Euklidske domene

Buntić, Dora

Master's thesis / Diplomski rad

2024

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:217:677787

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-12-30**

Repository / Repozitorij:

Repository of the Faculty of Science - University of Zagreb

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Dora Buntić

EUKLIDSKE DOMENE

Diplomski rad

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

Zagreb, srpanj, 2024.

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. _____

Hvala obitelji i prijateljima što su vjerovali u mene, bodrili me i bili moj oslonac. Hvala mentorici, izv. prof. dr. sc. Zrinki Franušić na svoj pomoći tijekom pisanja ovog rada.

Diplomski rad napravljen je u sklopu aktivnosti Projekta PK.1.1.02.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Sadržaj

Uvod

Euklidska domena je integralna domena u kojoj možemo definirati takozvanu euklidsku funkciju koja dopušta odgovarajuću generalizaciju Teorema o dijeljenju s ostatkom koji vrijedi u prstenu cijelih brojeva. Osim toga, u euklidskoj domeni možemo provoditi i Euklidov algoritam koji se koristi za određivanje najvećeg zajedničkog djelitelja bilo koja dva elementa. Konkretno, euklidska domena D je komutativni prsten s jedinicom u kojemu ne postoje djelitelji nule i u kojemu postoji funkcija $\phi : D \to \mathbb{Z}$ sa svojstvima:

(1) za sve $a, b \in D$, $b \neq 0$, vrijedi
$$\phi(ab) \geq \phi(a),$$

(2) za sve $a, b \in D$, $b \neq 0$ postoje $q, r \in D$ takvi da vrijedi
$$a = qb + r \ \text{ i } \ \phi(r) < \phi(b).$$

Svaka euklidska domena je domena glavnih ideala, a to znači da je ujedno i domena jedinstvene faktorizacije, odnosno elementi se mogu prikazati jedinstveno pomoću ireducibilnih elemenata na analogan način kao što je to opisano Osnovnim teoremom algebre za cijele brojeve.

Primjere euklidskih domena navodimo iz klasa prstena oblika $\mathbb{Z}[\sqrt{m}]$ i $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$. Na tim prstenima, odnosno općenito na kvadratnim poljima $\mathbb{Q}(\sqrt{m})$ definirali smo funkciju $\phi_m : \mathbb{Q}(\sqrt{m}) \to \mathbb{Q}$,
$$\phi_m\left(r + s\sqrt{m}\right) = |r^2 - ms^2|, \quad r, s \in \mathbb{Q},$$
koja za određene vrijednosti kvadratno slobodnog prirodnog broja m ima ulogu euklidske funkcije. Na primjer, ako je m nenegativan kvadratno slobodan cijeli broj, onda je prsten $\mathbb{Z}[\sqrt{m}]$ euklidska domena s obzirom na ϕ_m ako i samo ako $m = -1, -2$. Nadalje, ako je m pozitivan kvadratno slobodan cijeli broj takav da je $m \equiv 2, 3 \pmod 4$, onda je prsten $\mathbb{Z}[\sqrt{m}]$ euklidska domena s obzirom na ϕ_m ako i samo ako $m = 2, 3, 6, 7, 11, 19, 57$. Pokazali smo jednostavnije slučajeve navedene tvrdnje (i još nekih analognih za prstene oblika $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$) koje se mogu pokazati elementarnim tehnikama.

Zbog boljeg razumijevanja ove algebarske strukture u prvom dijelu rada ponovili smo osnovne strukture kao što su grupe, prsteni, polje i ideali.

Poglavlje 1

Prsteni i ideali

1.1 Grupa

Definicija 1.1.1. *Neka je S neprazan skup. Preslikavanje*

$$* : S \times S \Rightarrow S$$

*naziva se **binarna operacija** na skupu S. Binarna operacija $*$ svakom uređenom paru $(x, y) \in S \times S$ pridružuje element $z = x * y \in S$.*

Definicija 1.1.2. *Neka je G neprazan skup i $*$ preslikavanje s domenom $G \times G$. Uređeni par $(G, *)$ nazivamo **grupa** ako vrijede sljedeća svojstva:*

(1) za sve $x, y \in G$, $x * y \in G$ (zatvorenost),

(2) za sve $x, y, z \in G$, $(x * y) * z = x * (y * z)$ (asocijativnost),

(3) postoji e takav da za svaki $x \in G$ vrijedi $e * x = x * e = x$ (neutralni element),

(4) za svaki $x \in G$ postoji $y \in G$ takav da vrijedi $x * y = y * x = e$ (inverzni element).

Ako vrijedi i svojstvo komutativnosti, to jest ako za svaki $x, y \in G$ vrijedi

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

*onda kažemo da je $(G, *)$ **komutativna** ili **Abelova grupa**.*

Napomena 1.1.3. *U definiciji* 1.1.2 *provjera zatvorenosti operacije zapravo se odnosi na provjeru je li zadana binarna operacija. Također, ako neutralni element e i inverz od bilo kojeg elementa $x \in G$ postoje, jedinstveni su.*

Definicija 1.1.4. *Neka je $(G, *)$ grupa, a skup H podskup grupe G. Ako je $(H, *)$ grupa, kažemo da je H **podgrupa** od G i pišemo $H \leq G$.*

Propozicija 1.1.5. *Neka je $(G, *)$ (Abelova) grupa. Skup $H \subseteq G$ je (Abelova) podgrupa od G ako i samo ako vrijedi*

$$x * y \in H,\ x^{-1} \in H,$$

za sve $x, y \in H$. Odnosno, $H \leq G$ ako i samo ako je $x * y^{-1} \in H$, za sve $x, y \in H$.

Dokaz. Iz $x * y \in H$, za sve $x, y \in H$, slijedi da je operacija $*$ zatvorena na H. Svojstva asocijativnosti i komutativnosti (ako vrijedi) se nasljeđuju iz G. Neutralni element e je iz H zbog toga što pretpostavke $x \in H$ i $x^{-1} \in H$ daju $e = x * x^{-1} \in H$. □

1.2 Prsteni

Definicija 1.2.1. *Neka je R neprazan skup na kojem su definirane dvije binarne operacije $+$ i $\cdot$. Uređenu trojku $(R, +, \cdot)$ nazivamo **prsten** ako vrijede sljedeća svojstva:*

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

(2) $(R, \cdot)$ je polugrupa (to jest operacija $\cdot$ je asocijativna),

(3) distributivnost operacije $\cdot$ s obzirom na operaciju $+$:

$$a(b + c) = ab + ac,\ \ (a + b)c = ac + bc,$$

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

*Neutralni element grupe $(R, +)$ naziva se nula i označava s 0. Ako postoji neutralni element strukture $(R, \cdot)$, on se naziva jedinica i označava s 1, a $(R, +, \cdot)$ se onda naziva **prsten s jedinicom**. Ako je operacija $\cdot$ komutativna, govorimo o **komutativnom prstenu**.*

Definicija 1.2.2. *Neka je R prsten s obzirom na operacije $+$ i $\cdot$. Neprazni podskup $S \subseteq R$ je **potprsten** od R ako je $S = (S, +, \cdot)$ i sam prsten. Pišemo $S \leq R$.*

Propozicija 1.2.3. *Neka je $(R, +, \cdot)$ prsten. Neprazni podskup S od R je potprsten od R ako i samo ako vrijedi:*

(1) za svaki $x, y \in S$ vrijedi $x - y \in S$ (to jest $(S, +)$ je grupa),

(2) za svaki $x, y \in S$ vrijedi $x \cdot y \in S$ (to jest $(S, \cdot)$ je grupoid).

Dokaz. Svojstvo (1) ekvivalentno je tome da je S aditivna podgrupa od R, a prema svojstvu (2) zaključujemo da je $(S, \cdot)$ polugrupa (jer se asocijativnost množenja nasljeđuje). Distributivnosti se također nasljeđuju. □

Neka je m cijeli broj koji je kvadratno slobodan. Prisjetimo se, m je *kvadratno slobodan* ako je 1 najveći kvadrat prirodnog broja koji dijeli m, odnosno $k^2 \nmid m$, za sve $k \in \mathbb{N}$, $k > 1$. Definiramo skup

$$\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \ : \ a, b \in \mathbb{Z}\}.$$

Primjer 1.2.4. *Skup $\mathbb{Z}[\sqrt{m}]$ je komutativni prsten s jedinicom uz operacije standardnog zbrajanja i množenja.*

Rješenje. Budući da je $\mathbb{Z}[\sqrt{m}]$ podskup skupa kompleksnih brojeva, $\mathbb{C}$, koji uz standardno zbrajanje i množenje čini polje, jedino što treba provjeriti da je $(\mathbb{Z}[\sqrt{m}], +)$ podgrupa Abelove grupe $(\mathbb{C}, +)$ te da je $(\mathbb{Z}[\sqrt{m}], \cdot)$ komutativni monoid. U tu svrhu primjenjujemo propoziciju 1.1.5 prema kojoj treba ispitati zatvorenost na zbrajanje te provjeriti da suprotni element svakog elementa iz $\mathbb{Z}[\sqrt{m}]$ leži u $\mathbb{Z}[\sqrt{m}]$.

Neka su $a, b, c, d \in \mathbb{Z}$. Tada je

$$(a + b\sqrt{m}) + (c + d\sqrt{m}) = a + c + (b + d)\sqrt{m} \tag{1.1}$$

element skupa $\mathbb{Z}[\sqrt{m}]$ zbog zatvorenosti zbrajanja cijelih brojeva. Suprotni element od $a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ je $-a - b\sqrt{m}$ i on očito pripada skupu $\mathbb{Z}[\sqrt{m}]$. Dakle, $(\mathbb{Z}[\sqrt{m}], +)$ je Abelova grupa.

Množenje u $\mathbb{Z}[\sqrt{m}]$ je također zatvoreno. Zaista, umnožak

$$(a + b\sqrt{m}) \cdot (c + d\sqrt{m}) = ac + bdm + (ad + bc)\sqrt{m} \tag{1.2}$$

je iz $\mathbb{Z}[\sqrt{m}]$ jer su $ac + bdm, ad + bc \in \mathbb{Z}$. Asocijativnost i komutativnost množenja se nasljeđuje iz $\mathbb{C}$ pa je $(\mathbb{Z}[\sqrt{m}], \cdot)$ komutativna polugrupa. Nadalje, očito je neutrani element množenja $1 \in \mathbb{Z}[\sqrt{m}]$. S obzirom da je svojstvo distributivnosti nasljedno, zaključujemo da je $\mathbb{Z}[\sqrt{m}]$ komutativni prsten s jedinicom. □

Primjer 1.2.5. *Neka je m cijeli broj takav da je $m \equiv 1 \pmod 4$. Skup*

$$\mathbb{Z}\left[\frac{1 + \sqrt{m}}{2}\right] = \{a + b\frac{1 + \sqrt{m}}{2} \ : \ a, b \in \mathbb{Z}\}$$

je komutativni prsten s jedinicom uz operacije standardnog zbrajanja i množenja.

Rješenje. Koristeći analognu argumentaciju iz prethodnog primjera 1.2.4, jedino što trebamo pokazati jest da su operacije zbrajanje i množenje u $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ zatvorene, da je suprotni element svakog elementa iz $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ ponovno iz $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ (što je očito) te da je neutralni element množenja $1 \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ (što je također očito).

Neka su $a, b, c, d \in \mathbb{Z}$. Tada je

$$\left(a + b\frac{1+\sqrt{m}}{2}\right) + \left(c + d\frac{1+\sqrt{m}}{2}\right) = a + c + (b+d)\frac{1+\sqrt{m}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right].$$

Nadalje,

$$\begin{aligned}\left(a + b\frac{1+\sqrt{m}}{2}\right)\cdot\left(c + d\frac{1+\sqrt{m}}{2}\right) &= ac + bd\frac{(1+\sqrt{m})^2}{4} + (ad+bc)\frac{1+\sqrt{m}}{2} \\ &= ac + bd\frac{1+2\sqrt{m}+m}{4} + (ad+bc)\frac{1+\sqrt{m}}{2} \\ &= ac + bd\frac{m-1}{4} + (ad+bc+bd)\frac{1+\sqrt{m}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right],\end{aligned}$$

jer je $ad + bc + bd \in \mathbb{Z}$, a $ac + bd\dfrac{m-1}{4} \in \mathbb{Z}$ budući da je m cijeli broj koji pri dijeljenju s 4 daje ostatak 1. □

Napomena 1.2.6. *Lako se može pokazati da je*

$$\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] = \left\{\frac{a}{2} + \frac{b}{2}\sqrt{m} \,:\, a, b \in \mathbb{Z},\ a \equiv b \pmod 2\right\}.$$

1.3 Polje

Definicija 1.3.1. *Komutativni prsten s jedinicom $(R, +, \cdot)$ u kojem je svaki element $x \in R\backslash\{0\}$ invertibilan naziva se **polje**. Polje se često označava slovom $\mathbb{F}$. Drugim riječima, kažemo da je $(\mathbb{F}, +, \cdot)$ polje ako vrijede sljedeća svojstva:*

(1) $(\mathbb{F}, +)$ je Abelova grupa,

(2) $(\mathbb{F}^*, \cdot)$ je Abelova grupa (gdje je $\mathbb{F}^* = \mathbb{F}\backslash\{0\}$),

(3) distributivnost operacije $\cdot$ s obzirom na operaciju $+$.

Primjer 1.3.2. *Neka je m kvadratno slobodan cijeli broj. Skup*

$$\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} \,:\, a, b \in \mathbb{Q}\}$$

je polje, takozvano kvadratno polje.

Rješenje. Budući da je $\mathbb{Q}(\sqrt{m})$ podskup polja $\mathbb{C}$, prema propoziciji 1.1.5 dovoljno je pokazati:

- $(\mathbb{Q}(\sqrt{m}), +)$ je podgrupa Abelove grupe $(\mathbb{C}, +)$,
- $(\mathbb{Q}(\sqrt{m})^*, \cdot)$ je podgrupa Abelove grupe $(\mathbb{C}^*, \cdot)$.

Neka su $a, b, c, d \in \mathbb{Q}$. Uočimo da se zatvorenost zbrajanja i množenja pokazuje na isti način kao u primjeru 1.2.4, odnosno izrazi u (1.1) i (1.2) su iz $\mathbb{Q}(\sqrt{m})$. Budući da u polju ne postoje djelitelji nule, ako je jedan od faktora $a + b\sqrt{m}$ i $c + d\sqrt{m}$ različit od nule, onda je i njihov umnožak različit od nule pa smo argumentirali zatvorenost množenja na $\mathbb{Q}(\sqrt{m})^*$.

Suprotni element od $a + b\sqrt{m}$ je očito iz $\mathbb{Q}(\sqrt{m})$. Svaki element iz $\mathbb{Q}(\sqrt{m})^*$ je invertibilan. Preostaje jedino pokazati da je $(a + b\sqrt{m})^{-1} \in \mathbb{Q}(\sqrt{m})^*$. Zaista,

$$(a + b\sqrt{m})^{-1} = \frac{1}{a + b\sqrt{m}} = \frac{a - b\sqrt{m}}{a^2 - mb^2} = \frac{a}{a^2 - mb^2} + \frac{-b}{a^2 - mb^2}\sqrt{m} \in \mathbb{Q}(\sqrt{m})^*.$$

□

Napomena 1.3.3. *Kažemo da je $\alpha \in \mathbb{C}$* algebarski broj *ako je nultočka polinoma s racionalnim koeficijentima.* Algebarski cijeli broj *je nultočka polinoma s cjelobrojnim koeficijentima i vodećim koeficijentom jednakim 1. Skup svih algebarskih cijelih brojeva u kvadratnom polju $\mathbb{Q}(\sqrt{m})$ je prsten $\mathbb{Z}[\sqrt{m}]$, ako je $m \equiv 2 \pmod 4$ ili $m \equiv 3 \pmod 4$. Ako je $m \equiv 1 \pmod 4$, onda je skup svih algebarskih cijelih brojeva u $\mathbb{Q}(\sqrt{m})$ jednak prstenu $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$.*

1.4 Integralna domena

Definicija 1.4.1. *Neka je $(R, +, \cdot)$ prsten i neka su $a, b \in R$ sa svojstvom $a \neq 0$ i $b \neq 0$. Tada vrijedi $ab = 0$. Onda kažemo da su elementi a i b* ***djelitelji nule*** *u prstenu R.*

Uočimo da u polju ne postoje djelitelji nule. Zaista, ako su $a \neq 0$ i $b \neq 0$ iz nekog polja $\mathbb{F}$ i $ab = 0$, tada množenjem prethodne relacije s b^{-1} slijedi da je $a = 0$. Kontradikcija!

Primjer 1.4.2. *Prsteni $\mathbb{Z}[\sqrt{m}]$ i $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ su integralne domene.*

Definicija 1.4.3. ***Integralna domena*** *je komutativni prsten s jedinicom koja nema djelitelja nule.*

Propozicija 1.4.4. *Neka je D integralna domena i $a, b, c \in D$. Vrijedi:*

$$ab = ac, a \neq 0 \Rightarrow b = c,$$

$$ac = bc, c \neq 0 \Rightarrow a = b.$$

Dokaz. Zbog svojstva distributivnosti iz $ab = ac$ slijedi $a(b-c) = 0$. U integralnoj domeni ne postoje djelitelji nule pa je $b - c = 0$ zbog pretpostavke da je $a \neq 0$. □

Definicija 1.4.5. *Neka je D integralna domena, te $a, b \in D$. Kažemo da je a **djelitelj** od b, odnosno da a **dijeli** b ako postoji element $c \in D$ takav da vrijedi $b = ac$. Pišemo $a \mid b$. U suprotnom, ako a ne dijeli b, pišemo $a \nmid b$.*

Neka su a, b, c elementi integralne domene D. Direktno iz prethodne definicije možemo zaključiti sljedeće:

(a) $a \mid a$ (refleksivnost)

(b) $a \mid b$ i $b \mid c \;\Rightarrow\; a \mid c$ (tranzitivnost)

(c) $a \mid b$ i $a \mid c \;\Rightarrow\; a \mid (xb + yc)$ za sve $x, y \in D$

(d) $a \mid b \;\Rightarrow\; ac \mid bc$

(e) $ac \mid bc$ i $c \neq 0 \;\Rightarrow\; a \mid b$

(f) $1 \mid b$

(g) $a \mid 0$

(h) $0 \mid a \;\Rightarrow\; a = 0$.

Definicija 1.4.6. *Invertibilni element integralne domene D, odnosno djelitelj neutralnog elementa domene naziva se **jedinica**. Skup svih jedinica u D označavamo s $U(D)$.*

Za jedinice integralne domene D vrijede sljedeća svojstva:

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

(b) $a \in U(D) \;\Rightarrow\; -a \in U(D)$

(c) $a \in U(D) \;\Rightarrow\; a^{-1} \in U(D)$

(d) $a, b \in U(D) \;\Rightarrow\; ab \in U(D)$

(e) $a \in U(D) \;\Rightarrow\; \pm a^n \in U(D)$, za svaki $n \in \mathbb{Z}$

1.5 Ideali

Definicija 1.5.1. *Neka je R prsten. Podskup $I \subseteq R$ je **lijevi** (to jest **desni**) **ideal** u R ako vrijede sljedeća svojstva:*

(1) I je potprsten od R,

(2) Za sve $r \in R$ i $x \in I$ je $rx \in I$ (to jest $xr \in I$)

*Podskup $I \subseteq R$ je (dvostrani) **ideal** ako je on istovremeni i lijevi i desni ideal. Činjenicu da je I ideal u prstenu R označavamo s $I \trianglelefteq R$.*

Napomena 1.5.2. *U definiciji* 1.5.1 *drugi se uvjet može zapisati kao $RI \subseteq I$. Također, ideal I od R je pravi ideal ako je $I \neq R$ i $I \neq (0)$, gdje je* (0) *nul-ideal.*

U slučaju komutativnog prstena R nema smisla govoriti o jednostranim idealima.

Općenito, operacija presjeka čuva algebarsku strukturu. Zbog toga je presjek dva ideala iz prstena R, opet ideal u R. Štoviše, presjek familije ideala iz R je ideal. Zbog toga za neprazni podskup $S \subseteq R$ ima smisla definirati ideal koji dobivamo kao presjek svih ideala koji sadrže skup S, odnosno

$$\langle S \rangle := \bigcap_{J \trianglelefteq R,\ S \subseteq J} J.$$

Jasno je da je $\langle S \rangle$ najmanji ideal koji sadrži skup S. Ako je $I = \langle S \rangle$, onda kažemo da je ideal I generiran skupom S.

Definicija 1.5.3. *Ideal I je **konačno generiran** ako postoji konačan podskup $S \subseteq R$ takav da je $I = \langle S \rangle$. Ideal I je **glavni ideal** ako postoji neki element $r \in R$ takav da je $I = \langle r \rangle$.*

*Kažemo da je R **prsten glavnih ideala**, ili kraće PGI, ako je svaki ideal u R glavni.*

1.6 Dijeljenje s ostatkom

Teorem 1.6.1 (Teorem o dijeljenju s ostatkom u $\mathbb{Z}$)**.** *Ako su $a \in \mathbb{Z}$ i $b \in \mathbb{N}$, onda postoje jedinstveni $q \in \mathbb{Z}$ i $r \in \mathbb{N}_0$, takvi da je $a = qb + r$, pri čemu je $0 \leq r < b$.*

Dokaz. Promotrimo skup $\{a - bn : n \in \mathbb{Z}\}$. Najmanji nenegativan član tog skupa označimo s r. Tada po definiciji $0 \neq r < a$ i postoji $q \in \mathbb{Z}$ takav da je $a - qb = r$, to jest $a = qb + r$. Nakon što smo dokazali egzistenciju, pokažimo i jedinstvenost. Pretpostavimo suprotno, pretpostavimo da postoje $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ te $0 \neq r_1, r_2 < b$ takvi da vrijedi

$$a = q_1 b + r_1, \quad a = q_2 b + r_2.$$

Oduzimanjem dobivamo

$$b(q_1 - q_2) = r_1 - r_2 \text{ i } 0 < r_1 - r_2 < b.$$

Neka je $q_1 \neq q_2$, tada vrijedi

$$r_1 - r_2 = b(q_1 - q_2) \geq b,$$

što je u kontradikciji s pretpostavkom, stoga je $r_1 = r_2$ i $q_1 = q_2$. □

Definicija 1.6.2. *Neka su $b, c \in \mathbb{Z}$. Cijeli broj a zovemo **zajednički djelitelj** od b i c ako $a \mid b$ i $a \mid c$. Ako je barem jedan od brojeva b i c različit od nule, onda postoji samo konačno mnogo zajedničkih djelitelja od b i c. Najveći među njima zove se **najveći zajednički djelitelj** od b i c i označava se s* $\operatorname{nzd}(b, c)$ *(ili* $\gcd(b, c)$ *od "greatest common divisor" ili samo $\langle b, c \rangle$).*

Slično definiramo najveći zajednički djelitelj brojeva $b_1, b_2, \ldots, b_n$ koji su različiti od nule, te označavamo s $\operatorname{nzd}(b_1, b_2, \ldots, b_n)$

Uočimo da je $\operatorname{nzd}(b, c) \geq 1$.

Teorem 1.6.3 (Teorem o dijeljenju polinoma s ostatkom)**.** *Za svaka dva polinoma $p, s \in \mathbb{R}[x]$, $s \neq 0$, postoje jedinstveni polinomi $q, r \in \mathbb{R}[x]$ takvi da vrijedi*

$$p(x) = s(x)q(x) + r(x), \text{ za svaki } x \in \mathbb{R}$$

pri čemu je $r = 0$ ili $\deg r < \deg s$.

Dokaz. Egzistencija: Ako je $p = 0$, onda tvrdnja vrijedi za $q = r = 0$. Ako je $p \neq 0$, razlikujemo slučajeve: $\deg p < \deg s$ i $\deg p \geq \deg s$. U slučaju kada je $\deg p < \deg s$, jednakost zadovoljavaju polinomi $q = 0$ i $r = p$.

U slučaju kada je $\deg p \geq \deg s$, tvrdnja se dokazuje matematičkom indukcijom.

Jedinstvenost: Pretpostavimo da postoje polinomi q_1, r_1 i q_2, r_2 takvi da za svaki $x \in \mathbb{R}$ vrijedi:

$$p(x) = s(x)q_1(x) + r_1(x), \text{uz } r_1 = 0 \text{ ili } \deg r_1 < \deg s$$

i

$$p(x) = s(x)q_2(x) + r_2(x), \text{uz } r_2 = 0 \text{ ili } \deg r_2 < \deg s$$

Oduzimanjem jednakosti, slijedi

$$s(x)(q_1(x) - q_2(x)) + (r_1(x) - r_2(x)) = 0.$$

Ako je $r_1(x) - r_2(x) = 0$, onda je i $s(x)(q_1(x) - q_2(x)) = 0$ za svaki $x \in \mathbb{R}$. Budući da je $s \neq 0$, to povlači da je $q_1(x) - q_2(x) = 0$ odnosno da je $q_1(x) = q_2(x)$.

Ako je $q_1(x) - q_2(x) = 0$, također slijedi da je $r_1(x) = r_2(x)$. Pretpostavimo da su $r_1(x) \neq r_2(x)$ i $q_1(x) \neq q_2(x)$. Iz jednakosti koju smo dobili oduzimanjem, usporedimo stupnjeve:

$$\deg s + \deg(q_1 - q_2) = \deg(r_1 - r_2).$$

Znamo da za oduzimanje i zbrajanje polinoma vrijedi

$$\deg(r_1 - r_2) \leq \max\{\deg r_1, \deg r_2\}.$$

Kako je $\deg(q_1 - q_2) \geq 0$ dobivamo

$$\deg s \leq \deg s + \deg(q_1 - q_2) = \deg(r_1 - r_2) \leq \max\{\deg r_1, \deg r_2\}.$$

S obzirom da je $\deg r_1 < \deg s$ i $\deg r_2 < \deg s$ slijedi:

$$\deg s \leq \deg s + \deg(q_1 - q_2) = \deg(r_1 - r_2) \leq \max\{\deg r_1, \deg r_2\} < \deg s.$$

Dobili smo da je $\deg s < \deg s$, što je kontradikcija. Dakle, zaključujemo da je pretpostavka bila pogrešna. □

Poglavlje 2

Definicija i svojstva euklidske domene

2.1 Euklidska funkcija

Kako bismo definirali euklidsku domenu, najprije trebamo definirati euklidsku funkciju.

Definicija 2.1.1 (Euklidska funkcija)**.** *Neka je D integralna domena. Preslikavanje $\phi : D \to \mathbb{Z}$ nazivamo **euklidska funkcija** na D ako zadovoljava sljedeća svojstva:*

(1) za sve $a, b \in D$, $b \neq 0$, vrijedi

$$\phi(ab) \geq \phi(a), \tag{2.1}$$

(2) za sve $a, b \in D$, $b \neq 0$ postoje $q, r \in D$ takvi da vrijedi

$$a = qb + r \ \text{ i } \ \phi(r) < \phi(b). \tag{2.2}$$

Primjer 2.1.2. *Funkcija apsolutne vrijednosti na prstenu svih cijelih brojeva $\mathbb{Z}$ je euklidska funkcija.*

Rješenje. Neka je

$$\phi : \mathbb{Z} \to \mathbb{Z}, \ \phi(a) = |a|, \ a \in \mathbb{Z}.$$

Lako se vidi da vrijedi prvo svojstvo iz definicije 2.1.1. Zaista za $a, b \in \mathbb{Z}$ i $b \neq 0$ vrijedi

$$\phi(ab) = |ab| = |a| \cdot |b| \geq |a| = \phi(a),$$

jer je $|b| \geq 1$.

Drugo svojstvo iz definicije 2.1.1 vrijedi prema Teoremu o djeljenju s ostatkom 1.6.1. Neka su $a, b \in \mathbb{Z}$ i $b \neq 0$. Tada primjenom teorema 1.6.1 na a i $|b|$, slijedi da postoje cijeli brojevi q i r

$$a = q \cdot |b| + r \ \text{ i } \ 0 \leq r < |b| = \phi(b).$$

Jasno je da je $a = qb + r$ ili $a = (-q)b + r$ u ovisnosti o tome je li $b > 0$ ili $b < 0$. □

Primjer 2.1.3. *Skup svih polinoma s realnim koeficijentima, $\mathbb{R}[x]$, čini integralnu domenu. Definiramo preslikavanje $\phi : \mathbb{R}[x] \to \mathbb{Z}$ s*

$$\phi(p) = \begin{cases} \deg p, & \text{ako } p \neq 0, \\ -1, & \text{ako } p = 0. \end{cases} \tag{2.3}$$

ϕ je euklidska funkcija na $\mathbb{R}[x]$.

Rješenje. Pokažimo da vrijedi prvo svojstvo definicije. Imamo

$$\phi(pq) = \deg(pq) = \deg p + \deg q \geq \deg p = \phi(p).$$

Drugo svojstvo vrijedi direktno iz Teorema o dijeljenju s ostatkom za polinome 1.6.3. □

Općenito elementi q i r u (2.2) nisu jednoznačno određeni. Pokažimo na primjeru.

Primjer 2.1.4. *U prstenu cijelih brojeva $\mathbb{Z}$ uz apsolutnu vrijednost kao euklidsku funkciju za $a = 3$ i $b = 2$ vrijedi*

$$\begin{aligned} 3 &= 1 \cdot 2 + 1, \quad |1| < |2|, \\ 3 &= 2 \cdot 2 - 1, \quad |-1| < |2|. \end{aligned}$$

Dakle, kvocijent q i ostatak r nisu jednoznačno određeni.

Ako je D integralna domena koja nije polje i posjeduje euklidsku funkciju ϕ za koju su kvocijent q i ostatak r u (2.2) uvijek jednoznačno određeni s a i b, tada je D polje ili prsten polinoma nad poljem, odnosno $D = \mathbb{F}$ ili $D = \mathbb{F}[x]$ za neko polje $\mathbb{F}$.

Teorem 2.1.5 (Svojstva euklidske funkcije)**.** *Neka je D integralna domena, a preslikavanje $\phi : D \to \mathbb{Z}$ euklidska funkcija na D. Neka su $a, b \in D$. 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 je $\phi(a) > \phi(0)$.

Dokaz. **(a)** Pretpostavimo da vrijedi $a \sim b$, tada postoji $u \in U(D)$ takav da je $a = ub$. Iz (2.1) slijedi $\phi(a) = \phi(ub) \geq \phi(b)$. Kako je $u \in U(D)$, imamo $u^{-1} \in U(D)$ i $b = u^{-1}a$, pa opet iz (2.1) slijedi $\phi(b) = \phi(u^{-1}a) \geq \phi(a)$. Iz te dvije nejednakosti možemo zaključiti da vrijedi $\phi(a) = \phi(b)$.

(b) Prema (2.2) postoje $q, r \in D$ takvi da vrijedi $a = qb + r$ i $\phi(r) \leq \phi(b) = \phi(a)$. S obzirom da $a \mid b$, tada $a \mid r$. Pretpostavimo da je $r \neq 0$. Tada iz (2.1) slijedi $\phi(r) \geq \phi(a)$, što je kontradikcija. Stoga $r = 0$ i $a = qb$, odnosno $b \mid a$. Ali, s obzirom da $a \mid b$, tada je $q \in U(D)$ te $a \sim b$.

(c) Prema tvrdnji (a) vrijede implikacije

$$a \in U(D) \;\Rightarrow\; a \sim 1 \;\Rightarrow\; \phi(a) = \phi(1).$$

Obratno, prema tvrdnji (b) vrijede implikacije

$$1 \mid a, \phi(1) = \phi(a) \;\Rightarrow\; 1 \sim a \;\Rightarrow\; a \in U(D).$$

(d) Prema (2.2) postoje $q, r \in D$ takvi da je $0 = qa + r, \phi(r) < \phi(a)$. Pretpostavimo da je $r \neq 0$. Tada je $q \neq 0$ i iz (2.1) slijedi da vrijedi $\phi(r) = \phi((-q)a) \geq \phi(a)$, što je kontradikcija. Stoga, $r = 0$ i $\phi(0) < \phi(a)$. □

2.2 Definicija euklidske domene

Definicija 2.2.1. *Neka je D integralna domena. Ako postoji funkcija $\phi : D \to \mathbb{Z}$, onda se D naziva **euklidska domena** s obzirom na ϕ.*

Dokažimo fundamentalni teorem da je svaka euklidska domena domena glavnih ideala.

Teorem 2.2.2. *Svaka euklidska domena je domena glavnih ideala.*

Dokaz. Neka je D euklidska domena s normom $\phi : D \to \mathbb{N} \cup \{0\}$ i neka je I ideal u D. Ako je $I = \{0\}$, onda je $I = \langle 0 \rangle$ glavni ideal. Pretpostavimo $I \neq \{0\}$. Skup

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

je omeđen odozdo pa postoji $a \in I, a \neq 0$, koji ima minimalnu normu u S. Pokažimo da je $I = \langle a \rangle$. Očito je $\langle a \rangle \subseteq I$. Neka je $b \in I, b \neq 0$. Kako je D euklidska domena, postoje $q, r \in D$ takvi da je

$$b = qa + r \;\text{ i }\; \phi(r) < \phi(a).$$

Primijetimo da je $r = b - aq \in I$. Ako je $r \neq 0$, onda iz $0 < \phi(r) < \phi(a)$ dobivamo kontradikciju zbog minimalnosti norme $\phi(a)$. Dakle, $r = 0$. Stoga $b = aq \in \langle a \rangle$. Zaključujemo da je $I \subseteq \langle a \rangle$, što povlači $I = \langle a \rangle$. □

2.3 Euklidov algoritam

U prstenu cijelih brojeva $\mathbb{Z}$ se najveći zajednički djelitelj dva broja može odrediti pomoću Euklidova algoritma koji se zasniva na Teoremu o dijeljenju s ostatkom.

Primjer 2.3.1. *Pomoću Euklidova algoritma odredite najveći zajednički djelitelj 326 i 96.*

Rješenje. Primjenom Euklidovog algoritma dobivamo

$$\begin{aligned} 326 &= 96 \cdot 3 + 38 \\ 96 &= 38 \cdot 2 + 20 \\ 38 &= 20 \cdot 1 + 18 \\ 20 &= 18 \cdot 1 + 2 \\ 18 &= 2 \cdot 9 \end{aligned}$$

Zaključujemo da je $\text{nzd}(326, 96) = 2$. □

Euklidov algoritam iz prstena cijelih brojeva može se poopćiti u svakoj euklidskoj domeni D pri čemu se zadržava i njegova primjena za određivanje najvećeg zajedničkog djelitelja dvaju elemenata a i b iz D. Budući da je $\text{nzd}(c, 0) = \text{nzd}(0, c) = c$ za sve $c \in D\backslash\{0\}$, dovoljno je razmotriti slučaj u kojem su elementi a i b različiti od nule.

Teorem 2.3.2 (Euklidov algoritam)**.** *Neka su $a, b \neq 0$ elementi euklidske domene D s euklidskom funkcijom ϕ te neka su elementi $q_1, q_2, \ldots$ i $r_{-1}, r_0, r_1, r_2, \ldots$ iz D zadani rekurzivno:*

$$r_{-1} = a, r_0 = b, \tag{2.4}$$

i

$$r_j = q_{j+2} r_{j+1} + r_{j+2},\ \phi(r_{j+2}) < \phi(r_{j+1}), \tag{2.5}$$

za $j = -1, 0, 1, 2, \ldots, k$ gdje je k najmanji cijeli broj veći ili jednak -1 za koji je $r_{k+2} = 0$. Tada je

$$\text{nzd}(a, b) = r_{k+1}.$$

Dokaz. Najprije uočimo da su nizovi (r_i) i (q_i) dobro definirani pomoću (2.5) zbog svojstva (2.2) euklidske funkcije ϕ. Nadalje, algoritam u (**??**) mora završiti nakon konačnog broja koraka. Zaista, niz $(\phi(r_i))_{i \geq 0}$ je padajući niz cijelih brojeva, odnosno

$$\phi(r_0) > \phi(r_1) > \phi(r_2) > \cdots > \phi(r_i) > \phi(r_{i+1}) > \cdots$$

S druge strane taj je niz ograničen odozdo brojem $\phi(0)$ prema svojstvu (d) teorema 2.1.5. Stoga postoji $k + 2 \geq 1$ takav da je $r_{k+2} = 0$ (jer se algoritam može provoditi sve dok je r_i različit od 0).

Iz (2.5) zaključujemo da vrijedi

$$\langle r_j, r_{j+1} \rangle = \langle q_{j+2} r_{j+1} + r_{j+2}, r_{j+1} \rangle = \langle r_{j+2}, r_{j+1} \rangle = \langle r_{j+1}, r_{j+2} \rangle$$

za $j = -1, 0, 1, 2, \ldots, k$. Stoga je

$$\langle a, b \rangle = \langle r_{-1}, r_0 \rangle = \langle r_0, r_{-1} \rangle = \ldots = \langle r_k, r_{k+1} \rangle = \langle r_{k+1}, r_{k+2} \rangle = \langle r_{k+1}, 0 \rangle = \langle r_{k+1} \rangle$$

tako da je

$$\text{nzd}(a, b) = r_{k+1}.$$

□

Poglavlje 3

Primjeri euklidskih domena

U prethodnom poglavlju uočili smo da su prsten cijelih brojeva $\mathbb{Z}$ i prsten polinoma $\mathbb{R}[x]$ euklidske domene (primjeri 2.1.2 i 2.1.2). U ovom poglavlju ćemo istražiti kada su integralne domene $\mathbb{Z}[\sqrt{m}]$ za $m \equiv 2, 3 \pmod 4$ i $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ za $m \equiv 1 \pmod 4$ euklidske domene s obzirom na funkciju

$$r + s\sqrt{m} \mapsto |r^2 - ms^2|,$$

gdje su $r, s \in \mathbb{Q}$.

3.1 Funkcija ϕ_m

Definicija 3.1.1 (Funkcija ϕ_m)**.** *Neka je m kvadratno slobodan cijeli broj. Funkciju*

$$\phi_m : \mathbb{Q}(\sqrt{m}) \to \mathbb{Q}$$

definiramo kao

$$\phi_m\left(r + s\sqrt{m}\right) = |r^2 - ms^2|,$$

za $r, s \in \mathbb{Q}$.

U sljedećoj lemi pokazat ćemo neka osnovna svojstva funkcije ϕ_m.

Lema 3.1.2. *Neka je m kvadratno slobodan cijeli broj. Vrijede svojstva:*

(a) $\phi_m : \mathbb{Z}[\sqrt{m}] \to \mathbb{N} \cup \{0\}$.

(b) Ako je $m \equiv 1 \pmod 4$, *tada je* $\phi_m : \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] \to \mathbb{N} \cup \{0\}$.

(c) Neka je $\alpha \in \mathbb{Q}(\sqrt{m})$. *Tada je* $\phi_m(\alpha) = 0$ *ako i samo ako je* $\alpha = 0$.

(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* $\alpha, \beta \in \mathbb{Z}[\sqrt{m}]$ *te* $\beta \neq 0$.

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

Dokaz. (a) Neka je $\alpha \in \mathbb{Z}[\sqrt{m}]$. Stoga je $\alpha = x + y\sqrt{m}$ za neke $x, y \in \mathbb{Z}$. Kako je $x^2 - my^2 \in \mathbb{Z}$ i $|x^2 - my^2| \geq 0$, zaključujemo da je

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

(b) Neka je $m \equiv 1 \pmod 4$ i $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$. Tada postoje $x, y \in \mathbb{Z}$ takvi da je

$$\alpha = x + y\left(\frac{1+\sqrt{m}}{2}\right) = \left(x + \frac{y}{2}\right) + \frac{y}{2}\sqrt{m}.$$

Uvrštavanjem u formulu za ϕ_m dobivamo:

$$\begin{aligned}\phi_m(\alpha) = \phi_m\left(\left(x + \frac{y}{2}\right) + \frac{y}{2}\sqrt{m}\right) &= \left|\left(x + \frac{y}{2}\right)^2 - m\left(\frac{y}{2}\right)^2\right| \\ &= \left|x^2 + xy + \frac{1}{4}(1-m)y^2\right|.\end{aligned}$$

Kako je $\frac{1}{4}(1-m) \in \mathbb{Z}$ (jer je $m = 4k+1$, za neki $k \in \mathbb{Z}$), zaključujemo da je $\phi_m(\alpha)$ nenegativan cijeli broj.

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

$$\phi_m(\alpha) = 0 \iff r^2 - ms^2 = 0.$$

Ako je $s = 0$, onda je nužno i $r = 0$. Nadalje, ako je $s \neq 0$, onda je $\sqrt{m} = \left|\frac{r}{s}\right|$ što nije moguće jer je $\sqrt{m}$ iracionalan broj. Stoga je $\alpha = 0$.

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

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

(e) Neka su $\alpha, \beta \in \mathbb{Z}[\sqrt{m}]$ te $\beta \neq 0$. Prema tvrdnjama iz (a) i (c) zaključujemo da je $\phi_m(\beta)$ prirodni broj. Nadalje, prema tvrdnji (d) imamo

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

(f) Analogno kao u tvrdnji (e) samo što u dokazu koristimo tvrdnju (b) umjesto tvrdnje (a).

□

3.2 Prsten $\mathbb{Z}[\sqrt{m}]$

U sljedećem teoremu, koristeći svojstva iz leme 3.1.2, iznosimo nužne i dovoljne uvjete da bi prsten $\mathbb{Z}[\sqrt{m}]$ bio euklidska domena s obzirom na preslikavanje ϕ_m.

Teorem 3.2.1. *Neka je m kvadratno slobodan cijeli broj. Tada je prsten $\mathbb{Z}[\sqrt{m}]$ euklidska domena s obzirom na preslikavanje ϕ_m ako i samo ako za svaki $x, y \in \mathbb{Q}$ postoje $a, b \in \mathbb{Z}$ takvi da vrijedi*

$$\phi_m((x + y\sqrt{m}) - (a + b\sqrt{m})) < 1. \tag{3.1}$$

Dokaz. $\boxed{\Rightarrow}$: Pretpostavimo da je $\mathbb{Z}[\sqrt{m}]$ euklidska domena s obzirom na preslikavanje ϕ_m. Neka su $x, y \in \mathbb{Q}$. Tada je

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

za neke cijele brojeve r, s, t, pri čemu je $t \neq 0$. S obzirom da je ϕ_m euklidska funkcija na $\mathbb{Z}[\sqrt{m}]$, postoje $a + b\sqrt{m}, c + d\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ takvi da vrijedi

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

Stoga, prema tvrdnji (d) iz leme 3.1.2 slijedi

$$\begin{aligned}
\phi_m((x + y\sqrt{m}) - (a + b\sqrt{m})) &= \phi_m\left(\frac{r + s\sqrt{m}}{t} - (a + b\sqrt{m})\right) \\
&= \phi_m\left(\frac{r + s\sqrt{m} - t(a + b\sqrt{m})}{t}\right) \\
&= \phi_m\left(\frac{c + d\sqrt{m}}{t}\right) \\
&= \frac{\phi_m(c + d\sqrt{m})}{\phi_m(t)} < 1.
\end{aligned}$$

$\boxed{\Leftarrow}$: Pretpostavimo da vrijedi (3.1). Kako bismo pokazali da je $\mathbb{Z}[\sqrt{m}]$ euklidska domena s obzirom na preslikavanje ϕ_m, moramo pokazati da vrijedi (2.1) i (2.2). Nejednakost (2.1) slijedi iz leme 3.1.2. Provjerimo da vrijedi (2.2). Neka su $r+s\sqrt{m}, t+u\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$, gdje je $t + u\sqrt{m} \neq 0$. Tada je

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

gdje su

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

Primijetimo da $t + u\sqrt{m} \neq 0$ povlači da $t^2 - mu^2 \neq 0$. Prema pretpostavci (3.1) postoji $a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ takav da vrijedi

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

Definiramo

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

Stoga, za $r + s\sqrt{m}$ i $t + u\sqrt{m}$ postoje $a + b\sqrt{m}, c + d\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ takvi da je

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

Nadalje, prema lemi 3.1.2 vrijedi

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

□

Pomoću teorema 3.2.1 odrediti ćemo sve negativne kvadratno slobodne cijele brojeve m za koje je $\mathbb{Z}[\sqrt{m}]$ euklidska domena s obzirom na ϕ_m.

Teorem 3.2.2. *Neka je m negativan kvadratno slobodan cijeli broj. Tada je prsten* $\mathbb{Z}[\sqrt{m}]$ *euklidska domena s obzirom na* ϕ_m *ako i samo ako* $m = -1, -2$.

Dokaz. $\boxed{\Rightarrow}$: Pokažimo prvo da je $\mathbb{Z}[\sqrt{m}]$ euklidska domena s obzirom na ϕ_m za $m = -1$ i $m = -2$. Neka su $x, y \in \mathbb{Q}$. Odaberimo $a, b \in \mathbb{Z}$ takve da vrijedi

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

Tada

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

Prema prethodnom teoremu, zaključujemo da je $\mathbb{Z}[\sqrt{m}]$ euklidska domena s obzirom na ϕ_m za $m = -1$ i $m = -2$.
$\boxed{\Leftarrow}$: Pretpostavimo da je $\mathbb{Z}[\sqrt{m}]$ euklidska domena s obzirom na ϕ_m. Tada prema prethodnom teoremu, postoje $a, b \in \mathbb{Z}$ takvi da vrijedi

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

S obzirom da je $-m = |m|$, imamo

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

Ali za bilo koji cijeli broj x vrijedi

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

pa slijedi

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

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

Određivanje pozitivnih kvadratno slobodno cijelih brojeva m za koje su $\mathbb{Z}[\sqrt{m}]$ (u slučaju $m \equiv 2, 3 \pmod 4$) i $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ (u slučaju $m \equiv 1 \pmod 4$ u kojem će biti riječi u sljedećem odjeljku) euklidske domene s obzirom na ϕ_m mnogo je teže te je predstavljalo vrhunac napora brojnih matematičara 19. i 20. stoljeća. Posljednji korak pri određivanju takvih pozitivnih kvadratno cijelih brojeva su napravili matematičari Chatland i Davenport. Godine 1950. su ustanovili teoreme 3.2.3 i 3.3.3 koje nećemo dokazivati.

Teorem 3.2.3. *Neka je m pozitivan kvadratno slobodan cijeli broj takav da je $m \equiv 2, 3 \pmod 4$. Tada je prsten $\mathbb{Z}[\sqrt{m}]$ euklidska domena s obzirom na ϕ_m ako i samo ako*

$$m = 2, 3, 6, 7, 11, 19.$$

Pokažimo djelomično teorem 3.2.3.

Propozicija 3.2.4. *Neka je $m \in \{2, 3, 6\}$. Tada je prsten $\mathbb{Z}[\sqrt{m}]$ euklidska domena s obzirom na ϕ_m.*

Dokaz. Neka je $m = 2$ ili 3. Za $x, y \in \mathbb{Q}$ neka su $a, b \in \mathbb{Z}$ takvi da vrijedi

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

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

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

Stoga

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

pa tvrdnja vrijedi prema teoremu 3.2.1

Pokažimo sada za $m = 6$. Pretpostavimo suprotno, to jest da $\mathbb{Z}[\sqrt{6}]$ nije euklidska domena s obzirom na ϕ_6. Tada prema teoremu 3.2.1, postoje $r, s \in \mathbb{Q}$ takvi da za svaki $x, y \in \mathbb{Z}$ vrijedi

$$\phi_6((r + s\sqrt{6}) - (x + y\sqrt{6})) \geq 1,$$

to jest za svaki $x, y \in \mathbb{Z}$ vrijedi

$$|(r - x)^2 - 6(s - y)^2| \geq 1.$$

Možemo odabrati $\varepsilon_1 = \pm 1$ i $u_1 \in \mathbb{Z}$ takve da

$$0 \leq \varepsilon_1 r + u_1 \leq \frac{1}{2}$$

i $\varepsilon_2 = \pm 1$ i $u_2 \in \mathbb{Z}$ takve da

$$0 \leq \varepsilon_2 r + u_2 \leq \frac{1}{2}.$$

Stavimo

$$r_1 = \varepsilon_1 r + u_1 \in \mathbb{Q}, x_1 = \varepsilon_1 x + u_1 \in \mathbb{Z},$$
$$s_1 = \varepsilon_2 s + u_2 \in \mathbb{Q}, y_1 = \varepsilon_1 y + u_2 \in \mathbb{Z},$$

tako da vrijedi

$$0 \leq r_1 \leq \frac{1}{2}, 0 \leq s_1 \leq \frac{1}{2}, \tag{3.2}$$

i za svaki $x_1, y_1 \in \mathbb{Z}$ vrijedi

$$|(r_1 - x_1)^2 - 6(s_1 - y_1)^2| \geq 1. \tag{3.3}$$

Uzimajući $(x_1, y_1) = (0,0), (1,0)$ i $(-1,0)$ u (3.3), dobivamo sljedeće nejednakosti

$$\begin{cases} |r_1^2 - 6s_1^2| \geq 1, \\ |(1-r_1)^2 - 6s_1^2| \geq 1, \\ |(1+r_1)^2 - 6s_1^2| \geq 1. \end{cases} \tag{3.4}$$

Iz (3.2) dobivamo

$$\begin{cases} -\frac{3}{2} \leq r_1^2 - 6s_1^2 \leq \frac{1}{4}, \\ -\frac{5}{4} \leq (1-r_1)^2 - 6s_1^2 \leq 1, \\ -\frac{1}{2} \leq (1+r_1)^2 - 6s_1^2 \leq \frac{9}{4}. \end{cases} \tag{3.5}$$

Iz (3.4) i (3.5), zaključujemo da vrijedi

$$-\frac{3}{2} \leq r_1^2 - 6s_1^2 \leq -1, \tag{3.6}$$

$$\text{(i) } (1-r_1)^2 - 6s_1^2 \text{ ili (ii) } -\frac{5}{4} \leq (1-r_1)^2 - 6s_1^2 \leq 1, \tag{3.7}$$

$$1 \leq (1+r_1)^2 - 6s_1^2 \leq \frac{9}{4}. \tag{3.8}$$

Iz (3.6) i (3.8) dobivamo

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

pa je $r_1 \geq \frac{1}{2}$. S obzirom da je $r_1 \leq \frac{1}{2}$ (3.2), mora vrijediti $r_1 = \frac{1}{2}$. Tada, iz (3.8) (i) slijedi $\frac{1}{4} - 6s_1^2 = 1$, što je nemoguće. Iz (3.8) (ii) slijedi $\frac{1}{4} - 6s_1^2 \leq -1$, pa je $s_1^2 \geq \frac{5}{24}$. Ali, iz (3.7) 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 $\mathbb{Z}[\sqrt{6}]$ euklidska domena s obzirom na ϕ_6. □

3.3 Prsten $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$

Kao što smo dokazali teorem 3.2.1, na sličan način možemo dokazati sljedeće navedene teoreme.

Teorem 3.3.1. *Neka je m kvadratno slobodan cijeli broj takav da vrijedi $m \equiv 1 \pmod 4$. Tada je prsten $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ 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 vrijedi*

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

Kako smo dokazali teorem 3.2.2, na sličan način u teoremu 3.3.1 možemo odrediti nenegativne kvadratno slobodne cijele brojeve $m \equiv 1 \pmod 4$ za koje je $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ euklidska domena s obzirom na ϕ_m.

Teorem 3.3.2. *Neka je m negativan kvadratno slobodan cijeli broj takav da je $m \equiv 1($ (mod 4)). Tada je prsten $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ euklidska domena s obzirom na ϕ_m ako i samo ako $m = -3, -7, -11$.*

Analogno teoremu 3.2.3 vrijedi za pozitivan m sljedeći teorem.

Teorem 3.3.3. *Neka je m pozitivan kvadratno slobodan cijeli broj takav da je $m \equiv 1($ (mod 4)). Tada je prsten $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ euklidska domena s obzirom na ϕ_m ako i samo ako*

$$m = 5, 13, 17, 21, 29, 33, 37, 41, 73.$$

Poglavlje 4

Primjeri *neeuklidskih* domena

4.1 Legendreov simbol

Legendreov simbol je funkcija koja daje informaciju o tome je li broj kvadratni ostatak modulo nekog neparnog prostog broja. Stoga iskažimo najprije definiciju kvadratnog ostatka.

Definicija 4.1.1. *Neka su p i m relativno prosti cijeli brojevi i $p \geq 1$. Kažemo da je m* ***kvadratni ostatak modulo*** *p ako kongruencija*

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

ima rješenja. Ako ova kongruencija nema rješenja, onda kažemo da m ***kvadratni neostatak modulo*** *p.*

Na primjer, 1, 2 i 4 su kvadratni ostatci modulo 7, a 3, 5 i 6 su kvadratni neostatci modulo 7. Odnosno, općenito cijeli broj m je kvadratni neostatak modulo 7 ako i samo ako je $m \equiv 1, 2$ ili $4 \pmod{7}$.

U želji da dokaže Gaussov kvadratni zakon reciprociteta, francuski matematičar Adrien-Marie Legendre 1798. godine uveo je simbol koji se danas naziva njegovim imenom. Označava se s $\left(\frac{m}{p}\right)$ gdje je m cijeli broj, a p neparni prosti broj p. Legendreov simbol može poprimiti samo tri vrijednosti 1, -1 ili 0 u ovisnosti o tome je li broj m kvadratni ostatak modulo p, kvadratni neostatak modulo p ili ako je m djeljiv s p. Dakle,

$$\left(\frac{m}{p}\right) = \begin{cases} 1, & \text{ako je } m \text{ kvadratni ostatak modulo } p \\ -1, & \text{ako je } m \text{ kvadratni neostatak modulo } p \\ 0, & \text{ako je } m \equiv 0 \pmod{p}. \end{cases} \tag{4.1}$$

Legendreov simbol može se poopćiti za svaki neparan broj m. Tada se definira takozvani Jacobijev simbol

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2}\cdots\left(\frac{a}{p_k}\right)^{\alpha_k},$$

gdje je $m = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$.

Navedimo i neka osnovna svojstva.

Propozicija 4.1.2. *(i) Legendreov simbol je periodičan u gornjem argumentu. Ako je* $m \equiv n \pmod{p}$, *onda je*

$$\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right). \tag{4.2}$$

(ii) Legendreov simbol je multiplikativna funkcija svojeg gornjeg argumenta, odnosno

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right). \tag{4.3}$$

(iii) Ako je $(m, p) = 1$, *onda je* $\left(\frac{m^2}{p}\right) = 1$.

(iv) $\left(\frac{1}{p}\right) = 1, \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

4.2 Prsten $\mathbb{Z}[\sqrt{m}]$

Teorem 4.2.1. *Neka je m pozitivan kvadratno slobodan cijeli broj. Ako postoje različiti neparni brojevi p i q takvi da vrijedi*

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

te pozitivni cijeli brojevi t i u takvi da vrijedi

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

i cijeli broj r takav da

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

tada $\mathbb{Z}[\sqrt{m}]$ *nije euklidska domena s obzirom na* ϕ_m.

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

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

Neka su $x, y \in \mathbb{Z}$ takvi da je $\gamma = x + y\sqrt{m}$. Stoga je

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

to jest

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

Dijeljenjem prethodne relacije s m, dobivamo

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

Budući da je

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

i

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

mora vrijediti

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

Stoga, uz supstituciju $X = x$ i $Y = my - r$, vrijedi

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

Pretpostavimo da je $mX^2 - Y^2 = -pt$. S obzirom da je $\left(\frac{m}{p}\right) = -1$, prema (4.1) slijedi da $p \nmid m$. Također, kako $p \nmid t$, slijedi $p \parallel -pt$[1]. Stoga $p \nmid X$ i $p \nmid Y$ (jer bi u suprotnom p^2 dijelio pt). Prema tome

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

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

Pretpostavimo sada $mX^2 - Y^2 = qu$. Kako je $\left(\frac{m}{q}\right) = -1$,pa prema (4.1) slijedi $q \nmid m$. Također, s obzirom da $q \nmid u$, slijedi $q \parallel qu$. Stoga $q \nmid X$ i $q \nmid Y$.
Prema tome i prema (4.2) te (4.3), vrijedi

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

[1] $p^\alpha \parallel n$ znači da je α najveća potencija broja p koja dijeli n

što je u kontradikciji s $\left(\frac{m}{q}\right) = -1$. To dokazuje da $\mathbb{Z}[\sqrt{m}]$ nije euklidska domena s obzirom na ϕ_m. □

Prethodni teorem koristimo kako bi ustanovili da $\mathbb{Z}[\sqrt{m}]$ nije euklidska domena s obzirom na ϕ_m za neke eksplicitne vrijednosti prirodnog broja m.

Korolar 4.2.2. *$\mathbb{Z}[\sqrt{m}]$ nije euklidska domena s obzirom na ϕ_m 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

□

U sljedećem teoremu pokazujemo da ako je m dovoljno velik, onda $\mathbb{Z}[\sqrt{m}]$ nije euklidska domena nije euklidska domena.

Teorem 4.2.3. *Prsten $\mathbb{Z}[\sqrt{m}]$ nije euklidska domena s obzirom na funkciju ϕ_m u sljedećim slučajevima:*

(i) $m \equiv 2 \pmod 4$ *i* $m \geq 42$,

(ii) $m \equiv 3 \pmod 4$ *i* $m \geq 91$.

Dokaz. (i) Kako je $m \geq 42$, imamo da je $m > 20 + 8\sqrt{6} = 4(\sqrt{3} + \sqrt{2})^2$ tako da $\sqrt{m} > 2(\sqrt{3} + \sqrt{2})$ te na taj način dobivamo

$$\left(\frac{\sqrt{3m}-1}{2}\right) - \left(\frac{\sqrt{2m}-1}{2}\right) = \left(\frac{\sqrt{3}-\sqrt{2}}{2}\right)\sqrt{m}$$
$$> \frac{(\sqrt{3}-\sqrt{2})}{2} 2(\sqrt{3}+\sqrt{2}) = 1.$$

Stoga postoji cijeli broj u koji zadovoljava

$$\frac{\sqrt{2m}-1}{2} < u < \frac{\sqrt{3m}-1}{2}.$$

Postavimo $t = 2u + 1$ tako da je t neparan cijeli broj koji zadovoljava

$$2m < t^2 < 3m.$$

Pretpostavimo sada da je $\mathbb{Z}[\sqrt{m}]$ euklidska domena s obzirom na ϕ_m. Tada postoje $\gamma, \delta \in \mathbb{Z}[\sqrt{m}]$ takvi da vrijedi

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

S obzirom da je $\gamma \in \mathbb{Z}[\sqrt{m}]$ tada postoje $xy, \in \mathbb{Z}$ takvi da vrijedi $\gamma = x + y\sqrt{m}$ te

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

to jest

$$|m^2x^2 - m(t - my)^2| < m^2$$

te vrijedi

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

Stavimo $X = my - t \in \mathbb{Z}$ i $Y = x \in \mathbb{Z}$ tako da vrijedi

$$|X^2 - mY^2| < m$$

i

$$X^2 - mY^2 \equiv X^2 \equiv t^2 \pmod{m}.$$

S obzirom da je $2m < t^2 < 3m$ imamo

$$X^2 - mY^2 = t^2 - 2m$$

ili

$$X^2 - mY^2 = t^2 - 3m.$$

U prvom slučaju, kako je $t^2 \equiv 5 \pmod 8$ (s obzirom da je t neparan) i $m \equiv 2 \pmod 4$, imamo

$$X^2 - mY^2 \equiv 5 \pmod 8.$$

Stoga je X neparan, pa $X^2 \equiv 1 \pmod 8$ i

$$mY^2 \equiv 4 \pmod 8.$$

Ovo je očito nemoguće jer

$$mY^2 \equiv \begin{cases} 0 \pmod 8, \text{ako } Y \equiv 0 \pmod 2 \\ 2 \pmod 4, \text{ako } Y \equiv 1 \pmod 2. \end{cases}$$

U drugom slučaju kako je $t^2 \equiv 1 \pmod 8$, imamo

$$X^2 - mY^2 \equiv 1 - 3m \pmod 8.$$

Kako je m paran broj, možemo zaključiti da je X neparan broj. Stoga $X^2 \equiv 1 \pmod 8$ i

$$m(Y^2 - 3) \equiv 0 \pmod 8.$$

Stoga, kako je $2 \parallel m$, imamo

$$Y^2 \equiv 3 \pmod 4,$$

što je nemoguće.

(ii) Kako je $m \geq 91$, imamo $m > 44 + 3\sqrt{30} = 4(\sqrt{6} + \sqrt{5})^2$ tako da $\sqrt{m} > 2(\sqrt{6} + \sqrt{5})$ te na taj način dobivamo

$$\left(\frac{\sqrt{6m} - 1}{2}\right) - \left(\frac{\sqrt{5m} - 1}{2}\right) = \frac{(\sqrt{6} - \sqrt{5})}{2}\sqrt{m}$$
$$> \frac{(\sqrt{6} - \sqrt{5})}{2} 2(\sqrt{6} + \sqrt{5}) = 1.$$

Stoga postoji cijeli broj u koji zadovoljava

$$\frac{\sqrt{5m} - 1}{2} < u < \frac{\sqrt{6m} - 1}{2}.$$

Postavimo $t = 2u + a$ tako da je t neparan cijeli broj koji zadovoljava

$$5m < t^2 < 6m.$$

Pretpostavimo sada da je $\mathbb{Z}[\sqrt{m}]$ euklidska domena s obzirom na ϕ_m. Tada postoje $\gamma, \delta \in \mathbb{Z}[\sqrt{m}]$ takvi da vrijedi

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

Kako je $\gamma \in \mathbb{Z}[\sqrt{m}]$ tada postoje $x, y \in \mathbb{Z}$ takvi da vrijedi $\gamma = x + y\sqrt{m}$, i

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

to jest

$$|m^2x^2 - m(t - my)^2| < m^2$$

te vrijedi

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

Stavimo $X = my - t \in \mathbb{Z}$ i $Y = x \in \mathbb{Z}$ tako da vrijedi

$$|X^2 - mY^2| < m$$

i

$$X^2 - mY^2 \equiv X^2 \equiv t^2 \pmod{m}.$$

S obzirom da je $5m < t^2 < 6m$ imamo

$$X^2 - mY^2 = t^2 - 5m$$

ili

$$X^2 - mY^2 = t^2 - 6m.$$

U prvom slučaju, kako je $t^2 \equiv 1 \pmod 8$ (s obzirom da je t neparan) i $m \equiv 3 \mod 4$, imamo

$$X^2 - mY^2 = t^2 - 5m \equiv 1 - 15 = -14 \equiv 2 \pmod 8$$

tako da vrijedi

$$X \equiv Y \equiv 1 \pmod 2.$$

Stoga $X^2 \equiv Y^2 \equiv 1 \pmod 8$ tako da vrijedi

$$1 - 5m \equiv t^2 - 5m = X^2 - mY^2 \equiv 1 - m \pmod 8,$$

što daje $4m \equiv 0 \pmod 8$, a to je očito nemoguće.
U drugom slučaju, kako je $t^2 \equiv 1 \pmod 8$ i $m \equiv 3 \pmod 4$ imamo

$$X^2 - mY^2 = t^2 - 6m \equiv 1 - 18 = -7 \equiv 7 \pmod 8.$$

Ako je X neparan, slijedi $X^2 \equiv 1 \pmod 8$ te vrijedi

$$mY^2 \equiv 2 \pmod 8,$$

što je nemoguće. Ako je X paran, onda je $X^2 \equiv 0 \pmod 4$. Tada je $-3Y \equiv 3 \pmod 4$, pa slijedi $Y^2 \equiv 3 \pmod 4$, što je nemoguće.

□

4.3 Prsten $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$

U iskazu sljedećeg teorema oznaka $\lfloor\cdot\rfloor$ označava funkciju najveće cijelo, to jest $\lfloor x\rfloor$, $x \in \mathbb{R}$, je najveći cijeli broj koji je manji ili jednak broju x.

Teorem 4.3.1. *Neka je m pozitivan kvadratno slobodan cijeli broj takav da* $m \equiv 1 \pmod 4$. *Ako postoje različiti neparni brojevi p i q takvi da vrijedi*

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

te neparan cijeli broj r takav da

$$p \parallel (m-1)r^2 - 4m\left\lfloor \frac{(m-1)r^2}{4m} \right\rfloor,$$

$$q \parallel (m-1)r^2 - 4m\left\lfloor \frac{(m-1)r^2}{4m} \right\rfloor - 4m,$$

tada $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ *nije euklidska domena s obzirom na* ϕ_m.

Dokaz. S obzirom da su m i r oba neparna, slijedi $\frac{m-r}{2} \in \mathbb{Z}$. Stoga

$$\frac{m + r\sqrt{m}}{2} = \frac{m-r}{2} + r\left(\frac{m + r\sqrt{m}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right].$$

Pretpostavimo da $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ je euklidska domena s obzirom na ϕ_m. Tada postoje $\gamma, \delta \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ takvi da vrijedi

$$\frac{m + r\sqrt{m}}{2} = m\gamma + \delta,\ \phi_m(\delta) < \phi_m(m).$$

S obzirom da je $\gamma \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$, tada postoje $x, y \in \mathbb{Z}$ takvi da $\gamma = x + y\left(\frac{1+\sqrt{m}}{2}\right)$, pa prema tome vrijedi

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

Stoga

$$\left|\left(\frac{m}{2} - mx - \frac{my}{2}\right)^2 - m\left(\frac{r}{2} - \frac{my}{2}\right)^2\right| < m^2.$$

Množenjem obje strane ove nejednakosti s $\frac{4}{m}$, dobivamo

$$|m(1-2x-y)^2 - (r-my)^2| < 4m.$$

Uz $X = 1 - 2x - y \in \mathbb{Z}$ i $Y = r - my \in \mathbb{Z}$, prethodna nejednakost glasi

$$|mX^2 - Y^2| < 4m.$$

S obzirom da je $m \equiv 1 \pmod 4$, r neparan i $(u+2v)^2 \equiv u^2 \pmod 4$ za svaki $u, v \in \mathbb{Z}$, zaključujemo da vrijedi

$$mX^2 - Y^2 \equiv (1-y)^2 - (1-y)^2 \equiv 0 \pmod 4.$$

Također,

$$mX^2 - Y^2 \equiv -Y^2 \equiv -r^2 \pmod{m}.$$

Označimo s $a = mX^2 - Y^2$. Tada imamo

$$a \equiv 0 \pmod{4},\ a \equiv -r^2 \pmod{m}.$$

Budući da su 4 i m relativno prosti, prema Kineskom teoremu o ostatcima postoji jedinstveno rješenje sustava od te dvije linearne kongruencije modulo $4m$. Uočimo da $(m-1)r^2$ zadovoljava prvu kongruenciju jer 4 dijeli $m-1$. Također, zadovoljava i drugu jer je $(m-1)r^2 \equiv -r^2 \pmod{m}$. Stoga je

$$a \equiv (m-1)r^2 \pmod{4m},$$

odnosno

$$mX^2 - Y^2 \equiv (m-1)r^2 \pmod{4m}.$$

Budući da je $mX^2 - Y^2 \equiv (m-1)r^2 \pmod{4}$ i $|mX^2 - Y^2| < 4m$, slijedi da je $mX^2 - Y^2$ ostatak pri dijeljenju broja $(m-1)r^2$ s brojem $4m$, ali samo u slučaju $mX^2 - Y^2 \geq 0$. Ako je $mX^2 - Y^2 < 0$, onda je ostatak pri dijeljenju broja $(m-1)r^2$ s brojem $4m$ jednak $4m - |mX^2 - Y^2| = 4m + (mX^2 - Y^2)$.
Dakle, za $mX^2 - Y^2 \geq 0$ vrijedi

$$(m-1)r^2 = 4m\left\lfloor \frac{(m-1)r^2}{4m} \right\rfloor + (mX^2 - Y^2),$$

a za $mX^2 - Y^2 < 0$ vrijedi

$$(m-1)r^2 = 4m\left\lfloor \frac{(m-1)r^2}{4m} \right\rfloor + 4m + (mX^2 - Y^2).$$

Prema tome, slijedi

$$mX^2 - Y^2 = (m-1)r^2 - 4m\left\lfloor \frac{(m-1)r^2}{4m} \right\rfloor$$

ili

$$mX^2 - Y^2 = (m-1)r^2 - 4m\left\lfloor \frac{(m-1)r^2}{4m} \right\rfloor - 4m.$$

U prvom slučaju imamo $p \parallel mX^2 - Y^2$. S obzirom da je $\left(\frac{m}{p}\right) = -1$, slijedi $p \nmid m$. Stoga $p \nmid X$ i $p \nmid Y$. No

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

što je u kontradikciji s $\left(\frac{m}{p}\right) = -1$. Drugi slučaj se dokazuje analogno. □

Primjer 4.3.2. $\mathbb{Z}\left[\frac{1+\sqrt{53}}{2}\right]$ *nije euklidska domena s obzirom na* ϕ_{53}.

Rješenje. Uzimamo

$$m = 53, p = 5, q = 19, r = 29.$$

Očito

$$\left(\frac{m}{p}\right) = \left(\frac{53}{5}\right) = \left(\frac{3}{5}\right) = -1,$$

$$\left(\frac{m}{q}\right) = \left(\frac{53}{19}\right) = \left(\frac{-4}{19}\right) = \left(\frac{-1}{19}\right) = -1,$$

$$\begin{aligned}(m-1)r^2 - 4m\left\lfloor\frac{(m-1)r^2}{4m}\right\rfloor &= 52\cdot 29^2 - 4\cdot 53\cdot \lfloor\frac{52\cdot 29^2}{4\cdot 53}\rfloor \\ &= 43732 - 212\cdot 206 \\ &= 43732 - 43672 \\ &= 60 \\ &= 5\cdot 2^2\cdot 3,\end{aligned}$$

i

$$(m-1)r^2 - 4m\left\lfloor\frac{(m-1)r^2}{4m}\right\rfloor - 4m = 60 - 212 = -152 = -19\cdot 2^3.$$

Stoga rezultat slijedi iz teorema 4.3.1. □

Bibliografija

[1] S. Alaca, K. S. Williams, *Introductory Algebraic Number Theory*, Cambridge University Press, 2003.

[2] A. Dujella, *Teorija brojeva*, Školska knjiga, 2019.

[3] Z. Franušić, J. Šiftar, *Linearna algebra*, PMF, Zagreb, 2022., https://web.math.pmf.unizg.hr/~fran/LA-udzbenik.pdf

[4] K. Horvatić, Linearna algebra, PMF, Zagreb, https://www2.irb.hr/korisnici/zskoda/horvaticla.pdf

[5] H. Kraljević, *Algebra*, PMF, Sveučilište Josipa Jurja Strossmayera, Osijek, 2008.,https://web.math.pmf.unizg.hr/~hrk/nastava/2007-08/algebra_Osijek_2007_8.pdf

[6] M. R. Murty, J. Esmonde, *Problems in Algebraic Number Theory*, Springer, 2005.

[7] B. Širola, *Algebarske strukture*, Golden marketing - Tehnička knjiga, Zagreb, 2004.,https://web.math.pmf.unizg.hr/nastava/alg_prof/predavanja/ASpred.pdf

[8] *Legendreov simbol*, https://hr.wikipedia.org/wiki/Legendreov_simbol

Sažetak

Teorem o dijeljenju s ostatkom kaže da za dane cijele brojeve a i $b \neq 0$ postoje jedinstveni cijeli brojevi q i r takvi da je

$$a = bq + r \text{ i } 0 \leq r < |b|.$$

Klasa integralnih domena, to jest komutativnih prstena s jedinicom bez djelitelja nule, koji posjeduju svojstvo analogno teoremu o dijeljenju s ostatkom, nazivaju se *euklidske domene*. Štoviše, euklidske domene dopuštaju oblik Euklidova algoritma za određivanje najvećeg zajedničkog djelitelja.

U ovom diplomskom radu pokazujemo neka svojstva euklidskih domena te primjere primjere iz klase prstena oblika $\mathbb{Z}[\sqrt{m}]$ i $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$.

Summary

The quotient-remainder theorem says that for given integers a and $b \neq 0$, there exist unique integers q and r such that

$$a = bq + r \text{ and } 0 \leq r < |b|.$$

A class of integer domains, i.e. commutative rings with unity that has no zero divisors, that posseses a property analogous to the quotient-remainder theorem are called *Euclidean domains*. Moreover, Euclidean domains admits a form of the Euclidean algorithm for calculating the greatest common divisor.

In this thesis, we show some properties of Euclidean domains and give some examples in the class of rings of the form $\mathbb{Z}[\sqrt{m}]$ and $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$.

Životopis

Rođena sam 23.studenog 1998.godine u Zagrebu. Osnovnoškolsko obrazovanje završavam u Zagrebu, u Osnovnoj školi Vjenceslava Novaka te potom upisujem opći gimnazijski smjer u XII. gimnaziji, u Zagrebu. Godine 2017. upisujem Preddiplomski sveučilišni studij Matematika na Prirodoslovno-matematičkom fakultetu Sveučilišta u Zagrebu; smjer nastavnički. Godine 2022. stječem naziv sveučilišne prvostupnice edukacije matematike te iste godine upisujem Diplomski sveučilišni studij Matematika; smjer nastavnički.