Komutativni prsteni i ideali

Pod prstenom se uvek (osim ako nije drukčije eksplicitno navedeno) podrazumeva *komutativni prsten sa jedinicom*. To je skup A sa dve binarne operacije, sabiranjem $+$ i množenjem $-$, takvim da je A Abelova grupa u odnosu na sabiranje, množenje je asocijativno i komutativno i ima jedinični element, i važi distributivni zakon:

$$a(b+c) = ab + ac$$

Homomorfizam prstena $h : A \to B$ je homomorfizam za sabiranje, za množenje i prevodi jedinicu u jedinicu:

$$\begin{aligned} h(a+b) &= h(a) + h(b); \\ h(ab) &= h(a)h(b); \\ h(1) &= 1. \end{aligned}$$

Kompozicija homomorfizama je homomorfizam. Homomorfizam koji je 1-1" je *monomorfizam*, homomorfizam koji je na" - *epimorfizam*, homomorfizam koji je bijekcija - *izomorfizam* prstena. Identično preslikavanje $A \longrightarrow A$, $a \mapsto a$ je izomorfizam.

Podskup $S \subset A$ prstena A je *potprsten*, ako je zatvoren za sabiranje, za množenje i sadrži jedinicu tj. ako je

$$\begin{aligned} a, b &\in S \Rightarrow a + b \in S; \\ a, b &\in S \Rightarrow ab \in S; \\ 1 &\in S. \end{aligned}$$

Inkluzija $S \hookrightarrow A$, $a \mapsto a$ potprstena S u prsten A je monomorfizam.

Primeri. Prsten celih brojeva $\mathbb{Z}$, prsten polinoma više promenljivih $B\left[x_{1,} \ldots, x_n\right]$ sa koeficijentima u polju ili prstenu B, prsten $\mathbb{Z}_n = \{0, 1, \ldots n-1\}$ ostataka po modulu n.

Ideal I prstena A je aditivna podgrupa prstena, koja izdržava množenje elementima iz A, tj. ako $a \in I$ i $b \in A$, tada $ab \in I$. Ovo se može zapisati i na sledeći način: $IA \subset I$.

Ideal I je *glavni* (ili monogeni) ako je $I = (a) := \{ax | x \in A\} = aA$ za neko $a \in A$. Kažemo da je I generisan elementom a. Ideal I je *konačnogenerisan*, ako je generisan konačnim skupom $\{a_1, \ldots a_k\}$:

$$I = (a_1, \ldots, a_k) := \left\{a_1 x_1 + \cdots + a_k x_k \,|x_1, \ldots, x_k \in A\right\}.$$

Trivijalni ideali prstena A su nula-ideal $(0) = \{0\}$ i jedinični ideal $(1) = A$. Ako ideal I sadrži jedinicu 1, tada je on obavezno jedinični jer $1 \cdot a = a \in I$. Prsten A je polje $\Leftrightarrow$ A nema druge ideale osim trivijalnih ideala (0) i (1).

Primeri. (1) Parni brojevi čine ideal u prstenu $\mathbb{Z}$: ako parni broj pomnožimo bilo kojim celim brojem, dobićemo opet paran broj. Uopšte, skup $d\mathbb{Z} := \{dn | n \in \mathbb{Z}\} \subset \mathbb{Z}$ je za svako fiksirano $d \in \mathbb{Z}$ ideal u $\mathbb{Z}$, glavni ideal generisan brojem d.

(2) Polinomi bez konstantnog člana čine ideal u prstenu $B[x_1, \ldots, x_n]$: ako je $f(0, \ldots, 0) = 0$, onda je i $g(0, \ldots, 0) \cdot f(0, \ldots, 0) = 0$ za bilo koji polinom $g \in B[x_1, \ldots, x_n]$.

(3) *Jezgro* $\operatorname{Ker}\varphi := \{a \in A | \varphi(a) = 0\}$ bilo kog homomorfizma prstena $\varphi : A \to B$ je ideal u A. *Slika* homomorfizma $\operatorname{Im}\varphi := \{\varphi(a) \in B | a \in A\}$ je potprsten ali ne mora biti ideal: elementi iz $\operatorname{Im}\varphi$ izdržavaju množenje elementima iz slike ali ne obavezno i svim elementima prstena B. Opštije, inverzna slika $\varphi^{-1}(J) \subset A$ bilo kog ideala $J \subset B$ je ideal u A, što za direktne slike nije tačno (naite kontraprimer).

Količnički prsten ili *faktor-prsten* prstena A po idealu I je skup $A/I := \{a + I | a \in A\}$ svih klasa ekvivalencije po relaciji $a \sim b \Leftrightarrow a - b \in I$. Ovo je količnička brupa Abelove grupe A po podgrupi I koja nasleuje operaciju množenja jer je I ideal: ako $a + I, b + I \in A/I$, tada $(a + I)(b + I) := ab + I$ ne zavisi od izbora predstavnika, jer ako $b - b' = c \in I$, tada $ab - ab' = a(b - b') \in I$. Jedinični element u tom prstenu je klasa jedinice $1 + I$, pa je A/I pravi prsten (komutativan, sa jedinicom). U slučaju kada je $a - b \in I$ piše se i $a \equiv b \bmod I$. Preslikavanje $\varphi : A \to A/I$, $a \mapsto a + I$ je epimorfizam prstena, tzv. *kanonska projekcija* odreena idealom I. Njeno jezgro je upravo ideal I: $\varphi^{-1}(0) = \{a | a + I = I\} = \{a | a \in I\} = I$.

Teorema o homomorfizmu (prva teorema o izomorfizmu) kod Abelovih grupa prenosi se i na prstene: $A/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$ za svaki homomorfizam prstena $\varphi : A \to B$. Važi i opštije tvrenje.

Tvrenje. Ako je I ideal prstena A i $\varphi : A \to A/I$ kanonska projekcija, tada za svaki ideal J u A/I, ideal $\varphi^{-1}(J)$ u A sadrži J. Preslikavanje $J \mapsto \varphi^{-1}(J)$ je monotona bijekcija tj. izomorfizam struktura ureenih skupova svih ideala u B i onih ideala u A koji sadrže dati ideal I.

Primeri: (1) Količnički prsten $\mathbb{Z}/d\mathbb{Z}$ je izomorfan prstenu $\mathbb{Z}_n$ ostataka po modulu n.

(2) Ako je $\varphi : k[x_1, \ldots, x_n] \to k$ preslikavanje definisano sa $\varphi(f) = f(0, \ldots, 0)$, tada je to epimorfizam prstena, čije je jezgro upravo ideal I polinoma bez konstantnog člana. Prema tome, $k[x_1, \ldots, x_n]/I \cong k$.

Delitelji nule, nilpotenti, invertibilni elementi. Prosti i maksimalni ideali.

U prstenu A element $a \neq 0$ je delitelj nule ako postoji element $b \neq 0$ takav da je $ab = 0$. Prsten bez delitelja nule naziva se *domen*. Prsten celih brojeva $\mathbb{Z}$ i prsten polinoma više promenljivih $k[x_1, \ldots, x_n]$ sa koeficijentima u polju k su domeni (dokažite za domaći).

Još dve standardne konstrukcije za prsten $\mathbb{Z}$ i za polje k se prenose na proizvoljne domene. To su konstrukcija polja razlomaka i konstrukcija prstena polinoma.

Tvrdjenje-definicija. Ako je A domen, skup $K = A_{(0)} = A \times A^*/\sim$ gde je $\sim$ relacija ekvivalencije $(a,b) \sim (c,d) \Longleftrightarrow ad = bc$, klasa ekvivalencije $cl(a,b) =: \frac{a}{b}$, sa operacijama $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}, \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$ je polje, tzv. *polje razlomaka* $K = A_{(0)}$ domena A. Preslikavanje $A \longrightarrow K$, $a \mapsto \frac{a}{1}$ je monomorfizam prstena pomoću koga se A identifikuje sa potprstenom u K. Dokaz ovog tvrdjenja u potpunosti prati standardni dokaz za cele odnosno racionalne brojeve. Dakle, svaki se domen može na standardan način utopiti u polje svojih razlomaka.

Tvrdjenje-definicija. Ako je A prsten, neka je

$$A^{fin} = \{(a_0, a_1, \ldots, a_n, \ldots) \,|a_n \text{ je niz sa konačnim nosačem}\} \subset A^{\mathbb{N}}$$

skup svih nizova (a_n) takvih da je $\operatorname{supp}(a_n) := \{n \,|a_n \neq 0\} \subset \mathbb{N}$ konačan. Ako se u taj skup uvedu operacije sabiranja i množenja formulama

$$\begin{aligned}(a_0, \ldots, a_n, \ldots) + (b_0, \ldots, b_n, \ldots) &= (a_0 + b_0, \ldots, a_n + b_n, \ldots) \\ (a_0, \ldots, a_n, \ldots) \cdot (b_0, \ldots, b_n, \ldots) &= (a_0b_0, a_0b_1 + a_1b_0, \ldots, a_0b_n + a_1b_{n-1} + \cdots + a_nb_0, \ldots)\end{aligned}$$

dobijamo novi prsten, *prsten polinoma* $A[x]$ sa koeficijentima iz A. Preslikavanje $A \longrightarrow A[x]$, $a \mapsto (a, 0, 0, \ldots)$ je izomorfizam prstena A i njegove slike, na osnovu koga smatramo da je $A \subset A[x]$. Niz $(0, 1, 0, \ldots)$ se obeležava sa x i svaki polinom (a_n) se jednoznačno zapisuje u standardnom obliku $(a_n) = f = a_0 + a_1x + \cdots + a_mx^m$. Dva polinoma su jednaka ako i samo ako su im jednaki svi odgovarajući koeficijenti, što je neposredna posledica definicije: $(a_n) = (b_n) \Longleftrightarrow \forall n \in \mathbb{N}_0, a_n = b_n$. Najveći indeks m takav da je $a_m \neq 0$ naziva se *stepenom* $\deg(f) \in \mathbb{N}_0$ polinoma f. Pri tome je $\deg(fg) \leq \deg(f)\deg(g)$, a ako je A domen važi jednakost (dokažite za domaći). U tom slučaju je i $A[x]$ domen.

Višestrukom primenom konstrukcije prstena polinoma dobijamo polinome sa više promenljivih: induktivno definišemo $A[x_1, \ldots, x_n] := (A[x_1, \ldots, x_{n-1}])[x_n]$.

Pojam stepena ovde postaje složeniji: možemo posmatrati stepen po svakoj promenljivoj ponaosob ali i ukupni stepen po svim promenljivim zajedno.

Element a prstena A je *invertibilan* (ili *jedinica* u A) ako postoji $b \in A$ takvo da je $ab = ba = 1$. Element a je invertibilan $\Leftrightarrow (a) = A$. Svi invertibilni elementi u A čine multiplikativnu grupu A^*. Na primer, $\mathbb{Z}^* = \{-1, 1\} \cong \mathbb{Z}_2$, $A[x_1, \ldots, x_n]^* = A^*$. Ovaj skup nije i aditivna podgrupa u A, jer zbir dva invertibilna elementa ne mora biti invertibilan: $1 + (-1) = 0$.

Elementi a i b prstena A su *asocirani*, ako je $a = b\varepsilon$ gde je ε invertibilan u A. Asociranost je relacija ekvivalencije na A. Na primer, n i $-n$ su asocirani u $\mathbb{Z}$, $f(x_1, ..., x_n)$ i $a \cdot f(x_1, ..., x_n)$ ($a = const \in A^*$) su asocirani u $A[x_1, \ldots, x_n]$. U problemima vezanim sa deljivošću i faktorizacijom (v. sledeći odeljak) asocirane elemente ne razlikujemo tj. radimo sa odgovarajućim klasama ekvivalencije.

Element $a \in A$ je *nilpotentan*, ako postoji n takvo da je $a^n = 0$. Najmawe takvo n naziva se stepen nilpotentnosti. Svaki netrivijalni ($\neq 0$) nilpotentan element je delitelj nule, ali mogu postojati i nenilpotentni delitelji nule (u prstenu $\mathbb{Z}_{36}$ je $6^2 = 0$, a takoe i $4 \cdot 9 = 0$ pri čemu ni 4 ni 9 nisu nilpotentni). Prsten bez nilpotenata je *redukovan prsten* (prsten $\mathbb{Z}_6$ je redukovan, ali nije domen).

Skup svih nilpotenata $\operatorname{nil} A$ prstena A je ideal, tzv. *nilradikal* prstena A. Naime, ako $a, b \in \operatorname{nil} A$, tada je $a^n = 0$ i $b^m = 0$, pa je $(a + b)^{n+m} = 0$ na osnovu binomne formule. Ostale osobine ideala se lako proveravaju. Prsten $A/\operatorname{nil} A$ je redukovan. Na primer, $\operatorname{nil} \mathbb{Z}_{36} = \{0, 6, 12, 18, 24, 30\} = (6)$ i $\mathbb{Z}_{36}/\operatorname{nil} \mathbb{Z}_{36} \cong \mathbb{Z}_6$.

Ideal I prstena A je *prost ideal*, ako $ab \in I \Rightarrow a \in I \vee b \in I$. Lako se vidi da je ideal I prost ako i samo ako je A/I domen.

Primer. Ideal $(p) = p\mathbb{Z}$ u $\mathbb{Z}$ je prost ako i samo ako je p prost broj. Odavde naziv i vodi poreklo.

Ideal $P \subset A$ je prost $\Leftrightarrow$ prsten A/P je domen. Ovo se neposredno vidi.

Ideal I prstena A je *maksimalan ideal*, ako nije sadržan ni u jednom pravom idealu prstena A, tj. ako iz $I \subset J$, $J \neq A$ sledi $I = J$.

Ideal $M \subset A$ je maksimalan $\Leftrightarrow$ prsten A/M je polje. Zato je svaki maksimalni ideal prost.

Operacije nad idealima. Nilradikal i Džekobsonov radikal

Ako su I, J dva ideala prstena A, definisani su ideali $I + J$, IJ i $I \cap J$. Unija $I \cup J$ u opštem slučaju nije ideal.

Primer. U prstenu $\mathbb{Z}$, $(m) + (n) = (NZD(m, n))$, $(m)(n) = (mn)$, $(m) \cap (n) = (NZS(m, n))$.

Jasno je da je $IJ \subset I \cap J$. Jednakost u opštem slučaju ne važi.

Primer. U prstenu $\mathbb{Z}$, $(m)(n) = (m) \cap (n) \Leftrightarrow (m) + (n) = (1)$ tj. ako i samo ako su brojevi m i n uzajamno prosti.

Ideali I, J prstena A su *uzajamno prosti* ako je $I + J = (1)$. Ako su I i J uzajamno prosti, tada je $IJ = I \cap J$ (dokažite za domaći).

Pojam zbira, proizvoda i preseka dva ideala se definiše i za konačno mnogo ideala, a presek i za beskonačne familije ideala: presek $\bigcap_{s\in S} I_s$ bilo kakve familije ideala $\{I_s \,|s \in S\}$ je opet ideal, što se neposredno proverava. Suma i proizvod beskonačne familije se ne mogu jednostavno definisati, ali ipak dopuštaju generalizaciju. Tako, suma beskonačne familije ideala $\{I_s \,|s \in S\}$ je ideal generisan **konačnim** zbirovima elemenata sabiraka (setite se nizova sa konačnim nosačem):

$$I = \sum_{s\in S} I_s := \left\{ a_{s_1} + \cdots + a_{s_i} \,\middle|\, a_{s_j} \in I_{s_j},\ j = 1, \ldots, i,\ i \in \mathbb{N} \right\}.$$

Ako je $f : A \to B$ homomorfizam prstena i $J \subset B$ prost ideal u B, tada je $f^{-1}(J) \subset A$ prost ideal u A. Inverzna slika maksimalnog ideala ne mora biti maksimalan (primer: inkluzija domena u polje razlomaka, recimo $\mathbb{Z} \hookrightarrow \mathbb{Q}$).

Svaki prsten ima maksimalni ideal. I više od toga, svaki pravi ideal sadržan je u maksimalnom. U dokazu ove činjenice koristi se aksioma izbora u obliku Cornove leme.

Tvrenje. Presek svih prostih ideala prstena jednak je njegovom nil-radikalu.

Dokaz. Naime, neka je N presek svih prostih ideala u A. Ako je a nilpotentan element i P prost ideal, tada za neko n, $a^n = 0 \in P$, pa je $a \in P$. Zato $\operatorname{nil} A \subset N$. Obrnuto, neka a nije nilpotentan. Tada skup $S = \{a, a^2, a^3, \ldots\}$ ne sadrži 0. Neka je $\mathcal{F}$ familija svih ideala I koji ne seku skup S. Primenom Cornove leme možemo naći maksimalni element familije $\mathcal{F}$, neka je to $P \in \mathcal{F}$. Dokažimo da je P prost. Neka $x, y \notin P$. Tada zbog maksimalnosti P, $P + (x)$ i $P + (y) \notin \mathcal{F}$ pa zato $a^n \in P + (x)$ i $a^m \in P + (y)$ za neke $n, m \in \mathbb{N}$. Sada $a^{n+m} \in P + (xy)$. Zato je $P + (xy) \neq P$ i $xy \notin P$.

Džekobsonov radikal $J(A)$ prstena A je presek svih maksimalnih ideala prstena A.

Tvrenje. $x \in J(A) \Leftrightarrow$ za svako $a \in A$, element $1 - ax$ je invertibilan u A.

Dokaz. Neka $1 - ax$ nije invertibilan. Tada je on sadržan u nekom maksimalnom idealu M . Sada je $x \in J(A) \subset M$ pa mora biti $1 \in M$, što je kontradikcija. Obrnuto, neka $x \notin M$ za neki maksimalni ideal M. Tada je

zbog maksimalnosti $M + (x) = (1)$ tj. za neko $m \in M$ i $a \in A$, $m + ax = 1$, odakle je $1 - ax \in M$ i ne može biti invertibilan.

Deljivost, nerastavljivi elementi i euklidski prsteni

Neka je A prsten i $p, q \in A$. Kaže se da neinvertibilni element q *deli* p i piše $q \mid p$ ako je $p = qc$ za neko $c \in A$, pri čemu je $c \notin A^*$. Element q je (pravi) *delilac* ili *faktor* elementa p. Invertibilni elementi dele p u smislu gornje definicije, ali nisu pravi delioci. Reč pravi" ćemo obično izostavljati. Element p je *nerastavljiv* (ili *atom*) ako nema (pravih) delilaca tj. ako $q \mid p \Longrightarrow q$ invertibilan ili asociran sa p.

Da li za svaki element $a \in A$ postoji nerastavljivi delilac elementa a? Ako je a nerastavljiv, tu je kraj. Ako nije, tada postoji a_1 takvo da $a_1 \mid a$. Isto rasudjivanje primenjujemo na a_1 itd. Dobijamo niz delilaca $...a_{n+1} \mid a_n \mid ... \mid a_2 \mid a_1 \mid a$. Da li će se ovaj postupak završiti i dati nerastavljivi faktor elementa a ili se može desiti da taj niz bude beskonačan?

Primeri. (1) Ako je $A = \mathbb{Z}$ prsten celih brojeva, tada je očigledno da $q \mid p \Longrightarrow |p| > |q| > 0$, pa za gornji niz $\ldots a_{n+1} \mid a_n \mid \cdots \mid a_2 \mid a_1 \mid a$ dobijamo strogo opadajući niz prirodnih brojeva

$$|a| > |a_1| > |a_2| > \cdots > |a_n| > |a_{n+1}| > \cdots > 0$$

koji se mora završiti posle konačno mnogo koraka (princip dobrog ureenja). Dakle, u prstenu celih brojeva, svaki broj ima nerastavljivi faktor.

(2) Ako je $A = k[x]$ prsten polinoma, tada je očigledno da $q(x) \mid p(x) \Longrightarrow 0 < \deg q(x) < \deg p(x)$ (ovde je od suštinske važnosti da su koeficijenti iz polja), pa za niz delitelja $...a_{n+1} \mid a_n \mid ... \mid a_2 \mid a_1 \mid a$ dobijamo strogo opadajući niz prirodnih brojeva

$$\deg a > \deg a_1 > ... > \deg a_n > \deg a_{n+1} > ... > 0$$

koji se mora završiti posle konačno mnogo koraka. Dakle, u prstenu polinoma sa koeficijentima iz polja svaki polinom ima nerastavljivi faktor.

(3) Neka je prsten $A_1 = \mathbb{Q}\left[\sqrt{2}\right] \subset \mathbb{R}$ raširenje polja $A_0 = \mathbb{Q}$ dobijeno dodavanjem broja $\sqrt{2}$. Dakle, $A_1 = \left\{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\right\}$. Nastavimo ovaj postupak na sledeći način: $A_n = A_{n-1}\left[\sqrt[2^n]{2}\right]$. Pošto je $\sqrt[2^n]{2} = \sqrt[2^{n-1}]{2} \cdot \sqrt[2^{n-1}]{2}$ odnosno $\sqrt{\left(\sqrt[2^{n-1}]{2}\right)} = \left(\sqrt[2^n]{2}\right)$, dobija se rastući niz prstena

$$A_0 \subset A_1 \subset \cdots \subset A_n \subset \cdots \subset \mathbb{R},$$

pa je i $A = \bigcup_{n=1,\infty} A_n \subset \mathbb{R}$ potprsten u polju $\mathbb{R}$. Jasno je da je $... \sqrt[2^{n+1}]{2} \mid \sqrt[2^n]{2} \mid ... \mid \sqrt[2^2]{2} \mid \sqrt{2} \mid 2$ beskonačan niz delilaca broja 2 koji se neće završiti.

Dakle, moguća su oba slučaja. Vidimo da je dovoljan uslov da se niz završi - postojanje funkcije $f : A \longrightarrow \mathbb{N}$ koja zadovoljava uslov $q \mid p \Longrightarrow f(q) < f(p)$. Ulogu ove funkcije u slučaju celih brojeva igra apsolutna vrednost, a u slučaju polinoma nad poljem - stepen polinoma. U ova dva poslednja slučaja važi i nešto oštriji uslov koji predstavlja osnovu za postojanje Euklidovog algoritma. Taj se pojam obično razmatra samo za domene tj. za prstene bez delitelja nule.

Definicija. Domen A je *euklidski prsten*, ako postoji *funkcija norme* $f : A \setminus \{0\} \longrightarrow \mathbb{N}$ sa sledećim svojstvom: za svaka dva elementa $a, b \in A$, $b \neq 0$ postoje elementi $q, r \in A$ takvi da je $a = b \cdot q + r$ i $f(r) < f(b)$ ili $r = 0$. Element q naziva se *količnik*, r *ostatak* od deljenja a sa b, a sama jednakost $a = b \cdot q + r$ *deljenjem s ostatkom.*

U uobičajenoj definiciji funkcije norme zahteva se i dodatni uslov $q \mid p \Longrightarrow f(q) \leq f(p)$ ili, što je isto, $f(q) \leq f(qa)$. Ovaj uslov, meutim, nije neophodan. Naime, ako je f funkcija norme u prvom, opštijem smislu, tada je sa $g(p) = \min_{a \in A \setminus \{0\}} f(pa)$ definisana funkcija norme u drugom, užem smislu i ona zadovoljava isti uslov euklidskog deljenja s ostatkom (proveriti za domaći).

U euklidskom prstenu svaki element ima nerastavljivi faktor, jer niz rastavljanja uvek mora da se završi: iz niza deljivosti $...a_{n+1} \mid a_n \mid ... \mid a_2 \mid a_1 \mid a$ dobija se strogo opadajući niz prirodnih brojeva

$$f(a) > f(a_1) > ... > f(a_n) > f(a_{n+1}) > ... > 0$$

koji se zbog dobre ureenosti skupa $\mathbb{N}$ mora završiti.

Jasno je da su prsten celih brojeva $\mathbb{Z}$ i prsteni polinoma sa koeficijentima u polju $k[x]$ euklidski prsteni. Ovi prsteni zadovoljavaju u stvari nešto jači, algoritamski uslov: postoji algoritam koji po datim a i b odredjuje količnik q i ostatak r, tzv. algoritam deljenja s ostatkom. Manje je poznat primer Gausovih celih brojeva $\mathbb{Z}[i]$ sa funkcijom norme $f(a+bi) = a^2 + b^2$ (dokažite za domaći).

Definicija. Neka je A domen i $a, b \in A$. *Najveći zajednički delilac* $NZD(a, b)$ elemenata a, b je $d \in A$ takav da: (1) $d \mid a$ i $d \mid b$; (2) ako $d' \mid a$ i $d' \mid b$, onda $d' \mid d$.

Ako postoji, $NZD(a, b)$ je odreen jednoznačno do asociranog elementa: ako su d i d' dva elementa koji zadovoljavaju definiciju, tada su oni asocirani tj. $d' = d \cdot \varepsilon$ za neki invertibilni $\varepsilon \in A^*$.

Dokažimo da u euklidskom prstenu NZD uvek postoji.

Euklidov algoritam. Obeležimo $a = r_{-1}, b = r_0$. Zbog euklidovosti domena A postoje q_0 i r_1 takvi da je $r_{-1} = r_0 q_0 + r_1$. Ako je $r_1 \neq 0$, tada je $f(r_0) > f(r_1)$ i postupak možemo nastaviti sa r_0 i r_1 umesto r_{-1} i r_0. Višestrukom primenom deljenja sa ostatkom dobijamo niz elemenata $r_i \neq 0$ $(i = 0, 1, \dots)$ takvih da je $r_{i-1} = r_i q_i + r_{i+1}$ i strogo opadajući niz prirodnih brojeva $f(r_0) > f(r_1) > \cdots > f(r_i) > 0$. Zbog dobre ureenosti skupa $\mathbb{N}$ niz se mora završiti tj. na nekom koraku moramo doći do $r_{i+1} = 0$. Tada je $r_i = d$ najveći zajednički delilac elemenata a i b.

Dokaz. Svojstvo (1) se dokazuje počev od poslednje jednakosti $r_{i-1} = r_i q_i$ prema prvim dvema $a = bq_0 + r_1$ i $b = r_1 q_0 + r_2$, a svojstvo (2) obrnutim redom, od prve dve prema poslednjoj.

Postupak primenjen u Euklidovom algoritmu je u odreenom smislu obrnut metodi matematičke indukcije. Koristio ga je Ferma, pa se zbog toga naziva metoda *Fermaovog* (ili *beskonačnog*) *spuštanja*[1]. U stvari, princip matematičke indukcije je ekvivalentan principu dobrog ureenja skupa prirodnih brojeva (dokažite za domaći). Primetimo da se Euklidov algoritam može sprovesti u svakom prstenu u kome svaka dva elementa imaju NZD. To su tzv. NZD-prsteni. Pored Euklidovog algoritma, u takvim prstenima važi i sledeće tvrenje.

Bezuova jednakost. Ako je $d = NZD\,(a, b)$, tada postoje $u, v \in A$ takvi da je $ua + vb = d$.

Ovo se lako dokazuje primenom Euklidovog algoritma.

Posledica. Ako $p \mid ab$ i $NZD(a, p) = 1$, tada $p \mid b$. Naime, iz $ab = pc$ i $ua + vp = 1$ sledi $b = uab + vpb = upc + vpb = p(uc + vb)$ tj. $p \mid b$.

Definicija. *Najmanji zajednički sadržalac* $NZS\,(a, b)$ elemenata a, b je $s \in A$ takav da: (1) $a \mid s$ i $b \mid s$; (2) ako $a \mid s'$ i $b \mid s'$ onda $s \mid s'$.

Ova dva pojma su ekvivalentna: ako dva elementa domena A imaju NZD, onda oni imaju NZS i obrnuto. Naime, iz $a = da', b = db', d = ua+vb$ sledi $1 = ua' + vb'$. Ako uzmemo $s = da'b'$ očigledno je $s = ab' = a'b$ odnosno $a \mid s$ i $b \mid s$, što dokazuje (1). Ako sad $a \mid s'$ i $b \mid s'$, tada je $s' = ap = bq$ i imaćemo $s' = ua's' + vb's' = ua'bq + vb'ap = uda'b'q + vda'b'p = s(uq + vp)$, odnosno $s \mid s'$, što dokazuje (2). (Za domaći dokažite obrnutu implikaciju). Kao posledicu dobijamo i jednakost

$$NZD(a, b) \cdot NZS(a, b) = a \cdot b.$$

[1] infinite descent (eng.)

Iz svega sledi da u euklidskom prstenu svaka dva elementa imaju i NZD i NZS.

Glavnoidealski i Neterini prsteni

Neka je A domen. Kažemo da je A *glavnoidealski prsten*[2] ako je svaki njegov ideal glavni odnosno monogen tj. generisan jednim elementom $I = (a)$. Kažemo da je A *Neterin prsten*[3], ako je svaki njegov ideal konačnogenerisan tj. generisan konačnim skupom elemenata $I = (a_1, \ldots, a_k)$.

Može se pokazati da je uslov neterinosti ekvivalentan uslovu konstantnosti rastućih lanaca ideala[4]: ako je $I_0 \subset I_1 \subset \cdots \subset I_n \subset \ldots$ rastući niz ideala, tada postoji k takvo da je $I_k = I_{k+1} = \ldots$, tj. počev od nekog k taj niz je stacionaran (dokažite za domaći).

Svaki euklidski prsten je glavnoidealski. Dokaz ove činjenice kopira odgovarajući dokaz u prstenu celih brojeva. Naime, ako je $I \subset A$ ideal, neka je $f(I) = \{f(a) \,|a \in I\} \subset \mathbb{N}$ i $m = \min f(I) \in \mathbb{N}$. Takav postoji zbog dobre uredjenosti skupa prirodnih brojeva. Postoji element $d \in I$ za koji se taj minimum dostiže: $f(d) = m$. Jasno je da je $(d) \subset A$. Na proizvoljno $a \in I$ primenimo deljenje s ostatkom sa d. Postoje $q, r \in A$ takvi da je $a = qd + r$. Sada je $r = a - qd \in I$. Ako je $r \neq 0$, mora biti $f(r) < f(a) = m$ što je kontradikcija sa minimalnošću m. Zato je $r = 0, a = qd$ i $I \subset (d)$, što zajedno sa prethodnim daje $I = (d)$.

Dakle, prsteni $\mathbb{Z}$ i $k\,[x]$ su glavnoidealski. Prsten $\mathbb{Z}\,[x]$ polinoma sa celobrojnim koeficijentima nije glavnoidealski: ideal $(2, x)$ se ne može generisati jednim celobrojnim polinomom. Proverite. Dokažite da prsten $k\,[x, y]$ takoe nije glavnoidealski. Odavde sledi i da se svojstvo prstena da bude glavnoidealski ne nasleuje na prstenu polinoma: ako je A glavnoidealski, prsten polinoma $A\,[x]$ ne mora biti glavnoidealski. Tim je značajnija sledeća teorema.

Teorema (Hilbertova teorema o bazi). Ako je prsten A Neterin, tada je i $A\,[x]$ Neterin.

Dokaz. Primetimo da zbog dobre uredjenosti skupa prirodnih brojeva u svakom nepraznom skupu $S \subset A\,[x]$ polinoma postoji polinom najmanjeg stepena. Neka je sad $I \subset A\,[x]$ ideal koji nije konačnogenerisan. Neka je $f_1 \in I$ polinom najmanjeg stepena m_1 u I. Neka je $I_2 = I \setminus (f_1) \neq \emptyset$ i neka je sad $f_2 \in I_2$ element najmanjeg stepena m_2 u I_2. Očigledno, $m_1 \leq m_2$. Postupak

[2] *principal ideal domain* (PID)

[3] po Emi Neter (*Amalie Emmy Noether*, 1882–1935), jednoj od najpoznatijih žena matematičara, ćerki matematičara Maksa Netera (*Max Noether*, 1844–1921). Zato je Neterin, a ne Neterov prsten.

[4] *ascending chain condition* (ACC) (eng.)

nastavljamo: neka je f_k najmanjeg stepena m_k u $I_k = I \setminus (f_1, \ldots, f_{k-1}) \neq \emptyset$. Dobijamo beskonačan niz polinoma $f_1, \ldots, f_k, \ldots$ stepena respektivno $m_1 \leq \cdots \leq m_k \leq \ldots$. Neka je $a_k \in A$ najstariji koeficijent polinoma f_k, $f_k = a_k x^{m_k} + \ldots$ i neka je $(a_1) \subset (a_1, a_2) \subset \cdots \subset (a_1, \ldots, a_k) \subset$ rastući niz ideala u A. Pošto je A Neterin prsten, njihova unija je ideal J generisan konačnim skupom tih koeficijenata, tj. za neko k, $J = (a_1, \ldots, a_k)$. Po konstrukciji, $f_{k+1} \in I_{k+1}$ je najmanjeg stepena i $a_{k+1} \in (a_1, \ldots, a_k)$. To znači da je $a_{k+1} = b_1 a_1 + \cdots + b_k a_k$ i najstariji član polinoma f_{k+1} je

$$a_{k+1} x^{m_{k+1}} = b_1 a_1 x^{m_1} x^{m_{k+1}-m_1} + \cdots + b_k a_k x^{m_k} x^{m_{k+1}-m_k}.$$

Iz ove jednakosti sledi da će se u polinomu $g = f_{k+1} - (b_1 x^{m_{k+1}-m_1} f_1 + \cdots + b_k x^{m_{k+1}-m_k} f_k) \in I$ poništiti najstariji član, pa je $\deg g < m_{k+1} = \deg f_{k+1}$. Ako je $g \in (f_1, \ldots, f_k)$, tada je

$$f_{k+1} = g + (b_1 x^{m_{k+1}-m_1} f_1 + \cdots + b_k x^{m_{k+1}-m_k} f_k) \in (f_1, \ldots, f_k),$$

što je nemoguće jer $f_{k+1} \in I_{k+1}$. Dakle, $g \in I_{k+1}$ je polinom stepena manjeg od f , što je kontradikcija koja dokazuje da je $I_{k+1} = \emptyset$ i $I = (f_1, \ldots, f_k)$.

Egzistencija faktorizacije. U glavnoidealskom prstenu postoji faktorizacija na nerastavljive elemente. Primetimo prvo da

(1) $(b) \subset (a) \Longleftrightarrow a \mid b$,

(2) $(a) = (b) \Longleftrightarrow a$ asocirano sa b,

a zatim dokažimo sledeće činjenice.

(1) Svaki element $a \in A$ ima nerastavljivi faktor $d \in A$, $d \mid a$.

Naime, niz nerastavljivih faktora $...a_{n+1} \mid a_n \mid ... \mid a_2 \mid a_1 \mid a$ definiše rastući niz ideala

$$(a) \subset (a_1) \subset (a_2) \subset \cdots \subset (a_n) \subset (a_{n+1}) \subset \ldots.$$

Njihova unija $\bigcup_n (a_n) = I$ je ideal prstena A pa je zato glavni ideal: $I = (d)$ i $(a) \subset (a_1) \subset \cdots \subset (a_n) \subset \cdots \subset (d)$. Element $d \in \bigcup_n (a_n)$ pripada nekom (a_m) tj. neko a_m deli d. Ali pošto d deli sve a_n, onda su d i a_m asocirani pa je niz $(a_n) \subset \cdots \subset (a_m) = \ldots$ stacionaran počev od a_m. Ovo znači da je a_m nerastavljivi faktor elementa a.

(2) Svaki element a se razlaže na nerastavljive $a = a^{(1)} \cdot a^{(2)} \cdot \cdots \cdot a^{(k)}$. Naime, a ima nerastavljivi faktor $a^{(1)}$ i $a = a^{(1)} a_1$. Sada a_1 ima nerastavljivi faktor $a^{(2)}$ i $a_1 = a^{(2)} a_2$. Dobijamo niz $...a_{n+1} \mid a_n \mid ... \mid a_2 \mid a_1 \mid a$ koji, kao malopre, definiše rastući niz ideala

$$(a) \subset (a_1) \subset (a_2) \subset \cdots \subset (a_n) \subset (a_{n+1}) \subset \ldots$$

i (glavni) ideal $\bigcup_n (a_n) = (d)$. Taj niz mora biti stacionaran, d asociran sa nekim a_k (i sa svim sledećim a_n, $n \geq k$) $\blacksquare$ $(a_k) = (a_{k+1}) = \ldots$. Odatle je $a = a^{(1)} \cdot a^{(2)} \cdot \ldots \cdot (a^{(k)} \cdot \varepsilon)$ gde je ε invertibilan.

Prosti elementi. Jednoznačnost faktorizacije

Jednoznačnost faktorizacije. Naredni korak je da se utvrde uslovi jednoznačnosti faktorizacije. Ako imamo dve nerastavljive faktorizacije istog elementa $a = a_1 \cdot \ldots \cdot a_k = b_1 \cdot \ldots \cdot b_m$ bilo bi poželjno da možemo skratiti nerastavljive faktore sa leve i desne strane. To je razlog za uvodjenje sledećeg pojma.

Definicija. Element $p \in A$ je *prost* ako važi: $p \mid ab \Longrightarrow p \mid a$ ili $p \mid b$.

Ako je p prost, onda je nerastavljiv. Naime, ako je p prost, $p = ab$ i $p \nmid a$, onda $p \mid b$. Dakle, $b = pb'$, $p = apb'$, $ab' = 1$ i a je invertibilan. Zato je p nerastavljiv. Pitanje je da li važi obrnuto, tj. da li iz nerastavljivosti sledi prostost?

Tvrdjenje. (1) U glavnoidealskom prstenu za svaka dva elementa a, b postoji $NZD(a, b)$. Naime, neka su $a, b \in A$. Tada je ideal (a, b) glavni: $(a, b) = (d)$, tj. postoje u, v, p, q takvi da je $d = ua + vb$, $a = pd$, $b = qd$. Ako je $a = p'd', b = q'd'$ za neko d', onda je $d = up'd' + vq'd' = (up' + vq')d'$ pa $d' \mid d$. Ovo upravo znači da je $d = NZD(a, b)$.

(2) U glavnoidealskom prstenu nerastavljivi elementi su prosti. Naime, neka je p nerastavljiv i neka $p \mid ab$, $p \nmid a$, $ab = pq$. Neka je $NZD(a, p) = d$. Tada postoje u, v, q, r takvi da je $d = ua + vp, a = qd, p = rd$. Ali p je nerastavljiv, pa je ili r ili d invertibilan. S tačnošću do asociranih elemenata možemo smatrati da je ili $d = p$ ili $d = 1$. Ako je $d = p$ onda p deli a, što je kontradikcija. Zato je $d = 1$ i $NZD(a, p) = 1$. Odatle sledi $p \mid b$.

Zaključak je da je u glavnoidealskom prstenu nerastavljiv element isto što i prost element. Ova dva pojma se u prstenu celih brojeva $\mathbb{Z}$ i u prstenu polinoma $k[x]$ obično i ne razlikuju. Primetimo da u opštem slučaju ovo ipak nije tačno.

Primer. U domenu $\mathbb{Z}\left[\sqrt{-3}\right]$ važi jednakost $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$, a elementi $2, 1 + \sqrt{-3}$ i $1 - \sqrt{-3}$ nisu medjusobno asocirani, pa je 2 nerastavljiv ali nije prost. Primetimo da su to dve suštinski različite faktorizacije broja 4 na nerastavljive, tj. prsten $\mathbb{Z}\left[\sqrt{-3}\right]$ nije prsten sa jednoznačnom faktorizacijom (a zato nije ni glavnoidealski).

Tvrdjenje. U glavnoidealskom prstenu faktorizacija na nerastavljive elemente je jedinstvena s tačnošću do redosleda i asociranosti faktora.

Dokaz. Neka su $a = a_1 \cdot \ldots \cdot a_k = b_1 \cdot \ldots \cdot b_m$ dve faktorizacije istog

elementa a u proizvod nerastavljivih. Tada je a_1 nerastavljiv i deli proizvod $b_1 \cdot \cdots \cdot b_m$. Pošto je a_1 prost, on deli neko b_{i_1}. Ali b_{i_1} je nerastavljiv, pa su a_1 i b_{i_1} asocirani odnosno $a_1 = b_{\sigma(1)} \cdot \varepsilon_1$. Stavimo $\sigma(1) = i_1$ i skratimo a_1 sa leve i $b_{\sigma(1)}$ sa desne strane jednakosti. Postupak se može induktivno nastaviti, odakle je $k = m$ i dobijamo permutaciju $\sigma \in S_k$ takvu da je $a_i = b_{\sigma(i)} \cdot \varepsilon_i$.

Domen u kome svaki element dopušta jedinstvenu faktorizaciju na nerastavljive (s tačnošću do redosleda i asociranosti faktora) naziva se *prsten sa jednoznačnom faktorizacijom*[5].

Svaki glavnoidealski prsten, a posebno svaki euklidski prsten, je prsten sa jednoznačnom faktorizacijom. Posebno, $\mathbb{Z}$ i $k[x]$ su UFD prsteni. Dokazaćemo da je i prsten $k[x_1, \ldots, x_n]$ polinoma sa više promenljivih takodje UFD, iako nije glavnoidealski.

U svakom prstenu sa jednoznačnom faktorizacijom, svaki nerastavljiv element je prost. Iz dokaza prethodne teoreme vidi se da je jednoznačnost faktorizacije u stvari ekvivalentna prostosti nerastavljivih elemenata (dokažite za domaći).

Navedimo nekoliko osobina u vezi sa prstenom polinoma $A[x]$ sa koeficijentima u prstenu A.

(1) Za svako $a \in A$ i $f \in A[x]$ važi da a deli $f \Longleftrightarrow a$ deli sve koeficijente polinoma f. Smer $\Longleftarrow$ je očigledan. Pretpostavimo da $a \mid a_0 + a_1x + \cdots + a_nx^n$. To znači da je $a_0 + a_1x + \cdots + a_nx^n = a(b_0$

(2) Element a je prost u $A \Longleftrightarrow a$ je prost u $A[x]$. Smer $\Longleftarrow$ je očigledan. Neka je sad a prost u A i neka $a \mid fg$ u $A[x]$. Neka je $f = a_0 + a_1x + \cdots + a_nx^n, g = b_0 + b_1x + \cdots + b_mx^m$. Pretpostavimo da $a \nmid g$ i neka je b_k prvi koeficijent u g koji a ne deli. Dakle, $a \mid b_0, \ldots, b_{k-1}$. Imamo

$$\begin{aligned} fg &= (a_0 + a_1x + \cdots + a_nx^n)(b_0 + b_1x + \cdots + b_mx^m) = \\ &= a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + (a_0b_k + \cdots + a_kb_0)x^k + \cdots + a_nb_mx^{n+m}. \end{aligned}$$

Pošto $a \mid (a_0b_k + \cdots + a_kb_0)$, $a \mid b_0, \ldots, b_{k-1}$ i $a \nmid b_k$, mora biti da $a \mid a_0$ jer je a prost u A. Iz narednih koeficijenata dobijamo da $a \mid a_1, a \mid a_2, \ldots, a \mid a_n$, odakle sledi da $a \mid f$.

(3)

Teorema. Ako je A prsten sa jednoznačnom faktorizacijom, onda je i $A[x]$ takodje prsten sa jednoznačnom faktorizacijom.

U dokazu ove teoreme koristi se jedno istorijski značajno pomoćno tvrdjenje - Gausova lema.

[5]unique factorisation domain (UFD) (eng.)

Definicija. Neka je A prsten sa jednoznačnom faktorizacijom i $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$. *Sadržaj* $\text{cont}(f)$ polinoma f je $\text{cont}(f) := NZD(a_0, \ldots, a_n)$. Biće $f = \text{cont}(f) \cdot g$ pri čemu je $\text{cont}(g) = 1$. Za takav polinom g kažemo da je *primitivan*. Sadržaj je jednoznačno odredjen: ako je $f = a \cdot g$ za neko $a \in A$ pri čemu je $g \in A[x]$ primitivan tada je $a = \text{cont}(f)$.

U prstenu polinoma se može desiti da je $f \in A[x]$ rastavljiv samo zato što ima faktor iz A. Na primer, $2x+4$ u $\mathbb{Z}[x]$ nije nerastavljiv jer je $6x+4 = 2(3x+2)$. Medjutim, faktorizacija $2(3x+2)$ nam jednostavno nije zanimljiva. Ako, pak, odvojimo sadržaj $\text{cont}(f) = 2$ polinoma f, preostaje primitivni polinom $3x + 2$ i on jeste nerastavljiv.

Tvrdjenje (Gausova lema). $\text{cont}(fg) = \text{cont}(f) \cdot \text{cont}(g)$. Posebno, proivod primitivnih polinoma je primitivan.

Dokaz se može izvesti analogno dokazu tačke (2) malopre.

Primetimo sledeće. Neka je K polje razlomaka domena A i $A[x] \subset K[x]$. Svaki polinom $f \in K[x]$ je oblika $f = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_n}{b_n}x^n$. Ako je $s = NZS(b_0, \ldots, b_k)$ i $s = b_ib_i'$ u A, tada je $f = \frac{1}{s}(a_0b_0' + a_1b_1'x + \cdots + a_nb_n'x^n) = \frac{1}{s}g$ pri čemu $g \in A[x]$. Ako je $a = \text{cont}(g)$, sledi da se svaki polinom $f \in K[x]$ može zapisati kao $\left(\frac{a}{s}\right) \cdot f^*$ gde je f^* primitivan polinom iz $A[x]$ pri čemu je element $\alpha = \frac{a}{s} \in K$ jednoznačno odredjen.

Primetimo još da je primitivan polinom $g \in A[x]$ nerastavljiv u $A[x] \iff$ g je nerastavljiv u $K[x]$. Smer $\Longleftarrow$ je očigledan. Ako je $g = g_1g_2$ u $K[x]$, zapišimo $g_i = \alpha_i \cdot g_i^*$ sa primitivnim $g_i^* \in A[x]$ i $\alpha_i \in K$. Dobijamo $g = (\alpha_1\alpha_2)(g_1^*g_2^*) \in A[x]$ i $g_1^*g_2^*$ je primitivan na osnovu Gausove leme, odakle sledi da je $\alpha_1\alpha_2 = 1$ (dokažite) i $g = g_1'g_2'$ u $A[x]$, što je kontradikcija koja dokazuje smer $\Longrightarrow$.

Dokaz teoreme. Neka je $f \in A[x]$, $f = \text{cont}(f) \cdot g$, g primitivan u $A[x]$. Prsten $K[x]$ polinoma sa koeficijentima u polju je prsten sa jednoznačnom faktorizacijom, pa se g u $K[x]$ jednoznačno razlaže u proizvod $g = g_1 \ldots g_k$ nerastavljivih polinoma $g_1, \ldots, g_k \in K[x]$. Dobijamo $f = \frac{1}{s_1 \ldots s_k} g_1^* \ldots g_k^*$ odnosno $sf = g_1^* \ldots g_k^*$ pri čemu je $s = s_1 \ldots s_k \in A$, $g_1^*, \ldots, g_k^* \in A[x]$. Svaki nerastavljivi faktor p elementa s deli neki od $g_1^*, \ldots, g_k^*$ u $A[x]$ pa je $f = h_1 \cdot \cdots \cdot h_k$ tražena faktorizacija u $A[x]$. Jednoznačnost faktorizacije se može dokazati analogno ranijim postupcima (završite za domaći).