O prstenima oblika \(\mathbb{Z}\) i \(\mathbb{Z}\sqrt{m}\)

Belina, Anamarija

Master's thesis / Diplomski rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:502228

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Anamarija Belina

O PRSTENIMA OBLIKA $\mathbb{Z} + \mathbb{Z}\sqrt{m}$

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Zrinka Franušić

Zagreb, srpanj, 2016.

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

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

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

U ovom radu bavit ćemo se integralnim i euklidskim domenama. Razvit ćemo koncept djeljivosti u takvoj domeni koji je zapravo generalizacija Euklidovog teorema o djeljivosti s ostatkom u skupu cijelih brojeva.

U prvom poglavlju definirat ćemo integralnu domenu te proučiti i dokazati neka njezina svojstva. Navest ćemo primjere skupova koji jesu i koji nisu integralne domene. Iskazat ćemo i dokazati zanimljiva svojstva koja vrijede za neke elemente integralne domene kao što su asocirani, ireducibilni i prosti elementi integralne domene te navesti primjere nekih od njih. Proučit ćemo i vezu između ovih elemenata. Bavit ćemo se i podskupovima integralne domene zatvorene na zbrajanje i množenje elemenata tog skupa. Takve podskupove nazivamo idealima. Specijalno ćemo proučiti domenu glavnih ideala kao posebnu klasu ideala. Vidjet ćemo da u toj klasi vrijede neka svojstva ireducibilnih i prostih elemenata koja ne vrijede općenito. Definirat ćemo i proučiti osnovna svojstva prostih i maksimalnih ideala. Na kraju poglavlja, dokazana svojstva omogućit će nam prikaz prostog broja p u obliku $u^2 - mv^2$ ili $mv^2 - u^2$, za dani kvadratno slobodan cijeli broj m i za neke cijele brojeve u i v. Odnosno, pokazat ćemo pod kojim uvjetim je moguć takav prikaz.

U drugom poglavlju bavimo se euklidskom domenom za čiju je definiciju potrebno prethodno definirati i euklidsku funkciju za koju ćemo dokazati neka svojstva. Također ćemo dokazati da je euklidska domena domena glavnih ideala. Posebno ćemo istražiti kada su integralne domene oblika $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ za $m \equiv 2, 3 \pmod 4$ i $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ za $m \equiv 1 \pmod 4$ euklidske domene s obzirom na funkciju koja preslikava $r + s\sqrt{m}$ u $|r^2 - ms^2|$. Odnosno, ispitat ćemo za koje konkretne vrijednosti cijelog broja m navedeni skupovi tvore euklidsku domenu. Zbog složenosti dokaza, provest ćemo samo za neke od njih. Ovim dokazima se i danas bave poznati matematičari, a tijekom 20. stoljeća to je bilo područje u koje su mnogi ulagali veliki napor unutar algebarske teorije brojeva. Posljednje rezultate u ovom području objavila su dva matematičara sredinom prošlog stoljeća. Bili su to H. Chatland i H. Davenport. Harold Chatland (1911.-1999.) je bio kanadski matematičar koji se na početku svoje karijere bavio matematičkom analizom, a tek nešto kasnije teorijom brojeva. Radio je na poznatim američkim sveučilištima kao na primjer u Montani gdje je i započeo svoju karijeru, Chicagu, Ohiu... Bavio se još i astronomijom i fizikom. Harold Davenport (1907.-1969.) bio je engleski matematičar koji se najviše bavio područjem teorije brojeva,

kasnije u životu odlučuje se posvetiti diofantskim aproksimacijama i geometriji brojeva. Bio je član Londonskog matematičkog društva, a u jednom periodu i njegov predsjednik. Tijekom života radio je i predavao na prestižnim sveučilištima diljem Velike Britanije. Na kraju života zažalio je što više vremena nije posvetio dokazu Riemannove hipoteze.

Konačno, dokazana svojstva ovih stuktura omogućit će nam karakterizaciju reprezentabilnosti prostog broja p pomoću binarne kvadratne forme oblika $x^2 + y^2$, $x^2 + 2y^2$, $x^2 + xy + y^2$, $x^2 + xy + 2y^2$ i $x^2 + xy + 3y^2$.

Poglavlje 1

Integralna domena

1.1 Definicija i primjeri integralne domene

Prije nego što definiramo pojam integralne domene prisjetit ćemo se nekih važnijih algebarskih struktura kao što su grupa, prsten i polje.

Neka je G neki neprazan skup na kojem je definirana samo jedna binarna operacija koju označimo s $\circ$. Dakle, binarna operacija $\circ$ pridružuje svakom paru elemenata iz G element iz G, to jest još kažemo da je skup G zatvoren s obzirom na operaciju $\circ$. Kažemo da je $(G, \circ)$ *grupa* ako vrijede sljedeća svojstva:

(i) $(xy)z = x(yz)$ za sve $x, y, z \in G$ (asocijativnost);

(ii) Postoji $e \in G$ takav da je $ex = xe = x$ za sve $x \in G$ (postojanje neutralnog elementa);

(iii) Za svaki $e \in G$ postoji $y \in G$ takav da je $xy = yx = e$ (postojanje inverza).

Kraće ćemo reći da je skup G grupa s obzirom na operaciju $\circ$. Ako je operacija $\circ$ i komutativna, to jest $a \circ b = b \circ a$, za sve $a, b \in G$, onda kažemo da je G komutativna ili Abelova grupa

Neka je sada R neprazan skup na kome su definirane dvije binarne operacije koje označimo s $+$ i $\cdot$, a tradicionalno ih nazivamo zbrajanje i množenje. Kažemo da je $(R, +, \cdot)$ *prsten* ako je

(i) $(R, +)$ komutativna grupa;

(ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, za sve $a, b, c \in R$ (asocijativnost operacije $\cdot$);

(iii) $(a + b) \cdot c = a \cdot c + b \cdot c$, $a \cdot (b + c) = a \cdot b + a \cdot c$, za sve $a, b, c \in R$ (distributivnost).

Ako je operacija $\cdot$ komutativna, onda je kažemo da je *R komutativan prsten*. Ako u strukturi $(R, \cdot)$ postoji neutralni element, obično ga označavamo s 1 i zovemo jedinicom, onda se *R* naziva *komutativan prsten s jedinicom.*

Da bismo definirali integralnu domenu potreban nam je pojam djelitelja nule. Za element $a \neq 0$ komutativnog prstena R kažemo da je *djelitelj nule* ako postoji $b \neq 0$ takav da $ab = 0$. Onda je i b djelitelj nule.

Definicija 1.1. Integralna domena *je komutativni prsten s jedinicom koja nema djelitelja nule. Integralna domena D je* polje *ako je svaki nenul element ima multiplikativni inverz, to jest ako za svaki* $a \in D$, $a \neq 0$ *postoji* $b \in D$ *takav da je* $ab = 1$.

Uočimo, ako je D polje onda je D Abelova grupa s obzirom na zbrajanje i $D^* = D\backslash\{0\}$ je Abelova grupa s obzirom na množenja. Nula - neutralni element aditivne Abelove grupe - ne može biti invertibilan. Zaista, vrijedi $0 \cdot a = a \cdot 0 = 0$, za sve $a \in D$.

U sljedećim primjerima predstavit ćemo neke podskupove polja kompleksnih (i realnih) brojeva i pokazati da imaju struktruru integralne domene s obzirom na standardne operacije zbrajanja i množenja iz polja. Jedino što trebamo uočiti jest da su dani skupovi aditivne podgrupe, te da je množenje na njima zatvorena operacija. Sva ostala svojstva se nasljeđuju, uključujući i bitno svojstvo integralne domene da nema djelitelja nule.

Primjer 1.2. Prsten cijelih brojeva, $\mathbb{Z} = \{0, \pm 1, \pm 2, ...\}$, je integralna domena.

□

Primjer 1.3. Skup

$$\mathbb{Z} + \mathbb{Z}i = \{a + bi \,|\, a, b \in \mathbb{Z}\}$$

je integralna domena. Zaista, skup $\mathbb{Z} + \mathbb{Z}i$ je očito aditivna podgrupa od $\mathbb{C}$, te vrijedi da je množenje zatvoreno, odnosno $(a+bi)(c+di) = ac-bc+(ad+bd)i \in \mathbb{Z}+\mathbb{Z}i$ za $a, b, c, d \in \mathbb{Z}$. Nadalje, u $\mathbb{C}$ nema djelitelja nule (jer je to polje). Elementi skupa $\mathbb{Z} + \mathbb{Z}i$ nazivaju se *Gaussovi cijeli brojevi*, odnosno skup $\mathbb{Z} + \mathbb{Z}i$ nazivat ćemo *Gaussovom domenom*. Dobili su ime po poznatom matematičaru Carlu Fridrichu Gaussu (1777.-1855.) koji je izučio njihova glavna svojstva.

□

Primjer 1.4. Neka je

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

gdje je

$$\omega = \frac{-1 + \sqrt{-3}}{2}.$$

Broj ω predstavlja treći (kompleksni) korijen iz jedinice, 1. Provjerimo da je skup zatvoren na množenje. Neka su $a + b\omega, c + d\omega \in \mathbb{Z} + \mathbb{Z}\omega$. Tada vrijedi

$$(a + b\omega)(c + d\omega) = ac + bd\omega^2 + (ad + bc)\omega. \tag{1.1}$$

Kako je

$$\omega^2 = \frac{(-1 + \sqrt{-3})^2}{4} = \frac{-2 + 2i\sqrt{-3}}{4} = \frac{-1 + \sqrt{-3}}{2} = -\frac{-1 + \sqrt{-3}}{2} - 1 = -\omega - 1,$$

iz (1.1) dobivamo

$$(a + b\omega)(c + d\omega) = ac + bd(-\omega - 1) + (ad + bc)\omega = ac - bd + (ad + bc - bd)\omega,$$

pa zaključujemo da je $(a+b\omega)(c+d\omega) \in \mathbb{Z}+\mathbb{Z}\omega$. Stoga je skup $\mathbb{Z}+\mathbb{Z}\omega$ je također integralna domena. Elementi ovog skupa nazivaju se *Einsteinovi cijeli brojevi* prema matematičaru Gottholdu Einsteinu (1823.-1852.), odnosno skup $Z + \mathbb{Z}\omega$ se naziva *Einsteinova domena*.

Uočimo da je

$$\mathbb{Z} + \mathbb{Z}\omega = \mathbb{Z} + \mathbb{Z}\omega^2$$

jer smo pokazali da je $\omega^2 = -\omega - 1$. Broj ω^2 je još jedan treći korijen iz 1.

□

Prisjetimo se, reći ćemo da je broj $m \in \mathbb{Z}$ *potpun kvadrat* ako postoji $x \in \mathbb{Z}$ takav da je $|m| = x^2$.

Primjer 1.5. Neka je $m \in \mathbb{Z}$ i m nije potpun kvadrat. Definiramo skup

$$\mathbb{Z} + \mathbb{Z}\sqrt{m} = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}.$$

Pokažimo da je ovaj skup integralna domena. Kako se sva bitna svojstva nasljeđuju iz polja $\mathbb{R}$ (ako je $m > 0$), odnosno iz polja $\mathbb{C}$ (ako je $m < 0$), treba samo provjeriti zatvorenost operacije množenja:

$$(a + b\sqrt{m})(c + d\sqrt{m}) = ac + bdm + (ac + bd)\sqrt{m} \in \mathbb{Z} + \mathbb{Z}\sqrt{m},$$

za sve $a, b, c, d \in \mathbb{Z}$. Ova domena se ponekad naziva *kvadratna domena*, jer je $\sqrt{m}$ korijen kvadratnog polinoma $p(x) = x^2 - m$.

Ako je k cijeli broj različit od nule takav da k^2 dijeli m, onda je

$$\mathbb{Z} + \mathbb{Z}\sqrt{m} \subseteq \mathbb{Z} + \mathbb{Z}\sqrt{m/k^2},$$

pri čemu jednakost vrijedi ako i samo ako $k^2 = 1$. Za $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ kažemo da je *poddomena* od $\mathbb{Z} + \mathbb{Z}\sqrt{m/k^2}$. Na primjer, $\mathbb{Z} + 2\mathbb{Z}i$ je poddomena od $\mathbb{Z} + \mathbb{Z}i$.

□

Primjer 1.6. Neka je m cijeli broj koji nije potpuni kvadrat i kongruentan je 1 modulo 4, to jest $m \equiv 1 \pmod 4$. Zadan je skup

$$\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right) = \{a + b\left(\frac{1+\sqrt{m}}{2}\right) \mid a, b \in \mathbb{Z}\}.$$

Vrijedi

$$(a + b\left(\frac{1+\sqrt{m}}{2}\right))(c + d\left(\frac{1+\sqrt{m}}{2}\right)) = ac + bd\left(\frac{1+\sqrt{m}}{2}\right)^2 + (ad + bc)\left(\frac{1+\sqrt{m}}{2}\right).$$

Kako je $m \equiv 1 \pmod 4$, postoji $k \in \mathbb{Z}$ takv da je $m = 4k + 1$, pa je

$$\left(\frac{1+\sqrt{m}}{2}\right)^2 = \frac{1 + 2\sqrt{m} + m}{4} = \frac{1 + 2\sqrt{m} + 4k + 1}{4} = \frac{1+\sqrt{m}}{2} + k,$$

odnosno

$$(a + b\left(\frac{1+\sqrt{m}}{2}\right))(c + d\left(\frac{1+\sqrt{m}}{2}\right)) = ac + bdk + (ad + bc + bd)\left(\frac{1+\sqrt{m}}{2}\right)$$

je element skupa $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$. Dakle, $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ je integralna domena koju također nazivamo *kvadratna domena* jer je $\frac{1+\sqrt{m}}{2}$ korijen kvadratnog polinoma (uglavnom polinoma $p(x) = x^2 - x + \frac{1-m}{4}$).

Bitno je naglasiti da $\mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{m}}{2})$ nije integralna domena u slučaju kada $m \not\equiv 1 \pmod 4$ jer tada operacija množenja nije zatvorena. Na primjer,

$$\underbrace{\left(\frac{1+\sqrt{m}}{2}\right)}_{\in \mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)} \underbrace{(1 - \left(\frac{1+\sqrt{m}}{2}\right))}_{\in \mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)} = \left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1-\sqrt{m}}{2}\right) = \frac{1-m}{4} \notin \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right).$$

Uočimo da elemente skupa $\mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{m}}{2})$ možemo zapisati i u obliku $\frac{1}{2}(x + y\sqrt{m})$, gdje su x i y cijeli brojevi takvi da $x \equiv y \pmod 2$. Zaista,

$$a + b\left(\frac{1+\sqrt{m}}{2}\right) = \frac{2a + b + b\sqrt{m}}{2} = \frac{x + y\sqrt{m}}{2},$$

pa je $x = 2a + b \equiv b = y \pmod 2$. Očito vrijedi da je domena $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ poddomena od $\mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{m}}{2})$.

□

Primjer 1.7. Neka je $\mathbb{F}$ polje. Skup svih polinoma u jednoj varijabli x s koeficijentima iz polja $\mathbb{F}$ označava se s $\mathbb{F}[x]$. Poznato je da je $\mathbb{F}[x]$ prsten, kojeg nazivamo *prsten polinoma*. Budući $p(x)q(x) \neq 0$ za sve $p, q, \in \mathbb{F}[x]\backslash\{0\}$, slijedi da je $\mathbb{F}[x]$ integralna domena. Štoviše, ako je D integralna domena, onda će i skup svih polinoma u jednoj varijabli x s koeficijentima iz polja D, biti također integralna domena. Naprimjer, $\mathbb{Z}[x]$, to jest prsten polinoma sa cjelobrojnim koeficijentima je integralna domena.

Prsten polinoma u dvije varijable x i y s koeficijentima iz polja $\mathbb{F}$, $\mathbb{F}[x, y]$, je također integralna domena.

□

Primjer 1.8. Zadan je skup

$$\mathbb{Z} + \mathbb{Z}\Theta + \mathbb{Z}\Theta^2 = \{a + b\Theta + c\Theta^2 \mid a, b, c \in \mathbb{Z}\},$$

gdje je Θ rješenje kubne jednadžbe $\Theta^3 + \Theta + 1 = 0$. Pokazujemo da je $\mathbb{Z} + \mathbb{Z}\Theta + \mathbb{Z}\Theta^2$ integralna domena. Kao i do sada ključno je provjeriti zatvorenost množenja. Vrijedi

$$(a + b\Theta + c\Theta^2)(d + e\Theta + f\Theta^2) = ad + (ae + bd)\Theta + (af + be + cd)\Theta^2 + (bf + ce)\Theta^3 + cf\Theta^4.$$

Kako je

$$\Theta^3 = -\Theta - 1,$$

te

$$\Theta^4 = \Theta \cdot \Theta^3 = \Theta(-\Theta - 1) = -\Theta^2 - \Theta,$$

slijedi

$$\begin{aligned} & (a + b\Theta + c\Theta^2)(d + e\Theta + f\Theta^2) = \\ = \;& ad + (ae + bd)\Theta + (af + be + cd)\Theta^2 + (bf + ce)(-\Theta - 1) + cf(-\Theta^2 - \Theta) \\ = \;& ad - bf - ce + (ae + bd - bf - ce - cf)\Theta + (af + be + cd - cf)\Theta^2, \end{aligned}$$

pa smo pokazali da je umnožak u $\mathbb{Z} + \mathbb{Z}\Theta + \mathbb{Z}\Theta^2$. Zvat ćemo ga *kubna domena*.

□

Primjer 1.9. Neka je

$$D = \left\{ a + bi + \frac{c + di}{2}\sqrt{2} \;\mid\; a, b, c, d \in \mathbb{Z},\ c \equiv d \pmod 2 \right\}.$$

Skup D je integralna domena. Provjerimo zatvorenost množenja. Vrijedi

$$\begin{aligned}
&(a_1 + b_1 i + \frac{c_1 + d_1 i}{2}\sqrt{2})(a_2 + b_2 i + \frac{c_2 + d_2 i}{2}\sqrt{2}) = \\
= \;& (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)i + \frac{(a_1 c_2 - b_1 d_2)}{2}\sqrt{2} + \frac{(a_1 d_2 - b_1 c_2)i}{2}\sqrt{2} + \\
&+ \frac{c_1\sqrt{2} + d_1\sqrt{2}i}{2} \cdot \frac{c_2\sqrt{2} + d_2\sqrt{2}i}{2} = \\
= \;& (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)i + \frac{(a_1 c_2 - b_1 d_2)}{2}\sqrt{2} + \frac{(a_1 d_2 - b_1 c_2)i}{2}\sqrt{2} + \frac{c_1 c_2 - d_1 d_2}{2} + \\
&+ \frac{(c_1 d_2 - d_1 c_2)i}{2},
\end{aligned}$$

jer je $c_1 \equiv d_1 \pmod 2$ i $c_2 \equiv d_2 \pmod 2$ slijedi

$$\begin{aligned}
&(a_1 a_2 - b_1 b_2 + \frac{c_1 c_2 - d_1 d_2}{2}) + (a_1 b_2 + b_1 a_2 + \frac{c_1 d_2 - d_1 c_2}{2})i + \frac{(a_1 c_2 - b_1 d_2)}{2}\sqrt{2} + \\
&+ \frac{(a_1 d_2 - b_1 c_2)i}{2}\sqrt{2} \in D.
\end{aligned}$$

□

Napomena 1.10. Očito vrijedi $\mathbb{Z} + \mathbb{Z}\sqrt{2} \subset D, \mathbb{Z} + \mathbb{Z}i \subset D, \mathbb{Z} + \mathbb{Z}i\sqrt{2} \subset D$.

1.2 Svojstva integralne domene

Propozicija 1.11. *Neka je D integralna domena. Tada vrijede sljedeća svojstva:*

a) *Multiplikativni neutralni element u D je jedinstven.*

b) *Ako vrijedi da je $ab = ac$, pri čemu su $a, b, c \in D$ i $a \neq 0$, onda je $b = c$.*

c) *Ako vrijedi da je $ac = bc$, pri čemu su $a, b, c \in D$ i $a \neq 0$, onda je $a = b$.*

Dokaz. **a)** Pretpostavimo suprotno, to jest neka su 1 i $1'$ neutralni elementi množenja. Tada vrijedi $1 = 1 \cdot 1'$ jer je $1'$ neutralni element, te $1' = 1 \cdot 1'$ jer je i 1 neutralni element.

b) Vrijedi

$$ab = ac \iff ab - ac = 0 \iff a(b - c) = 0 \iff a = 0 \text{ ili } b - c = 0.$$

Kako je $a \neq 0$ i u D ne postoje djelitelji nule, slijedi $b - c = 0$, to jest $b = c$.

c) Analogno kao u b).

□

Definicija 1.12. *Neka su a i b elementi integralne domene D. Kažemo da je a* djelitelj *od b ili da a* dijeli *b ako postoji c iz D takav da $b = ac$ i pišemo $a \mid b$. Ako a nije djelitelj od b, to jest a ne dijeli b, pišemo $a \nmid b$.*

Primjer 1.13.

a) $1 + i \mid 2$ u $\mathbb{Z} + \mathbb{Z}i$, jer je $2 = (1 + i)(1 - i)$;

b) $x^2 + x + 1 \mid x^4 + x^2 + 1$ u $\mathbb{Z}[x]$, jer je $x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$;

c) $(1 - \omega)^2 \mid 3$ u $Z + \mathbb{Z}\omega$, jer je $3 = (1 - \omega)^2(1 + \omega)$;

d) $1 + \Theta - \Theta^2 \mid -\Theta - 2\Theta^2$ u $\mathbb{Z} + \mathbb{Z}\Theta + \mathbb{Z}\Theta^2$, jer je $-\Theta - 2\Theta^2 = (1 + \Theta - \Theta^2)(1 - \Theta)$;

e) $2 + \sqrt{2} \nmid 3$ u $\mathbb{Z} + \mathbb{Z}\sqrt{2}$, jer $\frac{3}{2+\sqrt{2}} = 3 - \frac{3}{2}\sqrt{2} \notin \mathbb{Z} + \mathbb{Z}\sqrt{2}$.

□

U sljedećoj propoziciji navodimo neka svojstva djelitelja iz integralne domene.

Propozicija 1.14. *Neka je D integralna domena i $a, b, c \in D$. Tada vrijede sljedeća svojstva:*

a) *$a \mid a$ (refleksivnost);*

b) *Ako $a \mid b$ i $b \mid c$, onda $a \mid c$ (tranzitivnost);*

c) *Ako $a \mid b$ i $a \mid c$, onda $a \mid xb + yc$ za svaki $x, y \in D$;*

d) *Ako $a \mid b$, onda $ac \mid bc$;*

e) *Ako $ac \mid bc$ i $c \neq 0$, onda $a \mid b$;*

f) *$1 \mid a$;*

g) *$a \mid 0$;*

h) *Ako $0 \mid a$, onda $a = 0$.*

Dokaz. Tvrdnje slijede odmah iz Definicije 1.12. □

Definicija 1.15. *Element a integralne domene D naziva se* jedinica *ako $a \mid 1$. Skup svih jedinica od D označavamo s $U(D)$ (od engl. unit).*

U sljedećoj propoziciji i teoremu navodimo neka svojstva skupa jedinica integralne domene.

Propozicija 1.16. *Neka je D integralna domena. Tada za $U(D)$ vrijede sljedeća svojstva:*

a) $\pm 1 \in U(D)$*;*

b) *Ako je $a \in U(D)$, onda je $-a \in U(D)$;*

c) *Ako je $a \in U(D)$, onda je a invertilibilan i $a^{-1} \in U(D)$;*

d) *Ako je $a \in U(D)$ i $b \in U(D)$, onda je $ab \in U(D)$;*

e) *Ako je $a \in U(D)$, onda je $\pm a^n \in U(D)$, za svaki $n \in \mathbb{Z}$.*

Dokaz. **a)** Vidimo da $\pm 1 \mid 1$ jer $(\pm 1) \cdot (\pm 1) = 1$.

b) Ako je $a \in U(D)$, onda postoji $b \in D$ takav da je $1 = a \cdot b$. Kako je $1 = (-a) \cdot (-b)$, slijedi da $-a \mid 1$, odnosno $-a \in U(D)$.

c) Ako je $a \in U(D)$, onda je $a \cdot b = 1$, za neki $b \in D$. Stoga je a invertibilan i $b = a^{-1}$ pa slijedi tvrdnja.

d) Prema pretpostavci je $a \cdot c = 1$, $b \cdot d = 1$, za neke $c, d \in D$. Otuda je $(ac)(bd) = 1$. Kako je operacija množenja u D komutativna i asocijativna, slijedi $(ab)(cd) = 1$, odnosno $ab \in U(D)$.

e) Iz svojstva d) za $b = a$ te primjenom principa matematičke indukcije slijedi $a^n \in U(D)$, za sve $n \in \mathbb{N}$. Dalje, prema svojstvu b) i svojstvu c) slijedi da je $\pm(a^n)^{-1} \in U(D)$, za sve $n \in \mathbb{N}$, odnosno $\pm a^n \in U(D)$, za sve $n \in \mathbb{Z}$.

□

Primjer 1.17.

a) $i \in U(\mathbb{Z} + \mathbb{Z}i)$, jer je $i(-1) = 1$;

b) $\omega, \omega + 1 \in U(\mathbb{Z} + \mathbb{Z}\omega)$, jer $-\omega(\omega + 1) = 1$;

c) $\Theta, \Theta^2 + 1 \in U(\mathbb{Z} + \mathbb{Z}\Theta + \mathbb{Z}\Theta^2)$, jer je $1 = -\Theta(\Theta^2 + 1)$.

d) $1 + \sqrt{2} \in U(\mathbb{Z} + Z\sqrt{2})$, jer je $(1 + \sqrt{2})(-1 + \sqrt{2}) = 1$.

□

Teorem 1.18. *Ako je D integralna domena, onda je $U(D)$ Abelova grupa s obzirom na množenje.*

Dokaz. Da bismo pokazali svojstva Abelove grupe koristimo se Propozicijom 1.16.

$U(D)$ je zatvoren na množenje prema svojstvu d). Kako je D integralna domena, to je množenje u skupu $U(D)$ asocijativno i komutativno. Prema svojstvu a), neutralni element množenja 1 je iz $U(D)$. Prema svojstvu c), svaki element skupa $U(D)$ ima multiplikativni inverz i on je u $U(D)$. Dakle, $U(D)$ je Abelova grupa obzirom na množenje. □

Uočimo da je svaki invertibilan element iz D, također iz $U(D)$. Stoga prema Propozicijom 1.16 c), slijedi da je $U(D)$ zapravo grupa invertibilnih elemenata u domeni D.

Sada ćemo definirati pojam asociranih, odnosno pridruženih elemenata.

Definicija 1.19. *Za dva nenul elementa a i b iz domene D kažemo da su* pridruženi *ili* asocirana *ako svaki od njih dijeli drugoga, to jest $a|b$ i $b|a$. Pišemo $a \sim b$. Ako a i b nisu asocirani pišemo $a \nsim b$.*

Propozicija 1.20. *Neka je D integralna domena te neka su $a, b, c \in D^* = D \setminus \{0\}$. Tada vrijede sljedeća svojstva.*

a) *$a \sim a$ (refleksivnost);*

b) *Ako $a \sim b$, onda $b \sim a$ (simetričnost);*

c) *Ako $a \sim b$ i $b \sim c$, onda $a \sim c$ (tranzitivnost);*

d) *Ako $a \sim b$ i ako je b invertibilan, onda $ab^{-1} \in U(D)$;*

e) *$a \sim 1$ ako i samo ako je a jedinica;*

f) *$a \sim b$ ako i samo ako je $a = \beta b$ za neki $\beta \in U(D)$.*

Dokaz. **a)** Trivijalno, $a = a \cdot 1$, za sve $a \in D$.

b) Svojstvo simetričnosti slijedi direktno iz definicije.

c) Neka su $a, b, c \in D^*$. Iz $a \sim b$ i $b \sim c$ prema definiciji asociranih elemenata slijedi $a \mid b, b \mid a, b \mid c$ i $c \mid b$. Budući da $a \mid b$ i $b \mid c$, slijedi da $a \mid c$. Prema Propoziciji 1.14 b) slijedi da $c \mid a$. Prema tome $a \sim c$.

d) Prema pretpostavci $a \mid b$ i $b \mid a$, to jest $b = \alpha a$, $a = \beta b$, za neke $\alpha, \beta \in D$. Ako je b invertibilan, množenjem $b = \alpha a$ s b^{-1} slijedi $1 = \alpha a b^{-1}$, odnosno $ab^{-1} \in U(D)$.

e) Ako $a \sim 1$, onda $1 \mid a$ i $a \mid 1$, pa je $a \in U(D)$. S druge strane ako $a \in U(D)$, onda $a \mid 1$. Uvijek vrijedi $1 \mid a$, pa $a \sim 1$.

f) Neka je $a \sim b$, to jest $a \mid b$ i $b \mid a$, tada trivijalno slijedi da je $a = \beta b$ za neki $\beta \in U(D)$. Obratno, neka je $a = \beta b$ za neki $\beta \in U(D)$. Tada vrijedi $a \mid b$. Nadalje, kako je za $b = \beta^{-1}a$ i $\beta^{-1} \in U(D)$, slijedi $b \mid a$. Dakle, $a \sim b$.

□

Napomena 1.21. Svojstva a), b) i c) ukazuju na to da je relacija $\sim$ - relacija ekvivalencije. Klasa ekvivalencije generirana elementom $a \in D$ je skup $[a] = \{ua \mid u \in U(D)\}$.

Primjer 1.22.

a) Ako $a \sim b$ u $\mathbb{Z}$, onda je $a = \pm b$, odnosno $|a| = |b|$;

b) U domeni $\mathbb{Z} + \mathbb{Z}i$ je

$$1 + i \sim 1 - i,$$

jer je $1 + i = i(i - 1)$ i $i \in U(\mathbb{Z} + \mathbb{Z}i)$;

c) U domeni $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ je

$$1 + 3\sqrt{2} \sim 5 - 2\sqrt{2},$$

gdje je $1 + 3\sqrt{2} = (1 + \sqrt{2})(5 - 2\sqrt{2})$ i $1 + \sqrt{2} \in U(\mathbb{Z} + Z\sqrt{2})$.

□

Pojam prostog broja definirali smo na skupu prirodnih brojeva većih od 1. Prisjetimo se, za prirodan broj p veći od 2 reći ćemo da je *prost* ako nema djelitelja većeg od od 1 i manjeg od p. Dakle, jedini pozitivni djelitelji broja p su 1 i p. Lako se mogu pokazati sljedeća svojstva prostih brojeva:

Propozicija 1.23. *Neka je $p \in \mathbb{N}$ prost. Ako za $a, b \in \mathbb{Z}$ vrijedi da je*

a) *$p = ab$, onda je $a = \pm 1$ ili $b = \pm 1$;*

b) *$p \mid ab$, onda je $p \mid a$ ili $p \mid b$.*

Prethodna svojstva poslužit će nam za karakterizaciju elemenata u domeni D.

Definicija 1.24. *Neka je a iz integralne domene D, te $a \neq 0$ i $a \notin U(D)$. Kažemo da je a* ireducibilan*, ako iz $a = bc$ za $b, c \in D$ slijedi da je $b \in U(D)$ ili $c \in U(D)$.*

Primjer 1.25. Broj 2 je ireducibilan u $\mathbb{Z}$. Budući da vrijedi $2 = ab$, $a, b \in \mathbb{Z}$, očito slijedi da je $a = \pm 1$ ili $b = \pm 1$. □

Primjer 1.26. Broj 2 je ireducibilan u $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Pretpostavimo da je

$$2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$$

gdje su $a, b, c, d \in \mathbb{Z}$. Otuda je

$$4 = |a + b\sqrt{-5}|^2 |c + d\sqrt{-5}|^2,$$

odnosno

$$4 = (a^2 + 5b^2)(c^2 + 5d^2).$$

Prema tome, $a^2 + 5b^2$ je pozitivan cijeli djelitelj od 4 pa mora vrijediti

$$a^2 + 5b^2 = 1, 2 \text{ ili } 4.$$

Stoga vidimo da je

$$(a, b) = (\pm 1, 0) \text{ ili } (a, b) = (\pm 2, 0).$$

pa je

$$a + b\sqrt{-5} = \pm 1 \text{ ili } a + b\sqrt{-5} = \pm 2.$$

Ako je $a + b\sqrt{-5} = \pm 1$, onda smo pokazali tvrdnju. Ako je $a + b\sqrt{-5} = \pm 2$, onda je

$$c + d\sqrt{-5} = \frac{2}{a + b\sqrt{-5}} = \frac{2}{\pm 2} = \pm 1,$$

to jest element iz $U(\mathbb{Z} + \mathbb{Z}\sqrt{-5})$. Prema tome, 2 je ireducibilan u $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$.

□

Primjer 1.27. Broj 2 nije ireducibilan u $\mathbb{Z} + \mathbb{Z}\sqrt{2}$.
Zaista,

$$2 = (2 + \sqrt{2})(2 - \sqrt{2}),$$

ali ni $2 + \sqrt{2}$ ni $2 - \sqrt{2}$ nisu jedinice u $\mathbb{Z} + \mathbb{Z}\sqrt{2}$. □

Definicija 1.28. *Neka je p element integralne domene D, te $p \neq 0$ i $p \notin U(D)$. Kažemo da je p* prost *ako iz $p \mid ab$, gdje su $a, b \in D$, slijedi da $p \mid a$ ili $p \mid b$.*

Je li neki broj prost ovisi o 'ambijentu' u kojem se nalazimo, odnosno ovisi o integralnoj domeni čiji je on element.

Primjer 1.29. Broj 2 je prost u $\in \mathbb{Z}$. Pretpostavimo da $2 \mid ab$, gdje su $a, b \in \mathbb{Z}$ takvi da je ab paran broj. Da bi umnožak dva cijela broja bio paran, barem jedan od njih mora biti paran. Slijedi da $2 \mid a$ ili $2 \mid b$. Time smo pokazali da je 2 prost. □

Primjer 1.30. Broj 2 nije prost u $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Očito je

$$2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

no $2 \nmid 1 + \sqrt{-5}$ i $2 \nmid 1 - \sqrt{-5}$. Zaista, $2 = \frac{1+\sqrt{5}}{2}(1 - \sqrt{5})$ i $\frac{1+\sqrt{5}}{2} \notin \mathbb{Z} + \mathbb{Z}\sqrt{-5}$.

Primjer 1.31. Broj $1 + i$ je prost u $\mathbb{Z} + \mathbb{Z}i$. Pretpostavimo da je

$$1 + i \mid (a + bi)(c + di),$$

gdje su $a, b, c, d \in Z$. Tada postoje cijeli brojevi x i y takvi da vrijedi

$$(a + bi)(c + di) = (1 + i)(x + yi)$$

Stoga su i pripadni moduli jednaki, pa dobivamo

$$(a^2 + b^2)(c^2 + d^2) = 2(x^2 + y^2)$$

Kako je 2 prost u $\mathbb{Z}$, slijedi

$$2 \mid a^2 + b^2 \text{ ili } 2 \mid c^2 + d^2.$$

Bez smanjenja općenitosti pretpostavimo da $2 \mid a^2 + b^2$. Prema tome, ili su oba a i b parni ili su oba neparni brojevi. U prvom slučaju stavimo $a = 2r$ i $b = 2s$, gdje su r i s cijeli brojevi. Kako je

$$a + bi = 2(r + si) = (1 + i)((r + s) + (-r + s)i),$$

slijedi da je $1 + i \mid a + bi$. U drugom slučaju stavimo $a = 2r + 1$ i $b = 2s + 1$, gdje su r i s cijeli brojevi. Jer je

$$a + bi = 2(r + si) + (1 + i) = (1 + i)((r + s + 1) + (-r + s)i),$$

dobivamo $1 + i \mid a + bi$. Stoga zaključujemo da je $1 + i$ prost u $\mathbb{Z} + \mathbb{Z}i$. □

Teorem 1.32. *Neka je D integralna domena i $p \in D$. Ako je p prost u D, onda je p ireducibilan u D.*

Dokaz. Neka je $p \in D$ prost takav da vrijedi $p = ab$, gdje su $a, b \in D$. Kako je p prost, zaključujemo da $p \mid a$ ili $p \mid b$. Odnosno, $a = \alpha p$ ili $b = \beta p$, za neke $\alpha, \beta \in D$. Bez smanjenja općenitosti pretpostavimo da je $a = \alpha p$. Vrijedi $ab = \alpha pb$. Odnosno, $p = (\alpha b)p$. Prema Propoziciji 1.11 c) slijedi $1 = \alpha b$, to jest $b \mid 1$, odnosno $b \in U(D)$. Prema tome, p je ireducibilan element u D. □

Napomena 1.33. Obrat Teorema 1.32 ne vrijedi. Pogledajmo Primjer 1.27 i Primjer 1.30. Vidimo da je 2 ireducibilan u $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$, ali nije prost u $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$.

Sada ćemo proučiti podskupove integralne domene D koji su zatvoreni na zbrajanje i množenje elemenata iz te integralne domena. Te podskupove nazivamo *ideali*.

Definicija 1.34. *Neka je D integralna domena. Neprazan podskup I integralne domene D je* ideal *ako vrijede svojstva:*

1) *Ako su $a, b \in I$, onda je $a + b \in I$;*

2) *Ako je $a \in I$ i $r \in D$, onda je $ra \in I$.*

Napomena 1.35. Očito vrijedi da ako je $a_1, a_2, ..., a_n \in I$, onda je i $a_1r_1, a_2r_2, ..., a_nr_n \in I$, za sve $r_1, r_2, ..., r_n \in D$. Nadalje, ako je $a \in I$ i $b \in I$, onda je i $-a \in I$ i $a - b \in I$. Također, $0 \in I$ te ako je $1 \in I$, onda je $I = D$.

Primjer 1.36. Neka je D integralna domena. Ako je $\{a_1, a_2, ..., a_n\}$ skup elemenata integralne domene D, onda je skup svih linearnih kombinacija od $a_1, a_2, ..., a_n$

$$\left\{ \sum_{i=1}^{n} r_i a_i \mid r_1, r_2, ..., r_n \in D \right\}$$

ideal u D. Zapisujemo ga kao $\langle a_1, a_2, ..., a_n \rangle$.

Istaknutu ulogu imaju tzv. glavni ideali i pravi ideali.

Definicija 1.37. *Ideal I integralne domene D naziva se* glavni ideal *ako postoji $a \in I$ takav da $I = \langle a \rangle$. Odnosno, ideal je glavni ako je generiran skupom koji ima samo jedan element. Tada element a nazivamo* generatorom *ideala I.*

Napomena 1.38. Ako je D integralna domena, glavni ideal $\langle a \rangle$ generiran elementom $a \in D$ je skup $\{ra \mid r \in D\}$. Očito je da je glavni ideal $\langle 0 \rangle$ jednočlan skup $\{0\}$, a glavni ideal $\langle 1 \rangle$ je D.

Definicija 1.39. *Ideal I integralne domene D je* pravi ideal *od D ako je $I \neq \langle 0 \rangle, \langle 1 \rangle$.*

Napomena 1.40. Pravi ideal integralne domene D je ideal I takav da vrijedi $\{0\} \subset I \subset D$.

Primjer 1.41. Za svaki pozitivan cijeli broj k, skup

$$k\mathbb{Z} = \{0, \pm k, \pm 2k, ...\}$$

je ideal od $\mathbb{Z}$. Štoviše, $k\mathbb{Z}$ je glavni ideal generiran elementom k (ili $-k$) pa je

$$k\mathbb{Z} = \langle k \rangle = \langle -k \rangle.$$

Napomena 1.42. *Ako su a i $b \in D^* = D \setminus \{0\}$ takvi da vrijedi $a = \alpha b$, onda broj α označavamo s a/b.*

Teorem 1.43. *Neka je D integralna domena i neka su $a, b \in D^* = D \setminus \{0\}$. Tada je $\langle a \rangle = \langle b \rangle$ ako i samo ako $a/b \in U(D)$.*

Dokaz. Neka je $a/b = \alpha \in U(D)$. Slijedi da je $a = \alpha b$ za neki $\alpha \in U(D)$. Neka je $x \in \langle a \rangle$. Tada je $x = \beta a$ za neki $\beta \in D$. Slijedi da je $x = \alpha\beta b$ za neke $\alpha, \beta \in D$. Prema tome, $x \in \langle b \rangle$. Time smo pokazali da je $\langle a \rangle \subseteq \langle b \rangle$. Kako je $\alpha \in U(D)$ i $U(D)$ grupa zatvorena na množenje, pomnožimo li $a = \alpha b$ s α^{-1} imamo $\alpha^{-1}b = \alpha^{-1}a$. Slijedi, $b/a = (a/b)^{-1} = \alpha^{-1} \in U(D)$. Sada potpuno analogno dobivamo $\langle b \rangle \subseteq \langle a \rangle$. Odnosno, $\langle b \rangle = \langle a \rangle$.

Obratno, pretpostavimo da je $\langle b \rangle = \langle a \rangle$. Tada je $a = \alpha b$ za neki $\alpha \in D$ i $b = \beta a$ za neki $\beta \in D$. Prema tome, $b = \alpha\beta b$. Kako je $b \neq 0$, zaključujemo da je $1 = \alpha\beta$ pa je $\alpha \in U(D)$. Dakle, $a/b = \alpha \in U(D)$. □

Proučit ćemo sada klasu integralnih domena u kojoj je svaki ideal glavni.

Definicija 1.44. *Neka je D integralna domena. D je* domena glavnih ideala *ako je svaki ideal u D glavni.*

Teorem 1.45. *$\mathbb{Z}$ je domena glavnih ideala.*

Dokaz. Neka je I ideal u $\mathbb{Z}$. Ako je $I = \{0\}$, onda je $I = \langle 0 \rangle$. Prema tome, možemo pretpostaviti da je $I \neq \{0\}$. Stoga, I sadrži nenul element a. Kako se oba elementa a i $-a$ nalaze u I, možemo pretpostaviti da je $a > 0$. Dakle, I sadrži barem jedan pozitivan cijeli broj a. Neka je m najmanji pozitivan cijeli broj u I. Dijeljenjem broja a brojem m, dobivamo cijele brojeve q i r takve da vrijedi

$$a = mq + r \text{ i } 0 \leq r < m.$$

Kako je $a \in I$ i $m \in I$, imamo $r = a - mq \in I$. Time smo dobili kontradikciju s pretpostavkom da je m najmanji element u I. Promotrimo još slučaj $r = 0$. Tada je $a = mq$. Odnosno, $I = \langle m \rangle = m\mathbb{Z}$. □

Prisjetimo se Teorema 1.32. Za bilo koju integralnu domenu vrijedi ako je neki njezin element prost, onda je i ireducibilan. Obrat vrijedi samo uz uvjet da je integralna domena domena glavnih ideala, što ćemo sada i pokazati.

Teorem 1.46. *U domeni glavnih ideala svaki ireducibilan element je prost.*

Dokaz. Neka je D integralna domena te neka je p ireducibilan element te domene. Pretpostavimo da $p \mid ab$, gdje su $a, b \in D$. Ako $p \nmid a$, onda je I ideal $\langle p, a \rangle$ u D. Kako je D domena glavnih ideala, to postoji element $c \in D$ takav da je $I = \langle c \rangle$. Kako je $a \in I$ i $p \in I$,

mora vrijediti $c \mid a$ i $c \mid p$. Ako su c i p asocirani, to jest ako $c \sim p$, onda $p \mid a$, što je u kontradikciji s pretpostavkom $p \nmid a$. Stoga mora vrijediti da c i p nisu asocirani, to jest $c \nsim p$. Kako je p ireducibilan, mora vrijediti da je c jedinica. Prema tome, postoji $d \in D$ takav da je $cd = 1$. Sada imamo $c \in \langle a, p\rangle$ pa postoje $x, y \in D$ takvi da je $c = xa + yp$. Slijedi

$$1 = cd = dax + dyp,$$

pa je

$$b = (dx)ab + (bdy)p.$$

Kako $p \mid ab$, vidimo da vrijedi $p \mid b$. Prema tome, $p \mid a$ ili $p \mid b$ pa je p prost u D. □

Korolar 1.47. *U domeni glavnih ideala, element je ireducibilan ako i samo ako je prost.*

Dokaz. Nužnost slijedi direktno iz Teorema 1.46. Kako je domena glavnih ideala jedna od klasa integralne domene, iz Teorema 1.32 slijedi dovoljnost. □

Primjer 1.48. Integralna domena $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ nije domena glavnih ideala. Štoviše, ideal $\langle 2, 1 + \sqrt{-5}\rangle$ u $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ nije glavni.
Već smo pokazali da je 2 ireducibilan, ali ne i prost u $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ (vidi Primjer 1.27 i Primjer 1.30). Pretpostavimo suprotno, to jest da je ideal $\langle 2, 1 + \sqrt{-5}\rangle$ glavni. Neka je $\langle 2, 1 + \sqrt{-5}\rangle = \langle \alpha\rangle$, za neki $\alpha \in \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Stoga imamo $2 \in \langle \alpha\rangle$ i $1 + \sqrt{-5} \in \langle \alpha\rangle$ pa vrijedi da $\alpha \mid 2$ i $\alpha \mid 1 + \sqrt{-5}$. Kako je 2 ireducibilan u $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$, mora vrijediti $\alpha \sim 1$ ili $\alpha \sim 2$. Ako $\alpha \sim 2$, onda $2 \mid 1 + \sqrt{-5}$, što nije moguće jer $\dfrac{1 + \sqrt{-5}}{2} = \dfrac{1}{2} + \dfrac{1}{2}\sqrt{-5} \notin \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Stoga mora biti $\alpha \sim 1$, pa je $\langle 2, 1 + \sqrt{-5}\rangle = \langle 1\rangle$. Ovo pokazuje da je 1 linearna kombinacija od 2 i $1 + \sqrt{-5}$ s koeficijentima iz $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$. To znači da postoje $x, y, z, w \in \mathbb{Z}$ takvi da vrijedi

$$1 = (x + y\sqrt{-5})2 + (z + w\sqrt{-5})(1 + \sqrt{-5}).$$

Izjednačimo li koeficijente uz 1 i $\sqrt{-5}$, dobivamo sljedeće

$$1 = 2x + z - 5w, 0 = 2y + z + w.$$

Oduzimanjem druge jednadžbe od prve, imamo

$$1 = 2(x - y - 3w),$$

što očito nije moguće jer se na lijevoj strani jednadžbe nalazi neparan pozitivan cijeli broj, a na desnoj paran. Prema tome, ideal $\langle 2, 1 + \sqrt{-5}\rangle$ u $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ nije glavni u $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$. □

Definicija 1.49. *Neka je D domena glavnih ideala i neka je $\{a_1, a_2, ..., a_n\}$ skup elemenata iz D. Tada je ideal $\langle a_1, a_2, ..., a_n\rangle$ glavni. Generator ovog ideala naziva se* najveći zajednički djelitelj *od $a_1, a_2, ..., a_n$.*

Neka je D domena glavnih ideala. Ako su a i b najveći zajednički djelitelji od $a_1, a_2, ..., a_n \in D$, onda

$$\langle a \rangle = \langle a_1, a_2, ..., a_n \rangle = \langle b \rangle,$$

pa su po Teoremu 1.43 a i b asocirani, to jest pišemo $a \sim b$. Najveći zajednički djelitelj od $a_1, a_2, ..., a_n$ označavamo $(a_1, a_2, ..., a_n)$. Uočimo da je $(a_1, a_2, ..., a_n) = 0$ ako $a_1 = ... = a_n = 0$. Također, $(a_1, a_2, ..., a_n) = (a_1, a_2, ..., a_{n-1})$ ako $a_n = 0$. Nadalje,

$$a \in \langle a \rangle = \langle a_1, a_2, ..., a_n \rangle,$$

pa je

$$a = r_1 a_1 + ... + r_n a_n$$

za neke $r_1, ..., , r_n \in D$. Stoga, ako je $c \in D$ takav da

$$c \mid a_j \ (j = 1, 2, ..., n),$$

onda

$$c \mid a.$$

Štoviše, za $j = 1, 2, ..., n$, imamo

$$a_j \in \langle a_1, a_2, ..., a_n \rangle = \langle a \rangle$$

pa vrijedi da

$$a \mid a_j.$$

Ovime smo pokazali da je a najveći zajednički djelitelj od $a_1, a_2, ..., a_n$. Elemente $a_1, a_2, ..., a_n$ nazivamo relativno prostima ako je $(a_1, a_2, ..., a_n)$ jedinica. Odnosno,

$$\langle a_1, a_2, ..., a_n \rangle = \langle 1 \rangle = D.$$

Sada se lako vidi da vrijedi

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

Najveći zajednički djelitelj nalazimo tako da nađemo najveći zajednički djelitelj parova elemenata. Na primjer, $(a_1, a_2) = b$, $(a_1, a_2, a_3) = (b, a_3)$ i tako dalje.

U sljedećem teoremu iskoristit ćemo svojstva prostih i ireducibinih elemenara u domeni glavnih ideala kako bismo vidjeli pod kojim uvjetima možemo neki prost element p izraziti kao $u^2 - mv^2$ ili $mv^2 - u^2$ za neke cijele brojeve u i v te m cijeli broj za kojeg vrijedi da $|m|$ nije potpuni kvadrat.

U tu svrhu treba će nam pojam *Legedreovog simbola*. Neka je $p \in \mathbb{Z}$ prost broj, te $a \in \mathbb{Z}$ i $p \nmid a$. Kažemo da je *a kvadratni ostatak modulo p* ako kongruencija

$$x^2 \equiv a \pmod{p}$$

ima rješenja (u $\mathbb{Z}$), u suprotnom (kada prethodna kongruencija nema rješenja) kažemo da je *a kvadratni neostatak modulo p*. Pišemo

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ako je } a \text{ kvadratni ostatak modulo } p \\ -1, & \text{ako je } a \text{ kvadratni neostatak modulo } p \\ 0, & \text{ako je } p|a \end{cases},$$

i zovemo ga Legedreovim simbolom.

Teorem 1.50. *Neka je m cijeli broj takav da $|m|$ nije potpuni kvadrat te neka je $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ domena glavnih ideala. Neka je p neparan prost broj za kojeg je Legendreov simbol*

$$\left(\frac{m}{p}\right) = 1.$$

Ako je $m < 0$, onda postoje cijeli brojevi u i v takvi da je

$$p = u^2 - mv^2.$$

Ako je $m > 0$ i postoje cijeli brojevi T, U takvi da vrijedi $T^2 - mU^2 = -1$, onda

$$p = u^2 - mv^2,$$

za neke cijele brojeve u, v.
Ako je $m > 0$ i ne postoje cijeli brojevi T, U takvi da je $T^2 - mU^2 = -1$, onda

$$p = u^2 - mv^2 \text{ ili } p = mv^2 - u^2,$$

za neke cijele brojeve u, v.

Dokaz. Kako je $\left(\frac{m}{p}\right) = 1$, to postoji cijeli broj x takav da je $x^2 \equiv m \pmod{p}$. Stoga,

$$p \mid (x + \sqrt{m})(x - \sqrt{m}) \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$$

Očito $\frac{x \pm \sqrt{m}}{p} = \frac{x}{p} \pm \frac{1}{p}\sqrt{m} \notin \mathbb{Z} + \mathbb{Z}\sqrt{m}$, pa slijedi

$$p \nmid x \pm \sqrt{m}$$

Prema tome, p nije prost u $\mathbb{Z}+\mathbb{Z}\sqrt{m}$. Kako je $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ domena glavnih ideala, prema Korolaru 1.47. p nije ireducibilan u $\mathbb{Z}+\mathbb{Z}\sqrt{m}$. Dakle,

$$p = (u + v\sqrt{m})(w + t\sqrt{m}) \tag{1.2}$$

za neke $u + v\sqrt{m} \in \mathbb{Z}+\mathbb{Z}\sqrt{m}$ i $w + t\sqrt{m} \in \mathbb{Z}+\mathbb{Z}\sqrt{m}$, gdje ni $u + v\sqrt{m}$ ni $w + t\sqrt{m}$ nisu jedinice u $\mathbb{Z}+\mathbb{Z}\sqrt{m}$. Iz (1.2) dobivamo

$$p - (uw + tvm) = (ut + vw)\sqrt{m}.$$

Kako m nije kvadrat, $\sqrt{m} \notin \mathbb{Q}$ pa je

$$p - (uw + tvm) = ut + vm = 0.$$

Slijedi

$$p^2 = (uw + tvm)^2 = (uw + tvm)^2 - m(ut + vm)^2$$

pa je

$$p^2 = (u^2 - mv^2)(w^2 - mt^2). \tag{1.3}$$

Kako $m, u, v, w, t \in \mathbb{Z}$ i $m \in \mathbb{N}$, slijedi da $u^2 - mv^2 \in \mathbb{Z}$ i $w^2 - mt^2 \in \mathbb{Z}$. Štoviše, $u^2 - mv^2 \neq \pm 1$ jer $u + v\sqrt{m}$ i $w + t\sqrt{m}$ nisu jedinice u $\mathbb{Z}+\mathbb{Z}\sqrt{m}$. Stoga, iz (1.3) i p je prost imamo $\pm p = u^2 - mv^2 = w^2 - mt^2$. Prema tome, postoje cijeli brojevi u i v takvi da je $p = u^2 - mv^2$ ili $p = -(u^2 - mv^2)$.
Ako je $m < 0$, onda $u^2 - mv^2 > 0$, pa mora vrijediti $p = u^2 - mv^2$.
Ako je $m > 0$, onda $p = -(u^2 - mv^2)$ i postoje cijeli brojevi T i U takvi da je $T^2 - mU^2 = -1$ pa je $p = u'^2 - mv'^2$, gdje su $u' = Tu + mUv$ i $v' = Uu + Tv$. □

U sljedećem teoremu osigurat ćemo uvjete za element p tako da se može izraziti u obliku $u^2 + uv + \frac{1}{4}(1-m)v^2$ ili $-(u^2 + uv + \frac{1}{4}(1-m)v^2)$ za neke cijele brojeve u, v gdje je m cijeli broj takav da $|m|$ nije potpun kvadrat i da vrijedi $m \equiv 1 \pmod 4$.

Teorem 1.51. *Neka je m cijeli broj takav da $|m|$ nije potpun kvadrat i da vrijedi $m \equiv 1 \pmod 4$ te da je $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ domena glavnih ideala. Neka je p neparan prost element za kojeg vrijedi $\left(\frac{m}{p}\right) = 1$.*
Ako je $m < 0$, onda postoje cijeli brojevi u i v takvi da je

$$p = u^2 + uv + \frac{1}{4}(1-m)v^2.$$

Ako je $m > 0$ *i postoje cijeli brojevi* T, U *takvi da vrijedi* $T^2 + TU + \frac{1}{4}(1-m)U^2 = -1$*, onda*

$$p = u^2 + uv + \frac{1}{4}(1-m)v^2,$$

za neke cijele brojeve u, v*.*
Ako je $m > 0$ *i ne postoje cijeli brojevi* T, U *takvi da je* $T^2 + TU + \frac{1}{4}(1-m)U^2 = -1$*, onda*

$$p = u^2 + uv + \frac{1}{4}(1-m)v^2 \text{ ili } p = -(u^2 + uv + \frac{1}{4}(1-m)v^2),$$

za neke cijele brojeve u, v*.*

Dokaz. Kako je $\left(\frac{m}{p}\right) = 1$, postoji cijeli broj z takav da je $z^2 \equiv -m \pmod{p}$. Stavimo da je

$$y = \begin{cases} z, & z \text{ neparan} \\ p - z, & z \text{ paran,} \end{cases}$$

pa je y neparan cijeli broj koji zadovoljava $y^2 \equiv m \pmod{p}$. Neka je $x = \frac{1}{2}(y-1) \in \mathbb{Z}$. Očito je $4(x^2 + x + \frac{1}{4}(1-m)) = (2x+1)^2 - m = y^2 - m \equiv 0 \pmod{p}$ pa slijedi da $p \mid x^2 + x + \frac{1}{4}(1-m)$. Prema tome $p \mid \left(x + \frac{1+\sqrt{m}}{2}\right)$ u $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$. Očito

$$\frac{x + \frac{1 \pm \sqrt{m}}{2}}{p} \notin \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$$

pa slijedi

$$p \nmid x + \frac{1 \pm \sqrt{m}}{2}.$$

Prema tome, p nije prost u $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$. Kako je $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ domena glavnih ideala, prema Korolaru 1.47 p nije ireducibilan u $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$. Prema tome,

$$p = \left(u + v\left(\frac{1+\sqrt{m}}{2}\right)\right)\left(w + t\left(\frac{1+\sqrt{m}}{2}\right)\right) \tag{1.4}$$

za neke $u + v\left(\frac{1+\sqrt{m}}{2}\right) \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ i $w + t\left(\frac{1+\sqrt{m}}{2}\right) \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ gdje niti jedan $u + v\left(\frac{1+\sqrt{m}}{2}\right)$ ni $w + t\left(\frac{1+\sqrt{m}}{2}\right)$ nisu jedinice u $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$. Iz (1.4) imamo

$$p = \left(u + \frac{v}{2}\right)\left(w + \frac{t}{2}\right) + \frac{vt}{4}m + \frac{(vw + ut + vt)}{2}\sqrt{m}.$$

Kako m nije potpun kvadrat, $\sqrt{m} \notin \mathbb{Q}$, pa su 1 i $\sqrt{m}$ linearno nezavisni u $\mathbb{Q}$. Prema tome,

$$p = \left(u + \frac{v}{2}\right)\left(w + \frac{t}{2}\right) + \frac{vt}{4}m, vw + ut + vt = 0.$$

Stoga

$$p = \left(u + v\left(\frac{1-\sqrt{m}}{2}\right)\right)\left(w + t\left(\frac{1-\sqrt{m}}{2}\right)\right). \tag{1.5}$$

Množenjem (1.4) i (1.5) dobivamo

$$p^2 = \left(u^2 + uv + \frac{1}{4}(1-m)v^2\right)\left(w^2 + wt + \frac{1}{4}(1-m)t^2\right) \tag{1.6}$$

jer je

$$\left(x + y\left(\frac{1-\sqrt{m}}{2}\right)\right)\left(x + y\left(\frac{1-\sqrt{m}}{2}\right)\right) = x^2 + xy + \frac{1}{4}(1-m)y^2.$$

Kako je $m \equiv 1 \pmod 4$, $u^2 + uv + \frac{1}{4}(1-m)v^2 \notin \mathbb{Z}$ i $w^2 + wt + \frac{1}{4}(1-m)t^2 \notin \mathbb{Z}$. Štoviše, $u^2 + uv + \frac{1}{4}(1-m)v^2 \neq \pm 1$ i $w^2 + wt + \frac{1}{4}(1-m)t^2 \neq \pm 1$ jer $u + v\left(\frac{1+\sqrt{m}}{2}\right)$ i $w + t\left(\frac{1+\sqrt{m}}{2}\right)$ nisu jedinice u $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$. Sada iz (1.6) i p je prost zaključujemo

$$\pm p = u^2 + uv + \frac{1}{4}(1-m)v^2 = w^2 + wt + \frac{1}{4}(1-m)t^2.$$

Prema tome, postoje cijeli brojevi u i v takvi da je

$$p = u^2 + uv + \frac{1}{4}(1-m)v^2 \text{ ili } p = -(u^2 + uv + \frac{1}{4}(1-m)v^2).$$

Ako je $m < 0$, onda $u^2 + uv + \frac{1}{4}(1-m)v^2 > 0$ pa je $p = u^2 + uv + \frac{1}{4}(1-m)v^2$.

Ako je $m > 0$, onda $p = -(u^2 + uv + \frac{1}{4}(1-m)v^2)$ i postoje cijeli brojevi T i U takvi da je $T^2 + TU + \frac{1}{4}(1-m)U^2 = -1$ pa slijedi $p = u'^2 + u'v' + \frac{1}{4}(1-m)v'^2$ gdje je $u' = uT + \frac{1}{4}(1-m)vU$ i $v' = uU + vT + vU$. □

1.3 Maksimalni i prosti ideali

U ovom dijelu definirat ćemo maksimalne i proste ideale te proučiti neka njihova osnovna svojstva.

Definicija 1.52. *Neka je M pravi ideal integralne domene D. M je* maksimalni ideal *ako za svaki ideal I integralne domane D takav da je $M \subseteq I \subseteq D$ vrijedi $I = M$ ili $I = D$.*

Primjer 1.53. Ideal $\langle x^2 + 1\rangle$ je maksimalan u $\mathbb{R}[x]$.
Pretpostavimo da je I ideal u $\mathbb{R}[x]$ takav da je $\langle x^2+1\rangle \subset I \subset \mathbb{R}[x]$. Kako je $\langle x^2+1\rangle$ sadržano u I, to postoji $f(x) \in I$ takav da $f(x) \notin \langle x^2 + 1\rangle$. Dijeljenjem $f(x)$ s $\langle x^2 + 1\rangle$, dobivamo

$$f(x) = (x^2 + 1)q(x) + r(x),$$

gdje je $r(x) \neq 0$ i $deg(r(x)) < 2$. Stoga, $r(x) = ax + b$, gdje su $a, b \in \mathbb{R}$ ne oba nula i vrijedi

$$ax + b = r(x) = f(x) - q(x)(x^2 + 1) \in I.$$

stoga,

$$a^2x^2 - b^2 = (ax + b)(ax - b) \in I$$

i

$$a^2(x^2 + 1) \in I.$$

Prema tome,

$$a^2 + b^2 = (a^2(x^2 + 1)) - (a^2x^2 - b^2) \in I.$$

Stoga, I sadrži realni broj različit od nule, to jest I sadrži jedinicu od $\mathbb{R}[x]$. Iz toga zaključujemo $I = \mathbb{R}[x]$, što je kontradikcija. Prema tome, ne postoji ideal I pa slijedi da je $\langle x^2 + 1\rangle$ maksimalan ideal u $\mathbb{R}[x]$. □

Teorem 1.54. *Neka je D integralna domena. Neka je $a \in D$ takav da $a \neq 0$ i $a \notin U(D)$. Tada vrijedi ako je $\langle a\rangle$ maksimalan u D, onda je a ireducibilan u D.*

Dokaz. Pretpostavimo da a nije ireducibilan element u D. Kako a nije nula ni jedinica, mora biti reducibilan element. Prema tome, postoje $b \in D$ i $c \in D$ takvi da $a = bc$, pri čemu ni b ni c nije ni nula ni jedinica. Stoga

$$\langle a\rangle \subset \langle b\rangle \subset D$$

pa $\langle a\rangle$ nije maksimalan ideal. Pokazali smo da ako je $\langle a\rangle$ maksimalan onda je a ireducibilan. □

U sljedećem primjeru vidjet ćemo da obrat Teorema 1.54 ne vrijedi općenito.

Primjer 1.55. $1+\sqrt{-5}$ je ireducibilan element u $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$, ali $\langle 1+\sqrt{-5}\rangle$ nije maksimalan ideal u $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$.
To se lako vidi jer je $\langle 1+\sqrt{-5}\rangle \subset \langle 2+\sqrt{-5}\rangle \subset \mathbb{Z}+\mathbb{Z}\sqrt{-5}$. □

Vidimo da obrat Teorema 1.54 ne vrijedi općenito, no vrijedi u domeni glavnih ideala.

Teorem 1.56. *Neka je D domena glavnih ideala. Neka je $a \in D$ takav da $a \neq 0$ i $a \notin U(D)$. Tada vrijedi da je a je ireducibilan u D ako i samo ako je $\langle a\rangle$ maksimalan u D.*

Dokaz. Dovoljnost slijedi direktno iz Teorema 1.54. Dokažimo još nužnost. Pretpostavimo da je a ireducibilan, ali $\langle a\rangle$ nije maksimalan ideal. Tada postoji ideal I takav da je

$$\langle a\rangle \subset I \subset D.$$

Kako je D domena glavnih ideala, $I = \langle b\rangle$ za neki $b \in D$. Stoga,

$$\langle a\rangle \subset \langle b\rangle \subset D$$

pa je

$$a = bc,$$

za neki $c \in D$. Kako je $\langle b\rangle \subset D$, slijedi da b nije jedinica, a kako $\langle a\rangle \subset \langle b\rangle$, c nije jedinica. Stoga, a je reducibilan što je kontradikcija s pretpostavkom pa slijedi tvrdnja. □

Teorem 1.57. *Neka je D integralna domena i neka je I ideal u D. Tada je D/I polje ako i samo ako je I maksimalan.*

Dokaz. Pretpostavimo da je D/I polje i da je J ideal u D takav da je

$$I \subset J \subset D.$$

Stoga postoji $b \in J$ takav da $b \notin I$. Tada je $b+I$ nenul element u D/I. Štoviše, kako je D/I polje, postoji element $c+I$ takav da je

$$(b+I)(c+I) = 1+I.$$

Stoga je

$$bc+I = 1+I$$

pa je

$$bc-1 \in I \subset J.$$

Kako je $b \in J$ i $c \in D$, imamo

$$bc \in J.$$

Prema tome,

$$1 = bc - (bc - 1) \in J,$$

pa je $J = \langle 1 \rangle = D$. Time smo dokazali da je I maksimalan.
Pretpostavimo sada da je I maksimalan. Da bismo pokazali da je D/I polje, dovoljno je pokazati da $b+I \neq 0+I$ ima multiplikativni inverz jer su sva ostala svojstva polja trivijalno zadovoljena. Kako je $b + I \neq 0 + I$, slijedi $b \notin I$. Promotrimo sljedeći skup

$$B = \{x \in D \mid x = by + w \text{ za neke } y \in D \text{ i neke } w \in I\}.$$

Lako se provjeri da je B ideal u D takav da je $I \subset B$. Kako je I maksimalan, mora vrijediti $B = D$. Stoga je $1 \in D$, pa je $1 = by' + w'$ za neke $y' \in D$ i neke $w+ \in I$. Dakle,

$$(b + I)(y' + I) = by' + I = 1 - w' + I = 1 + I$$

pa $(b + I)^{-1}$ postoji i jednak je $y' + I$. □

Definicija 1.58. *Neka je D integralna domena. Pravi ideal P integralne domene D je* prost ideal *ako za $a, b \in D$ i $ab \in P$ vrijedi da je $a \in P$ ili $b \in P$.*

Primjer 1.59. Ideal $I = \langle 1 + i \rangle$ je prost u $\mathbb{Z} + \mathbb{Z}i$.
Pretpostavimo da su $a + bi \in \mathbb{Z} + \mathbb{Z}i$ i $c + di \in \mathbb{Z} + \mathbb{Z}i$ takvi da je

$$(a + bi)(c + di) \in \langle 1 + i \rangle.$$

Tada postoji $x + yi \in \mathbb{Z} + \mathbb{Z}i$ takav da je

$$(a + bi)(c + di) = (1 + i)(x + yi).$$

Izjednačavanjem realnog i imaginarnog dijela dobivamo

$$ac - bd = x - y, ad + bc = x + y.$$

Zbrajanjem ovih dviju jednakosti dobivamo

$$ac + ad + bc - bd = 2x,$$

pa je

$$(a + b)(c + d) = ac + ad + bc + bd \equiv ac + ad + bc - bd = 2x \equiv 0 \pmod 2.$$

Prema tome, jedan od $a+b$ ili $c+d$ je paran. Bez smanjenja općenitosti smijemo pretpostaviti da je $a + b$ paran. Prema tome, postoje $u \in \mathbb{Z}$ i $v \in \mathbb{Z}$ takvi da je $a + b = 2u$ i $a - b = 2v$. Dakle,

$$a + bi = (u + v) + (u - v)i = (1 + i)(u - vi)$$

zato je $a + bi \in \langle 1 + i \rangle$. Time smo pokazali da je $\langle 1 + i \rangle$ prost ideal. □

Sada ćemo vidjeti uz koji uvjet je neki glavni ideal integralne domene prost ideal.

Teorem 1.60. *Neka je D integralna domena. Neka je $a \in D$ takav da $a \neq 0$ i $a \notin U(D)$. Tada je $\langle a \rangle$ prost ideal u D ako i samo ako je a prost u D.*

Dokaz. Neka je $\langle a \rangle$ prost ideal u D. Neka su $b, c \in D$ takvi da $bc \in \langle a \rangle$ pa $a \mid bc$. Kako je $\langle a \rangle$ prost ideal, vrijedi da je $b \in \langle a \rangle$ ili $c \in \langle a \rangle$. Prema tome, $a \mid b$ ili $a \mid c$. Time smo pokazali da je a prost.

Neka je sada a prost u D i neka su $b, c \in D$ takvi da je $bc \in \langle a \rangle$. Dakle, postoji $d \in D$ takav da je $bc = ad$, pa slijedi da $a \mid bc$. Kako je a prost, vrijedi da $a \mid b$ ili $a \mid c$. Bez smanjenja općenitosti smijemo pretpostaviti da $a \mid b$. Prema tome, postoji $e \in D$ takav da je $b = ae$ pa je $b \in \langle a \rangle$. Time smo dokazali i da je $\langle a \rangle$ prost ideal. □

Teorem 1.61. *Neka je D integralna domena i I ideal u D. Tada je D/I integralna domena ako i samo ako je I prost.*

Dokaz. Pretpostavimo prvo da je D/I integralna domena i da su $a, b \in D$ takvi da je $ab \in I$. Tada je $(a + I)(b + I) = ab + I = 0 + I$ nul element integralne domene D/I. Zato što je integralna domena nema djelitelja nule, imamo $a + I = 0 + I$ ili $b + I = 0 + I$, to jest imamo ili $a \in I$ ili $b \in I$, pa je I prost.

Pretpostavimo sada da je I prost ideal u D. Kako je I pravi ideal u D, D/I je komutativni prsten s jedinicom $1 + I$. Stoga preostaje provjeriti da ako je I prost, D/I nema djelitelja nule. Pretpostavimo da su $a + I \in D/I$ i $b + I \in D/I$ takvi da je $(a + I)(b + I) = 0 + I$. Tada je $ab + I = I$ pa je $ab \in I$. Kako je I prost, slijedi da je $a \in I$ ili $b \in I$, to jest $a + I = 0 + I$ ili $b + I = 0 + I$ iz čega slijedi da D/I nema djelitelja nule. □

Teorem 1.62. *Neka je D integralna domena te neka je I maksimalan ideal u D. Tada je I prost ideal u D.*

Dokaz. Neka je I maksimalan ideal u D. Tada je, prema Teoremu 1.57, D/I polje. No, svako polje je i integralna domena. Slijedi da je D/I integralna domena. Sada, iz Teorema 1.61 slijedi da je I prost ideal u D. □

Teorem 1.63. *Neka je D domena glavnih ideala. Neka je I pravi ideal u D. Tada je I maksimalan ako i samo ako je I prost.*

Dokaz. Iz prethodnog Teorema 1.62 direktno slijedi nužnost. Trebamo još dokazati dovoljnost. Pretpostavimo da je I prost ideal u D koji nije maksimalan. Tada postoji ideal J u D takav da je

$$I \subset J \subset D.$$

Kako je D domena glavnih ideala, imamo $I = \langle a \rangle$ i $J = \langle b \rangle$ za neke $a, b \in D$. Kako je $\langle a \rangle \subset \langle b \rangle$, imamo $a = bc$ za neki $c \in D$. Dakle, $bc = a \in \langle a \rangle = I$ i I je prost pa je $b \in I$ ili

$c \in I$. Ako je $b \in I$, onda je $J = \langle b \rangle \subseteq I \subset J$, što je kontradikcija. Prema tome, mora biti $c \in I$. Stoga je $c = ad$ za neki $d \in D$ pa je $a = bda$. No, $a \neq 0$ pa je $bd = 1$. Stoga je b jedinica i $J = \langle b \rangle = D \supset J$, što je kontradikcija. Dakle, I je maksimalan ideal u D. □

Poglavlje 2

Euklidska domena

2.1 Euklidska funkcija

U dokazu Teorema 1.45 iskoristili smo svojstvo cijelih brojeva da za svaki $a, b \in \mathbb{Z}$ i $b > 0$ postoje $q, r \in \mathbb{Z}$ takvi da vrijedi

$$a = qb + r,\ 0 \leq r < b. \tag{2.1}$$

Štoviše, cijeli brojevi q i r su jedinstveno određeni s a i b. Vrijedi

$$q = \lfloor a/b \rfloor,\ r = a - b\lfloor a/b \rfloor, \tag{2.2}$$

gdje je $\lfloor x \rfloor$ *najveće cijelo* realnog broja x, odnosno najveći cijeli broj manji ili jednak broju x. Cijeli broj q se naziva količnik, a cijeli broj r ostatak. Posebna klasa integralnih domena su one koje posjeduju svojstvo analogno svojstvu (2.1) u $\mathbb{Z}$. Takve integralne domene nazivamo *euklidske domene*. Kasnije ćemo dokazati da je euklidska domena domena glavnih ideala. Da bismo formalno definirali euklidsku domenu, najprije trebamo definirati euklidsku funkciju.

Definicija 2.1. *Neka je D integralna domena. Preslikavanje $\phi : D \longrightarrow \mathbb{Z}$ naziva se* euklidska funkcija *na D ako zadovoljava sljedeća dva svojstva:*

1) *za $a, b \in D$ i $b \neq 0$ je*

$$\phi(ab) \geq \phi(a), \tag{2.3}$$

2) *za $a, b \in D$ i $b \neq 0$, postoje $q, r \in D$ takvi da je*

$$a = qb + r \ \ i \ \ \phi(r) < \phi(b). \tag{2.4}$$

Primjer 2.2. *Preslikavanje $\phi(a) = |a|$, $a \in \mathbb{Z}$, je euklidska funkcija na $\mathbb{Z}$.*

Sada ćemo navesti neka svojstva euklidske funkcije.

Propozicija 2.3. *Neka je D integralna domena takva da posjeduje euklidsku funkciju ϕ. Tada vrijede sljedeća svojstva:*

a) *ako je $a \sim b$, onda je $\phi(a) = \phi(b)$;*

b) *ako $a \mid b$ i $\phi(a) = \phi(b)$, onda je $a \sim b$;*

c) *$a \in U(D)$ ako i samo ako $\phi(a) = \phi(1)$;*

d) *ako je $a \neq 0$, onda $\phi(a) > \phi(0)$;*

za sve $a, b \in D$.

Dokaz. **a)** Kako je $a \sim b$, postoji $u \in U(D)$ takav da je $a = ub$. Iz (2.3) slijedi $\phi(a) = \phi(ub) \geq \phi(b)$. Budući da je $u \in U(D)$, imamo $u^{-1} \in U(D)$ i $b = u^{-1}a$ pa opet prema (2.3) imamo $\phi(b) = \phi(u^{-1}a) \geq \phi(a)$. Iz ove dvije nejednakosti slijedi da je $\phi(a) = \phi(b)$.

b) Prema (2.4) postoje $q, r \in D$ takvi da je $a = qb + r$ i $\phi(r) < \phi(b) = \phi(a)$. Sada je $a \mid b$ slijedi da $a \mid r$. Pretpostavimo da je $r \neq 0$. Tada iz (2.3) imamo $\phi(r) \geq \phi(a)$, što je kontradikcija. Pretpostavimo sada da je $r = 0$, odnosno $a = qb$. No, $a \mid b$ pa je $q \in U(D)$ i slijedi $a \sim b$.

c) Prvo imamo da iz $a \in U(D)$ slijedi $a \sim 1$ pa prema tvrdnji a) vrijedi $\phi(a) = \phi(1)$. S druge strane, prema tvdrnji b) iz $1 \mid a$ i $\phi(1) = \phi(a)$ slijedi $1 \sim a$ pa je $a \in U(D)$.

d) Prema (2.4) postoje $q, r \in D$ takvi da je $0 = qa + r$, $\phi(r) < \phi(a)$. Pretpostavimo da je $r \neq 0$ i prema (2.3) imamo $\phi(r) = \phi((-q)a) \geq \phi(a)$, što je kontradikcija. Prema tome, $r = 0$ i $\phi(0) < \phi(a)$.

□

Definicija 2.4. *Neka je D integralna domena. Ako postoji euklidska funkcija $\phi : D \longrightarrow \mathbb{Z}$, onda se D naziva* euklidska domena s obzirom na ϕ.

Ako je D euklidska domena s obzirom na neku euklidsku funkciju ϕ, nije bitno specificirati ϕ, već D zovemo samo euklidska domena. Prije nego što iznesemo nekoliko primjera euklidske domene, dokazat ćemo fundamentalni teorem da je svaka euklidska domena domena glavnih ideala.

Teorem 2.5. *Euklidska domena je domena glavnih ideala.*

Dokaz. Neka je D euklidska domena. Prema tome, postoji euklidska funkcija ϕ u D. Neka je I ideal u D. Ako je $I = \{0\}$, onda je $I = \langle 0 \rangle$ glavni ideal. Ako je $I \neq \{0\}$ pretpostavljamo da je skup S skup cijelih brojeva definiran na sljedeći način

$$S = \{\phi(x) \mid x \in I, x \neq 0\}.$$

Budući da je $I \neq \{0\}$, S je neprazan skup. Prema Propoziciji 2.3 d), skup S je omeđen odozdo. Stoga S ima najmanji element $\phi(a), a \in I, a \neq 0$. Ako je $b \in I$, onda jer je ϕ euklidska funkcija postoje $q, r \in D$ takvi da

$$b = qa + r,\ \phi(r) < \phi(a).$$

Sada jer je I ideal, $r = b - aq \in I$ i kako je $\phi(a)$ najmanji element u S, slijedi da je $r = 0$. Stoga, $b = qa$ pa je $I = \langle a \rangle$. Prema tome, svaki ideal u D je glavni pa je D domena glavnih ideala. □

2.2 Primjeri euklidskih domena

U ovom poglavlju istražit ćemo kada su integralne domene oblika

- $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ za $m \equiv 2, 3 \pmod 4$,

- $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ za $m \equiv 1 \pmod 4$

euklidske domene s obzirom na funkciju ϕ_m. Funkciju ϕ_m definiramo na sljedeći način:

$$\phi_m : \mathbb{Q}(\sqrt{m}) \to \mathbb{Q},\ \ \phi_m(r + s\sqrt{m}) = |r^2 - ms^2|$$

za $r, s \in \mathbb{Q}$. U sljedećoj lemi dokazat ćemo neka osnovna svojstva funkcije ϕ_m. Ne zaboravimo da je naša pretpostavka cijelo vrijeme da je m kvadratno slobodan cijeli broj.

Lema 2.6. *Neka je m kvadratno slobodan. Vrijede sljedeća svojstva:*

a) $\phi_m : \mathbb{Z} + \mathbb{Z}\sqrt{m} \longrightarrow \mathbb{N} \cup \{0\}$*;*

b) *ako je* $m \equiv 1 \pmod 4$*, onda* $\phi_m : \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right) \longrightarrow \mathbb{N} \cup \{0\}$*;*

c) $\phi_m(\alpha) = 0$ *za* $\alpha \in \mathbb{Q}(\sqrt{m})$ *ako i samo ako* $\alpha = 0$*;*

d) $\phi_m(\alpha\beta) = \phi_m(\alpha)\,\phi_m(\beta)$*, za sve* $\alpha, \beta \in \mathbb{Q}(\sqrt{m})$*;*

e) $\phi_m(\alpha\beta) \geq \phi_m(\alpha)$, *za sve* $\alpha, \beta \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ *gdje je* $\beta \neq 0$*;*

f) *ako je* $m \equiv 1 \pmod 4$, *onda* $\phi_m(\alpha\beta) \geq \phi_m(\alpha)$, *za sve* $\alpha, \beta \in \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ *gdje je* $\beta \neq 0$.

Dokaz. **a)** Neka je $\alpha \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$. Tada vrijedi $\alpha = x + y\sqrt{m}$ za neke $x, y \in \mathbb{Z}$. Vrijedi $x^2 - my^2 \in \mathbb{Z}$ i $|x^2 - my^2| \geq 0$ pa je

$$\phi_m(\alpha) = \phi_m(x + y\sqrt{m}) = |x^2 - my^2| \in \mathbb{N} \cup \{0\}.$$

b) Ako je $m \equiv 1 \pmod 4$, onda je $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ integralna domena (vidi Primjer 1.6). Neka je $\alpha \in \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$. Tada je $\alpha = x + y\left(\frac{1+\sqrt{m}}{2}\right) = \left(x + \frac{y}{2}\right) + \frac{y}{2}\sqrt{m}$ za neke $x, y \in \mathbb{Z}$. Vrijedi

$$\phi_m(\alpha) = \phi_m\left(\left(x + \frac{y}{2}\right) + \frac{y}{2}\sqrt{m}\right) = \left|\left(x + \frac{y}{2}\right)^2 - m\left(\frac{y}{2}\right)^2\right| = |x^2 + xy + \underbrace{\frac{1}{4}(1-m)}_{\in\mathbb{Z}} y^2| \in \mathbb{N} \cup \{0\}.$$

c) Neka je $\alpha \in \mathbb{Q}(\sqrt{m})$ pa je oblika $\alpha = r + s\sqrt{m}$ za neke $r, s \in \mathbb{Q}$. Tada je

$$\phi_m(\alpha) = \phi_m(r + s\sqrt{m}) = 0$$

ako i samo ako je

$$|r^2 - ms^2| = 0,$$

to jest $r^2 = ms^2$. Budući da je m kvadratno slobodan to je jedino moguće za $r = s = 0$, pa je $\alpha = r + s\sqrt{m} = 0$, to jest $\alpha = 0$.

d) Neka su $\alpha, \beta \in \mathbb{Q}(\sqrt{m})$. Tada je $\alpha = x + y\sqrt{m}$ i $\beta = u + v\sqrt{m}$ za neke $x, y, u, v \in \mathbb{Z}$. Stoga je

$$\begin{aligned} \phi_m(\alpha\beta) &= \phi_m((x + y\sqrt{m})(u + v\sqrt{m})) = \phi_m((xu + myv) + (xv + yu)\sqrt{m}) \\ &= |(xu + myv)^2 - m(xv + yu)^2| = |x^2u^2 + m^2y^2v^2 - mx^2v^2 - my^2u^2| \\ &= |(x^2 - my^2)(u^2 - mv^2)| = \phi_m(\alpha)\phi_m(\beta). \end{aligned}$$

e) Neka su $\alpha, \beta \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ gdje je $\beta \neq 0$. Prema tvrdnji c) imamo $\phi_m(\beta) \neq 0$. Zatim, prema a) zaključujemo da je $\phi_m(\alpha) \geq 0$ i $\phi_m(\beta) \geq 1$. Stoga, iz tvrdnje d) slijedi

$$\phi_m(\alpha\beta) = \phi_m(\alpha)\,\phi_m(\beta) \geq \phi_m(\alpha)$$

.

f) Slijedi analogno kao i e) samo što u dokazu umjesto tvrdnje a) koristimo tvrdnju b).

□

U sljedećem teoremu vidjet ćemo koji je nužan i dovoljan uvjet da $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ bude euklidska domena s obzirom na preslikavanje ϕ_m.

Teorem 2.7. *Neka je m kvadratno slobodan cijeli broj. Tada je integralna domena* $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ *euklidska domena s obzirom na* ϕ_m *ako i samo ako za svaki* $x, y \in Q$ *postoje* $a, b \in \mathbb{Z}$ *takvi da je*

$$\phi_m((x + y\sqrt{m} - (a + b\sqrt{m})) < 1. \tag{2.5}$$

Dokaz. Pretpostavimo prvo da je $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ euklidska domena s obzirom na ϕ_m. Neka su $x, y \in \mathbb{Q}$. Tada je $x + y\sqrt{m} = (r + s\sqrt{m})/t$ za neke cijele brojeve r, s, t, gdje je $t \neq 0$. Budući da je ϕ_m euklidska funkcija na $\mathbb{Z} + \mathbb{Z}\sqrt{m}$, postoje $a + b\sqrt{m}, c + d\sqrt{m} \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ takvi da vrijedi

$$r + s\sqrt{m} = t(a + b\sqrt{m}) + (c + d\sqrt{m}), \quad \phi_m(c + d\sqrt{m}) < \phi_m(t).$$

Prema tome, iz Leme 2.6 d) slijedi

$$\phi_m((x + y\sqrt{m}) - (a + b\sqrt{m})) = \phi_m\left(\frac{r + s\sqrt{m}}{t} - (a + b\sqrt{m})\right) = \phi_m\left(\frac{r + s\sqrt{m} - t(a + b\sqrt{m})}{t}\right)$$

$$= \phi_m\left(\frac{c + d\sqrt{m}}{t}\right) = \frac{\phi_m(c + d\sqrt{m})}{\phi_m(t)} < 1.$$

Obrnuto, pretpostavimo da vrijedi (2.5). Da bismo dokazali da je $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ euklidska domena trebamo pokazati da je ϕ_m euklidska funkcija, to jest trebamo provjeriti da vrijedi (2.3) i (2.4). Nejednakost (2.3) slijedi iz Leme 2.6 e). Dakle, preostaje provjeriti (2.4). Neka su $r + s\sqrt{m}, t + u\sqrt{m} \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$, gdje je $t + u\sqrt{m} \neq 0$. Tada je

$$\frac{r + s\sqrt{m}}{t + u\sqrt{m}} = x + y\sqrt{m},$$

gdje je

$$x = \frac{tr - msu}{t^2 - mu^2} \in \mathbb{Q}, \quad y = \frac{st - ru}{t^2 - mu^2} \in \mathbb{Q}.$$

Uočimo da $t + u\sqrt{m} \neq 0$ povlači da $t^2 - mu^2 \neq 0$. Sada iz (2.5) slijedi da postoji $a + b\sqrt{m} \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ takav da

$$\phi_m((x + y\sqrt{m} - (a + b\sqrt{m})) < 1.$$

Stavimo $c = r - at - bum \in \mathbb{Z}$ i $d = s - au - bt \in \mathbb{Z}$ pa je

$$c + d\sqrt{m} = (r + s\sqrt{m}) - (a + b\sqrt{m})(t + u\sqrt{m}) \in \mathbb{Z} + \mathbb{Z}\sqrt{m}.$$

Prema tome vrijedi,

$$r + s\sqrt{m} = (a + b\sqrt{m})(t + u\sqrt{m}) + (c + d\sqrt{m})$$

i prema Lemi 2.6 d) imamo

$$\begin{aligned}
\phi_m(c + d\sqrt{m}) &= \phi_m((r + s\sqrt{m}) - (a + b\sqrt{m})(t + u\sqrt{m})) \\
&= \phi_m((x + y\sqrt{m})(t + u\sqrt{m}) - (a + b\sqrt{m})(t + u\sqrt{m})) \\
&= \phi_m((t + u\sqrt{m})((x + y\sqrt{m}) - (a + b\sqrt{m}))) \\
&= \phi_m(t + u\sqrt{m})\phi_m((x + y\sqrt{m}) - (a + b\sqrt{m})) \\
&< \phi_m(t + u\sqrt{m}).
\end{aligned}$$

□

Prethodni teorem nam omogućuje odrediti sve negativne kvadratno slobodne cijele brojeve m za koje je $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ euklidska domena s obzirom na ϕ_m.

Teorem 2.8. *Neka je m negativan kvadratno slobodan cijeli broj. Tada je integralna domena $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ euklidska s obzirom na ϕ_m ako i samo ako je $m = -1, -2$.*

Dokaz. Prvo ćemo dokazati da je $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ euklidska domena s obzirom na ϕ_m za $m = -1$ i $m = -2$. Neka su $x, y \in \mathbb{Q}$. Tada postoje $a, b \in \mathbb{Z}$ takvi da je

$$|x - a| \leq \frac{1}{2}, \quad |y - b| \leq \frac{1}{2}.$$

Za $m \in \{-1, -2\}$ vrijedi

$$\phi_m((x+y\sqrt{m})-(a+b\sqrt{m})) = \phi_m((x-a)+(y-b)\sqrt{m}) = |(x-a)^2-m(y-b)^2| \leq \frac{1}{4}+2\cdot\frac{1}{4} = \frac{3}{4} < 1.$$

Stoga prema Teoremu 2.7 zaključujemo da je $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ euklidska domena s obzirom na ϕ_m za $m = -1$ i $m = -2$.

Pretpostavimo sada da je $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ euklidska domena s obzirom na ϕ_m. Tada prema Teoremu 2.7 postoje $a, b \in \mathbb{Z}$ takvi da je

$$\phi_m\left((\frac{1}{2} + \frac{1}{2}\sqrt{m}) - (a + b\sqrt{m})\right) < 1.$$

Budući da je $-m = |m|$, imamo

$$\left(\frac{1}{2} - a\right)^2 + |m|\left(\frac{1}{2} - b\right)^2 < 1.$$

Za bilo koji cijeli broj x imamo

$$|\frac{1}{2} - x| \geq \frac{1}{2}, \ \left(\frac{1}{2} - x\right)^2 \geq \frac{1}{4},$$

pa je

$$\frac{1}{4} + \frac{|m|}{4} < 1,$$

odnosno $|m| < 3$. Prema tome, $m = -1$ i $m = -2$ su jedine mogućnosti. □

Iskazat ćemo još nekoliko teorema, no nećemo provesti i njihov dokaz. Dokaz sljedećeg teorema provodi se analogno kao i dokaz Teorema 2.8.

Teorem 2.9. *Neka je m kvadratno slobodan cijeli broj takav da je $m \equiv 1 \pmod 4$. Tada je integralna domena $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ euklidska domena s obzirom na ϕ_m ako i samo ako za svaki $x, y \in \mathbb{Q}$ postoje $a, b \in \mathbb{Z}$ takvi da*

$$\phi_m\left((x + y\sqrt{m}) - \left(a + b\left(\frac{1+\sqrt{m}}{2}\right)\right)\right) < 1.$$

Iz Teorema 2.9 možemo odrediti negativne kvadratno slobodne cijele brojeve $m \equiv 1 \pmod 4$ za koje je $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ euklidska domena s obzirom na ϕ_m. To ćemo iskazati u sljedećem teoremu.

Teorem 2.10. *Neka je m negativan kvadratno slobodan cijeli broj takav da je $m \equiv 1 \pmod 4$. Tada je integralna domena $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ euklidska domena s obzirom na ϕ_m ako i samo ako $m = -3, -7, -11$.*

Određivanje pozitivnih kvadratno slobodnih cijelih brojeva m za koje su $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ za $m \equiv 2, 3 \pmod 4$ i $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ za $m \equiv 1 \pmod 4$ euklidske domene s obzirom na ϕ_m je mnogo složenije. Bio je to vrhunac napora mnogih matematičara 20. stoljeća. Do sada poznati posljednji korak u određivanju takvim m-ova objavili su matematičari Chatland i Davenport 1950. Radi se o dva teorema čije dokaze također nećemo provoditi.

Teorem 2.11. *Neka je m pozitivan kvadratno slobodan cijeli broj takav da je $m \equiv 2, 3 \pmod 4$. Tada je integralna domena $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ euklidska domena s obzirom na ϕ_m ako i samo ako $m = 2, 3, 6, 7, 11, 19, 57$.*

Teorem 2.12. *Neka je m pozitivan kvadratno slobodan cijeli broj takav da je $m \equiv 1 \pmod 4$. Tada je integralna domena $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ euklidska domena s obzirom na ϕ_m ako i samo ako $m = 5, 13, 17, 21, 29, 33, 37, 41, 73$.*

Pokazat ćemo dio tvrdnje sadržane u iskazu Teorema 2.11, odnosno pokazat ćemo sljedeću propoziciju.

Propozicija 2.13. *Ako je $m \in \{2, 3, 6\}$, onda je $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ euklidska domena s obzirom na ϕ_m.*

Dokaz. Pokažimo prvo za $m = 2, 3$. Neka su $x, y \in \mathbb{Q}$. Tada postoje $a, b \in \mathbb{Z}$ takvi da je

$$|x - a| \leq \frac{1}{2},\ |y - a| \leq \frac{1}{2}.$$

Budući da je $(x-a)^2 \geq 0$ i $m(y-b)^2 \geq 0$, imamo

$$|(x-a)^2 - m(y-b)^2| \leq max(|x-a|^2, m|y-b|^2) \leq \frac{3}{4}.$$

Stoga

$$\phi_m((x + y\sqrt{m})^2 - (a + b\sqrt{m})) = |(x-a)^2 - m(y-b)^2| < 1,$$

pa tvrdnja slijedi prema Teoremu 2.7.

Neka je sada $m = 6$. Pretpostavimo da $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ nije euklidska domena s obzirom na ϕ_6. Tada, prema Teoremu 2.7 postoje $r, s \in \mathbb{Q}$ takvi da

$$\phi_6((r + s\sqrt{6}) - (x + y\sqrt{6})) \geq 1, \text{ za sve } x, y \in \mathbb{Z},$$

to jest

$$|(r-x)^2 - 6(s-y)^2| \geq 1 \text{ za sve } x, y \in \mathbb{Z}.$$

Uzmimo $\epsilon_1 = \pm 1$ i $u_1 \in \mathbb{Z}$ takve da

$$0 \leq \epsilon_1 r + u_1 \leq \frac{1}{2}$$

i $\epsilon_2 = \pm 1$ i $u_2 \in \mathbb{Z}$ takve da

$$0 \leq \epsilon_2 s + u_2 \leq \frac{1}{2}.$$

Stavimo

$$r_1 = \epsilon_1 r + u_1 \in \mathbb{Q},\ x_1 = \epsilon_1 x + u_1 \in \mathbb{Z},$$
$$s_1 = \epsilon_2 s + u_2 \in \mathbb{Q},\ y_1 = \epsilon_2 y + u_2 \in \mathbb{Z},$$

pa je

$$0 \leq r_1 \leq \frac{1}{2},\ 0 \leq s_1 \leq \frac{1}{2}, \tag{2.6}$$

i

$$|(r_1 - x_1)^2 - 6(s_1 - y_1)^2| \geq 1 \tag{2.7}$$

za sve $x_1, y_1 \in \mathbb{Z}$. Uvrštavajući $(x_1, y_1) = (0,0), (1,0)$ i $(-1,0)$ u (2.7), dobivamo sljedeće nejednakosti

$$\begin{cases} |r_1^2 - 6s_1^2| \geq 1, \\ |(1 - r_1)^2 - 6s_1^2| \geq 1, \\ |(1 + r_1)^2 - 6s_1^2| \geq 1. \end{cases} \tag{2.8}$$

Iz (2.6) dobivamo

$$\begin{cases} -\frac{3}{2} \leq r_1^2 - 6s_1^2 \leq \frac{1}{4}, \\ -\frac{5}{4} \leq (1 - r_1)^2 - 6s_1^2 \leq 1, \\ -\frac{1}{2} \leq (1 + r_1)^2 - 6s_1^2 \leq \frac{9}{4}. \end{cases} \tag{2.9}$$

Sada iz (2.8) i (2.9) slijedi

$$-\frac{3}{2} \leq r_1^2 - 6s_1^2 \leq 1, \tag{2.10}$$

$$\text{(i) } (1 - r_1^2) - 6s_1^2 = 1 \text{ ili (ii) } -\frac{5}{4} \leq (1 - r_1^2) - 6s_1^2 \leq -1, \tag{2.11}$$

$$1 \leq (1 + r_1)^2 - 6s_1^2 \leq \frac{9}{4}. \tag{2.12}$$

Iz (2.10) i (2.12) dobivamo,

$$1 \leq 1 + 2r_1 + (r_1^2 - 6s_1^2) \leq 2r_1,$$

pa je $r_1 \geq \frac{1}{2}$. No, znamo da je $r_1 \leq \frac{1}{2}$ pa mora biti $r_1 = \frac{1}{2}$. Sada iz (2.11 (i)) slijedi $\frac{1}{4} - 6s_1^2 = 1$, što je nemoguće. Iz (2.11 (ii)) imamo $\frac{1}{4} - 6s_1^2 \leq 1$ pa je $s_1^2 \geq \frac{5}{24}$. No, iz (2.12) slijedi da je $6s_1^2 \leq (1 + r_1)^2 - 1 = \frac{5}{4}$, to jest $s_1^2 \leq \frac{5}{24}$ pa je $s_1^2 = \frac{5}{24}$, što je nemoguće. Time smo dokazali da je $\mathbb{Z} + \mathbb{Z}\sqrt{6}$ euklidska domena s obzirom na ϕ_6. □

Navest ćemo jedan primjer domene koja nije euklidska. Za tu svrhu potreban nam je sljedeći teorem.

Teorem 2.14. *Neka je m pozitivan kvadratno slobodan cijeli broj. Ako postoje različiti neparni brojevi p i q takvi da je*

$$\left(\frac{m}{p}\right) = \left(\frac{m}{q}\right) = -1,$$

zatim pozitivni cijeli brojevi t i u takvi da je

$$pt + qu = m, p \nmid t, q \nmid u,$$

i cijeli broj r takav da je

$$r^2 \equiv pt \pmod{m},$$

onda $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ s obzirom na ϕ_m nije euklidska domena.

Dokaz. Pretpostavimo suprotno, to jest da $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ je euklidska domena s obzirom na ϕ_m. Tada postoje $\gamma, \delta \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ takvi da je

$$r\sqrt{m} = m\gamma + \delta,\ \phi_m(\delta) < \phi_m(m).$$

Stavimo $\gamma = x + y\sqrt{m}, x, y \in \mathbb{Z}$, pa dobivamo

$$\phi_m(r\sqrt{m} - m(x + y\sqrt{m})) < \phi_m(m),$$

to jest

$$|m^2x^2 - m(r - my)^2| < m^2,$$

pa je

$$|mx^2 - (my - r)^2| < m.$$

Budući da je

$$mx^2 - (my - r)^2 \equiv -r^2 \equiv -pt \pmod{m}$$

i

$$0 < pt < pt + qu = m,$$

mora biti

$$mx^2 - (my - r)^2 = -pt \text{ ili } m - pt;$$

pa je

$$mX^2 - Y^2 = -pt \text{ ili } qu$$

za cijele brojeve $X(= x)$ i $Y(= my - r)$.

Pretpostavimo prvo da je $mX^2 - Y^2 = -pt$. Kako je $\left(\frac{m}{p}\right) = -1$, slijedi da $p \nmid m$. Dalje, iz $p \nmid t$ slijedi $p \| -pt$. Prema tome, $p \nmid X$ i$p \nmid Y$. Stoga,

$$\left(\frac{m}{p}\right) = \left(\frac{mX^2}{p}\right) = \left(\frac{Y^2}{p}\right) = 1,$$

što je u kontradikciji $\left(\frac{m}{p}\right) = -1$.

Neka je sada $mX^2 - Y^2 = qu$. Kako je $\left(\frac{m}{q}\right) = -1$, slijedi da $q \nmid m$. Dalje, iz $q \nmid u$ slijedi $q \| -qu$. Prema tome, $q \nmid X$ i $q \nmid Y$. Stoga,

$$\left(\frac{m}{q}\right) = \left(\frac{mX^2}{q}\right) = \left(\frac{Y^2}{q}\right) = 1,$$

što je u kontradikciji $\left(\frac{m}{q}\right) = -1$. Dakle, $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ s obzirom na ϕ_m nije euklidska domena.

□

Teorem 2.15. *$\mathbb{Z} + \mathbb{Z}\sqrt{m}$ s obzirom na ϕ_m nije euklidska domena za $m = 23, 47, 59, 83$.*

Dokaz. Dokaz slijedi direktno iz prethodnog teorema i sljedeće tablice.

m	p	q	t	u	r
23	3	5	1	4	7
47	3	5	4	7	23
59	3	7	15	2	24
83	3	5	1	16	13

□

2.3 Reprezentabilnost prostog broja pomoću binarne kvadratne forme

Izraz oblika $ax^2 + bxy + cy^2$, gdje su $a, b, c \in \mathbb{Z}$ naziva se *binarna kvadratna forma*. Kažemo da je cijeli broj n reprezentiran pomoću binarne kvadratne forme $ax^2 + bxy + cy^2$ ako postoje cijeli brojevi x i y takvi da je $n = ax^2 + bxy + cy^2$. Na primjer, cijeli broj 31 se može reprezentirati formom $x^2 + xy + 3y^2$ jer je $31 = 1^2 + 1 \cdot 3 + 3 \cdot 3^2$, ali cijeli broj 2 se ne može reprezentirati formom $x^2 + 5y^2$.

Prema Teoremu 2.8 i Teoremu 2.10 slijedi da su $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ za $m = -1, -2$ i $\mathbb{Z} + \mathbb{Z}\left((1 + \sqrt{m})/2\right)$ za $m = -3, -7, -11$ euklidske domene pa možemo primijeniti Teorem 1.50 i Teorem 1.51 da odredimo kada je neparan prost broj p reprezentiran svakom od ovih formi:

- $x^2 + y^2, x^2 + 2y^2$,
- $x^2 + xy + y^2$,
- $x^2 + xy + 2y^2$,
- $x^2 + xy + 3y^2$.

Prisjetimo se Legendrovih simbola. Za neparan prost broj p vrijedi

$$\left(\frac{-1}{p}\right) = 1 \qquad \text{ako i samo ako } p \equiv 1 \pmod 4, \tag{2.13}$$

$$\left(\frac{-2}{p}\right) = 1 \qquad \text{ako i samo ako } p \equiv 1, 3 \pmod 8, \tag{2.14}$$

$$\left(\frac{-3}{p}\right) = 1 \qquad \text{ako i samo ako } p \equiv 1 \pmod 3, \tag{2.15}$$

$$\left(\frac{-7}{p}\right) = 1 \qquad \text{ako i samo ako } p \equiv 1, 2, 4 \pmod 7, \tag{2.16}$$

$$\left(\frac{-11}{p}\right) = 1 \qquad \text{ako i samo ako } p \equiv 1, 3, 4, 5, 9 \pmod{11}. \tag{2.17}$$

Primjer 2.16. $\left(\frac{-3}{p}\right) = 1$ ako i samo ako $p \equiv 1 \pmod 3$.

Kako je $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = 1$, imamo dvije mogućnosti:

1) $\left(\frac{-1}{p}\right) = 1$ i $\left(\frac{3}{p}\right) = 1$. Prvi uvjet je ekvivalentan s $p \equiv 1 \pmod 4$. Prema Gaussovom zakonu reciprociteta je $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1$, pa je $p \equiv 1 \pmod 3$. Zajedno ova dva uvjeta daju $p \equiv 1 \pmod{12}$.

2) $\left(\frac{-1}{p}\right) = -1$ i $\left(\frac{3}{p}\right) = -1$. Prvi uvjet je ekvivalentan s $p \equiv 3 \pmod 4$, a za drugi prema Gaussovom zakonu reciprociteta vrijedi $-1 = \left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ što je ekvivalentno s $p \equiv 1 \pmod 3$. Zajedno ova dva uvjeta daju $p \equiv 7 \pmod{12}$.

Iz prvog i drugog slučaja zaključujemo da je $p \equiv 1 \pmod 3$. □

Teorem 2.17. *Neka je p prost broj takav da je* $p \equiv 1 \pmod 4$. *Tada postoje cijeli brojevi x i y takvi da vrijedi* $p = x^2 + y^2$.

Dokaz. Kako je $p \equiv 1 \pmod 4$, iz (2.13) slijedi da je $\left(\frac{-1}{p}\right) = 1$. Budući da je $\mathbb{Z} + \mathbb{Z}\sqrt{-1}$ euklidska domena, prema Teoremu 2.5 to je i domena glavnih ideala. Prema tome, po Teoremu 1.50 postoje cijeli brojevi x i y takvi da vrijedi $p = x^2 + y^2$. □

Teorem 2.18. *Neka je p prost broj takav da je* $p \equiv 1, 3 \pmod 8$. *Tada postoje cijeli brojevi x i y takvi da vrijedi* $p = x^2 + 2y^2$.

Dokaz. Dokaz se provodi analogno kao i prethodni samo što umjesto (2.13) iskoristimo (2.14). □

Teorem 2.19. *Neka je p prost broj takav da je* $p \equiv 1 \pmod 3$. *Tada postoje cijeli brojevi x i y takvi da vrijedi* $p = x^2 + xy + y^2$.

Teorem 2.20. *Neka je p prost broj takav da je* $p \equiv 1, 2, 4 \pmod 7$. *Tada postoje cijeli brojevi x i y takvi da vrijedi* $p = x^2 + xy + 2y^2$.

Teorem 2.21. *Neka je p prost broj takav da je* $p \equiv 1, 3, 4, 5, 9 \pmod{11}$. *Tada postoje cijeli brojevi x i y takvi da vrijedi* $p = x^2 + xy + 3y^2$.

U Teoremu 2.13. pokazali smo da je $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ euklidska domena za $m = 2, 3, 6$. Prisjetimo se iz elementarne teorije brojeva da za neparan prost broj p vrijedi

$$\left(\frac{2}{p}\right) = 1 \qquad \text{ako i samo ako } p \equiv 1, 7 \pmod 8, \tag{2.18}$$

$$\left(\frac{3}{p}\right) = 1 \qquad \text{ako i samo ako } p \equiv 1, 11 \pmod{12}, \tag{2.19}$$

$$\left(\frac{6}{p}\right) = 1 \qquad \text{ako i samo ako } p \equiv 1, 5, 19, 23 \pmod{24}. \tag{2.20}$$

Iz Teorema 1.50, primjenjujući gore navedeno slijede tri teorema.

Teorem 2.22. *Neka je p prost broj takav da je* $p \equiv 1, 7 \pmod 8$. *Tada postoje cijeli brojevi x i y takvi da vrijedi* $p = x^2 - 2y^2$.

Dokaz. U dokazu se koristi činjenica da je $T^2 - 2U^2 = -1$ za $T = U = 1$. □

Teorem 2.23. *Neka je p prost broj takav da je* $p \equiv 1, 11 \pmod{12}$. *Tada postoje cijeli brojevi x i y takvi da je* $p = x^2 - 3y^2$ *ili* $p = 3y^2 - x^2$.

Dokaz. U dokazu se koristi činjenica da ne postoje cijeli brojevi T i U takvi da je $T^2 - 3U^2 = -1$. □

Teorem 2.24. *Neka je p prost broj takav da je $p \equiv 1, 4, 19, 23 \pmod{24}$. Tada postoje cijeli brojevi x i y takvi da je $p = x^2 - 6y^2$ ili $p = 6y^2 - x^2$.*

Dokaz. U dokazu se koristi činjenica da ne postoje cijeli brojevi T i U takvi da je $T^2 - 6U^2 = -1$. □

Bibliografija

[1] S. Alca, K. S. Williams, *Introductory Algebraic Number Theory*, Univer- sity Press, Cambridge, 2004.

[2] A. Dujella, *Uvod u teoriju brojeva (skripta)*, dostupno na `http://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf`, (travanj, 2016.)

[3] K.Horvatić, *Linearna algebra I, II*, PMF-Matematički odjel, Zagreb 1995.

[4] S. Lang, *Algebraic Number Theory*, Springer-Verlag, 1994.

[5] Wikipedia, dostupno na `https://en.wikipedia.org/wiki/Harold_Davenport`, (svibanj 2016.)

Sažetak

Ukratko, u prvom dijelu ovog rada promatra se algebarska struktura integralne domene i dokazuju osnovna svojstva. Navode se primjeri integralnih domena s posebnim naglaskom na skupove oblika $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ i $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ gdje je m kvadratno slobodan cijeli broj. Nadalje, u radu se definiraju asocirani, ireducibilni te prosti elementi integralne domene i neka njihova svojstva. Radi opsežnijeg istraživanja djeljivosti, rasprava je ograničena na posebnu klasu integralnih domena, a to su domene glavnih ideala. U drugom poglavlju definira se euklidska domena te promatraju skupovi koji tvore takvu strukturu posebno skupovi oblika $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ i $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$. Zanimljivo je da ti skupovi tvore euklidsku domenu s obzirom na funkciju $\phi_m(r+s\sqrt{m}) = |r^2 - ms^2|$ ako i samo ako je $m \in \{-1, -2, -3, -7, -11\}$ za $m < 0$ i $m \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$ za $m > 0$. Dokazana svojstva omogućuju prikaz neparnog prostog broja p pomoću binarne kvadratne forme $(x^2 + y^2, x^2 + 2y^2, x^2 + xy + y^2, x^2 + xy + 2y^2$ i $x^2 + xy + 3y^2)$.

Summary

In the first part of this thesis we study the algebraic structure of integral domains and prove some basic properties of them. We give the examples of integral domains with the emphasis on sets of the form $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ and $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$, where m is a squarefree integer. Moreover, associates, irreducible and prime elements of an integral domain with their properties are introduced. Also, for a deeper investigation of divisibility, we limit our discussion to a special class of integral domains - a principal ideal domain.

In the second part, we discuss Euclidean domains especially among the sets $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ and $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$. It is interesting that these sets are Euclidean domains with respect to the function $\phi_m(r+s\sqrt{m}) = |r^2 - ms^2|$ if and only if $m \in \{-1,-2,-3,-7,-11\}$ for $m < 0$ and $m \in \{2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73\}$ for $m > 0$. We apply these results to determine when an odd prime can be represented by a binary quadratic form (x^2+y^2, x^2+2y^2, x^2+xy+y^2, $x^2+xy+2y^2$ and $x^2+xy+3y^2$).

Životopis

Rođena sam 13.9.1991. u Zagrebu. U osnovnu školu Ksavera Šandora Gjalskog u Zaboku krenula sam 1998. godine, a završila 2006. godine. Iste sam godine upisala Opću gimnaziju Antuna Gustava Matoša u Zaboku gdje sam redovito pohađala dodatnu nastavu matematike i informatike. Srednju školu završila sam 2010. godine i polagala državnu maturu s fizikom kao izbornim predmetom na kojoj sam ostvarila izvrstan uspjeh. Te sam godine upisala Fakultet elektrotehnike i računarstva u Zagrebu na kojem sam bila redovan student jednu akademsku godinu. Sljedeće godine, 2011. upisala sam nastavnički smjer preddiplomskog studija Prirodoslovno-matematičkog fakulteta Matematičkog odsjeka Sveučilišta u Zagrebu. U roku sam završila preddiplomski studij i u jesen 2014. godine upisala diplomski studij Matematike nastavnički smjer koji sam završila 2016. godine. Od 2014. godine volontiram u projektu RADDAR u organizaciji XV. gimnazije u Zagrebu i Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu gdje pripremam matematičke radionice za nadarenu djecu osnovnih škola.