$$\mathfrak{V} = Ax \cap Ay$$

divizorski ideal u A, odakle je $\mathfrak{U} = \mathfrak{V}A_\mathfrak{m}$ i $\mathfrak{V}$ je prema pretpostavci invertibilan. Sada je primenom teoreme 3.4.3, $\mathfrak{U} = \mathfrak{V}A_\mathfrak{m}$ je glavni ideal, za svaki maksimalan ideal $\mathfrak{m}$, tj. $\mathfrak{U} \in F(A_\mathfrak{m})$. Odavde je $Cl(A_\mathfrak{m}) = D(A_\mathfrak{m})/F(A_\mathfrak{m}) = 0$, pa je $A_\mathfrak{m}$ UFD.

(*b*) Neka je sada $\mathfrak{U}$ divizorski ideal u A, tj. $\mathfrak{U} = Ax \cap Ay$, za neke $x, y \in k^*$. Tada, budući da je $A_\mathfrak{m}$ ravan A-modul, važi:

$$\mathfrak{U}\,A_\mathfrak{m} = (Ax \cap Ay)A_\mathfrak{m} = xA_\mathfrak{m} \cap yA_\mathfrak{m}$$

[6] Neke od ovih tehnika opisane su u [10].
[7] Npr. u Neterinim prstenima.

Odavde je $\mathfrak{U}\,A_{\mathfrak{m}}$, kao presek dva glavna, divizorski ideal u $A_{\mathfrak{m}}$. Kako je $A_{\mathfrak{m}}$ prema pretpostavci UFD, biće $Cl(A_{\mathfrak{m}}) = 0$, odnosno $D(A_{\mathfrak{m}}) = F(A_{\mathfrak{m}})$, pa je $\mathfrak{U}\,A_{\mathfrak{m}} \in F(A_{\mathfrak{m}})$. $\mathfrak{U}\,A_{\mathfrak{m}}$ je prema tome glavni ideal za svaki maksimalan ideal $\mathfrak{m}$ u A i $\mathfrak{U}$ je konačno generisan. Može se dakle ponovo primeniti teorema 3.4.3 prema kojoj je $\mathfrak{U}$ invertibilan. $\square$
Primenom ove teoreme faktorijalne domene možemo okarakterisati na sledeći način ([15]);

Teorema 5.6.13. *Domen A je UFD akko su ispunjeni sledeći uslovi:*
(1) *$A_{\mathfrak{m}}$ je UFD za svaki maksimalan ideal $\mathfrak{m}$ u A.*
(2) *Svaki minimalan prost ideal $\mathfrak{p} \in \mathcal{P}(A)$ je konačno generisan.*
(3) *Svaki invertibilan ideal u A je glavni.*

Dokaz. ($\Rightarrow$) : Neka je domen A faktorijalan. Uslov (1) je ispunjen jer je svaka lokalizacija UFD-a UFD (teorema 2.2.2). Uslov (2) važi jer je svaki minimalan prost ideal u faktorijalnom domenu glavni (teorema 1.1.21). Takodje je invertibilan ideal u UFD-u glavni (teorema 3.4.2), tj. ispunjen je i uslov (3).
($\Leftarrow$) : Neka su sada ispunjeni uslovi (1), (2) i (3). Prema uslovu (1) $A_{\mathfrak{m}}$ je UFD, pa je i Krulov, za svaki maksimalan ideal $\mathfrak{m}$. Kako je svaki domen presek svojih lokalizacija po maksimalnim idealima, to je $A = \cap A_{\mathfrak{m}}$ Krulov domen prema teoremi 5.2.8. Grupa $D(A)$ generisana je familijom minimalnih prostih ideala $\mathfrak{p} \in \mathcal{P}(A)$, koji su prema uslovu (2) konačno generisani, pa je onda i svaki divizorski ideal konačno generisan. Ispunjeni su dakle uslovi teoreme 5.6.12 (b), pa je svaki divizorski ideal invertibilan. Iz uslova (3) sada je svaki divizorski ideal i glavni, tj $D(A) = F(A)$, pa je $Cl(A) = 0$, A je UFD. $\square$
Primedba. Može se dati i direktan dokaz ove teoreme ([15]). Najpre se pokaže da pod uslovima (1), (2) i (3) svaki pravi prost ideal u A sadrži prost element a zatim se primeni teorema 1.1.17.

Definicija 5.6.14. *Domen A je lokalno faktorijalan ako je $A_{\mathfrak{m}}$ UFD za svaki maksimalan ideal $\mathfrak{m}$ u A.*

U Dedekindovom domenu svaki razlomljeni ideal je invertibilan, pa to posebno važi i za sve divizorske ideale. Na taj način zadovoljen je uslov (a) teoreme 5.6.12, pa je svaki Dedekindov domen lokalno faktorijalan.

Primer 5.6.15 (Prsten polinomnih funkcija na sferi)**.**

$$A_n = \mathbb{R}\,[X_0, X_1, \ldots, X_n\,]\,/(X_0^2 + X_1^2 + \cdots + X_n^2 - 1\,)$$

$$B_n = \mathbb{C}\,[X_0, X_1, \ldots, X_n\,]\,/(X_0^2 + X_1^2 + \cdots + X_n^2 - 1\,)$$

a) $n \geq 3 \Rightarrow Cl(A_n) = Cl(B_n) = 0$.
b) $n = 1 \Rightarrow Cl(A_1) \cong \mathbb{Z}/2\mathbb{Z}\,,\ Cl(B_1) = 0$.
c) $n = 2 \Rightarrow Cl(A_2) = 0\,,\ Cl(B_2) = \mathbb{Z}$.

Dokaz. a) Oba slučaja mogu se posmatrati istovremeno ako sa C_n označimo prstene A_n i B_n i sa k polja $\mathbb{R}$ ili $\mathbb{C}$. Prema 5.5.10 $Cl(C_n) = Cl(C_n[t])$ za neodredjenu t, pa je prema Nagatinoj teoremi ispunjeno:

$$Cl(C_n) = Cl(C_n[t, t^{-1}]) \qquad (i)$$

Ako sa F označimo ideal $F = (X_0^2 + X_1^2 + \cdots + X_n^2 - 1)$ i sa x_i odgovarajuće slike pri kanonskom homomorfizmu, $x_i = X_i + F$, $i = 0, 1, \ldots, n$, dobija se:

$$C_n = k[X_0, X_1, \ldots, X_n]/(X_0^2 + X_1^2 + \cdots + X_n^2 - 1) = k[x_0, x_1, \ldots, x_n],$$

sa definišućom relacijom:

$$x_0^2 + x_1^2 + \cdots + x_n^2 - 1 = 0$$

Ako se ova relacija pomnoži sa t^2 i uvede transformacija $y_i = x_i t$, odnosno $x_i = y_i t^{-1}$, $i = 0, 1, \ldots n$ dobija se ekvivalentna definišuća relacija:

$$y_0^2 + y_1^2 + \cdots + y_n^2 - t^2 = 0$$

Sada je $C_n[t, t^{-1}] = k[x_0, x_1, \ldots, x_n, t, t^{-1}] = k[y_0, y_1, \ldots, y_n, t, t^{-1}]$, pa je

$$Cl\big(C_n[t, t^{-1}]\big) = Cl\big(k[y_0, y_1, \ldots, y_n, t][t^{-1}]\big) = Cl\big(k[y_0, y_1, \ldots, y_n, t]\big), \quad (ii)$$

pri čemu je poslednja jednakost ispunjena prema Nagatinoj teoremi, za multiplikativan podskup $S = \{1, t, t^2, \ldots\}$. Dalje je

$$Cl\big(k[y_0, y_1, \ldots, y_n, t]\big) = Cl\big(k[Y_0, Y_1, \ldots, Y_n, T]/(F_1)\big) \overset{(*)}{=} 0 \qquad (iii)$$

Kvadratna forma $F_1 = Y_0^2 + Y_1^2 + \cdots + Y_n^2 - T^2$ je nedegenerisana i broj neodredjenih je $n + 2 \geq 5$ prema pretpostavci. Sada tražena jednakost $(*)$ sledi iz Klajn-Nagatine teoreme (2.3.4).
Iz $(i), (ii), (iii)$ dobija se $Cl(C_n) = 0$ tj. A_n, B_n su faktorijalni domeni za $n \geq 3$.

b) U drugom delu dokaza koristi se Samuelova lema[8] geometrijskog karaktera.

$$A_1 = \mathbb{R}[X_0, X_1]/(X_0^2 + X_1^2 - 1)$$

Na isti način kao u delu dokaza *a*) dobija se:

$$Cl(A_1) = Cl\big(A_1[t, t^{-1}]\big) = Cl\big(\mathbb{R}[y_0, y_1, t, t^{-1}]\big) = Cl\big(\mathbb{R}[y_0, y_1, t]\big),$$

gde je: $\qquad y_0 = x_0 t \quad , \quad y_1 = x_1 t \quad , \quad y_0^2 + y_1^2 = t^2$

Smenom neodredjenih dobija se nedegenerisana kvadratna forma pa se može primeniti Samuelov rezultat. Jednačina $Y_0^2 + Y_1^2 - T^2 = 0$ naravno ima netrivijalnih realnih rešenja pa je:

$$Cl(A_1) = Cl\big(\mathbb{R}[Y_0, Y_1, T]/(Y_0^2 + Y_1^2 - T^2)\big) = \mathbb{Z}/2\mathbb{Z}$$

S druge strane $\quad B_1 = \mathbb{C}[X_0, X_1]/(X_0^2 + X_1^2 - 1) = \mathbb{C}[u, v]$,

gde je: $\qquad u = x_0 + ix_1 \quad , \quad v = x_0 - ix_1 \quad , \quad uv = 1$

[8]Neka je F nedegenerisana kvadratna forma u $A = k[x, y, z]$ i $A_F = A/(F)$. Tada je $Cl(A_F) = \mathbb{Z}/2\mathbb{Z}$ akko $F(x, y, z) = 0$ ima netrivijalno rešenje u k. Ako takvih rešenja nema $Cl(A_F) = 0$.

Odavde je $B_1 = \mathbb{C}[u, u^{-1}] = \mathbb{C}[u]_{(u)}$ UFD kao lokalizacija UFD-a, pa je $Cl(B_1) = 0$.

c) $B_2 = \mathbb{C}[X_0, X_1, X_2]/(X_0^2 + X_1^2 + X_2^2 - 1)$

Uz iste oznake važi:

$$Cl(B_2) = Cl\big(\mathbb{C}[y_0, y_1, y_2, t, t^{-1}]\big) = Cl\big(\mathbb{C}[y_0, y_1, y_2, t]\big)$$

Kako je $y_0^2 + y_1^2 + y_2^2 - t^2 = uv + ws$, gde je $u = y_0 + iy_1, v = y_0 - iy_1$, $w = y_2 - t, s = y_2 + t$, dobija se:

$$Cl(B_2) = Cl\big(\mathbb{C}[u, v, w, s]/(uv + ws)\big) = \mathbb{Z}$$

Slično je $Cl(A_2) = Cl\big(\mathbb{R}[y_0, y_1, y_2, t]\big)$, gde je $y_0^2 + y_1^2 + y_2^2 - t^2 = 0$. Forma $F = y_0^2 + y_1^2 + y_2^2 - t^2$ može se predstaviti u obliku $F = y_0^2 + y_1^2 + uv$, gde je $u = y_2 + t$, $v = y_2 - t$, pa je $Cl(A_2) = Cl(A_F) = Cl\big(k[y_0, y_1, u, v]\big)$. Na isti način kao u dokazu teoreme 2.3.4 pokazuje se da je u prost u A_F i lokalizuje se po skupu $S = \{1, u, u^2, \dots\}$. Dobija se da je $(A_F)_S = A_F[u^{-1}]$ UFD, pa je $0 = Cl\left(A_F[u^{-1}]\right) = Cl(A_F)$, odakle sledi poslednji deo tvrdjenja. $\square$

Glava 6

Lokalni prsteni, algebarska geometrija i faktorijalnost

6.1 Definicije, oznake i važnija tvrdjenja

Glavni rezultat vezan za faktorizaciju u lokalnim prstenima je teorema o jednoznačnoj faktorizaciji regularnih lokalnih prstena (Auslander & Buchsbaum, 1959). Sam dokaz ove teoreme zahteva nešto drugačiji pristup faktorizaciji, uz naglašenije homološke metode. Obiman materijal u vezi sa lokalnim prstenima, kao i dokazi svih navedenih tvrdjenja, može se naći u [22], [15], [21] i [9]. Manji deo ove materije potreban za faktorijalnost može se izložiti kao spisak sledećih teorema i definicija.

Definicija 6.1.1. *Neka je R prsten, A R-modul i neka $Z(A)$ označava nula delitelje modula A, $Z(A) = \{\, r \in R \mid ru = 0 \text{ za neko } u \in A\,,\, u \neq 0 \,\}$. Uredjen niz $x_1, \ldots, x_n$ elemenata iz prstena R je R-niz na A ako su ispunjeni sledeći uslovi :*
(a) $(x_1, \ldots, x_n)A \neq A$.
(b) $x_1 \notin Z(A)$, $x_i \notin Z(A/(x_1, \ldots, x_{i-1})A)$, $i \geq 2$.

Specijalno, ako se za modul A uzme sam prsten R, R-niz na R zovemo samo R-nizom. Npr. u prstenu polinoma $R = A\,[\,x_1, x_2, \ldots, x_n\,]$, gde je A komutativan prsten, neodredjene $x_1, x_2, \ldots, x_n$ čine jedan R-niz. U ovom primeru svaka permutacija $x_{i_1}, x_{i_2}, \ldots, x_{i_n}$, je takodje jedan R-niz, pa uredjenost ovde nije bitna. U opštem slučaju medjutim, niz dobijen permutacijom članova R-niza ne mora biti R-niz. Jedan od dovoljnih uslova daje sledeće tvrdjenje.

Tvrdjenje 6.1.2. *Neka je R Neterin prsten, A konačno generisan A-modul, $J = \bigcap_{\mathfrak{m} \in Spec_M(R)} \mathfrak{m}$ Džekobsonov radikal i $x_1, x_2, \ldots, x_n$ R-niz na A, $x_i \in J$. Tada je i svaka permutacija $x_{i_1}, x_{i_2}, \ldots, x_{i_n}$ R-niz na A.* □

Specijalno, ako je $(R, \mathfrak{m})$ lokalan prsten, onda je $J = \mathfrak{m}$, pa je za R-niz $x_1, x_2, \ldots, x_n$, $x_i \in \mathfrak{m}$, svaka permutacija takodje R-niz. Iz uslova (a) definicije

R-niza, medju elementima $x_1, x_2, \ldots, x_n$ nema invertibilnih, pa svi moraju biti u maksimalnom idealu $\mathfrak{m}$, odakle se dobija sledeća posledica.

Posledica 6.1.3. *Ako je R lokalan prsten i A konačno generisan R-modul, onda je svaka permutacija R-niza na A opet R-niz na A.* □

Može se pokazati da je za svaki R-niz $x_1, x_2, \ldots, x_n$ u A, lanac ideala :

$$(x_1) \subseteq (x_1, x_2) \subseteq \cdots \subseteq (x_1, x_2, \ldots, x_n)$$

strogo rastući. Ako je prsten R Neterin ovakvi lanci su konačni, pa se svaki R-niz na A može proširiti do R-niza maksimalne dužine. Važi sledeće tvrdjenje.

Teorema 6.1.4. *Neka je R Neterin prsten, A konačno generisan R-modul, $I \triangleleft R$ ideal za koji je $IA \neq A$. Tada svaka dva maksimalna R-niza sadržana u I imaju istu dužinu.* □

Definicija 6.1.5. *Ako su ispunjeni uslovi teoreme 6.1.4, zajedničku dužinu svih maksimalnih R-nizova u I (na A) zovemo dubinom I na A, u oznaci* $\operatorname{depth}(\mathrm{I}, \mathrm{A})$ *ili* $\operatorname{Grade}(\mathrm{I}, \mathrm{A})$.

Dubina ideala može se definisati i u slučaju da prsten A nije Neterin, ali se tada može desiti da je $\operatorname{depth}(\mathrm{I}, \mathrm{A}) = \infty$. Ako se za modul A uzme prsten R onda se $\operatorname{depth}(\mathrm{I}, \mathrm{R})$ kraće označava sa $\operatorname{depth}(\mathrm{I})$. U slučaju lokalnog prstena $(R, \mathfrak{m})$ i konačno generisanog modula A, koristi se oznaka $\operatorname{depth}(\mathrm{A})$ za $\operatorname{depth}(\mathfrak{m}, \mathrm{A})$. Ako je uz to i $A = R$, oznaka je $\operatorname{depth}(\mathrm{R})$. Ako ideal I sadrži R-niz dužine n, može se pokazati da je $\operatorname{ht}(I) \geq n$, pa je u opštem slučaju

$$\operatorname{ht}(I) \geq \operatorname{depth}(\mathrm{I}) \tag{1}$$

Neterini prsteni kod kojih u (1) važi jednakost za svaki ideal I su Cohen-Macaulay-evi, ili kraće CM prsteni[1]. Za lokalan prsten $(R, \mathfrak{m})$ važi $\operatorname{ht}(\mathfrak{m}) = \dim(R)$, pa se može reći da je lokalan prsten R CM prsten ako je $\dim(R) = \operatorname{depth}(\mathrm{R})$. Može se takodje pokazati da klasi CM prstena pripadaju svi 1-dimenzioni domeni, što će specijalno značiti i da su Dedekindovi domeni CM prsteni. Kako postoje Dedekindovi domeni koji nisu faktorijalni, postoje i CM prsteni koji nisu UFD domeni. Mogu se takodje lako naći primeri i u višim dimenzijama; npr. $A = k[X, Y, Z]/(XY - Z^2)$ je CM prsten dimenzije 2 i nije UFD jer je $Cl(A) = \mathbb{Z}/2\mathbb{Z}$. S druge strane, primer UFD domena koji nije CM prsten nije baš tako lako konstruisati. Jedan takav primer dao je Bertin, 1967. koristeći tehniku *Galuaovih spuštanja*. Ova tehnika u osnovi se zasniva na sledećem tvrdjenju; za faktorijalan domen A i njegovu konačnu grupu automorfizama G definiše se skup A^G svih invarijantnih elemenata, $A^G = \{a \in A \mid g(a) = a \ , \forall g \in G\}$. A^G je potprsten prstena A i pri tom je A^G UFD ako je kohomološka grupa $H^1(G, A^*) = 0$. Posebno, ako je $A = k[X_1, \ldots, X_n]$ prsten

[1]CM prsteni definišu se nešto strožije. R je CM prsten ako je Neterin i ako za svaki maksimalan ideal $\mathfrak{m}$ u R važi $\operatorname{depth}(\mathfrak{m}) = \operatorname{ht}(\mathfrak{m})$. Detaljan prikaz CM prstena i njihovih raširenja dat je u [15].

polinoma nad poljem k karakteristike $p \neq 0$, i G ciklična grupa reda p^j koja deluje kao grupa k-automorfizama prstena A onda je $H^1(G, A^*) = 0$ tj. A^G je UFD. Dokaz ovog tvrdjenja može se naći u [10]. Ova tehnika predstavlja dobar metod za konstrukciju faktorijalnih domena sa raznim željenim osobinama. Tako se npr. može konstruisati UFD nad kojim prsten formalnih redova nije faktorijalan. Na ovaj način konstruisan je i primer UFD-a koji nije CM prsten; posmatra se prsten $A = k[X_1, X_2, X_3, X_4]$, gde je k polje karakteristike 2, i $\sigma : A \to A$, k-automorfizam prstena A, definisan sa $\sigma(X_1) = X_1 + X_2$, $\sigma(X_2) = X_2 + X_3$, $\sigma(X_3) = X_3 + X_4$, $\sigma(X_4) = X_4$. Dalje se pokazuje da je A^σ UFD koji nije CM. Slično, neka je sada $A = k[X_1, X_2]$, $Char(k) = p > 0$ i $\sigma : A \to A$ k-automorfizam definisan sa $\sigma(X_1) = X_1 + X_2$, $\sigma(X_2) = X_2$. Tada element $u = (X_1 + X_2)(X_1 + 2X_2) \dots (X_1 + pX_2)$ pripada A^σ tj. $\sigma(u) = u$. Može se dalje pokazati da je $A^\sigma = k[X_1, u]$ koji je UFD i CM. Detaljnije o ovim i sličnim primerima može se naći u [10].

Lema 6.1.6 (Nakayama)**.** *Neka je $(R, \mathfrak{m})$ kvazilokalan prsten i A konačno generisan R-modul. Ako je $\mathfrak{m}A = A$, onda je $A = 0$.* □

Skup generatora $(a_1, \dots, a_k)$ R-modula A je *minimalna baza* modula A ako ni jedan pravi podskup ne generiše A. Dve minimalne baze istog modula ne moraju medjutim imati isti broj elemenata. Ova nepravilnost se gubi ako se posmatraju moduli nad lokalnim prstenima; Neka je $(R, \mathfrak{m})$ lokalni prsten, A konačno generisan R-modul i neka je $\hat{A} = A/\mathfrak{m}A$. Kako je $\mathfrak{m}$ maksimalan ideal, $R/\mathfrak{m} = k$ je polje i $\hat{A}$ je konačno dimenzionalan vektorski prostor nad k. Neka je $\dim(\hat{A}) = n$. Tada se, koristeći lemu 6.1.6, može dokazati sledeće tvrdjenje.

Teorema 6.1.7. *Neka je $(\overline{a}_1, \dots, \overline{a}_n)$ baza vektorskog prostora $\hat{A}$, gde je $\overline{a}_i = a_i + \mathfrak{m}A$, $i = 1, \dots, n$. Tada je $(a_1, \dots, a_n)$ minimalna baza modula A. Sve minimalne baze modula A mogu se dobiti na ovaj način, tj. sve minimalne baze imaju $n = \dim(\hat{A})$ elemenata.* □

Posebno, ako se uz iste oznake u prethodnoj teoremi za modul A uzme ideal $\mathfrak{m}$, dobija se sledeća posledica.

Posledica 6.1.8. *Neka je $(R, \mathfrak{m})$ lokalan prsten. Tada je $\mathfrak{m} = (a_1, \dots, a_k)$ akko je $(\overline{a}_1, \dots, \overline{a}_k)$ baza vektorskog prostora $\mathfrak{m}/\mathfrak{m}^2$ nad poljem $k = R/\mathfrak{m}$.* □

Ako važe uslovi prethodnog tvrdjenja, primenom Krulove glavnoidealske teoreme, dobija se $\mathrm{ht}(\mathfrak{m}) \leq n$. Ovde je $\mathrm{ht}(\mathfrak{m}) = \dim(R)$, jer je R lokalan prsten, i još je $n = \dim(\mathfrak{m}/\mathfrak{m}^2)$, nad poljem $k = R/\mathfrak{m}$. Iz ovoga se vidi da je za lokalne prstene ispunjena sledeća nejednakost :

$$\dim(R) \leq \dim(\mathfrak{m}/\mathfrak{m}^2) \tag{2}$$

Nejednakost (2) može se pročitati i na sledeći način : visina maksimalnog ideala $\mathfrak{m}$ lokalnog prstena $(R, \mathfrak{m})$, nije veća od minimalnog broja generatora za $\mathfrak{m}$. Lokalni prsteni za koje je u (2) ispunjena jednakost posebno su interesantni sa stanovišta faktorijalnosti. Faktorizacija u njima je jednoznačna (6.2.7).

Definicija 6.1.9. *Lokalan prsten* $(R, \mathfrak{m})$ *je regularan lokalan ako je* $\dim(R) = \dim(\mathfrak{m}/\mathfrak{m}^2)$*, tj. ako se njegov maksimalan ideal* $\mathfrak{m}$ *može generisati sa tačno* $n = \dim(R)$ *elemenata.*

Definicija 6.1.10. *Neterin prsten* R *je regularan ako je lokalizacija* $R_{\mathfrak{m}}$ *regularan lokalan prsten za svaki maksimalan ideal* $\mathfrak{m}$ *u* R*.*

Neka je $(R, \mathfrak{m})$ lokalan prsten i $\mathfrak{m} = (a_1, \ldots, a_n)$, gde je n minimalan broj generatora za $\mathfrak{m}$. Iz prethodnih tvrdjenja i Krulove glavnoidealske teoreme proizilaze sledeće nejednakosti :

$$\mathrm{depth}(\mathfrak{m}) \leq \mathrm{ht}(\mathfrak{m}) \leq \mathrm{n}\,,$$

odnosno, $$\mathrm{depth(R)} \leq \dim(\mathrm{R}) \leq \dim(\mathfrak{m}/\mathfrak{m}^2)$$

Kod CM prstena prva nejednakost postaje jednakost, dok druga to postaje kod regularnih lokalnih prstena. U vezi sa regularnim lokalnim prstenima važe sledeća tvrdjenja ([15],[9]).

Teorema 6.1.11. *Neka je* $(R, \mathfrak{m})$ *lokalan prsten čiji se maksimalni ideal može generisati* R*-nizom dužine* n*. Tada je* R *regularan lokalan i* $n = \dim(R) = \dim(\mathfrak{m}/\mathfrak{m}^2)$*.* □

Teorema 6.1.12. *Ako je* $(R, \mathfrak{m})$ *regularan lokalan i* $x \in \mathfrak{m} \setminus \mathfrak{m}^2$*, onda je i* $R/(x)$ *regularan lokalan prsten.* □

Teorema 6.1.13. *Neko je* $(R, \mathfrak{m})$ *regularan lokalan i* $x \in \mathfrak{m} \setminus \mathfrak{m}^2$*, takav da* x *ne pripada minimalnom prostom idealu u* R*. Tada, ako je* $R/(x)$ *regularan, onda je i* R *regularan.* □

Teorema 6.1.14. *Regularan lokalan prsten je domen.* □

Teorema 6.1.15. *Regularan lokalan prsten je CM prsten.* □

Teorema 6.1.16. *Regularan lokalan prsten dimenzije* 1 *je DVR.* □

6.2 Faktorizacija u regularnim lokalnim prstenima

Iz teorije modula poznato je da je A-modul P projektivan akko je direktan sumand slobodnog modula, kao i da su projektivni moduli nad lokalnim prstenima slobodni. Takodje je svaki modul homomorfna slika projektivnog modula, tj. za proizvoljan modul M postoji projektivan modul P_0 i epimorfizam $f_0 : P_0 \to M$. To znači da se svakom modulu može pridružiti tačan niz : $0 \to \ker(f_0) \to P_0 \to M \to 0$. Ovakav niz može se dobiti i za modul $\ker(f_0)$: $0 \to \ker(f_1) \to P_1 \xrightarrow{f_1} \ker(f_0) \to 0$. Nastavljajući ovaj postupak dolazi se do kompleksa,

$$P_* : \qquad \cdots \to P_n \to P_{n-1} \to \cdots \to P_0 \to 0$$

pridruženog modulu M. Kompleks P_* je *projektivna rezolucija* modula M. Specijalno, ako je A Neterin i M konačno generisan A-modul, za P_0 može se uzeti slobodan modul konačnog ranga, pa je onda $\ker(f_0)$ takodje konačno generisan. Iz ovoga se može formulisati sledeće tvrdjenje.

Tvrdjenje 6.2.1. *Neka je A Neterin prsten i M konačno generisan A-modul. Tada M ima projektivnu rezoluciju P_*, u kojoj su P_i slobodni, konačno generisani moduli.* □

Definicija 6.2.2. *Konačna slobodna rezolucija, kraće FFR[2], A-modula M je tačan niz:*

$$0 \to F_n \to \cdots \to F_0 \to M \to 0 \tag{3}$$

gde su F_i , $i = 0, \ldots, n$ slobodni, konačno generisani moduli.

Ako A-modul M ima FFR (1) onda je, s obzirom da lokalizacija čuva tačnost, za svaki prost ideal $\mathfrak{p}$ prstena A, niz :

$$0 \to (F_n)_{\mathfrak{p}} \to \cdots \to (F_0)_{\mathfrak{p}} \to M_{\mathfrak{p}} \to 0 \tag{4}$$

FFR $A_{\mathfrak{p}}$-modula $M_{\mathfrak{p}}$. Kako su projektivni moduli nad lokalnim prstenima slobodni, to nad regularnim lokalnim prstenom svaki konačno generisani modul ima FFR. Može se pokazati da je konačno generisan modul M nad Neterinim prstenom R projektivan akko je $M_{\mathfrak{p}}$ slobodan $R_{\mathfrak{p}}$ modul, za svaki prost ideal $\mathfrak{p}$ u A. U terminima ideala, razlomljeni ideal $I \in I(A)$ biće projektivan A-modul akko je invertibilan. Tačnije, važi sledeća teorema, koja predstavlja proširenje teoreme 3.4.3.

Teorema 6.2.3 ([3])**.** *Neka je A domen i $I \in I(A)$ razlomljen ideal. Sledeći uslovi su tada ekvivalentni:*
(1) *I je invertibilan.*
(2) *I je konačno generisan i $I_{\mathfrak{m}}$ je glavni ideal u $A_{\mathfrak{m}}$ za svaki maksimalan ideal $\mathfrak{m}$.*
(3) *I je projektivan A-modul.* □

Lema 6.2.4 ([21])**.** *Ako svaki konačno generisan modul nad Neterinim prstenom A ima FFR, onda je A regularan.* □

Lema 6.2.5 ([15])**.** *Projektivan modul P sa FFR je stabilno slobodan tj. postoje slobodni moduli F, F' takvi da je*

$$P \oplus F \cong F' \qquad \square$$

Ako je M stabilno slobodan A-modul, onda se iz $M \oplus F \cong F'$, dobija FFR za $M : 0 \to F \to F \to M \to 0$. Kako je M i projektivan kao direktan sumand slobodnog modula, vidi se da su stabilno slobodni moduli konačno generisani projektivni moduli sa FFR.

[2]Finite Free Resolution.

Lema 6.2.6 ([21]). *Neka je A domen i I ideal u A takav da je $I \oplus A^n \cong A^{n+1}$. Tada je I glavni ideal*[3]. $\square$

Teorema 6.2.7 (Auslander & Buchsbaum). *Regularan lokalan prsten je UFD.*

Dokaz. (Indukcijom po $\dim(A)$)
Regularan lokalan prsten dimenzije 1 je prema 6.1.16 DVR, pa je zato i UFD. Pretpostavimo da je teorema tačna za sve regularne lokalne prstene dimenzije manje od n, i neka je $(A, \mathfrak{m})$ regularan lokalan prsten, $\dim(A) = n$. Neka je $x \in \mathfrak{m} \setminus \mathfrak{m}^2$. Tada je prema 6.1.12 A/xA regularan lokalan prsten. Prema 6.1.14 A/xA je domen tj. x je prost element domena A. Neka je $S = \{ 1, x, x^2, \dots \}$ multiplikativan podskup u A generisan sa x i $A_x = A_S$ odgovarajuća lokalizacija. Tada je prema Nagatinoj teoremi $Cl(A) \cong Cl(A_S)$, pa je dovoljno dokazati da je A_S UFD. Kako je A_x Neterin dovoljno je pokazati da je svaki minimalan prost ideal $\overline{\mathfrak{p}} \in \mathcal{P}(A_x)$ glavni. Neka je zato $\overline{\mathfrak{p}} \lhd A_x$, $\mathrm{ht}(\overline{\mathfrak{p}}) = 1$, $\overline{\mathfrak{p}} = (\overline{\mathfrak{p}} \cap A)A_x = \mathfrak{p}A_x$. Kako je A regularan lokalan prsten i $\mathfrak{p}$ je konačno generisan kao A-modul, $\mathfrak{p}$ ima FFR :

$$0 \to F_n \to \cdots \to F_0 \to \mathfrak{p} \to 0$$

gde su F_i slobodni moduli, odakle je:

$$0 \to (F_n)_x \to \cdots \to (F_0)_x \to \overline{\mathfrak{p}} \to 0$$

FFR za A_x-modul $\overline{\mathfrak{p}}$. Kako je lokalizacija regularnog lokalnog prstena, regularan lokalan prsten, to je za svaki prost ideal $\mathfrak{q} \lhd A_x$, $(A_x)_{\mathfrak{q}}$ regularan lokalan prsten. Dalje, $\dim(A_x)_{\mathfrak{q}} < \dim(A)$, jer je $(A_x)_{\mathfrak{q}} = A_{\mathfrak{q} \cap A}$, pa je $(A_x)_{\mathfrak{q}}$ UFD prema pretpostavci. Odavde je $\overline{\mathfrak{p}}_{\mathfrak{q}}$ glavni ideal, pa je slobodan $(A_x)_{\mathfrak{q}}$-modul, za svaki prost ideal $\mathfrak{q}$. To znači da je $\overline{\mathfrak{p}}$ projektivan A_x-modul. Prema lemi 6.2.5 $\overline{\mathfrak{p}}$ je stabilno slobodan. Prema lemi 6.2.6, stabilno slobodni moduli ranga 1 su slobodni, pa je $\overline{\mathfrak{p}}$ slobodan. $\square$

Teorema 6.2.8. *Neka je A Neterin domen. Ako svaki konačno generisan A-modul ima FFR, A je UFD.*

Dokaz. Prema lemi 6.2.4 A je regularan Neterin domen. Neka je $\mathfrak{p} \in \mathcal{P}(A)$ minimalan prost ideal. Dovoljno je, prema teoremi 4.2.2, pokazati da je $\mathfrak{p}$ glavni. Neka je $\mathfrak{m} \lhd A$ proizvoljan maksimalan ideal. $A_{\mathfrak{m}}$ je regularan lokalan, pa je prema teoremi 6.2.7 UFD. To znači da je $\mathfrak{p}_{\mathfrak{m}}$ glavni ideal u $A_{\mathfrak{m}}$, pa je slobodan $A_{\mathfrak{m}}$-modul. Kako to važi za svaki maksimalan ideal $\mathfrak{m}$ u A, $\mathfrak{p}$ je projektivan A-modul. Modul $\mathfrak{p}$ je konačno generisan projektivan modul sa FFR, pa je prema lemi 6.2.5 stabilno slobodan. Kako je $\mathrm{ht}(\mathfrak{p}) = 1$, može se primeniti lema 6.2.6, prema kojoj je $\mathfrak{p}$ slobodan tj. glavni. $\square$
Iz definicije regularnog prstena A neposredno sledi da je $A_{\mathfrak{p}}$ regularan lokalan prsten za svaki prost ideal $\mathfrak{p}$ u A. Ovo važi, jer je prost ideal $\mathfrak{p}$ sadržan u nekom maksimalnom idealu $\mathfrak{m}$, pa je iz teoreme o korespodenciji $\mathfrak{p} = \mathfrak{p}A_{\mathfrak{m}} \cap A$. Odavde je $A_{\mathfrak{p}} = A_{\mathfrak{p}A_{\mathfrak{m}} \cap A} = (A_{\mathfrak{m}})_{\mathfrak{p}A_{\mathfrak{m}}}$. $(A_{\mathfrak{m}})_{\mathfrak{p}A_{\mathfrak{m}}}$ je lokalizacija regularnog lokalnog

[3] Može se dati i sledeća ekvivalentna formulacija; Ako je A domen stabilno slobodni moduli ranga 1 su slobodni.

prstena pa je i sam regularan lokalan, odakle se dobija tražena osobina. Ova osobina regularnih prstena koristi se u dokazu sledeće teoreme, koja predstavlja generalizaciju teoreme 6.2.7.

Teorema 6.2.9. *Regularan polulokalan*[4] *domen je UFD.*

Dokaz. Neka je A regularan polulokalan domen, $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_n$ njegovi maksimalni ideali i neka je $\mathfrak{p} \in \mathcal{P}(A)$ minimalan prost ideal. A je regularan, pa su $A_{\mathfrak{m}_1}, \ldots, A_{\mathfrak{m}_n}$ regularni lokalni prsteni, odnosno UFD-ovi, prema teoremi 6.2.7. Odavde su ideali $\mathfrak{p}A_{\mathfrak{m}_1}, \ldots, \mathfrak{p}A_{\mathfrak{m}_n}$ glavni, $\mathfrak{p}A_{\mathfrak{m}_i} = (p_i)$ za neke elemente $p_i \in \mathfrak{p}$, $i = 1, \ldots, n$. Neka je $\mathfrak{m} = \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_n$ i neka su $a_i \in A$ elementi takvi da $a_i \in \mathfrak{m} \setminus \mathfrak{m}_i$. Tada je $\mathfrak{p}A_{\mathfrak{m}_i} = (p_i a_i)$ i prema konstrukciji je $p_j a_j \in \mathfrak{p}\mathfrak{m}_i A_{\mathfrak{m}_i}$ za $i \neq j$. Element $p = \sum p_j a_j$ generiše ideale $\mathfrak{p}A_{\mathfrak{m}_i}$, za svako i. Kako je $A = A_{\mathfrak{m}_1} \cap \cdots \cap A_{\mathfrak{m}_n}$, to je

$$\mathfrak{p} = \mathfrak{p}A = \mathfrak{p}A_{\mathfrak{m}_1} \cap \cdots \cap \mathfrak{p}A_{\mathfrak{m}_n} = (p)A \,,$$

odakle je $\mathfrak{p}$ glavni ideal. □

Teorema 6.2.10. *Ako je A regularan, ideal $Au \cap Av$ je projektivan za svako $u, v \in A$.*

Dokaz. Neka je $\mathfrak{m}$ maksimalan ideal u A i neka je $I = Au \cap Av$. Prelaskom u $A_{\mathfrak{m}}$ dobija se:

$$I_{\mathfrak{m}} = (Au \cap Av)A_{\mathfrak{m}} = uA_{\mathfrak{m}} \cap vA_{\mathfrak{m}} \tag{5}$$

Prema (5), $I_{\mathfrak{m}}$ je divizorski ideal u $A_{\mathfrak{m}}$. Takodje je $Cl(A_{\mathfrak{m}}) = 0$, jer je $A_{\mathfrak{m}}$ UFD prema pretpostavci. To znači da su divizorski ideali u $A_{\mathfrak{m}}$ glavni, pa je i $I_{\mathfrak{m}}$ glavni ideal. Kako to važi za proizvoljan maksimalan ideal $\mathfrak{m}$, I je projektivan A-modul prema teoremi 6.2.3. □

Teorema 6.2.11. *Ako je A UFD, projektivan ideal je glavni.*

Dokaz. Neposredna primena teoreme 6.2.3 i teoreme 3.4.2. □

Teorema 6.2.12. *Ako je A regularan, onda je $Cl(A) = Pic(A)$.*

Dokaz. Neposredna primena teoreme 6.2.3 i teoreme 6.2.10. □

6.3 Primena na formalne redove

Neka je R prsten i I pravi ideal u R, sa osobinom:

$$\bigcap_{n \in \mathbb{N}} I^n = 0 \tag{6}$$

Tada se pomoću ideala I na R može definisati topologija, tako što, za $a \in R$, otvorene okoline tačke a definišemo sa $a + I^n$, $n \in \mathbb{N}$. Ako ove skupove uzmemo

[4] Neterin domen sa konačno mnogo maksimalnih ideala.

za bazne otvorene skupove, prsten R sa takvom topologijom je Hausdorfov. Topologija indukovana idealom I je *I-adična topologija*. Skup svih klasa ekvivalencije Košijevih nizova elemenata iz R, u oznaci $\hat{R}$ je takodje prsten, koji zovemo *kompletiranjem* prstena R. Važi $R \subseteq \hat{R}$. U slučaju $R = \hat{R}$, kaže se da je prsten R *kompletan* u I-adičnoj topologiji. Uslov (6), neophodan za definisanje I-adične topologije, ispunjen je u sledećim karakterističnim slučajevima :
- R Neterin domen, $I \lhd R$ bilo koji pravi ideal.
- R polulokalan sa maksimalnim idealima $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ i $I \subseteq \bigcap_{i=1}^{n} \mathfrak{m}_i$.
- $(R, \mathfrak{m})$ lokalan, $I \lhd R$ bilo koji pravi ideal. Često se uzima upravo $I = \mathfrak{m}$ i tada je $\dim(R) = \dim(\hat{R})$, $\hat{\mathfrak{m}} \cap R = \mathfrak{m}$.

Primer 6.3.1.

$$A = \mathbb{R}\,[\,X, Y\,]$$

Neka je $I = (X^2+Y^2-1)$ i $\hat{A}$ kompletiranje prtena A u I-adičnoj topologiji. Na sličan način kao u primeru 5.6.15 može se pokazati da je $Cl(\hat{A}) = \mathbb{Z}/2\mathbb{Z}$. Na taj način, vidi se da kompletiranje UFD-a ne mora biti UFD. □

Za razliku od faktorijalnosti, regularnost se čuva kompletiranjem. Preciznije, uz prethodno uvedene oznake važi: R je regularan akko je $\hat{R}$ regularan ([24]). Konstrukcija kompletiranja korisna je kod formalnih redova, jer za proizvoljan prsten R, prsten formalnih redova $R[[X]]$ je kompletiranje prstena polinoma $R[X]$ u (X)-adičnoj topologiji. U opštem slučaju, za multiplikativan podskup $S \subseteq R$, važi $R[[X]]_S \subsetneq R_S[[X]]$. Medjutim u (X)-adičnoj topologiji $R_S[[X]]$ je kompletiranje prstena $R[[X]]_S$ tj. važi $R[[\hat{X}]]_S = R_S[[X]]$.

Tvrdjenje 6.3.2 ([21])**.** *Ako je prsten A regularan, onda su i $A[X], A[[X]]$ regularni.* □

Prsten formalnih redova je Neterin, CM, regularan, Krulov, kompletno integralno zatvoren akko je, respektivno, prsten R takav. Prsten formalnih redova medjutim ne čuva faktorijalnost (primer 2.6.2). Dovoljne uslove za jednoznačnu faktorizaciju u prstenu formalnih redova $R[[X]]$ daje sledeća teorema.

Teorema 6.3.3. *Ako je prsten A regularan UFD, onda je i $A[[X]]$ takav.*

Dokaz. A je Krulov domen, s obzirom da je UFD. Tada je, prema teoremi 5.3.3, i $B = A[[X]]$ Krulov domen. Neka je $I = uB \cap vB\,,\ u, v \in B$ divizorski ideal u B. Dovoljno je dokazati da je $Cl(B) = 0$, odnosno da je I glavni ideal. Prema teoremi 6.2.10, $I = uB \cap vB$ je projektivan A-modul, pa je $I \otimes_B A = I \otimes_B B/\mathrm{x}\,B = I/\mathrm{x}\,I$ projektivan A-modul. Neka je

$$I = \mathrm{x}^k J \quad , \quad J \nsubseteq \mathrm{x}\,B \tag{7}$$

Tada je $I/\mathrm{x}\,I = \mathrm{x}^k J/\mathrm{x}^{k+1} J \cong J/\mathrm{x}\,J$, pa je $J \cong I$ i J je projektivan. Dokazujemo sada da je $J \cap B\,\mathrm{x} = J\,\mathrm{x}$:
$\supseteq$: Očigledno, jer $J\,\mathrm{x} \subseteq J\,,\ J\,\mathrm{x} \subseteq B\,\mathrm{x} \Rightarrow J\,\mathrm{x} \subseteq J \cap B\,\mathrm{x}$.
$\subseteq$: Neka je sada $c \in J \cap B\,\mathrm{x}$. J je projektivan, pa je $J = u_1 B \cap v_1 B$, odakle

je $c = u_1u_1' = v_1v_1'$, $u_1', v_1' \in B$, $u_1, v_1 \in J \not\subseteq B\,\mathrm{x}$. $B\,\mathrm{x}$ je prost ideal u B pa $u_1u_1' \in B\,\mathrm{x}$, $u_1 \notin B\,\mathrm{x} \Rightarrow u_1' \in B\,\mathrm{x}$. Odavde je $u_1' = u_1''\mathrm{x}$, $u_1'' \in B$ i iz istih razloga $v_1' = v_1''\mathrm{x}$, $v_1'' \in B$. Sada se iz $u_1u_1' = v_1v_1'$ dobija $u_1''u_1 = v_1''v_1$, tj. $u_1''u_1 \in Bu_1 \cap Bv_1 = J$, pa $c = u_1u_1' = u_1u_1''\mathrm{x} \in J\,\mathrm{x}$.
Odavde je

$$J/J\,\mathrm{x} = J/J \cap B\,\mathrm{x} \cong J + B\,\mathrm{x}/B\,\mathrm{x} \lhd B/B\,\mathrm{x} = A,$$

pa je $J/J\,\mathrm{x}$ projektivan ideal u A. Kako je A UFD, $J/J\,\mathrm{x}$ je prema 6.2.11 glavni ideal u A tj. slobodan A-modul. Sada je

$$J/J\,\mathrm{x} = (\,\mathrm{y}) \Rightarrow J = \mathrm{y}\,B + \mathrm{x}\,J \Rightarrow J = \mathrm{y}\,B\,, \tag{8}$$

gde se poslednja implikacija dobija primenom leme Nakayame, jer $(\mathrm{x}) \subseteq Rad(B)$. Prema (7) i (8) je $I = \mathrm{x}^k\mathrm{y}\,B$ glavni ideal. Time je dokazana ova teorema jer je $A[[X]]$ regularan prema 6.3.2. □

Posledica 6.3.4. *Ako je A regularan UFD onda je i $A[[X_1, \ldots, X_n]]$ takav.*

Dokaz. Indukcijom, s obzirom da je $A[[X_1, \ldots, X_n]] = A[[X_1, \ldots, X_{n-1}]][[X_n]]$. □

Posledica 6.3.5. *Ako je A regularan UFD, onda je svaki prsten oblika*

$$A[X_1, \ldots, X_m][[Y_1, \ldots, Y_n]][Z_1, \ldots, Z_p][[T_1, \ldots, T_q]]$$

regularan UFD. □

6.4 Jednoznačna faktorizacija u algebarskoj geometriji

Jednoznačna faktorizacija ima i svoju geometrijsku interpretaciju; faktorijalnost koordinatnog prstena neke mnogostrukosti dimenzije n znači da se svaka podmnogostrukost dimenzije $n-1$ može definisati jednom jednačinom. S druge strane, ako posmatramo jednu tačku mnogostrukosti, onda radimo sa lokalnim prstenima, važnim objektima algebarske geometrije. Oni se prirodno javljaju kao prsteni "klica" O_x funkcija definisanih u nekoj tački x mnogostrukosti Y. Mnogostrukost Y biće nesingularna u tački x ako je O_x regularan, dakle i UFD prema teoremi 6.2.7. Ukratko ćemo izložiti ovaj novi, geometrijski karakter faktorijalnosti prstena.

Neka je k algebarski zatvoreno polje i $A^n = \{\,(a_1, \ldots, a_n) \mid a_i \in k\,\}$ afini n-dimenzioni prostor nad k. Elemente prstena polinoma $A = k[x_1, \ldots, x_n]$ interpretiramo kao polinomne funkcije: $f \in A$ akko $f : A^n \to k$. Za podskup $I \subseteq k[x_1, \ldots, x_n]$ definišemo odgovarajući *afini algebarski skup, mnogostrukost*:

$$Z(I) = \{\,(a_1, \ldots, a_n) \in A^n \mid f(a_1, \ldots, a_n) = 0 \ \ \forall f \in I\,\}$$

Podskup I može se zameniti idealom koji on generiše. Kako je $A = k[x_1, \ldots, x_n]$ Neterin taj ideal je konačno generisan, pa je $Z(I) = Z(f_1, \ldots, f_n)$, za neke polinome $f_1, \ldots, f_n \in I$. Na A^n sada se može definisati topologija Zariskog, tako što se za zatvorene skupove uzimaju algebarski skupovi u A^n. Pri tome je algebarski skup V *ireducibilan* ako nije unija dva neprazna algebarska podskupa različita od V. Ireducibilne algebarske skupove zovemo *ireducibilnim mnogostrukostima.* Posebno, ako je $V = Z(f)$, gde je f (ireducibilan) polinom, mnogostrukost V je *(ireducibilna) hiperpovrš.* Obratno, za $X \subseteq A^n$ može se definisati ideal:

$$I(X) = \{\, f \in k[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \ \ \forall (a_1, \ldots, a_n) \in X \,\}$$

Restrikcije polinomnih funkcija sa A^n na X zovemo *regularnim* funkcijama na X. Ako identifikujemo polinomne funkcije jednake u svim tačkama iz X, dobijamo *koordinatni prsten* $A(X)$ skupa X:

$$A(X) = k[x_1, \ldots, x_n]/I(X)$$

Pri tome, X je ireducibilna mnogostrukost akko je $A(X)$ domen tj. akko je ideal $I(X)$ prost. Primenom poznate Hilbertove teoreme o nulama[5] pokazuje se da za ideal I prstena polinoma važi $I(Z(I)) = \sqrt{I}$, pa korespodencije $I \mapsto Z(I)$, $X \mapsto I(X)$ indukuju bijekcije medju algebarskim skupovima u A^n i radikalnim idealima u $k[x_1, \ldots, x_n]$. *Dimenzija* mnogostrukosti X definiše se kao dužina n najdužeg lanca $Y_0 \subsetneq Y_1 \subsetneq \cdots \subsetneq Y_n \subsetneq X$, gde su $Y_0, \ldots, Y_n$ ireducibilni. Može se pokazati da je $\dim(X) = \dim A(X)$, tj. da se dimenzija afinog algebarskog skupa poklapa sa Krulovom dimenzijom njegovog koordinatnog prstena. Takodje se može pokazati ([16]), da za domen B koji je konačno generisana k-algebra, i prost ideal $\mathfrak{p}$ u B važi:

$$\mathrm{ht}\,(\mathfrak{p}) + \dim B/\mathfrak{p} = \dim B \tag{9}$$

Jednoznačnost faktorizacije u prstenu polinoma $A = k[x_1, x_2, \ldots, x_n]$ daje puno značajnih tvrdjenja u algebarskoj geometriji. Najpre, koristeći faktorijalnost prstena A, može se pokazati da svaka mnogostrukost ima jednoznačnu dekompoziciju na ireducibilne podmnogostrukosti. Na taj način mnoga složena pitanja u vezi sa mnogostrukostima redukuju se na ispitivanje ireducibilnih mnogostrukosti. Pogledajmo ovu osobinu za hiperpovrši; neka je $Y = Z(f)$ hiperpovrš definisana polinomom $f \in A$. Kako je A UFD f ima dekompoziciju:

$$f = \prod_{i=1}^{n} f_i^{\alpha_i} \quad \text{gde su} \ \ f_i \ \ \text{ireducibilni i} \ \ \alpha_i \geq 1.$$

Hiperpovrši $Y_i = Z(f_i)$ definisane ireducibilnim polinomima f_i zovemo *ireducibilnim komponentama* hiperpovrši Y. Hiperpovrš Y biće jednaka njihovoj uniji,

$$Y = Y_1 \cup Y_2 \cup \cdots \cup Y_n \ ,$$

[5] Hilbert Nullstellensatz

dok je njen ideal glavni ideal:

$$I(Y) = (f_1 f_2 \dots f_n).$$

Dokaz poslednjeg tvrdjenja može se naći u [16, 19]. Pretpostavimo da hiperpovrš Y ima i drugu reprezentaciju ovog oblika:

$$Y = Y_1' \cup Y_2' \cup \dots \cup Y_m' \ ,$$

gde je $I(Y_j') = (g_j)$, za neke ireducibilne polinome $g_j \in A$. Tada je:

$$I(Y) = (f_1 f_2 \dots f_n) = (g_1 g_2 \dots g_m) \ ,$$

pa imamo jednakost glavnih ideala u $A = k[x_1, \dots, x_n]$. Odavde su $f_1 f_2 \dots f_n$ i $g_1 g_2 \dots g_m$ asocirani u A, tj.

$$f_1 f_2 \dots f_n = u g_1 g_2 \dots g_m \quad \text{za neko} \ \ u \in k^*.$$

Iz faktorijalnosti prstena polinoma mora biti $n = m$, odnosno $Y_i = Y_i'$ ako ignorišemo redosled. Ovim je dokazana sledeća teorema;

Teorema 6.4.1. *Svaka hiperpovrš Y ima, do na redosled, jednoznačnu reprezentaciju oblika*

$$Y = Y_1 \cup Y_2 \cup \dots \cup Y_n \quad , \quad Y_i \neq Y_j \ ,$$

gde su Y_i ireducibilne hiperpovrši. □

Teorema 6.4.2. *Neka je A Neterin faktorijalan domen i I pravi radikalan ideal u A. Tada su sledeća tvrdjenja ekvivalentna:*
(i) $\dim(A/\mathfrak{p}) = \dim(A) - 1$ *za svaki minimalan prost ideal* $\mathfrak{p}$ *nad* I.
(ii) I *je glavni ideal.*

Dokaz. $(i) \Rightarrow (ii)$: Neka je $\mathfrak{p}$ minimalan prost ideal nad I. Tada se iz jednakosti $\mathrm{ht}(\mathfrak{p}) + \dim(A/\mathfrak{p}) = \dim(A)$ i uslova (i) dobija $\mathrm{ht}(\mathfrak{p}) = 1$ tj. $\mathfrak{p} \in \mathcal{P}(A)$. Kako je A UFD, minimalni prosti ideali su glavni, pa je i $\mathfrak{p}$ glavni ideal. Prsten A je Neterin, pa nad idealom I ima samo konačno mnogo minimalnih prostih ideala $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ i svi su glavni, $\mathfrak{p}_i = (p_i)$. Tada je $I = \sqrt{I} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_n = (p_1 p_2 \dots p_n)$ glavni ideal.
$(ii) \Rightarrow (i)$: Neka je sada I glavni ideal generisan elementom a. Kako je A UFD element a ima prostu faktorizaciju $a = p_1 p_2 \dots p_n$. Tada su $\mathfrak{p}_i = (p_i)$ minimalni prosti ideali nad $I = (a)$, pa je iz Krulove glavnoidealske teoreme $\mathrm{ht}(\mathfrak{p}_i) = 1$, za $i = 1, 2, \dots, n$. Odavde se primenom jednakosti (9) dobija $\dim(A/\mathfrak{p}_i) = \dim(A) - 1$ za svaki minimalan prost ideal $\mathfrak{p}_i$ nad I. □

Posledica 6.4.3. *Neka je X mnogostrukost čiji je koordinatni prsten $A(X)$ UFD, i neka je $Y \subsetneq X$, $Y \neq \emptyset$ podmnogostrukost. Sve ireducibilne komponente mnogostrukosti Y imaju kodimenziju 1 u X akko je $I(Y)$ glavni ideal u $A(X)$.*

Dokaz. Neposredna primena prethodnog tvrdjenja. □

Tvrdjenje 6.4.4. *Ireducibilna mnogostrukost X je hiperpovrš u A^n akko je* $\dim(X) = n - 1$.

Dokaz. Neka je X hiperpovrš u A^n tj. $X = Z(f)$ za neki ireducibilan polinom $f \in k[x_1, \ldots, x_n]$ i neka je $\mathfrak{p} = I(X) = (f)$, prost ideal ove hiperpovrši. Prema Krulovoj glavnoidealskoj teoremi $\mathrm{ht}(\mathfrak{p}) = 1$ pa je: $\dim Z(f) = \dim A(Z(f)) = \dim A/I(Z(f)) = \dim A/(f) = \dim A - \mathrm{ht}(\mathfrak{p}) = n - \mathrm{ht}(\mathfrak{p})$.
Obratno, neka je sada $\dim(X) = n-1$. Tada je: $n-1 = \dim X = \dim A(X) = \dim A/I(X) = \dim A/\mathfrak{p} = \dim A - \mathrm{ht}(\mathfrak{p}) = n - \mathrm{ht}(\mathfrak{p})$. Odavde je $\mathrm{ht}(\mathfrak{p}) = 1$, pa mnogostrukosti X dimenzije $n-1$ odgovara odgovara minimalan prost ideal $\mathfrak{p} \in \mathcal{P}(A)$. Kako je $A = k[x_1, \ldots, x_n]$ UFD, $\mathfrak{p}$ je glavni ideal generisan nekim ireducibilnim polinomom $f \in A$ i $X = Z(f)$ je hiperpovrš u A^n. $\square$

Kako je afini koordinatni prsten $A(Y) = k[x_1, x_2, \ldots, x_n]/I(Y)$ Neterin, a Neterin domen je, prema teoremi 4.2.2, UFD akko su minimalni prosti ideali glavni, ova teorema imaće konkretan geometrijski smisao; minimalnom prostom idealu $\mathfrak{p} \in \mathcal{P}(A(Y))$ odgovara naime maksimalna ireducibilna podmnogostrukost $X \subseteq Y$. Na taj način, kombinujući prethodna tvrdjenja, dobija se sledeća teorema:

Teorema 6.4.5 (geometrijski smisao jednoznačne faktorizacije)**.**
Koordinatni prsten ireducibilne mnogostrukosti je UFD akko je svaka ireducibilna podmnogostrukost kodimenzije 1 *definisana glavnim idealom.* $\square$

U vezi sa ovim kažemo da je ireducibilna mnogostrukost Y u projektivnom prostoru $\mathbf{P}^n$ *kompletan presek* ako se njen ideal $I(Y)$ može generisati sa $codim(Y)$ elemenata, gde je $codim(Y) = n - dim(Y)$. U tom slučaju Y se može predstaviti kao presek $codim(Y)$ hiperpovrši. Teorema 6.4.5 može se sada formulisati i u sledećem obliku: $A(Y)$ je UFD akko je svaka maksimalna ireducibilna podmnogostrukost kompletan presek.

Primer 6.4.6.

$$A(Y) = \mathbb{C}[x, y, z, t]/(f) \quad , \quad f = xy - zt$$

Kvadrika $xy = zt$ je ireducibilna u projektivnom prostoru $\mathbf{P}^3$ jer je (f) prost ideal. S druge strane, od ranije je poznato da $A(Y)$ nije faktorijalan, što prema prethodnoj teoremi znači da na Y postoji kriva koja se ne može definisati jednom jednačinom. ▼
U vezi sa ovim može se pogledati sledeći primer [12]; afina kriva $Y \subseteq A^3$ zadata parametarski sa $x = t^3$, $y = t^4$, $z = t^5$ nije kompletan presek. Njen ideal $I(Y)$ je prost u $k[x, y, z]$ i $\mathrm{ht}(I(Y)) = 2$, medjutim on se ne može generisati sa dva elementa. Minimalan broj generatora za $I(Y)$ zapravo je jednak 3; $I(Y) = (x^2y - z^2, xz - y^2, x^3 - yz)$. Rešenje ovog i sličnih pitanja vezanih za kompletne preseke može se naći u [16]. Razmatra se naime nešto opštiji problem, u klasi prostornih afinih krivih datih parametarski:

$$x = t^m \ , \ y = t^n \ , \ z = t^p \quad \text{gde je} \quad \mathrm{nzd}(m, n, p) = 1 \ ,$$

eksplicitno se odredjuju kompletni preseci.

Iz prethodnog se jasno vidi kakve posledice faktorijalnost prstena ima u algebarskoj geometriji. Medjutim moguć je i obratan proces: geometrijskim metodama može se dokazati faktorijalnost nekih prstena. Za lokalan prsten A kažemo da je *kompletan presek* ako je $A \cong R/I$, gde je R regularan lokalan prsten i I ideal generisan regularnim R-nizom. Ako je $A_{\mathfrak{p}}$ UFD za sve proste ideale $\mathfrak{p}$ u A takve da je $\mathrm{ht}(\mathfrak{p}) \leq 3$, onda je i A UFD. Ovu teoremu dokazao je Grothendieck koristeći teoriju shema u algebarskoj geometriji, dok čisto algebarski dokaz nije poznat. Primenom ovog tvrdjenja može se dobiti sledeći rezultat (Lefshetz): Neka je $Y \subseteq \mathbf{P}^n$ nesingularna afina ireducibilna mnogostrukost takva da je $dim(Y) \geq 3$. Ako se ideal $I(Y)$ može generisati sa $codim(Y)$ generatora (kompletan presek), onda je $A(Y)$ UFD.
Od ostalih rezultata iz ove oblasti najzanimljivija je teorema Brieskorna. Koristeći istu tehniku kao i Grothendieck, Brieskorn je 1967. dokazao da medju kompletnim lokalnim prstenima dimenzije 2 nad algebarski zatvorenim poljem k ima svega dva faktorijalna: regularni prsten formalnih redova $k[[X, Y]]$ i prsten $k[[X, Y, Z]]/(X^2 + Y^3 + Z^5)$.

Glava 7

Faktorizacija u nekomutativnim prstenima

Polazeći od uobičajene definicije komutativnog faktorijalnog domena, isticanjem osobina **A1** i **A2**, atomičnosti i jednoznačnosti, videli smo da se komutativan UFD može definisati i na druge načine, pronalaženjem ekvivalenata ovih uslova ili u terminima njegove grupe valuacija, odnosno grupe divizor klasa. Ako pokušamo da neke od ovih definicija prenesemo na nekomutativne prstene dolazimo do raznih problema. Najpre, sam uslov **A2** implicitno podrazumeva komutativnost jer elementi faktorizacije $up_1p_2 \dots p_n$ mogu medjusobno da menjaju mesta. Takodje sam pojam deljivosti ovde podrazumeva levu ili desnu deljivost, pa se iz tog razloga ni definicija prostog elementa ne može preneti na nekomutativan slučaj bez odredjenih izmena. Ovo već ukazuje da je u nekomutativnim domenima faktorizacija dosta komplikovaniji pojam, pa i samo njeno definisanje iziskuje drugi pristup. Osnovni zahtev pri definisanju nekomutativnog UFD-a sastoji se u tome da dobijemo izvesnu generalizaciju komutativnih UFD domena, tj. da se restrikcijom na komutativan slučaj dobiju komutativni faktorijalni domeni.

7.1 Definicija nekomutativnog UFD-a

U skladu sa uvodnim napomenama, postoji nekoliko načina za definisanje faktorizacije u nekomutativnom domenu: *metod UF monoida, metod mreža i metod stroge faktorizacije*[1]. Da bi razmotrili svaki od ovih metoda potrebno je najpre uvesti neke osnovne pojmove u teoriji nekomutativnih prstena. Uvodimo zato sledeće oznake i definicije; prsten R biće nekomutativan bez delitelja nule, dakle domen, i $R^\times$ svi njegovi nenulti elementi. Element $u \in R$ je invertibilan ako postoji $u^{-1} \in R$ t.d. $uu^{-1} = u^{-1}u = 1$; grupu svih invertibilnih elemenata označavamo sa $U(R)$. Element a je *ireducibilan* ili *atom* ako nije invertibilan i

[1] Restrikcija ovog metoda na komutativne prstene ne daje sve UFD domene, već samo DVR prstene.

nije proizvod neinvertibilnih. Elementi $a, b \in R$ su *desno (levo) asocirani*, ako je $a = bu$ $(a = ub)$, za neko $u \in R$; ako je $a = ubv$, gde su $u, v \in U(R)$, kažemo da su elementi a i b *asocirani*; posebno, ako je $v = u^{-1}$ elementi a i b su *konjugovani*. Za faktorizaciju $a_1 a_2 \dots a_n$ kažemo da je *prava* ako su svi faktori neinvertibilni, odnosno da je *kompletna* ako su svi faktori atomi. Ako postoje $a', b' \in R$ takvi da je:

$$ab' = ba' \neq 0 \qquad (i)$$

kažemo da su a i b *desno proporcionalni*. Relacije tipa (i) imaju bitnu ulogu u nekomutativnim prstenima jer na neki način odredjuju uslovnu komutativnost ovih elemenata. Ako je $aR + bR = R$ elementi a i b su *desno komaksimalni*. S druge strane, ako su jedini zajednički desni faktori za a i b invertibilni, onda su a i b *desno koprosti* elementi. Analogne definicije važe za levu stranu. Za relaciju

$$ab' = ba'$$

kažemo da je *komaksimalna* ako je $aR + bR = R$ i $Ra' + Rb' = R$, odnosno da je *koprosta* ako su a, b levo koprosti i a', b' desno koprosti. Iz definicije neposredno sledi da je svaki komaksimalan odnos ujedno i koprost. Za faktorizaciju su posebno važni moduli tipa R/aR; za elemente a i b domena R kažemo da su *desno slični*, ako

$$R/aR \cong R/bR\,, \qquad (ii)$$

kao desni R-moduli. Može se pokazati da je ova definicija levo-desno simetrična, odnosno da iz (ii) sledi $R/Ra \cong R/Rb$ i obratno, pa levo (desno) slične elemente zovemo prosto sličnim. Uslovi kidanja lanaca ACC i ACC_1 definišu se isto kao u komutativnom slučaju, s tim što se posmatraju lanci desnih, odnosno levih ideala i u skladu s tim definiše se levi ili desni Neterin domen. Lokalizacija u nekomutativnim domenima moguća je samo kada skup po kome lokalizujemo zadovoljava *Ore-ov uslov*; podmonoid T monoida S je desni Ore-ov skup ako važi uslov $sT \cap tS \neq \emptyset$, za sve $s \in S$, $t \in T$. Posebno, u slučaju da je:

$$aR \cap bR \neq 0 \quad \text{za sve } a, b \in R^{\times} \qquad (iii)$$

kažemo da je R *desni Ore-ov domen*. Lako se pokazuje da svaki desni Neterin domen zadovoljava uslov (iii), t.j. da je svaki desni Neterin domen i desni Ore-ov.

Metod UF-monoida. Ovaj metod sastoji se u prostoj reinterpretaciji rezultata iz komutativne algebre njihovim uopštenjem na nekomutativan slučaj. Da bi se to postiglo osnovne pojmove bitne za faktorizaciju, pre svega pojam deljivosti, treba prilagoditi nekomutativnim domenima dajući im nešto generalniju formu. U Glavi 3 već je rečeno da je komutativan monoid sa kraćenjem S, UF-monoid akko je njegov asocirani konični monoid S/U slobodan komutativan kao i da je komutativan domen UFD akko njegovi nenulti elementi formiraju UF-monoid u odnosu na množenje. Ovaj rezultat ne može se medjutim proširiti na nekomutativne domene bez odredjenih izmena. Definišemo zato *invarijantan* element nekomutativnog monoida S, kao element $a \in S$ koji zadovoljava uslov:

$$aS = Sa \qquad (iv)$$

Monoid S je invarijantan ako su svi njegovi elementi invarijantni[2]. Ako su sada a i b elementi invarijantnog monoida S i ako $b \mid a$ sleva, tj. $a = bc$ za neko $c \in S$, onda je prema uslovu (iv) $bc = c_1 b$, za neko $c_1 \in S$ pa $b \mid a$ zdesna. Na taj način pojmovi leve i desne deljivosti u invarijantnom monoidu su ekvivalentni, uredjenja monoida u odnosu na levu i desnu deljivost se poklapaju, pa možemo postupiti isto kao u komutativnom slučaju i definisati prost element p invarijantnog monoida S kao element koji zadovoljava uslov:

$$p \mid ab \Rightarrow p \mid a \vee p \mid b \qquad (v)$$

Iz uslova (iv) takodje sledi da se u invarijantnom monoidu levi i desni uslovi kidanja lanaca glavnih ideala poklapaju, pa govorimo prosto o uslovu ACC_1 kao i u komutativnim monoidima. Posebno je svaki invarijantan monoid u kome važi uslov ACC_1 i atomičan, što će slediti iz naredne leme.

Lema 7.1.1. *Svaki domen u kome važi levi i desni uslov ACC_1 je atomičan.*

Dokaz. Neka je $a \in R^\times$ neinvertibilan. To znači da je $aR \neq R$, pa prema desnom uslovu ACC_1 postoji maksimalan desni ideal $p_1 R$, gde je p_1 atom, takav da je $aR \subseteq p_1 R \subsetneq R$. Odavde je $a = p_1 a_1$, za neko $a_1 \in R$, što posebno znači da je i $a \in Ra_1$. Ako a_1 nije invertibilan ovaj postupak može se ponoviti, pa dobijamo $a_1 = p_2 a_2$, za neko $a_2 \in R$ i još je $a_1 \in Ra_2$ i p_2 je atom. Jasno je da se na ovaj način dobija strogo rastući lanac $Ra \subseteq Ra_1 \subseteq Ra_2 \subseteq \ldots$, levih glavnih ideala, koji se prema levom ACC_1 uslovu prekida, pa je svaki neinvertibilan element u R proizvod atoma tj. R je atomičan. $\square$
Osim prostih elemenata i uslova ACC_1 u invarijantnom monoidu može se za par elemenata $a, b \in S$ na isti način kao i u komutativnim monoidima definisati $\mathrm{nzd}[a, b], \mathrm{nzs}[a, b]$, što za posledicu daje poznatu teremu o komutativnim UFD domenima.

Teorema 7.1.2. *U invarijantnom monoidu sa kraćenjem S sledeći uslovi su ekvivalentni:*
(1) *S je UF-monoid.*
(2) *S zadovoljava uslov ACC_1 i svaka dva elementa imaju* nzd.
(3) *S zadovoljava uslov ACC_1 i svaka dva elementa imaju* nzs.
(4) *S zadovoljava uslov ACC_1 i presek glavnih ideala je glavni ideal.*
(5) *S je atomičan i svaki atom je prost.*

Sa malim modifikacijama dokaz ove teoreme izvodi se isto kao i u komutativnom slučaju i može se naći u [6]. Može se reći da je primena ove teoreme na nekomutativan domen R ipak ograničena samo na one domene kod kojih je $R^\times$ invarijantan monoid sa kraćenjem. Zbog toga se uvodi opštiji pojam *invarijantnog elementa domena* R, kao elementa $a \in R$ koji zadovoljava uslov:

$$aR = Ra \qquad (vi)$$

[2]U komutativnom slučaju ova definicija gubi smisao, jer su svi komutativni monoidi očigledno invarijantni.

Skup svih invarijantnih elemenata domena R, u oznaci $I(R)$, uvek je invarijantan monoid sa kraćenjem, pa se prethodna teorema uz male korekcije može primeniti na $I(R)$. Pre svega, ako prost element domena R definišemo kao invarijantan neinvertibilan element koji zadovoljava uslov (v), onda je skup prostih elemenata $\mathcal{P}(R) \subseteq I(R)$. Proste elemente monoida $I(R)$ zovemo *I-prostim* dok atome u $I(R)$ zovemo *I-atomima*. Prema definiciji svaki prost (atom) je i I-prost (I-atom), dok obratno ne mora da važi. Ako je $I(R)$ UF-monoid kažemo da je R domen sa jednoznačnom faktorizacijom invarijantnih elemenata. Prema prethodnoj teoremi to će važiti akko R zadovoljava uslov ACC na invarijantnim glavnim idealima i svaka dva invarijantna elementa imaju nzd (nzs) u $I(R)$, odnosno akko je $I(R)$ atomičan i svaki I-atom je I-prost. Svaki atomičan 2-fir zadovoljava ove uslove ([6]), pa je u ovim prstenima faktorizacija invarijantnih elemenata jednoznačna.
Još jedna bitna osobina ovog pristupa ogleda se u mogućnosti lokalizacije. Naime, proizvoljan podmonoid T invarijantnog monoida sa kraćenjem S je desni Ore-ov skup, pa postoji i odgovarajuća lokalizacija S_T. Uz male izmene možemo sada dobiti Nagatinu teoremu za nekomutativne domene.

Teorema 7.1.3. *Neka je S invarijantan atomičan monoid sa kraćenjem i T njegov podmonoid generisan prostim elementima koji sadrži sve jedinice iz S. Ako je S_T UF-monoid onda je to i S.*

Ako sada za monoid S uzmemo $I(R)$ i proste elemente zamenimo I-prostim, dobija se odgovarajuća teorema za nekomutativne domene, dok se u slučaju komutativnog domena R dobija Nagatina teorema 2.3.1.

Metod mreže. Definisanje pojma jednoznačne faktorizacije u nekomutativnom domenu R pomoću UF-monoida ima bitni nedostatak. Ovim pristupom može se naime utvrditi samo faktorijalnost invarijantnih elemenata iz $I(R)$, dok se ništa ne može reći za njegove ostale elemente. U tom smislu metod mreža daje opštiju definiciju. Neka je sada R nekomutativan domen i $c, d \in R^\times$ sa nekim faktorizacijama:

$$c = a_1 a_2 \dots a_m \tag{1}$$

$$d = b_1 b_2 \dots b_n \tag{2}$$

Faktorizaciji (1) možemo pridružiti niz glavnih desnih ideala:

$$R \supseteq a_1 R \supseteq a_1 a_2 R \supseteq \dots \supseteq a_1 a_2 \dots a_m R = cR\,,$$

i odgovarajući niz faktormodula:

$$R/a_1 R\,,\ R/a_2 R \cong a_1 R/a_1 a_2 R\,,\ \dots\ ,\ R/a_m R$$

Naravno, isto važi i za faktorizaciju (2) sa odgovarajućim nizom faktormodula: $R/b_1 R\,,\ R/b_2 R\,, \dots\ ,\ R/b_n R$. Za faktorizacije (1) i (2) kažemo da su *izomorfne* ako je $m = n$ i postoji permutacija $i \mapsto i'$ skupa $\{1, 2, \dots, m\}$, tako da je $R/a_i R \cong R/b_{i'} R$, tj. ako je $a_i \sim b_{i'}$. Očigledno je da za ovako definisan

izomorfizam faktorizacija nema posebnog značaja da li posmatramo desne faktore R/a_iR ili leve R/Ra_i, drugim rečima definicija je levo-desno simetrična, i ova činjenica zove se *dualnost faktorizacije*. Sada možemo dati opštu definiciju nekomutativnog UFD domena.

Definicija 7.1.4. *Nekomutativan domen R je UFD ako je atomičan i svaka dva kompletna razlaganja elementa iz $R^\times$ su izomorfna.*

Restrikcija ove definicije na komutativan slučaj daje poznatu definiciju komutativnog UFD domena. Zaista, ako je domen R komutativan onda se pri izomorfizmu $R/aR \cong R/bR$ element $b + aR$ slika u nulu, pa $b + aR = aR$ tj. $b \in aR$. Odavde je $bR \subseteq aR$ i iz simetrije $aR \subseteq bR$, pa mora biti $aR = bR$, što znači da su elementi a i b asocirani. Obratno, ako je $aR = bR$, onda je očigledno i $R/aR \cong R/bR$. To posebno znači da se pojam sličnosti u komutativnom slučaju svodi na asociranost i definicija 7.1.4 se svodi na polaznu definiciju komutativnog UFD-a, atomičnog domena u kome je faktorizacija jednoznačna do na redosled faktora i množenje invertibilnim elementima. Sličnost u nekomutativnom slučaju je medjutim dosta komplikovaniji pojam, pa je poželjno imati što više kriterijuma za proveru. Neki od tih kriterijuma dati su sledećom lemom čiji se dokaz može naći u [6].

Lema 7.1.5. *Za elemente a, a' domena R sledeći uslovi su ekvivalentni:*
(a) $a \sim a'$
(b) Postoje $b, c' \in R$ *takvi da* $aR + bR = R$, $aR \cap bR = ba'R$ *i* $1 + c'b \in a'R$.
(c) Postoji $b \in R$ *takav da je* $aR + bR = R$ *i* $a'R = \{\, x \in R \mid bx \in aR \,\}$.
(d) Postoje matrice $\mu, \nu \in M_2(R)$ *takve da je:*

$$\mu = \begin{pmatrix} a & b \\ * & * \end{pmatrix}, \quad \nu = \begin{pmatrix} * & * \\ * & a' \end{pmatrix}, \quad \mu\nu = \begin{pmatrix} 1 & 0 \\ * & * \end{pmatrix}, \ \nu\mu = \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$$

(e) Postoje medjusobno inverzne matrice μ, $\mu^{-1} \in M_2(R)$ *oblika*

$$\mu = \begin{pmatrix} a & * \\ * & * \end{pmatrix}, \ \mu^{-1} = \begin{pmatrix} * & * \\ * & a' \end{pmatrix} \quad \square$$

Pored prednosti, definicija 7.1.4 ima i svoje nedostatke. Ako su p i q proizvoljni atomi nekomutativnog UFD-a koji medjusobno ne komutiraju, faktorizacije $a = pq$ i $b = qp$ su očigledno jednoznačne u smislu ove definicije, dok su elementi a i b potpuno različiti. Jednoznačna faktorizacija može se medjutim i strože definisati uvodjenjem pojma strogog domena.

Metod stroge faktorizacije. Element c domena R je *strog* ako:

$$c = ab' = ba' \ \Rightarrow \ aR \subseteq bR \ \vee \ bR \subseteq aR \qquad (vii)$$

Domen R je strog ako je svaki element $c \in R^\times$ strog, drugim rečima, ako je mreža $\mathbf{L}(cR, R)$ lanac. Posebno, ako je R komutativan domen, iz uslova (vii) vidimo da je R valuacioni, pa su strogi komutativni domeni upravo valuacioni domeni.

Definicija 7.1.6. *Nekomutativan prsten R je strogi UFD ako je atomičan strog domen.*

Može se pokazati da za ovako definisan strogi UFD R postoji jedinstven atom $p \in R$ takav da je svaki desni (levi) ideal u R dvostrani, oblika $Rp^n = p^nR$. Medjutim komutativan valuacioni domen je UFD akko je DVR, pa definicija 7.1.6 ne uključuje sve komutativne UFD domene već samo diskretne valuacione prstene. U tom smislu, definicija 7.1.4 je bolja, pa dalje pod nekomutativnim UFD domenom podrazumevamo domen R definisan sa 7.1.4.

7.2 Faktorizacija u prstenima slobodnih ideala

Pri razmatranju različitih pitanja vezanih za faktorizaciju u nekomutativnim prstenima od posebnog interesa su prsteni u kojima su svi ideali, posmatrani kao R-moduli, slobodni jedinstvenog ranga. Takav prsten zovemo *fir*-om. Ovi prsteni predstavljaju generalizaciju glavnoidealskih domena, naime komutativan domen R je glavnoidealski akko je svaki ideal u R slobodan kao R-modul (ako bi postojao ideal I u R sa bazom od dva različita elementa $a, b \in R$ onda je iz komutativnosti $ab - ba = 0$ netrivijalna relacija, što je u kontradikciji sa pretpostavkom da je (a, b) baza modula I). Ako su svi desni (levi) ideali u R slobodni, jedinstvenog ranga, prsten R je *desni (levi) fir*. Ako su svi desni (levi) ideali sa najviše n generatora u R slobodni, jedinstvenog ranga, prsten R je *desni (levi) n-fir*. Ako su svi konačno generisani ideali u R slobodni, jedinstvenog ranga, tj. ako je R n-fir za svako n, prsten R je *semifir*. Iz definicije neposredno sledi da je n-fir i m-fir za svako $m < n$, kao i da je 1-fir prsten bez delitelja nule, tj. domen. Klasa 2-firova posebno je važna za pitanja faktorijalnosti, kao i za druga bitna pitanja; izmedju ostalog, u komutativnom slučaju ova klasa sadrži sve semifirove. Postoji više ekvivalentnih uslova kojima se može definisati desni n-fir ([6],teorema 1.1), od kojih se sledeća dva često koriste:
(α) R je desni n-fir akko za svaki desni ideal u R generisan sa $m \leq n$ linearno zavisnih elemenata postoji familija od $k < m$ generatora.
(β) R je desni n-fir akko za svaki homomorfizam $\varphi : R^m \to F$, gde je F slobodni desni R-modul i $m \leq n$, postoji ceo broj $r \leq m$ i izomorfizmi μ , ν takvi da dijagram (1) komutira:

$$\begin{array}{ccccc} \operatorname{Ker}\varphi & \longrightarrow & R^m & \longrightarrow & \operatorname{Im}\varphi \\ \downarrow{\scriptstyle \mu_1} & & \downarrow{\scriptstyle \mu} & & \downarrow{\scriptstyle \nu} \\ R^r & \xrightarrow{i} & R^r \oplus R^s & \xrightarrow{\pi} & R^s \end{array} \tag{1}$$

gde je $r + s = m$ i preslikavanja i , π , μ_1 su redom prirodna inkluzija, projekcija i restrikcija izomorfizma μ.

Lema 7.2.1 (Rang formula u n-firu)**.** *Neka je R n-fir i A, B podmoduli slobodnog R-modula takvi da se $A \oplus B$ može generisati sa n elemenata. Tada se tačan niz*

$$0 \longrightarrow A \cap B \longrightarrow A \oplus B \longrightarrow A + B \longrightarrow 0 \tag{2}$$

cepa, svi moduli u (2) *su slobodni, jedinstvenog ranga i važi formula*

$$\rho(A+B)+\rho(A\cap B)=\rho(A)+\rho(B) \tag{3}$$

Dokaz. Neposredna posledica uslova (β), jer preslikavanje $(a,b)\mapsto a-b$ definiše homomorfizam $A\oplus B\to A+B$, sa jezgrom $A\cap B$. $\square$

Primena uslova $(\alpha),(\beta)$ *na* 2*-firove.* Ako su a i b linearno zavisni elementi, $ab'-ba'=0$, tj. $aR\cap bR\neq 0$, onda je prema uslovu (α) ideal $aR+bR$ generisan jednim elementom. Dakle:

$$aR\cap bR\neq 0 \;\Rightarrow\; aR+bR=dR \quad ,\ \text{za neko}\ \ d\in R \tag{4}$$

Odavde, možemo dati novu karakterizaciju 2-fira:

Teorema 7.2.2. *R je* 2*-fir akko je domen u kome je suma glavnih desnih ideala koji imaju nenulti presek takodje glavni desni ideal*[3]. $\square$

Neka je sada R 2-fir i $aR\,,\,bR$ glavni desni ideali takvi da je $aR\cap bR\neq 0$. Ako prethodnu lemu primenimo na niz:

$$0\longrightarrow aR\cap bR\longrightarrow aR\oplus bR\longrightarrow aR+bR\longrightarrow 0\,,$$

dobijamo da su $aR\cap bR$ i $aR+bR$ slobodni desni ideali i prema jednakosti (3) je $\rho(aR\cap bR)+\rho(aR+bR)=2$, pa je $\rho(aR\cap bR)=\rho(aR+bR)=1$, tj. oni su glavni.

Posledica 7.2.3. *Presek glavnih desnih ideala u* 2*-firu je glavni desni ideal.* $\square$

Ako je sada R 2-fir, $c\neq 0$ proizvoljan element i $\mathbf{L}(cR,R)$ skup svih glavnih desnih ideala u R koji sadrže c, onda $aR\,,\,bR\in\mathbf{L}(cR,R)$ imaju nenulti presek, i on je glavni ideal, prema 7.2.3. Zadovoljen je i uslov (4) pa je i njihov zbir dakle glavni ideal, št posebno znači da je $\mathbf{L}(cR,R)$ podmreža mreže svih desnih ideala $Lat_R(R_R)$ i kao takva je modularna tj. za $xR\,,yR\,,zR\in\mathbf{L}(cR,R)$ važi:

$$xR\subseteq zR\;\Longrightarrow\; xR+(yR\cap zR)=(xR+yR)\cap zR\,, \tag{5}$$

što zajedno sa prethodniom rezultatima za posledicu daje sledeću karakterizaciju 2-firova;

Teorema 7.2.4. *Za domen R sledeća tvrdjenja su ekvivalentna:*
(1) *R je* 2*-fir.*
(2) *Za $a,b\in R^\times$ važi: $aR\cap bR=mR$, za neko $m\in R$, dok je $aR+bR$ glavni akko je $m\neq 0$.*
(3) *Za $c\in R^\times$ $\mathbf{L}(cR,R)$ je podmreža mreže svih desnih ideala $Lat_R(R_R)$.*
(4) *Zbir dva glavna desna ideala sa nenultim presekom je glavni desni ideal.* $\square$

[3]Uslov (4) može se iskazati i u levoj formi (4′): $Ra\cap Rb\neq 0\Rightarrow Ra+Rb=Rd$. To posebno znači da se ova teorema može formulisati i u terminima levih ideala. Odavde je pojam 2-fira levo-desno simetričan i mada je njegova definicija data pomoću desnih ideala, govorimo prosto o 2-firu.

Ako se u uslovu (2) prethodne teoreme ispusti uslov $m \neq 0$, dobija se klasa *desnih Bezuovih domena;* to su domeni u kojima svaka dva elementa generišu glavni desni ideal ili ekvivalentno, domeni u kojima je svaki konačno generisan desni ideal glavni. Upravo zbog toga za 2-fir se nekad koristi i termin *slabi Bezuov domen*. Analogno se definiše i levi Bezuov domen uz napomenu da simetrija ne važi, tj. može se naći primer levog Bezuovog domena koji nije i desni. Levi i desni Bezuov domen zovemo prosto Bezuovim domenom; veza Bezuovih i slabih Bezuovih domena data je tvrdjenjem ([6]): R je desni Bezuov domen akko R je 2-fir i desni Oreov domen.

Komaksimalna relacija

$$ab' = ba'$$

uvek je koprosta, dok u 2-firu važi i obratno. Ako je $ab' = ba' \neq 0$ koprosta relacija onda iz $aR \cap bR \neq 0$ sledi da su i sume $aR + bR$, $Ra' + Rb'$ neki glavni ideali dR, Rd'. Kako su a, b levo, odnosno a', b' desno koprosti, mora biti $aR + bR = R$ i $Ra' + Rb' = R$, pa je relacija $ab' = ba'$ komaksimalna. Ovim je dokazana sledeća lema.

Lema 7.2.5. *Relacija $ab' = ba'$ u 2-firu je koprosta akko je komaksimalna.* □

Kombinujući ovaj rezultat sa kriterijumom sličnosti 7.1.5, dobijamo kao posledicu sledeći kriterijum sličnosti u 2-firu.

Posledica 7.2.6. *Elementi a, a' 2-fira R su slični akko postoji koprosta relacija $ab' = ba'$ za neke $b, b' \in R$.* □

Jednoznačna faktorizacija u 2-firu u suštini se svodi na proučavanje osobina mreže glavnih ideala $\mathbf{L}(cR, R)$ pa zato koristimo sledeće dve klasične teoreme iz teorije mreža;

Teorema 7.2.7 (Schreier)**.** *U modularnoj mreži svaka dva konačna lanca sa istim krajevima imaju izomorfna profinjenja.* □

Teorema 7.2.8 (**Jordan – Hölder**)**.** *U modularnoj mreži konačne dužine svaki lanac može se profiniti do maksimalnog lanca, i svaka dva maksimalna lanca su izomorfna.* □

Mreža podmodula datog modula uvek je modularna pa se ovi rezultati mogu interpretirati na sledeći način; neka su dati konačni lanci

$$\mathcal{L}: \quad A_1 \subseteq A_2 \subseteq \cdots \subseteq A_k \subseteq M$$

$$\mathcal{L}': \quad B_1 \subseteq B_2 \subseteq \cdots \subseteq B_l \subseteq M$$

podmodula modula M. Lanac $\mathcal{L}'$ zovemo *profinjenjem* lanca $\mathcal{L}$ a $\mathcal{L}$ *podlancem* lanca $\mathcal{L}'$ ako $\mathcal{L}$ dobijamo iz $\mathcal{L}'$ izbacivanjem nekih od podmodula B_j. Lanci $\mathcal{L}$ i $\mathcal{L}'$ su *izomorfni* ako je $k = l$ i postoji pesmutacija δ skupa indeksa takva da je $A_{i+1}/A_i \cong B_{\delta(i)+1}/B_{\delta(i)}$, $i = 1, \ldots, k-1$. Faktormoduli A_{i+1}/A_i su *faktori* lanca $\mathcal{L}$. Ako su svi faktori A_{i+1}/A_i prosti moduli, što je ekvivalentno sa uslovom da je A_i maksimalan podmodul u A_{i+1}, onda je lanac $\mathcal{L}$ *kompozicioni red* modula

M. Modul je konačne dužine ako ima kompozicioni red. Teorema 7.2.7 kaže da lanci $\mathcal{L}$ i $\mathcal{L}'$ imaju izomorfna profinjenja, dok teorema 7.2.8 kaže da se svaki lanac $\mathcal{L}$ može profiniti do kompozicionog reda i da su svaka dva kompoziciona reda modula izomorfna. Definicija 7.1.4 je prema tome sledeća interpretacija Žordan-Helderove teoreme i ujedno daje zgodan kriterijum za proveru faktorijalnosti prstena.

Teorema 7.2.9. *Domen R je UFD ako za svako $c \in R^\times$ skup $\mathbf{L}(cR, R)$ svih glavnih desnih ideala u R koji sadrže c predstavlja modularnu mrežu konačne dužine.* □

Uslove ove teoreme ispunjava svaki glavnoidealski domen[4]. Najpre, ako je $c \in R^\times$, onda je $\mathbf{L}(cR, R)$ očigledno jedna modularna mreža, jer su za $aR \supseteq cR$ i $bR \supseteq cR$ ideali $aR \cap bR$ i $aR + bR$ glavni. Konačnost ove mreže posledica je *principa dualnosti* u teoriji mreža; ako je $L(\leq, \sup, \inf)$ mreža onda je dualno i $L(\geq, \inf, \sup)$ takodje mreža pa se svaka teorema u mreži može dualizovati. U slučaju glavnoidealskog domena R desni uslov ACC važi jer je svaki desni ideal konačno generisan. S druge strane, kako važi i levi uslov ACC, dualno važi desni DCC uslov, tj. posmatrana mreža je konačne dužine. Ova razmatranja možemo formulisati u obliku sledeće teoreme.

Teorema 7.2.10. *Glavnoidealski domen je UFD.* □

Sada se možemo vratiti na definiciju nekomutativnog UFD-a 7.1.4 u slučaju atomičnog 2-fira R. Neka je $c \in R^\times$ proizvoljan element. Prema 7.2.4, skup $\mathbf{L}(cR, R)$ svih glavnih desnih ideala koji sadrže c je modularna mreža. Ova mreža je, uz pretpostavku atomičnosti, i konačne dužine, pa se na nju može primeniti teorema 7.2.8. Svakom atomičnom razlaganju odgovara maksimalan lanac, a svaka dva maksimalna lanca su prema ovoj teoremi izomorfna, što znači da su i proizvoljna dva atomična razlaganja elementa c izomorfna, odnosno R je UFD u smislu definicije 7.1.4. Ovim je dokazana sledeća teorema.

Teorema 7.2.11. *Atomičan 2-fir je UFD*[5]. □

Firovi u opštem slučaju nisu Neterini domeni ali imaju sličnu osobinu; uslovi kidanja lanaca u $\aleph_0$-firu važe na n-generisanim idealima ([6]). Koristeći ovu osobinu i lemu 7.1.1, dobija se da je svaki $\aleph_0$-fir (levi i desni) atomičan. Kako je svaki fir očigledno i 2-fir, teorema 7.2.11 daje sledeću posledicu;

Posledica 7.2.12. *Svaki levi i desni fir je UFD.* □

U komutativnom slučaju atomičan 2-fir je glavnoidealski domen pa se teorema 7.2.11 i posledica 7.2.12 svode na poznatu teoremu da su glavni komutativni domeni faktorijalni. Što se tiče veze 2-firova i strogo faktorijalnih domena, ona je data sledećom teoremom čiji se dokaz može naći u [6].

[4]Domen u kome su svi levi i desni ideali glavni.

[5]Svaki glavnoidealski domen je atomičan 2-fir, pa je teorema 7.2.10 neposredna posledica ove teoreme.

Teorema 7.2.13. *Prsten R je strogi UFD akko je atomičan 2-fir i lokalan prsten.* □

Pri definisanju komutativnog faktorijalnog domena videli smo da se uslovi atomičnosti i jednoznačnosti mogu odvojeno posmatrati i ti uslovi bili su označeni sa **A1** i **A2**. Ako isto postupimo i u nekomutativnom slučaju, odnosno ako oslabimo uslov definicije 7.1.4, ispuštajući uslov atomičnosti, dobijamo širu klasu prstena u kojima su svake dve atomične faktorizacije nekog elementa izomorfne u smislu ove definicije. Za faktorizaciju

$$c = a_1 a_2 \dots a_m \tag{1'}$$

kažemo da je *profinjenje* faktorizacije

$$c = b_1 b_2 \dots b_n \tag{2'}$$

ako se $(1')$ može dobiti iz $(2')$ daljim razlaganjem elemenata b_j.

Definicija 7.2.14. *Domen R u kome svake dve faktorizacije elementa $c \in R^\times$ imaju izomorfna profinjenja zovemo Šrajerovim ili kraće S-prstenom.*

Ako je sada R UFD onda iz atomičnosti svaki od faktora a_i, b_j faktorizacija $(1')$ i $(2')$ možemo razložiti u proizvod atoma. Da bi se dobile jednake dužine ovih faktorizacja možemo ubaciti i potreban broj invertibilnih faktora, pa su profinjenja dobijena na ovaj način su izomorfna, odnosno svaki UFD je S-prsten. Iz modularnosti mreže $\mathbf{L}(cR, R)$ u 2-firu i Šrajerove teoreme za modularne mreže dobija se posebno da klasi S-prstena pripadaju i svi 2-firovi.

Izmedju UFD domena i S-prstena postoji i medjuklasa takozvanih HCF-prstena, kojima u komutativnom slučaju odgovaraju Gausovi domeni. U terminima grupe valuacija $G(R)$, tj. grupe $\mathcal{P}^*$ glavnih razlomljenih ideala, komutativan domen R je faktorijalan akko je $G(R)$ slobodna abelova grupa, dok je R Gausov akko je uredjenje na $\mathcal{P}^*$ mrežasto. Ovaj rezultat ne može se medjutim proširiti na nekomutativan slučaj jer glavni desni ideali, parcijalno uredjeni inkluzijom, u opštem slučaju ovde ne obrazuju ni semigrupu. Zato se *desni HCF-prsten* definiše na sledeći način.

Definicija 7.2.15. *Domen R je desni HCF prsten ako skup svih glavnih desnih ideala u R formira modularnu mrežu u odnosu na inkluziju.*

Za ovako definisane prstene iz modularnosti očigledno važi Šrajerova teorema pa je svaki HCF-prsten i S-prsten. Iz svega rečenog sledi da medju ovim klasama nekomutativnih prstena važe sledeće implikacije:

$$\text{glavnoidealski} \Rightarrow \text{fir} \Rightarrow \text{atomičan 2-fir} \Rightarrow \text{UFD} \Rightarrow \text{HCF} \Rightarrow \text{S} \tag{6}$$

7.3 Primeri nekomutativnih UFD domena

Prsteni kosih polinoma kao i slobodne asocijativne algebre pokazuju se kao dobar izvor različitih primera vezanih za nekomutativne prstene. Ukratko ćemo

opisati konstrukciju ovih prstena.

Prsten kosih polinoma $R[x;\alpha,\delta]$ nad domenom R predstavlja izvesnu generalizaciju običnog prstena polinoma $R[x]$ nad komutativnim prstenom, s tim što ovde elementi prstena R ne komutiraju medjusobno, niti sa neodredjenom x. Neka je R domen, $\alpha{:}R \to R$ injektivan endomorfizam prstena R i $\delta{:}R \to R$ takozvana α-*derivacija*, preslikavanje sa osobinama:

$$\delta(a+b) = \delta(a) + \delta(b)\,, \quad \delta(ab) = \delta(a)\alpha(b) + a\delta(b) \tag{1}$$

Proizvoljan element prstena $R[x;\alpha,\delta]$ je polinom f čiji koeficijente pišemo sa desne strane:

$$f = a_0 + xa_1 + \cdots + x^n a_n\,, \quad a_i \in R \tag{2}$$

Pravilom

$$ax = x\alpha(a) + \delta(a)\,, \quad a \in R \tag{3}$$

potpuno je odredjeno množenje, jer je onda

$$x^m a \cdot x^n b = x^{m+1}\alpha(a)x^{n-1}b + x^m\delta(a)x^{n-1}b \tag{4}$$

Koristeći ovo pravilo i asocijativnost možemo sada naći fg, za proizvoljne elemente f, g oblika (2). Sada se pokazuje da je na ovaj način konstruisan jedan novi prsten $R[x;\alpha,\delta]$ koji je potpuno odredjen prstenom R, endomorfizmom α i α-derivacijom δ[6]. Iz definicije neposredno sledi da je $\alpha(1) = 1$, kao i da je $\delta(1) = 0$. Posebno, ako je $\delta = 0$ onda $R[x;\alpha,0]$ kraće označavamo sa $R[x;\alpha]$ i sa $R[x]$ ako je $\alpha = 1\,, \delta = 0$. U poslednjem slučaju, prema (3), dobija se običan prsten polinoma nad nekomutativnim prstenom R. Ova definicija nije medjutim levo-desno simetrična jer se koeficijenti u (2) pišu sa dene strane. Pokazuje se da je u slučaju automorfizma α, prsten $R[x;\alpha,\delta]$ i levi prsten kosih polinoma sa odgovarajućim levim komutirajućim pravilom (3). Slično kao i u komutativnom slučaju, dokazuje se da je $R[x;\alpha,\delta]$ desni Neterin ako je R desni Neterin i α automorfizam. Promenama osnovnog prstena R i preslikavanja α,δ mogu se dobiti razni prsteni kosih polinoma, što ih čini pogodnim za konstruisanje različitih primera. Koristeći činjenicu da je prsten kosih polinoma $k[x;\alpha,\delta]$, nad proizvoljnim telom k glavnoidealski ([6]), pa dakle prema 7.2.10 i faktorijalan, mogu se dati neki primeri nekomutativnih UFD domena. Jedan od prvih primera nekomutativnih faktorijalnih domena je prsten linearnih diferencijalnih operatora.

Primer 7.3.1 (Prsten linearnih diferencijalnih operatora)**.**

$$R = k[D;1,']$$

gde je $k = F(t)$ *polje racionalnih funkcija nad poljem* F *i* $f \mapsto f'$ *za* $f \in k$ *obično diferenciranje* $f' = df/dt$.

[6]Može se krenuti i obratnim putem. Najpre se definiše $R[x;\alpha,\delta]$ koristeći (3) a zatim se pokaže da α mora biti injektivan endomorfizam dok δ mora biti α-derivacija.

Obično diferenciranje je naravno i α-diferenciranje, gde je $\alpha = 1$ identitet, jer prema pravilima diferenciranja

$$(f+g)' = f' + g' \quad , \quad (fg)' = f'g + fg'$$

važe uslovi (1). Kosi polinomi

$$f_0 + Df_1 + D^2 f_2 + \cdots + D^n f_n \,,$$

gde su $f_i \in F(t)$ racionalne funkcije, sa množenjem:

$$fD = Df + f' \,, \tag{5}$$

formiraju glavnoidealski, dakle UFD domen. Ilustrujmo faktorijalnost ovog prstena jednim zanimljivim primerom faktorizacije u njemu. Neka je

$$a = D^2 - D\frac{1}{t}$$

fiksiran element ovog prstena. On se očigledno može faktorisati kao:

$$(i) \qquad D^2 - D\frac{1}{t} = D\left(D - \frac{1}{t}\right)$$

Ako probamo da faktorišemo element a na neki drugi način,

$$D^2 - D\frac{1}{t} = (D - A(t))(D - B(t)) = D^2 - D(A(t) + B(t)) + A(t)B(t) - A'(t)$$

dolazimo do jednakosti $A(t) + B(t) = 1/t$, $A(t)B(t) - A'(t) = 0$. Odavde dobijamo da $A(t)$ mora biti rešenje Rikatijeve jednačine $A' + A^2 = A \cdot (1/t)$. Jedno partikularno rešenje ove jednačine je $A(t) = 2/t$, pa za $B(t) = 1/t - A(t)$, odnosno $B(t) = -1/t$ dobijamo još jednu netrivijalnu faktorizaciju elementa a:

$$(ii) \qquad D^2 - D\frac{1}{t} = \left(D - \frac{2}{t}\right)\left(D + \frac{1}{t}\right)$$

Opšte rešenje gornje diferencijalne jednačine $A' + A^2 = A \cdot (1/t)$ dato je formulom $A(t) = 2/t + 2/(2ct^3 - t)$, pa npr. za $c = 1/2$ dobijamo racionalnu funkciju $A(t) = 2t/(t^2 - 1)$ i odgovarajuću funkciju $B(t) = -(t^2 + 1)/t(t^2 - 1)$. Faktorizacija elementa a sada ima oblik:

$$(iii) \qquad D^2 - D\frac{1}{t} = \left(D - \frac{2t}{t^2 - 1}\right)\left(D + \frac{t^2 + 1}{t(t^2 - 1)}\right)$$

Ova razlaganja mogu se neposredno proveriti koristeći pravila računanja u prstenu kosih polinoma. Naravno, faktorizacije (i), (ii), (iii) izomorfne su u smislu definicije 7.1.4. ▼

Primer 7.3.2 (Prsten polinoma nad telom kvaterniona)**.**

$$R = \mathbb{H}[t] \quad \textit{gde je} \quad \mathbb{H} = \mathbb{R}\,[i, j, k] \quad \textit{telo realnih kvaterniona}$$

$$\textit{sa množenjem:} \quad i^2 = j^2 = -1 \quad , \quad ij = -ji = k$$

Ovde se radi o običnim polinomima, dakle neodredjena t komutira sa koeficijentima iz tela $\mathbb{H}$. Kao prsten polinoma nad telom, R je glavnoidealski, dakle UFD. Za razliku od prstena polinoma nad poljem, gde polinom stepena n ima najviše n različitih nula, u ovom prstenu to ne važi. Polinom $t^2 + 1 \in \mathbb{H}[t]$ ovde ima bar 3 različite nule (i, j i k), tačnije, ima ih beskonačno mnogo. Ova pojava može se objasniti na sledeći način;
Neka je $F[t]$ prsten polinoma nad proizvoljnim telom F, $f(t) = g(t)h(t) \in F[t]$ i $c \in F$ takav da je $a = h(c) \neq 0$. Tada je $f(c) = g(aca^{-1})h(c)$. Posebno, ako je c koren polinoma f i nije koren polinoma h, onda je aca^{-1} koren polinoma g. Koreni polinoma $f \in F[t]$ stepena n leže u najviše n klasa konjugacije tela F. Ako je

$$f(t) = (t - a_1) \ldots (t - a_n) \quad , \quad a_1, \ldots, a_n \in F$$

onda je svaki koren polinoma f konjugovan nekom a_i. Dokazi ovih tvrdjenja mogu se naći u [6] ili u [18]. Opširnije, tu se mogu naći i rezultati o broju nula u datoj klasi konjugacije.
Ako iskoristimo činjenicu da je $F[t]$ UFD, proizvoljan polinom $f \in F[t]$ stepena n ima neku atomičku faktorizaciju:

$$f = p_1 p_2 \ldots p_k \quad \text{gde je} \quad k \leq n$$

Ona je jednoznačna u smislu definicije 7.1.4, dakle svaki atomičan faktor polinoma f sličan je nekom od atoma p_i. Medjutim, prema [6] (tvrdjenje 0.7.5.) elementi $t - a$, $t - b$ slični su u $F[t]$ akko su a, b konjugovani u F. S obzirom da i, j, k imaju beskonačno mnogo konjugata u $\mathbb{H}$, ovim je objašnjena egzistencija beskonačnog broja nula polinoma $t^2 + 1$ u $\mathbb{H}$, kao i prividna nesaglasnost sa faktorijalnošću u $\mathbb{H}[t]$. ▼

Primer 7.3.3 (Prsten kompleksno-kosih polinoma)**.**

$$R = \mathbb{C}\,[\,x\,;\,^{-}\,]$$

Ovde je $\mathbb{C}$ polje kompleksnih brojeva, $\delta = 0$ i $\alpha : \mathbb{C} \to \mathbb{C}$ automorfizam polja $\mathbb{C}$ koji svakom elementu $a \in \mathbb{C}$ pridružuje njegov konjugovani $\overline{a}$. Elementi prstena $\mathbb{C}\,[\,x\,;\,^{-}\,]$ su polinomi oblika

$$a_0 + xa_1 + x^2 a_2 + \cdots + x^n a_n \quad a_i \in \mathbb{C}\,,$$

za koje važi jednakost

$$ax = x\overline{a} \tag{6}$$

Prsten $\mathbb{C}\,[\,x\,;\,^{-}\,]$ je prema prethodnom UFD. Jedan primer netrivijalne faktorizacije u ovom prstenu je razlaganje polinoma $x^2 - 1$;

$$x^2 - 1 = (x - 1)(x + 1) \tag{7}$$

$$x^2 - 1 = (x + (1 + i\sqrt{3})/2)(x - (1 - i\sqrt{3})/2) \tag{8}$$

Faktorizacije (7) i (8) izomorfne su u smislu definicije 7.1.4. Važi i opštije, jer je prema (6), $x^2 - 1 = (x + u)(x - \overline{u})$ za svaki komplesan broj u koji leži na jediničnoj kružnici, pa polinom $x^2 - 1$ ima ovde beskonačno mnogo netrivijalnih izomorfnih faktorizacija. ▼

Drugi vid generalizacije prstena polinoma dobija se konstrukcijom *slobodnih asocijativnih algebri* i one takodje predstavljaju bitnu klasu nekomutativnih prstena pogodnu za razne primere. Konstrukcija slobodne asocijativne algebre može se ukratko opisati na sledeći način. Neka je $X = \{x_i\}$ neprazan skup, k komutativan prsten i X^* slobodan monoid nad X, sa elementima oblika

$$x_I = x_{i_1} x_{i_2} \dots x_{i_n} \tag{8}$$

gde $I = (i_1, \dots, i_n)$ prolazi svim konačnim nizovima indeksa, uključujući i prazan skup, kada je po konvenciji $x_\emptyset = 1$. Slobodne asocijativna algebra $k\langle X\rangle$ nad k je algebra monoida X^*. Njeni elementi jednoznačno se predstavljaju u obliku

$$f = \sum x_I a_I \quad , \quad a_I = 0 \ \text{ za skoro sve } \ a_I \in k \tag{9}$$

U slučaju jednočlanog skupa tj. za $|X| = 1$, dobija se običan (komutativan) prsten polinoma, $k\langle x\rangle = k[x]$. U ostalim slučajevima, za $|X| > 1$ slobodna algebra $k\langle X\rangle$ je nekomutativna, jer je definiše nekomutativan monoid. Posebno važan slučaj dobija se kada je k polje. Tada je skup svih invertibilnih elemenata $U(k\langle X\rangle) = k \cup \{0\}$ i kardinalnost slobodnog generatorskog skupa X je invarijanta ove algebre, nezavisna od izbora skupa X, koju zovemo njenim *rangom*. Za monom $x_1 x_2 \dots x_n \in k\langle X\rangle$ definiše se njegova *dužina* sa $l(x_1 x_2 \dots x_n) \stackrel{\text{def}}{=} n$. Za element $f \in k\langle X\rangle$ oblika (9) definiše se njegov *stepen* sa $d(f) = \max\{\, l(x_I) \mid a_I \neq 0 \,\}$ i *red* sa $o(f) = \min\{\, l(x_I) \mid a_I \neq 0 \,\}$. Koristeći ove pojmove pokazuje se da slobodne algebre zadovoljavaju takozvani *slabi algoritam*[7] kao i da je zbog toga svaka slobodna asocijativna algebra nad poljem k dvostrani fir, pa i UFD prema 7.2.12. Dokaz ovog netrivijalnog rezultata može se naći u [6].

Primer 7.3.4.

$$k\,\langle\, x_1, x_2, \dots, x_n \,\rangle$$

je UFD, gde je k proizvoljno polje. Kao primer jedne netrivijalne faktorizacije u slučaju slobodne algebre $k\,\langle\, x, y\,\rangle$ imamo:

$$xyx + x = x(yx + 1) = (xy + 1)x \tag{10}$$

Ove faktorizacije izomorfne su u smislu 7.1.4 tj. $xy+1$ i $yx+1$ su slični atomi. Njihova sličnost neposredno sledi iz 7.2.6, jer je relacija

$$(1 + xy)x = x(1 + yx)$$

koprosta. Elementi $1 + xy, x$ koprosti su sleva ($(1 + xy)R + xR = R$ je komaksimalna relacija sleva). Slično su i $x, 1 + yx$ koprosti zdesna, odakle je $1 + xy \sim 1 + yx$. ▼

[7] Generalizacija Euklidovog algoritma u nekomutativnim prstenima.

Literatura

[1] Baker A., *A Concise Introduction To the Theory of Numbers*, Cambridge University Press, Cambridge-New York-Melbourne, (1984).

[2] Боревич З.И., Шафаревич И.Р , *Теория Чисел* , Наука, Москва, (1972).

[3] Bourbaki N., *Algébre Commutative*, Hermann, Paris, (1971).

[4] Bourbaki N., *Algébre* [*Les Structures Fondamentales de L'analyse*] , Hermann, Paris, (1965).

[5] Cohn M.P., *Algebra* [Volume 1] , John Wiley & Sons, London-New York-Sydney-Toronto, (1974).

[6] Cohn M.P., *Free Rings and their Relations* [Second edition] , Academic Press, London, (1985).

[7] Cohn M.P., *Unique Factorizatin Domains*, Amer. Math. Monthly, (1973).

[8] Cohn M.P., *Noncommutative Unique Factorizatin Domains*,Trans. Amer. Math. Soc., (1963).

[9] Eisenbud D., *Commutative Algebra* [*With a View Toward Algebraic Geometry*] , Springer-Verlag, New York, (1995).

[10] Fossum M.R., *The Divisor Class Group of a Krull Domain*, Heidelberg, New York, (1973).

[11] Gilmer R., *Multiplicative Ideal Theory*, Marcel Dekker, New York, (1972).

[12] Hartshorn R., *Algebraic Geometry*, Springer, Heidelberg, (1977).

[13] Hungerford T., *Algebra*, Springer-Verlag, New York-Heidelberg-Berlin, (1987).

[14] Hutchins C.H., *Examples of Commutative Rings*, Polygonal Publishing House, New York, (1981).

[15] Kaplansky I., *Commutative Rings*, The University of Chicago Press, Chicago-London, (1974).

[16] Kunz E., *Introduction to Commutative Algebra and Algebraic Geometry* , Birkhäuser Boston-Basel-Stuttgart, (1981).

[17] Курош Г.А., *Лекции по Общей Алгебре*, Государственное Издательство Физико-Математической Литературь, Москва, (1962).

[18] Lam T.Y. , *A First Course in Noncommutative Rings*, Springer- Verlag, New York, (1990).

[19] Lelong-Ferrand J., Arnaudiès J.M., *Algèbre*, Dunod, Paris, (1971).

[20] Marcus A.D., *Number Fields*, Springer-Verlag, New York, (1977).

[21] Matsumura H., *Commutative Ring Theory*, Cambridge University Press, Cambridge-New York-Melbourne, (1990).

[22] Nagata M., *Local Rings*, John Wiley & Sons, New York-London, (1962).

[23] Ribenboim P., *Algebraic Numbers*, John Wiley & Sons, New York-London-Sydney-Toronto, (1972).

[24] Samuel P., *Anneaux Factoriels*, Instituto de Pesquisas Matematicas da Universidade de Sao Paulo e da Sociedade de Matematica de Sao Paulo, Sao Paulo, (1963).

[25] Samuel P., *Unique Factorization*, Amer. Math. Monthly, (1968).

[26] Samuel P., Zariski O., *Commutative Algebra* , Van Nostrand, Princeton, New Jersey, (1960).