Prsteni cijelih brojeva kvadratnih polja

Kurilovčan, Lucia

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Lucia Kurilovčan

PRSTENI CIJELIH BROJEVA KVADRATNIH POLJA

Diplomski rad

Voditelji rada:
doc. dr. sc. Nikola Adžaga
izv. prof. dr. sc. Zrinka Franušić

Zagreb, 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. _____

Zahvaljujem ocu Željku, majci Tereziji i bratu Stjepanu koji su me neprestano podupirali i bodrili. Juraju i svim svojim prijateljima koji su mi uljepšali razdoblje školovanja i bili tu uz mene dok mi je bilo teško. Zahvaljujem profesorici Zrinki Franušić i profesoru Nikoli Adžagi na vodstvu, pomoći i razumijevanju tijekom pisanja diplomskog 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

U ovom diplomskom radu bavimo se prstenima cijelih brojeva kvadratnih polja. Kvadratno polje je skup oblika

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

uz operacije standardnog zbrajanja i množenja, pri čemu je broj m cijeli broj koji je kvadratno slobodan (što znači da je broj 1 najveći kvadrat koji dijeli broj m). Za $m = -1$, kvadratno polje naziva se polje Gaussovih brojeva. Kvadratna polja su dio veće klase tzv. algebarskih proširenja polja $\mathbb{Q}$ oblika

$$\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \ : \ a_0, a_1, a_{n-1} \in \mathbb{Q}\},$$

pri čemu je α korijen ireducibilnog polinoma nad $\mathbb{Q}$ stupnja n. $\mathbb{Q}(\alpha)$ se može shvatiti kao vektorski prostor nad poljem $\mathbb{Q}$ s bazom $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

Algebarski cijeli broj je korijen normiranog polinoma (tj. polinoma s vodećim koeficijentom 1) s cjelobrojnim koeficijentima. Općenito, skup svih algebarskih cijelih brojeva u $Q(\alpha)$ čini komutativan prsten s jedinicom. U radu je to pokazno za kvadratna polja $\mathbb{Q}(\sqrt{m})$. Konkretno, prsten algebarskih cijelih brojeva u $\mathbb{Q}(\sqrt{m})$ je oblika

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

za $m \equiv 2$ ili $3 \pmod 4$ te

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

za $m \equiv 1 \pmod 4$.

U radu se proučava i problem jedinstvene faktorizacije u prstenima cijelih brojeva kvadratnih polja. Naime, zanima nas vrijedi li u nekim prstenima kvadratnih polja analogon Osnovnog teorema aritmetike koji kaže da je faktorizacija na proste faktore u $\mathbb{N}$ jedinstvena do na poredak faktora. Zbog toga je u prstenu potrebno definirati niz pojmova kao što su djeljivost, ireducibini element, prosti element, asocirani element itd. u prstenu. Ako se u

prstenu svaki element, različit od nule, može izraziti kao produkt ireducibinih elemenata do na poredak faktora i na množenje s jedinicama (tj. invertibilnim elementima) prstena, tada se taj prsten naziva se domena jedinstvene faktorizacije. Dakle, naši "osnovni građevni element" su tzv. ireducibilni elementi (c je ireducibilan ako iz $c = a \cdot b$ slijedi da je ili a ili b jedinica). Problem je u tome što ireducibilni elementi prstena ne moraju biti prosti (p je prost ako iz činjenice da p dijeli $a \cdot b$ slijedi da p dijeli a ili b), a ne mora vrijediti ni obrat. U radu dajemo primjere prstena kvadratnih polja koji jesu domene jedinstvene faktorizacije te oni koji to nisu. Prsten Gaussovih cijelih brojeva i prsten Eisensteinovih cijelih brojeva su domene jedinstvene faktorizacije. Štoviše, to su Euklidove domene, tj. strukture u kojima možemo provesti analogon Euklidova algoritma (odnosno možemo "dijeliti s ostatkom"). Postoje i prsteni nekih kvadratnih polja koji dopuštaju nejedinstvenu faktorizaciju, npr. u prstenu $\mathbb{Z}[\sqrt{-5}]$, broj 6 se može faktorizirati kao $2 \cdot 3$ i kao $(1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$.

Poglavlje 1

Pregled osnovnih algebarskih struktura

U prvom poglavlju bavit ćemo se osnovnim algebarskim strukturama poput grupa, prstena, polja i ideala. Za početak definirajmo što je to binarna operacija.

Definicija 1.1. *Neka je S neki neprazan skup.* ***Binarna operacija*** *na skupu S je preslikavanje oblika*

$$* : S \times S \to S.$$

Svakom uređenom paru $(a, b) \in S \times S$ binarna operacija $*$ pridružuje element $c = a * b \in S$.

1.1 Grupa

Definicija 1.2. *Neka je G neprazan skup i $*$ operacija na Kartezijevom produktu $G \times G$. Uređeni par $(G, *)$ naziva se* ***grupa*** *ukoliko vrijede sljedeća svojstva:*

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

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

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

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

Napomena 1.3.

- *Uvjet (i), tj. zatvorenost operacije na $G \times G$ ekvivalentna je tome da zahtijevamo da operacija $*$ bude binarna.*
- *Ako postoji neutralni element e dane operacije, on je jedinstven. Nadalje, neutralni element e se u aditivnim strukturama naziva nula, a u multiplikativnim jedinica.*

- *Ako postoji inverz nekog elementa x iz dane strukture, on je jedinstven pa ga obično označavamo s x^{-1}. U aditivnim strukturama, obično govorimo o suprotnom elementu kojeg označavamo s $-x$.*
- *Često samo kratko kažemo da je G grupa, ako je iz konteksta jasno s obzirom na koju binarnu operaciju skup G ima navedenu strukturu.*

Definicija 1.4. *Neka je $(G, *)$ grupa. Ako vrijedi svojstvo komutativnosti, tj. ako je*

$$x * y = y * x, \quad \forall\, x, y \in G,$$

*tada se $(G, *)$ naziva **komutativna** ili **Abelova grupa**.*

Definicija 1.5. *Neka je $(G, *)$ grupa, a skup H podskup grupe G. Ako je $(H, *)$ grupa, kažemo da je H **podgrupa** od G te pišemo $H \leq G$.*

Lako se pokazuje da je podskup H grupe G podgrupa od G ako i samo ako vrijede svojstva

(i) $x \cdot y \in H$ za sve $x, y \in H$

(ii) $x^{-1} \in H$ za svaki $x \in H$.

Definicija 1.6. *Neka je N podgrupa grupe G, tj. $N \leq G$. Ako vrijedi*

$$aNa^{-1} = N,$$

*za sve $a \in G$, tada kažemo da je N **normalna podgrupa** u G i označavamo s $N \trianglelefteq G$.*

1.2 Prsten

Definicija 1.7. *Neka je R neprazan skup i neka su $+$ i $\cdot$ dvije binarne operacije na skupu R. Uređenu trojku $(R, +, \cdot)$ nazivamo **prsten** ako vrijede sljedeća svojstva:*

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

(ii) u strukuri $(R, \cdot)$ *vrijede svojstva zatvorenosti i asocijativnosti, tj.* $(R, \cdot)$ *je polugrupa,*

(iii) operacija $\cdot$ je distributivna s obzirom na operaciju $+$, odnosno za sve $x, y, z \in R$ vrijede relacije

$$x \cdot (y + z) = x \cdot y + x \cdot z,$$

$$(x + y) \cdot z = x \cdot z + y \cdot z.$$

Prema napomeni 1.3, u prstenu $(R, +, \cdot)$ neutralni element Abelove grupe $(R, +)$ naziva se *nula* (i označava s 0), a neutralni element iz polugrupe $(R, \cdot)$, ako postoji, *jedinica* (i označava s 1).

Definicija 1.8. *Neka je $(R, +, \cdot)$ prsten. Ako u $(R, \cdot)$ postoji neutralni element, tj. jedinica množenja, tada $(R, +, \cdot)$ nazivamo* ***prsten s jedinicom****.*

Definicija 1.9. *Prsten $(R, +, \cdot)$ naziva se* ***komutativan prsten*** *ako je operacija $\cdot$ komutativna.*

Definicija 1.10. *Neka je $(R, +, \cdot)$ prsten, a S podskup prstena R. Ako je $(S, +, \cdot)$ prsten, kažemo da je S* ***potprsten*** *od R te analogno kao i kod podgrupe pišemo $S \leq R$.*

Podskup S prstena R je potprsten od R ako i samo ako vrijede sljedeća svojstva:

(i) $x - y \in S$ za sve $x, y \in S$,

(ii) $x \cdot y \in S$ za sve $x, y \in S$.

Definicija 1.11. *Neka je R prsten te neka su $a, b \in R$ takvi da vrijedi $a \neq 0$ i $b \neq 0$. Ako vrijedi $a \cdot b = 0$, onda se a i b nazivaju* ***djelitelji nule*** *prstena R.*

Definicija 1.12. *Ako je R komutativni prsten s jedinicom koji nema djelitelja nule, onda prsten R zovemo* ***integralna domena****.*

Dakle, komutativni prsten s jedinicom R je integralna domena ako za sve $x, y \in R$ vrijedi:

$$x \cdot y = 0 \;\Rightarrow\; x = 0 \text{ ili } y = 0.$$

Primjer 1.13. *Prsteni $\mathbb{Z}$ i $\mathbb{Z}/3\mathbb{Z}$ su integralne domene, ali prsten $\mathbb{Z}/6\mathbb{Z}$ nije integralna domena jer u prstenu $\mathbb{Z}/6\mathbb{Z}$ vrijedi $2 \cdot 3 = 0$, tj. postoje djelitelji nule.*

Definicija 1.14. *Neka je R prsten s jedinicom 1. Element $a \in R$ je* ***invertibilan*** *ako postoji neki $a' \in R$ takav da vrijedi*

$$aa' = a'a = 1.$$

Invertibilni element prstena se često naziva *jedinica*, što ne treba brkati s jedinicom – neutralnim elementom množenja. Jasno je da je neutralni element uvijek i invertibilan, ali obrat ne mora vrijediti. Skup svih jedinica (tj. invertibilnih elemenata) nekog prstena čini grupu.

1.3 Polje

Definicija 1.15. *Ako je $(R, +, \cdot)$ komutativni prsten s jedinicom kojem je svaki element $x \in R\backslash\{0\}$ invertibilan, tada se R naziva **polje**. Česta oznaka za polje jest $\mathbb{F}$.*

Može se reći da je $(\mathbb{F}, +, \cdot)$ polje ako vrijede sljedeća svojstva:

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

(ii) $(\mathbb{F}\backslash\{0\}, \cdot)$ je Abelova grupa,

(iii) operacija $\cdot$ je distributivna s obzirom na operaciju $+$, tj. vrijedi da za sve $x, y, z \in \mathbb{F}$,

$$x \cdot (y + z) = x \cdot y + x \cdot z,$$

$$(x + y) \cdot z = x \cdot z + y \cdot z.$$

Definicija 1.16. *Neka su $\mathbb{F}$ i $\mathbb{K}$ polja. Ako je $\mathbb{K}$ podkup od $\mathbb{F}$, onda kažemo da je $\mathbb{K}$ **potpolje** od $\mathbb{F}$, tj. $\mathbb{F}$ je **proširenje polja** $\mathbb{K}$. To označavamo s $\mathbb{F} \mid \mathbb{K}$.*

1.4 Ideal

Definicija 1.17. *Neka je R prsten. Skup I koji je podskup od R naziva se **lijevi** (odnosno **desni**) **ideal** u R ako vrijede sljedeća dva svojstva:*

(i) I je potprsten od R, tj. $I \leq R$,

(ii) $r \cdot x \in I$ (odnosno $x \cdot r \in I$) za sve $r \in R$ i $x \in I$

*I je (dvostrani) **ideal** u prstenu R ako je istovremeno i lijevi i desni ideal što se označava s $I \trianglelefteq R$.*

U slučaju komutativnog prstena, očito je da se definicije jednostranog (lijevog i desnog) i dvostranog ideala podudaraju.

Definicija 1.18. *Ideal $P \trianglelefteq R$ je **prost ideal** ako vrijede sljedeća svojstva:*
(i) $P \neq R$
(ii) $a \cdot b \in P \Rightarrow a \in P$ ili $b \in P$.

Primjer 1.19. *Skup svih parnih brojeva u prstenu $\mathbb{Z}$, odnosno $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ je ideal u $\mathbb{Z}$ jer je svaki cijeli broj pomnožen parnim brojem paran broj. U biti, ideali su upravo generalizacija podskupa parnih cijelih brojeva (ili općenito podskupa višekratnika nekog broja) u prstenu $\mathbb{Z}$.*

1.5 Vektorski prostor

Definicija 1.20. *Neka je V neprazan skup na kojem su zadane binarna operacija zbrajanja $+ : V \times V \to V$ i operacija množenje skalarima iz polja $\mathbb{F}$, $\cdot : \mathbb{F} \times V \to V$. Kažemo da je uređena trojka $(V, +, \cdot)$* ***vektorski prostor nad poljem*** *$\mathbb{F}$ ako vrijedi:*

(i) $(V, +)$ *je Abelova grupa,*

(ii) kvaziasocijativnost: za sve $\alpha, \beta \in \mathbb{F}, a \in V$ vrijedi

$$\alpha \cdot (\beta \cdot a) = (\alpha\beta) \cdot a,$$

(iii) distributivnost operacije $\cdot$ u odnosu na zbrajanje u $\mathbb{F}$: za sve $\alpha, \beta \in \mathbb{F}, a \in V$ vrijedi

$$(\alpha + \beta) \cdot a = \alpha \cdot a + \beta \cdot a,$$

(iv) distributivnost operacije $\cdot$ u odnosu na zbrajanje u V: za sve $\alpha \in \mathbb{F}, a, b \in V$ vrijedi

$$\alpha \cdot (a + b) = \alpha \cdot a + \alpha \cdot b,$$

(v) $1 \cdot a = a$, *za svaki $a \in V$.*

Kažemo da su elementi iz skupa V **vektori**, a elementi polja $\mathbb{F}$ **skalari**. Neutralni element, tj. nulu za zbrajanje u skupu V nazivamo **nulvektor**. Nulvektor označavamo oznakom 0_V. Ukoliko je naše polje $\mathbb{F}$ jednako polju realnih brojeva, tada V nazivamo realni vektorski prostor, dok polje kompleksnih brojeva, nazivamo V kompleksni vektorski prostor.

Definicija 1.21. *Neka je skup S podskup vektorskog prostora V nad poljem $\mathbb{F}$. Skup S je* ***sustav izvodnica*** *ili* ***generatora*** *za vektorski prostor V ako se svaki vektor iz V može zapisati kao linearna kombinacija konačno mnogo elemenata iz S, tj. ako je $V = [S]$ pri čemu $[S]$ označava linearnu ljusku skupa S. Kažemo da S* ***razapinje*** *ili* ***generira*** *V.*

Definicija 1.22. *Neka je skup $S = \{s_i, \ldots, s_k\}$ konačan podskup vektorskog prostora V nad poljem $\mathbb{F}$. Ako se nulvektor može na jedinstven način prikazati kao linearna kombinacija vektora iz skupa S, tada kažemo da je skup S* ***linearno nezavisan****. To upravo znači da jednadžba*

$$\alpha_1 s_1 + \alpha_2 s_2 + \cdots + \alpha_k s_k = 0_V \tag{1.1}$$

implicira $\alpha_1 = \cdots = \alpha_k = 0$. Ako postoji bar jedan skalar $\alpha_i \neq 0$ za koji vrijedi jednadžba (1.1), tada je skup S ***linearno zavisan****.*

Definicija 1.23. *Ako je A podskup vektorskog prostora V koji je sustav izvodnica za V i linearno nezavisan skup u V, tada skup A nazivamo* ***bazom*** *vektorskog prostora V.*

Poglavlje 2

Kvadratna polja

2.1 Definicija i osnovna svojstva

Definicija 2.1. *Kompleksni broj $\alpha \in \mathbb{C}$ je **algebarski broj** ako postoji nenul polinom f s racionalnim koeficijentima, takav da je $f(\alpha) = 0$, tj. ako je α nultočka tog polinoma. Kompleksni broj zove se **transcendentan** ako nije algebarski.*

Primjer 2.2. *Broj $\alpha = \frac{1}{2}$ je algebarski broj jer je nultočka polinoma $f(x) = 2x-1$. Eulerov broj e je transcendentan jer ne postoji polinom s racionalnim koeficijentima kojemu je e nultočka.*

Definicija 2.3. *Kompleksni broj α je **algebarski cijeli broj** ako postoji polinom $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, takozvani normirani polinom s cjelobrojnim koeficijentima, takav da je $f(\alpha) = 0$.*

Primjer 2.4. *Broj $\alpha = \sqrt{2}$ je algebarski cijeli broj jer je nultočka polinoma $f(x) = x^2 - 2$. Broj $i = \sqrt{-1}$ je također algebarski cijeli broj jer je nultočka polinoma $f(x) = x^2 + 1$.*

Uočimo da je broj $\sqrt{m}$, takav da je $m \in \mathbb{Z}$, općenito algebarski cijeli broj jer postoji polinom oblika $f(x) = x^2 - m$.

Primjer 2.5. *Broj $\alpha = \sqrt[n]{2}$ je algebarski cijeli broj jer je nultočka polinoma $f(x) = x^n - 2$.*

Neka je $m \in \mathbb{Z}$ *kvadratno slobodan broj*. To znači da je broj 1 najveći kvadrat koji dijeli broj m. Definiramo skup

$$\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}. \tag{2.1}$$

Uočimo da, ako ne bismo pretpostavili da je m kvadratno slobodan, tj. ako je $m = m'\ell^2$ za $m', \ell \in \mathbb{Z}$, onda bi vrijedilo $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{m'})$. Na primjer, $\mathbb{Q}(\sqrt{12}) = \mathbb{Q}(\sqrt{3})$. Također, ako je m potpuni kvadrat, $m = \ell^2$ za $\ell \in \mathbb{Z}$, onda je $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}$.

Teorem 2.6. *Skup* $\mathbb{Q}(\sqrt{m})$*,* $m \in \mathbb{Z}\backslash\{0\}$*, definiran s* (2.1) *je polje uz standarne operacije zbrajanja i množenja, odnosno potpolje polja kompleksnih brojeva.*

Dokaz. Najprije pokažimo da je $(\mathbb{Q}(\sqrt{m}), +)$ podgrupa od $(\mathbb{C}, +)$. Za to je dovoljno pokazati da je zbroj dva elementa iz $\mathbb{Q}(\sqrt{m})$ ponovo iz $\mathbb{Q}(\sqrt{m})$ te da svaki element iz $\mathbb{Q}(\sqrt{m})$ ima suprotni element u $\mathbb{Q}(\sqrt{m})$. Zaista, za $a + b\sqrt{m}, c + d\sqrt{m}, a, b, c, d \in \mathbb{Q}$ je

$$(a + b\sqrt{m}) + (c + d\sqrt{m}) = (a + c) + (b + d)\sqrt{m} \in \mathbb{Q}(\sqrt{m})$$

te očito $-(a + b\sqrt{m}) = -a - b\sqrt{m} \in \mathbb{Q}(\sqrt{m})$.

Sada pokažimo da je $(\mathbb{Q}(\sqrt{m})^*, \cdot)$ podgrupa od $(\mathbb{C}^*, \cdot)$ pri čemu smo s $(\mathbb{Q}(\sqrt{m})^*$ i $\mathbb{C}^*$ označili skupove ($\mathbb{Q}(\sqrt{m})$ i $\mathbb{C}$ bez nule - neutralnog elementa zbrajanja. Za $a + b\sqrt{m}, c + d\sqrt{m} \in \mathbb{Q}(\sqrt{m})^*$ je

$$\underbrace{(a + b\sqrt{m})}_{\neq 0} \cdot \underbrace{(c + d\sqrt{m})}_{\neq 0} = \underbrace{(ac + bdm)}_{\in\mathbb{Q}} + \underbrace{(ad + bc)}_{\in\mathbb{Q}}\sqrt{m} \neq 0,$$

što znači da je umnožak dva broja iz $\mathbb{Q}(\sqrt{m})^*$ element iz $\mathbb{Q}(\sqrt{m})^*$. Nadalje, inverz

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

je očito element iz $\mathbb{Q}(\sqrt{m})^*$. □

Zahvaljujući teoremu 2.6, skupove $\mathbb{Q}(\sqrt{m})$ nazivamo **kvadratnim poljima**. Za $m > 0$, govorimo o *realnom kvadratnom polju*, a za $m < 0$ o *imaginarnom kvadratnom polju*. Ako je $m = -1$, tada se $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$ naziva *polje Gaussovih brojeva*.

Teorem 2.7. *Neka je m cijeli broj koji nije potpun kvadrat. Skup* $\mathbb{Q}(\sqrt{m})$ *čini vektorski prostor nad poljem racionalnih brojeva dimenzije* 2*.*

Dokaz. U teoremu 2.6 smo pokazali da je $(\mathbb{Q}(\sqrt{m}), +)$ Abelova grupa. Lako se vidi da vrijede i preostala svojstva zbrajanja i množenja skalarom - racionalnim brojem. Stoga je $\mathbb{Q}(\sqrt{m})$ vektorski prostor nad poljem $\mathbb{Q}$.

Uočimo da skup $\{1, \sqrt{m}\}$ čini bazu za vektorski prostor $\mathbb{Q}(\sqrt{m})$. Direktno iz definicije samog prostora $\mathbb{Q}(\sqrt{m})$, jasno je da je skup $\{1, \sqrt{m}\}$ sustav izvodnica. Nadalje, $\{1, \sqrt{m}\}$ je linearno nezavisan skup jer je $a + b\sqrt{m} \neq 0$ za sve $a, b \in \mathbb{Q}$ i $a^2 + b^2 > 0$. Dakle, $\dim \mathbb{Q}(\sqrt{m})_{\mathbb{Q}} = 2$. □

Dimenzija vektorskog prostora $\mathbb{Q}(\sqrt{m})$ nad $\mathbb{Q}$ se još naziva **stupanj algebarskog proširenja** i zapisuje kao

$$[\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = \dim \mathbb{Q}(\sqrt{m})_{\mathbb{Q}} = 2,$$

uz uvjet da m nije potpuni kvadrat. Još se kaže da je $\mathbb{Q}(\sqrt{m})$ *polje proširenja* polja $\mathbb{Q}$, odnosno da je $\mathbb{Q}$ potpolje od $\mathbb{Q}(\sqrt{m})$. Općenito, svako polje proširenja K polja racionalnih brojeva $\mathbb{Q}$, čiji je stupanj proširenja konačan, odnosno, K shvaćen kao vektorski prostor nad $\mathbb{Q}$ je konačnodimenzionalan, naziva se **polje algebarskih brojeva** ili kraće **polje brojeva**. Dakle, kvadratno polje je primjer jednog polja algebarskih brojeva.

2.2 Prsten cijelih brojeva u kvadratnom polju

Neka je K polje algebarskih brojeva. Skup svih algebarskih cijelih brojeva standarno se označava s O_K. Općenito se može pokazati da O_K ima strukturu prstena pa ga se često naziva **prsten cijelih brojeva** polja K. No, mi ćemo opisati kako izgledaju algebarski cijeli brojevi u kvadratnom polju $\mathbb{Q}(\sqrt{m})$ te ustanoviti da je O_K prsten za $K = \mathbb{Q}(\sqrt{m})$.

Teorem 2.8. *Neka je $K = \mathbb{Q}(\sqrt{m})$ pri čemu je m kvadratno slobodan cijeli broj. Tada je skup svih algebarskih cijelih brojeva O_K u kvadratnom polju K oblika*

$$O_K = \begin{cases} \{a + b\sqrt{m} \ : \ a, b \in \mathbb{Z}\}, & m \equiv 2 \text{ ili } 3 \pmod 4 \\ \left\{ \dfrac{a + b\sqrt{m}}{2} \ : \ a, b \in \mathbb{Z},\ a \equiv b \pmod 2 \right\}, & m \equiv 1 \pmod 4 \end{cases}$$

gdje $a \equiv b \pmod 2$ znači da a i b moraju biti iste parnosti.

Dokaz. Neka je $\alpha = a + b\sqrt{m}$, $a, b \in \mathbb{Q}$. Prebacimo a na lijevu stranu jednakosti te kvadrirajući jednadžbu dobivamo

$$\alpha^2 - 2a\alpha + a^2 = mb^2,$$

odnosno

$$\alpha^2 - 2a\alpha + a^2 - mb^2 = 0.$$

Stoga je $\alpha = a + b\sqrt{m}$ nultočka normiranog polinoma

$$p(x) = x^2 - 2ax + a^2 - mb^2.$$

Prema definiciji 2.3 možemo zaključiti da je $\alpha = a + b\sqrt{m}$ ako i samo ako polinom p ima cjelobrojne koleficijente, odnosno ako i samo ako su $2a$ i $a^2 - mb^2$ cijeli brojevi. Očito je da za sve $a, b \in \mathbb{Z}$ vrijedi da su $2a$ i $a^2 - mb^2$ cijeli brojevi što znači da je $\alpha = a + b\sqrt{m}$ algebarski cijeli broj u svakom kvadratnom polju $\mathbb{Q}(\sqrt{m})$. Ispitajmo ima li još nekih oblika broja α koji su algebarski cijeli brojevi. S obzirom da je $2a \in \mathbb{Z}$, ako je $a = \dfrac{a'}{2}$ i $a' \in \mathbb{Z}$ neparan ili ako je $a \in \mathbb{Z}$, dokaz granamo na dva slučaja.

1. slučaj: Neka je $a = \frac{a'}{2}$ takav da je a' neparan cijeli broj. Tada je $2a$ neparan, odnosno $2a = 2k + 1$ za neki $k \in \mathbb{Z}$, što još možemo zapisati kao

$$2a \equiv 1 \pmod 2.$$

Kvadrat neparnog broja daje ostatak 1 pri dijeljenju s 4, odnosno

$$(2a)^2 \equiv 1 \pmod 4. \tag{2.2}$$

U tom slučaju je

$$a^2 - mb^2 = \frac{a'^2}{4} - mb^2 = \frac{1}{4} \cdot \left(a'^2 - 4mb^2\right) = \frac{1}{4} \cdot \left((2a)^2 - m(2b)^2\right).$$

Stoga je $\frac{1}{4}\left((2a)^2 - m(2b)^2\right)$ cijeli broj ako i samo ako je $\left((2a)^2 - m(2b)^2\right)$ djeljivo s 4, tj.

$$(2a)^2 - m(2b)^2 \equiv 0 \pmod 4.$$

Nadalje, zbog (3.2) dobivamo

$$m(2b)^2 \equiv 1 \pmod 4. \tag{2.3}$$

Kako je m kvadratno slobodan cijeli broj, $(2b)^2$ mora biti cijeli broj, pa je stoga i $2b \in \mathbb{Z}$. Kvadrat cijelog broja pri dijeljenju s 4 može dati samo ostatke 0 ili 1. Stoga, zaključujemo da relacija (2.3) vrijedi samo za

$$m \equiv 1 \pmod 4,\ (2b)^2 \equiv 1 \pmod 4.$$

Konačno, $(2b)^2 \equiv 1 \pmod 4$ ako i samo ako je $2b \equiv 1 \pmod 2$, odnosno ako i samo ako je $b = \frac{b'}{2}$ i b' neparan broj.

Dakle, ako je $m \equiv 1 \pmod 4$, brojevi oblika

$$\frac{a'}{2} + \frac{b'}{2}\sqrt{m},\ a' \equiv b' \equiv 1 \pmod 2$$

su algebarski cijeli brojevi. Kako smo već ustanovili da su u svakom polju $\mathbb{Q}(\sqrt{m})$ brojevi oblika $a + b\sqrt{m} = \frac{2a}{2} + \frac{2b}{2}\sqrt{m}$, $a, b \in \mathbb{Z}$ algebarski cijeli, konačno možemo zaključiti da je svaki broj oblika

$$\frac{a}{2} + \frac{b}{2}\sqrt{m},$$

gdje su a i b cijeli brojevi iste parnosti (tj. $a \equiv b \pmod 2$), algebarski cijeli broj u polju $\mathbb{Q}(\sqrt{m})$ uz uvjet $m \equiv 1 \pmod 4$.

2. slučaj: Neka je $a \in \mathbb{Z}$. Tada je i $a^2 \in \mathbb{Z}$. Iz $a^2 - mb^2 \in \mathbb{Z}$ zaključujemo da je onda i $mb^2 \in \mathbb{Z}$. S obzirom na to da je m kvadratno slobodan, slijedi da je $b^2 \in \mathbb{Z}$ te $b \in \mathbb{Z}$.

Na temelju slučajeva 1 i 2, zaključujemo da je za $m \equiv 2, 3 \pmod 4$ broj $a + b\sqrt{m}$ algebarski cijeli u $\mathbb{Q}(\sqrt{m})$ ako i samo ako su a i b cijeli brojevi te da je $m \equiv 1 \pmod 4$ broj $a + b\sqrt{m}$ algebarski cijeli u $\mathbb{Q}(\sqrt{m})$ ako i samo ako su $a, b \in \mathbb{Q}$ i $2a \equiv 2b \pmod 2$ (tj. ako i samo ako su a i b razlomci s nazivnikom dva, a njihovi brojnici su brojevi iste parnosti). □

Napomenimo da se u slučaju $m \equiv 2, 3 \pmod 4$ skup cijelih brojeva u $K = \mathbb{Q}(\sqrt{m})$ zapisuje kao

$$O_K = \mathbb{Z}[\sqrt{m}],$$

a u slučaju $m \equiv 1 \pmod 4$ kao

$$O_K = \mathbb{Z}\left[\frac{1 + \sqrt{m}}{2}\right].$$

Ako je $\alpha \in \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$, onda je

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

za neke $a, b \in \mathbb{Z}$. Iz

$$\alpha = \frac{2a + b}{2} + \frac{b}{2}\sqrt{m},$$

zaključujemo da su brojnici razlomaka iz prethodnog izraza iste parnosti. Dakle, ako je $\alpha \in \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$, onda je $\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{m}$, gdje su a i b iste parnosti.

Pokažimo sada i obrat, tj. ako je $\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{m}$, za $a, b \in \mathbb{Z}$ iste parnosti, onda je $\alpha \in \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$. Dodajmo i oduzmimo broj $\frac{b}{2}$:

$$z = \frac{a}{2} + \frac{b}{2}\sqrt{m} = \frac{a}{2} + \frac{b}{2}\sqrt{m} \pm \frac{b}{2} = \frac{a - b}{2} + b\left(\frac{1 + \sqrt{m}}{2}\right).$$

Kako je $a - b$ uvijek paran broj, jer su a i b iste parnosti, broj $\frac{a-b}{2}$ je cijeli. Stoga je $z \in \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$.

Teorem 2.9. *Skup algebarskih brojeva nekog kvadratnog polja čini komutativan prsten s jedinicom.*

Dokaz. Dovoljno je provjeriti zatvorenost na zbrajanje i množenje elemenata iz $\mathbb{Z}[\sqrt{m}]$ i $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$. Neka su $a + b\sqrt{m}, c + d\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$. Tada je

$$(a + b\sqrt{m}) + (c + d\sqrt{m}) = \underbrace{(a + c)}_{\in\mathbb{Z}} + \underbrace{(b + d)}_{\in\mathbb{Z}}\sqrt{m} \in \mathbb{Z}[\sqrt{m}],$$

$$(a + b\sqrt{m})(c + d\sqrt{m}) = (\underbrace{ac + bdm}_{\in\mathbb{Z}}) + (\underbrace{ad + bc}_{\in\mathbb{Z}})\sqrt{m} \in \mathbb{Z}[\sqrt{m}].$$

Za $a + b\frac{1+\sqrt{m}}{2}, c + d\frac{1+\sqrt{m}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ je

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

$$\left(a + b\frac{1+\sqrt{m}}{2}\right)\left(c + d\frac{1+\sqrt{m}}{2}\right) = \underbrace{(ac + bd\frac{m-1}{4})}_{\in\mathbb{Z}} + (\underbrace{bc + ad + bd}_{\in\mathbb{Z}})\frac{1+\sqrt{m}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right],$$

jer je $m \equiv 1 \pmod 4$. □

Poglavlje 3

Faktorizacija u prstenima cijelih brojeva nekih kvadratnih polja

3.1 Faktorizacija u $\mathbb{Z}$

Prsten cijelih brojeva $\mathbb{Z}$ ima lijepo svojstvo faktorizacije na proste faktore. Ono se sastoji u tome da se svaki (složeni) cijeli broj, različit od nule, može "razložiti" na "nerastavljive" dijelove - proste brojeve. O važnosti ovog svojstva najviše govori naziv tvrdnje na kojoj se temelji - *Osnovni teorem aritmetike*.

Teorem 3.1 (Osnovni teorem aritmetike)**.** *Svaki prirodni broj $n > 1$ faktorizira se jedinstveno do na poredak faktora kao*

$$n = p_1^{e_1} \cdots p_k^{e_k},$$

gdje su p_i različiti prosti brojevi, a e_i prirodni brojevi.

Dokaz. Prvo ćemo pomoću matematičke indukcije dokazati da se svaki prirodan broj $n > 1$ može prikazati u obliku umnoška prostih faktora. Za prirodan broj 2 znamo da je prost, pa se njegov rastav sastoji od njega samoga. Pretpostavimo da tvrdnja vrijedi za prirodne brojeve koji su manji od nekog prirodnog broja n. Ako je broj n prost, tada za njega vrijedi tvrdnja. Ako je n složen, onda se može faktorizirati na neka dva manja broja $n = n_1 \cdot n_2$. S obzirom na to da su brojevi n_1 i n_2 manji od n, prema pretpostavci indukcije možemo zaključiti da se n_1 i n_2 mogu faktorizirati na proste faktore, pa se množenjem tih faktora i sam broj n može faktorizirati na proste faktore.

Dokažimo sada jedinstvenost te faktorizacije. Pretpostavimo suprotno, tj. da postoji neki broj n koji ima barem dvije različite faktorizacije koje možemo izjednačiti. Nakon izjednačavanja tih dviju različitih faktorizacija i dijeljenja, tj. kraćenja s prostim brojevima koji se nalaze u obje faktorizacije, dobivamo jednakost

$$p_1 \cdot p_2 \cdots p_k = r_1 \cdot r_2 \cdots r_m$$

gdje su p_i i r_j različiti prosti brojevi za sve i i j. Stoga mora vrijediti da p_1 dijeli barem jedan od prostih faktora $r_1, r_2, \ldots, r_m$. Neka p_1 dijeli r_j. S obzirom na to da je r_j prost i broj $p_1 \neq 1$, vrijedi $p_1 = r_j$, što je kontradikcija i time smo dokazali jedinstvenost faktorizacije broja n. □

Svaki cijeli broj n, $n \neq 0, -1, 1$, se stoga jedinstveno (do na poredak faktora) prikazuje kao

$$n = \pm p_1^{e_1} \cdots p_k^{e_k},$$

pri čemu su $p_i, e_i \in \mathbb{N}$ i p_i su prosti. Ponekad se dopušta da su eksponenti $e_i \geq 0$. U tom slučaju u gornji prikaz možemo uključiti i brojeve 1 i -1. Uočimo da u navedenoj faktorizaciji nismo morali koristiti predznak $\pm$ ako dopustimo i negativne proste brojeve. Naime, cijeli broj je prost ako je jedino djeljiv s jedinicama iz prstena (1 i -1), sam sa sobom i asociranim brojem (koji je dobiven množenjem s jedinicama). Stoga u $\mathbb{Z}$ imamo p i $-p$, dvije "kopije" za svaki prost broj. Oni se ponašaju potpuno jednako u faktorizaciji i stoga nema razloga preferirati jednog u odnosu na drugog.

Nadalje, ovakva faktorizacija se zapravo jednostavno proširuje na polje $\mathbb{Q}$: bilo koji racionalni broj $\frac{m}{n} \in \mathbb{Q}$, različit od nule, može se jedinstveno zapisati kao umnožak

$$\frac{m}{n} = \pm p_1^{e_1} \cdots p_k^{e_k},$$

gdje je sada dopušteno da e_i budu i negativni cijeli brojevi. Naravno, p_i nisu zaista prosti u $\mathbb{Q}$, ali sve dok pamtimo da oni dolaze iz $\mathbb{Z}$, možemo ih smatrati "osnovnim građevnim elementima" u faktorizaciji racionalnog broja.

3.2 Pojam djeljivosti u prstenu. Domene jedinstvene faktorizacije

Budući da želimo istražiti imaju li prsteni cijelih brojeva kvadratnih polja slično svojstvo faktorizacije kao u prstenu $\mathbb{Z}$, trebamo najprije u prstenima definirati pojmove kao što su djeljivost, ireducibilnost, prost broj, itd. U sljedećim definicijama pretpostavimo da je R komutativni prsten s jedinicom 1.

Definicija 3.2. *Neka su $a, b \in R$. Kažemo da a **dijeli** b i pišemo $a \mid b$ ako postoji element $c \in R$ takav da je $b = ac$.*

Djelitelji neutralnog elementa prstena R, tj. od 1*, nazivaju se **jedinice**.*

Skup svih jedinica u nekom prstenu cijelih brojeva jednak je skupu svih invertibilnih elemenata u tom prstenu. U $\mathbb{Z}$ je skup jedinica jednak $\{-1, 1\}$, a u $\mathbb{Z}[i]$ je $\{-1, 1, -i, i\}$ (v. propoziciju 3.16).

Definicija 3.3. *Elementi $a, b \in R$ su **asocirani** ako je $a = ub$, gdje je u jedinica iz prstena.*

Direktno iz definicije 3.3 slijedi sljedeća propozicija.

Propozicija 3.4. *Neka su $a, b, c \in R$ te neka su a i b asocirani. Vrijedi:*

1. *c dijeli a ako i samo ako c dijeli b.*
2. *a dijeli c ako i samo ako b dijeli c.*

Definicija 3.5. *Neka je $p \in R$ različit od nule i nije invertibilan (tj. nije jedinica).*

1. *Kažemo da je p **prost element** ako ima svojstvo da ako broj p dijeli $a \cdot b$, $a, b \in R$, tada on dijeli a ili dijeli b.*
2. *Kažemo da je p **ireducibilan** ako iz $p = a \cdot b$, $a, b \in R$, slijedi da je ili a ili b jedinica. p se naziva **reducibilnim** ako p nije ireducibilan.*

U prstenu $\mathbb{Z}$, skup prostih brojeva jednak je skupu ireducibilnih, no općenito prost element nekog prstena ne mora biti ireducibilan niti ireducibilan mora biti prost. To možemo vidjeti iz sljedećih primjera.

Primjer 3.6. *Broj $2 + \sqrt{-5}$ je ireducibilan, ali nije prost element prstena $\mathbb{Z}[\sqrt{-5}]$.*

Rješenje. Pokažimo da je $2 + \sqrt{-5}$ ireducibilan. Pretpostavimo suprotno, odnosno da se taj element može zapisati u obliku umnoška

$$2 + \sqrt{-5} = z_1 \cdot z_2, \tag{3.1}$$

za neke $z_1, z_2 \in \mathbb{Z}[\sqrt{-5}]$. No, tada je i

$$|2 + \sqrt{-5}|^2 = |z_1|^2 \cdot |z_2|^2,$$

gdje je $|z|$ modul kompleksnog broja z. Uz $z_1 = a + b\sqrt{-5}$, $z_2 = c + d\sqrt{-5}$, $a, b, c, d \in \mathbb{Z}$, imamo

$$(a^2 + 5b^2)(c^2 + 5d^2) = 9.$$

Budući da su $a^2 + 5b^2$ i $c^2 + 5d^2$ nenegativni cijeli brojevi, mora vrijediti jedan od tri slučaja:

$$a^2 + 5b^2 = 3 \quad \text{i} \quad c^2 + 5d^2 = 3 \tag{3.2}$$

$$\text{ili} \quad a^2 + 5b^2 = 1 \quad \text{i} \quad c^2 + 5d^2 = 9 \tag{3.3}$$

$$\text{ili} \quad a^2 + 5b^2 = 9 \quad \text{i} \quad c^2 + 5d^2 = 1. \tag{3.4}$$

Jednadžba (3.2) nema rješenja u skupu cijelih brojeva. Iz jednadžbi (3.3) i (3.4) slijedi da je $a + b\sqrt{-5} = \pm 1$ ili $c + d\sqrt{-5} = \pm 1$, odnosno da su z_1 ili z_2 jedinice u prstenu. Time smo pokazali da je $2 + \sqrt{-5}$ ireducibilan element prstena $\mathbb{Z}[\sqrt{-5}]$.

Iz jednakosti

$$(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9 = 3 \cdot 3,$$

slijedi da $2 + \sqrt{-5}$ dijeli $3 \cdot 3$. Dakle, ako $2 + \sqrt{-5}$ dijeli 3, onda je

$$3 = (2 + \sqrt{-5})(a + b\sqrt{-5}),$$

za neki $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$. Prethodna relacija je ekvivalentna jednadžbi

$$3 = (2a - 5b) + (a + 2b)\sqrt{-5}. \tag{3.5}$$

Iz jednadžbe (3.5) slijedi da je $3 = 2a - 5b$ i $a + 2b = 0$, tj. $3 = -9b$, što nema rješenja za $b \in \mathbb{Z}$. Stoga, zaključujemo da $2 + \sqrt{-5}$ ne dijeli broj 3 pa broj $2 + \sqrt{-5}$ nije prost element prstena $\mathbb{Z}[\sqrt{-5}]$. □

Primjer 3.7. *Broj* 3 *je reducibilan i prost u prstenu* $\mathbb{Z}_6$.

Rješenje. $(\mathbb{Z}_6, +_6, \cdot_6)$ (ili kraće samo $\mathbb{Z}_6$) je komutativan prsten s jedinicom (1), pri čemu je

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\},$$

a $+_6$ i $\cdot_6$ su binarne operacije zbrajanja i množenja modulo 6. Invertibilni elementi prstena $\mathbb{Z}_6$ su 1 i 5. Dakle, 3 nije invertibilani element prstena $\mathbb{Z}_6$ te vrijedi da je

$$3 \cdot_6 3 = 3$$

iz čega zaključujemo da je element 3 reducibilan.

Sada ćemo pokazati da je 3 prost element ovog prstena. Neka su a, b iz prstena $\mathbb{Z}_6$ takvi da 3 dijeli $a \cdot_6 b$. Tada vrijedi

$$a \cdot_6 b = 3 \cdot_6 c,$$

za neki $c \in \mathbb{Z}_6$, odnosno

$$ab \equiv 3c \pmod 6.$$

Iz prethodnog zaključujemo

$$6 \mid ab - 3c \;\Rightarrow\; 3 \mid ab - 3c \;\Rightarrow\; 3 \mid ab.$$

Budući da je 3 prost u $\mathbb{Z}$, mora vrijediti da 3 dijeli a ili da 3 dijeli b. Slijedi da 3 dijeli a ili da 3 dijeli b i u prstenu $\mathbb{Z}_6$, pa zaključujemo da je 3 prost element prstena $\mathbb{Z}_6$. □

Definicija 3.8. *Neka je R komutativni prsten. Ideal prstena R je* ***glavni ideal*** *ako se može zapisati u obliku*

$$aR = \{ar : r \in R\},$$

za neki $a \in R$. Prsten R je ***domena glavnih ideala*** *ako je svaki ideal od R ujedno i glavni ideal.*

Primjer 3.9. *Ideal $2\mathbb{Z}$ (skup svih parnih brojeva u $\mathbb{Z}$) je glavni ideal jer se može generirati brojem 2. Pišemo: $2\mathbb{Z} = \langle 2 \rangle$.*

Nadalje, u $\mathbb{Z}$ je svaki ideal glavni. Ako je $\langle a, b \rangle$ ideal generiran cijelim brojevima a i b, to jest $\langle a, b \rangle = a\mathbb{Z} + b\mathbb{Z} = \{ax + by : x, y \in \mathbb{Z}\}$, lako se pokazuje da je $\langle a, b \rangle = \langle g \rangle$, gdje je g najveći zajednički djelitelj brojeva a i b. Analogno vrijedi i za ideale generirane s nekim konačnim skupom cijelih brojeva. Stoga je prsten cijelih brojeva $\mathbb{Z}$, domena glavnih ideala.

Primjer 3.10. *U prstenu polinoma $\mathbb{Z}[X]$ ideal generiran s dva elementa 2 i X, u oznaci $\langle 2, X \rangle = 2 \cdot \mathbb{Z}[X] + X \cdot \mathbb{Z}[X] = \{2\alpha + \beta : \alpha, \beta \in \mathbb{Z}[X]\}$ nije glavni ideal jer se ne može generirati samo jednim elementom.*

Definicija 3.11. *Prsten R je* ***domena jedinstvene faktorizacije*** *ako se svaki element prstena koji nije nula ili jedinica može zapisati kao umnožak ireducibilnih elemenata jedinstveno do na poredak faktora i asocirane elemente.*

Objasnimo prethodnu definiciju. Ako se element a (različit od nule ili jedinice) iz domene jedinstvene faktorizacije R može zapisati na dva načina kao umnožak ireducibilnih elemenata, to jest ako vrijedi

$$a = b_1 b_2 \cdots b_k = c_1 c_2 \cdots c_\ell,$$

onda je $k = \ell$ i postoji bijekcija $p : \{1, \ldots, k\} \to \{1, \ldots, k\}$ (to jest permutacija skupa $\{1, \ldots, k\}$) takva da za svaki $i \in \{1, \ldots, k\}$ vrijedi $b_i = uc_{p(i)}$, za neku jedinicu $u \in R$ (odnosno takva da su ireducibilni elementi b_i i $c_{p(i)}$ asocirani).

Ukratko, možemo reći da je domena jedinstvene faktorizacije prsten u kojem vrijedi tvrdnja analogna Osnovnom teoremu aritmetike 3.1. Mi ćemo pokazati da su prsteni cijelih brojeva nekih kvadratnih polja domene jedinstvene faktorizacije, a da neki nisu.

Može se pokazati da je svaka domena glavnih ideala ujedno i domena jedinstvene faktorizacije, ali nije svaka domena jedinstvene faktorizacije ujedno i domena glavnih ideala. Za dani $\alpha \neq 0$, koji nije jedinica, u domeni glavnih ideala R, sljedeće tvrdnje su ekvivalentne:

(i) α je ireducibilan.

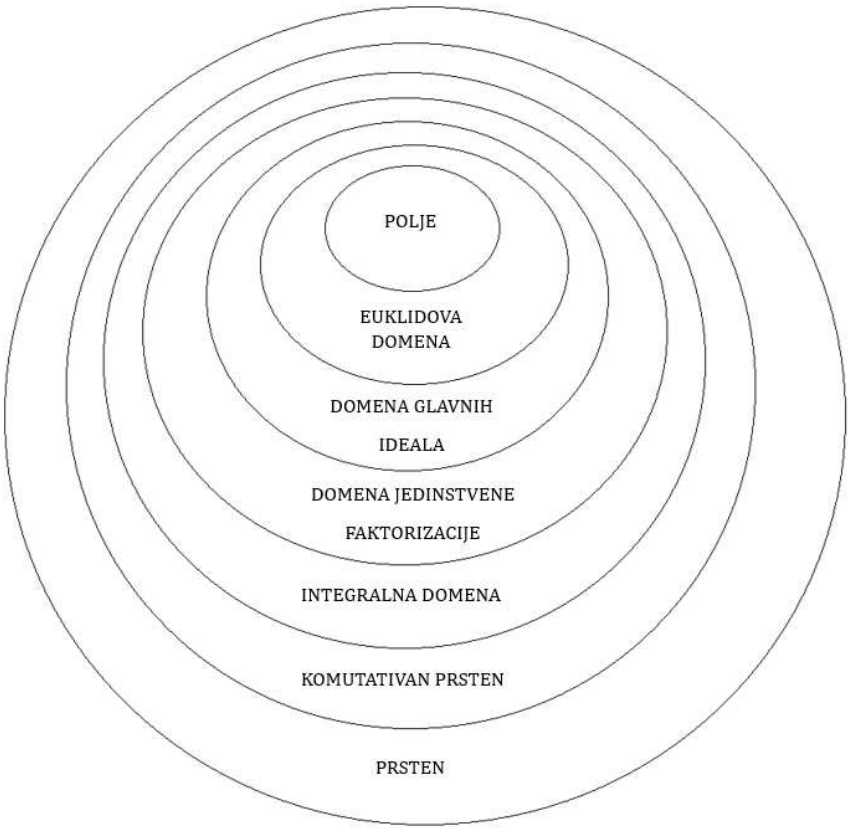
(ii) α je prost.

(iii) αR je prost ideal (ideal I od R je prost ako $\beta\gamma \in I$ implicira $\beta \in I$ ili $\gamma \in I$).

Definicija 3.12. *Neka je R integralna domena. Kažemo da je R* ***Euklidova domena*** *ako postoji funkcija $N : R\backslash\{0\} \to \mathbb{N}_0$ za koju vrijedi:*
za svaka dva elementa $a, b \in R$, $b \neq 0$, postoje elementi $q, r \in R$ takvi da je

$$a = bq + r,$$

pri čemu je $r = 0$ ili $N(r) < N(b)$.



Slika 3.1: Odnos između algebarskih struktura (prsteni, domene, polje)

Ukratko, možemo reći da su Euklidove domene prsteni u kojima vrijedi Euklidov algoritam. Pokazuje se da je svaka Euklidova domena ujedno i domena glavnih ideala, pa je

stoga i domena jedinstvene faktorizacije. Na slici 3.1 shematski je prikazan odnos između struktura o kojima smo govorili u ovom odjeljku.

3.3 Gaussovi cijeli brojevi

Skup *Gaussovih cijelih brojeva* je skup

$$Z[i] = \{a + bi : a, b \in \mathbb{Z}\},$$

odnosno prsten cijelih brojeva kvadratnog polja $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$. Pokazat ćemo da je taj prsten domena jedinstvene faktorizacije, što znači da se svi elementi mogu jedinstveno faktorizirati na ireducibilne elemente. Dokaz ovoga leži u činjenici da postoji algoritam dijeljenja. No, najprije trebamo neku mjeru veličine Gaussovog cijelog broja. Prirodan odabir za to je tzv. norma Gaussovog cijelog broja koju definiramo kao kvadrat apsolutne vrijednosti, odnosno modula tog broja:

$$\mathrm{N}(a + bi) = a^2 + b^2,\ a, b \in \mathbb{Z}$$

Za konjugirano kompleksni broj broja $\alpha = a + bi$ koristit ćemo oznaku $\overline{\alpha} = a - bi = \overline{a + bi}$, stoga normu možemo zapisati u obliku

$$\mathrm{N}(\alpha) = \alpha \cdot \overline{\alpha}$$

za sve $\alpha \in \mathbb{Z}[i]$. Uočimo da vrijedi

$$\mathrm{N}(\alpha) = \mathrm{N}(\overline{\alpha})$$

te da je $\mathrm{N}(\alpha) \in \mathbb{Z}$ za sve $\alpha \in Z[i]$. Štoviše, $\mathrm{N}(\alpha)$ je prirodan broj ako i samo je $\alpha \neq 0$.

Teorem 3.13. *Za sve $\alpha, \beta \in Z[i]$, gdje je $\beta \neq 0$, postoje $q, r \in Z[i]$ takvi da je*

$$\alpha = \beta q + r \ \ i \ \ 0 \leq N(r) \leq \frac{1}{2} N(\beta).$$

Dokaz. Kako je jednakost $\alpha = \beta q + r$ ekvivalentna jednakosti $\alpha\overline{\beta} = \beta\overline{\beta}q + \overline{\beta}r$, pri čemu je $\beta\overline{\beta} = \mathrm{N}(\beta) \in \mathbb{N}$, ideja dokaza je najprije primijeniti Teorem o dijeljenju s ostatkom za cijele brojeve.

Budući da su $\alpha, \beta \in \mathbb{Z}[i]$, tada je i $\alpha\overline{\beta} \in \mathbb{Z}[i]$, odnosno postoje $a, b \in \mathbb{Z}$ za koje je

$$\alpha\overline{\beta} = a + bi.$$

Prema Teoremu o dijeljenu s ostatkom za $a \in \mathbb{Z}$ i $\mathrm{N}(\beta) \in \mathbb{N}$ (jer je $\beta \neq 0$) postoje $r_1, q_1 \in \mathbb{Z}$ takvi da je

$$a = \mathrm{N}(\beta)q_1 + r_1 \ \text{ i } \ 0 \leq r_1 < \mathrm{N}(\beta). \tag{3.6}$$

Uočimo da ako je $r_1 > \frac{1}{2}\mathrm{N}(\beta)$, onda u (3.6) q_1 možemo zamijeniti s $q_1 + 1$, a r_1 s $r_1 - \mathrm{N}(\beta)$ pa imamo

$$a = \mathrm{N}(\beta)(q_1 + 1) + (r_1 - \mathrm{N}(\beta)) \text{ i } |r_i - \mathrm{N}(\beta)| \leq \frac{1}{2}\mathrm{N}(\beta).$$

Zbog toga, umjesto (3.6), imamo

$$a = \mathrm{N}(\beta)q_1 + r_1 \text{ i } 0 \leq |r_1| \leq \frac{1}{2}\mathrm{N}(\beta),$$

za neke cijele brojeve q_1 i r_1. Analogno, za $b \in \mathbb{Z}$ i $\mathrm{N}(\beta) \in \mathbb{N}$ postoje $r_2, q_2 \in \mathbb{Z}$ takvi da je

$$b = \mathrm{N}(\beta)q_2 + r_2 \text{ i } |r_2| \leq \frac{1}{2}\mathrm{N}(\beta).$$

Stoga vrijedi

$$a + bi = \mathrm{N}(\beta)q_1 + r_1 + (\mathrm{N}(\beta)q_2 + r_2)i,$$

odnosno

$$\underbrace{a + bi}_{=\alpha\overline{\beta}} = \underbrace{\mathrm{N}(\beta)}_{=\beta\overline{\beta}} (q_1 + q_2 i) + (r_1 + r_2 i)\,.$$

Dijeljenjem prethodne jednakosti s $\overline{\beta}$ dobivamo

$$\alpha = \beta\,(q_1 + q_2 i) + \frac{r_1 + r_2 i}{\overline{\beta}}$$

te uz $q = q_1 + q_2 i \in \mathbb{Z}[i]$ i $r = \dfrac{r_1 + r_2 i}{\overline{\beta}} \in Z[i]$ (jer je $r = \alpha - \beta\,(q_1 + q_2 i)$) imamo

$$\alpha = \beta q + r.$$

Još je preostalo pokazati da r zadovoljava željenu ogradu. Budući da vrijedi

$$\overline{\beta} r = r_1 + r_2 i,$$

i norme Gaussovih cijelih brojeva iz prethodne jednakosti su jednake. Zbog muliplikativnosti norme je

$$\mathrm{N}(\overline{\beta})\mathrm{N}(r) = \mathrm{N}\,(r_1 + r_2 i)\,.$$

Otuda je

$$\mathrm{N}(r) = \frac{\mathrm{N}\,(r_1 + r_2 i)}{\mathrm{N}(\overline{\beta})} = \frac{r_1^2 + r_2^2}{\mathrm{N}(\beta)}.$$

Kako je $|r_i| \leq \frac{1}{2}\mathrm{N}(\beta)$, zaključujemo da je

$$\mathrm{N}(r) = \frac{r_1^2 + r_2^2}{\mathrm{N}(\overline{\beta})} \leq \frac{\frac{1}{4}\mathrm{N}(\beta)^2 + \frac{1}{4}\mathrm{N}(\beta)^2}{\mathrm{N}(\overline{\beta})} = \frac{\frac{1}{2}\mathrm{N}(\beta)^2}{\mathrm{N}(\beta)} = \frac{1}{2}\mathrm{N}(\beta),$$

što je i trebalo pokazati. □

Budući da je $\mathbb{Z}[i]$ integralna domena, teorem 3.13 povlači da je $\mathbb{Z}[i]$ Euklidova domena, pa stoga i domena glavnih ideala.

Korolar 3.14. *Prsten Gaussovih cijelih brojeva je domena jedinstvene faktorizacije.*

U sljedećem primjeru pokazujemo kako "podijeliti s ostatkom" u prstenu $\mathbb{Z}[i]$.

Primjer 3.15. *Odredimo kvocijent q i ostatak r pri dijeljenju broja $1 + 4i$ brojem $1 + i$.*

Rješenje. Neka je $\alpha = 1 + 4i$ i $\beta = 1 + i$. Podijelimo α brojem β:

$$\frac{\alpha}{\beta} = \frac{1+4i}{1+i} = \frac{1+4i}{1+i} \cdot \frac{1-i}{1-i} = \frac{1-i+4i-4i^2}{1^2-i^2} = \frac{5+3i}{2} = \frac{5}{2} + \frac{3}{2}i \in \mathbb{Q}[i].$$

Budući da kvocijent brojeva α i β nije Gaussov cijeli broj, zaokružit ćemo njegov realni i imaginarni dio na najbliži cijeli broj i tako definirati q. Realni dio $\frac{5}{2} = 2.5$ je "jednako udaljen" i od broja 2 i od broja 3, stoga možemo birati na koji od ta dva broja ćemo ga zaokružiti. Mi ćemo ga zaokružiti na broj 3. Analogno, imaginarni dio $\frac{3}{2} = 1.5$ možemo zaokružiti ili na 1 ili na 2 te ćemo ga zaokružiti na broj 2. Stavimo

$$q = 3 + 2i$$

te iz relacije $\alpha = \beta q + r$ odredimo ostatak r:

$$r = \alpha - \beta q = 1 + 4i - (1+i)(3+2i) = 1 + 4i - (1+5i) = -i.$$

Uvjerimo se da vrijedi ograda za normu od r iz teorema 3.13:

$$0 \leq \mathrm{N}(r) = \mathrm{N}(-i) = 1 \leq 1 = \frac{1}{2} \cdot 2 = \frac{1}{2}\mathrm{N}(1+i) = \frac{1}{2}\mathrm{N}(\beta).$$

Uočimo da smo za q i r mogli izabrati i sljedeće vrijednosti (ako 2.5 zaokružimo na 2 itd.):

$$\begin{aligned} q &= 2 + i,\ r = i, \\ q &= 2 + 2i,\ r = 1, \\ q &= 3 + i,\ r = -1. \end{aligned}$$

Sve one zadovoljavaju $\mathrm{N}(r) \leq \frac{1}{2}\mathrm{N}(\beta)$, pa je jasno da u teoremu 3.13 ne možemo imati jedinstvenost brojeva q i r.

Slijedeći dokaz teorema 3.13 mogli smo q i r odrediti tako da nađemo kvocijente i ostatke pri dijeljenju realnog i imaginarnog dijela kompleksnog broja

$$\alpha\overline{\beta} = 5 + 3i$$

s $N(\beta) = 2$:

$$5 = 2 \cdot 2 + 1$$
$$3 = 2 \cdot 1 + 1.$$

Sada je

$$q = 2 + 2i,\ r = \frac{1+i}{\overline{\beta}} = \frac{1+i}{1-i} = i.$$

□

Prije nego li započnemo sa samom faktorizacijom elemenata od $\mathbb{Z}[i]$, trebamo odrediti skup svih jedinica (invertibilnih elementa) tog prstena te opisati skup ireducibilnih, odnosno prostih brojeva.

Propozicija 3.16. *Element Gaussovih cijelih brojeva $u \in \mathbb{Z}[i]$ je jedinica (invertibilni element) ako i samo ako je $N(u) = 1$. Također, skup svih jedinica u $\mathbb{Z}[i]$ je $\{1, -1, i, -i\}$.*

Dokaz. Prvo pretpostavimo da je $\mathrm{N}(u) = 1$. Tada, prema definiciji norme, vrijedi $u\overline{u} = 1$ i $\overline{u} \in \mathbb{Z}[i]$, iz čega zaključujemo da je $\overline{u}$ invertibilni element od u, tj. u je jedinica.

Dokažimo obrat. Ako je $u \in \mathbb{Z}[i]$ jedinica, tada postoji $v \in \mathbb{Z}[i]$ takav da vrijedi $uv = 1$. Stoga je $\mathrm{N}(u)\mathrm{N}(v) = 1$. S obzirom na to da su $\mathrm{N}(u)$ i $\mathrm{N}(v)$ cijeli brojevi, to implicira da je $\mathrm{N}(u) = \pm 1$. U $\mathbb{Z}[i]$ nije moguće da je norma $\mathrm{N}(u) = -1$ pa smo time dokazali da mora vrijediti $\mathrm{N}(u) = 1$.

Odredimo sada sve jedinice prstena $\mathbb{Z}[i]$. Za jedinicu $u = a + bi$, $a, b \in \mathbb{Z}$, prema prethodnom nužno vrijedi

$$\mathrm{N}(u) = \mathrm{N}(a + bi) = a^2 + b^2 = 1,$$

što može biti ispunjeno samo u dva slučaja: ako je $a = \pm 1$ i $b = 0$ ili ako je $a = 0$ i $b = \pm 1$. U prvom slučaju je $u = \pm 1$, a u drugom je $u = \pm i$ čime smo pokazali da $\mathbb{Z}[i]$ ima točno četiri jedinice. □

Prema definiciji 3.5, broj $\alpha \in \mathbb{Z}[i]$ je prost element ako $\alpha \mid \beta\gamma$, za $\beta, \gamma \in \mathbb{Z}[i]$, što implicira da $\alpha \mid \beta$ ili $\alpha \mid \gamma$. Iz same definicije prostog broja u prstenu $\mathbb{Z}[i]$ nemamo neku predodžbu o njima, no može nam pomoći njihova veza s prostim brojevima u $\mathbb{Z}$ koju opisujemo u sljedećoj lemi.

Lema 3.17. *Neka je $\pi \in \mathbb{Z}[i]$ prost element. Tada π dijeli (u $\mathbb{Z}[i]$) neki prost broj p u $\mathbb{N}$.*

Dokaz. Norma prostog elementa π je $\mathrm{N}(\pi) = \pi\overline{\pi} \in \mathbb{N}$ i broj π dijeli taj cijeli broj. Ako je $\mathrm{N}(\pi)$ prost broj, tada vrijedi tvrdnja leme. Ako $\mathrm{N}(\pi)$ nije prost broj, tada je $\mathrm{N}(\pi)$ jednak umnošku prostih brojeva u $\mathbb{N}$. Kako je π prost element u $\mathbb{Z}[i]$, on, prema definiciji 3.5, mora dijeliti barem jedan od brojeva u tom umnošku, odnosno postoji $p \in \mathbb{N}$ prost takav da $\pi \mid p$. □

Napomenimo da je prsten Gaussovih cijelih brojeva ujedno i domena glavnih ideala što znači da su prosti elementi isto što i ireducibilni. Stoga se *Gaussov prost broj* može karakterizirati kao onaj koji se ne može napisati kao umnožak dvaju ili više drugih Gaussovih brojeva pri čemu nijedan od brojeva u umnošku nije jedinica.

Lema 3.17 nam može pomoći u određivanju svih Gaussovih prostih brojeva tako što odredimo sve moguće faktorizacije prostih brojeva iz $\mathbb{N}$ u prstenu $\mathbb{Z}[i]$. Moguće faktorizacije prostog prirodnog broja p razmotrit ćemo u sljedećim slučajevima: $p = 2$, $p \equiv 1 \pmod 4$ i $p \equiv 3 \pmod 4$.

Slučaj $p = 2$: Iz $(a + bi)(c + di) = 2, a, b, c, d \in \mathbb{Z}$, slijedi da je

$$ac - bd = 2,\ bc - ad = 0.$$

Ako je $a = 0$, onda je $b \neq 0$, $c = 0$ i $bd = -2$ pa dobivamo faktorizacije $2 = i \cdot (-2i) = (-i) \cdot (2i)$. Ako je $a \neq 0$, onda iz $bc - ad = 0$ slijedi da je $d = -bc/a$ pa uvrštavanjem u $ac - bd = 2$ dobivamo

$$c(a^2 + b^2) = 2a.$$

Iz prethodne relacije slijedi da je $a = \pm 1$, $b = d = 0$ i $c = \pm 2$ ili $a = b = c = -d = \pm 1$. Dakle, moguće faktorizacije broja 2 su:

$$2 = (\pm 1) \cdot (\pm 2),\ \ 2 = (1 + i)(1 - i) = (-1 - i)(-1 + i).$$

Jedina faktorizacija koja ne uključuje jednicu je ova posljednja pa su $i + 1$ zajedno s pripadnim asociranim brojevima prosti u $\mathbb{Z}[i]$. Zanimljivo je i da vrijedi

$$2 = (-i)(1 + i)^2$$

jer su $1 + i$ i $1 - i$ asocirani.

Slučaj $p \equiv 3 \pmod 4$: Pretpostavimo da se p faktorizira nad $\mathbb{Z}[i]$, odnosno postoje $\alpha, \beta \in \mathbb{Z}[i]$ takvi da α i β nisu jedinice i $p = \alpha\beta$. Tada vrijedi

$$p^2 = \mathrm{N}(p) = \mathrm{N}(\alpha)\mathrm{N}(\beta).$$

Kako α i β nisu jedinice, prema lemi 3.16 zaključujemo da su $\mathrm{N}(\alpha)$ i $\mathrm{N}(\beta)$ prirodni brojevi veći od 1 te je jedino moguće

$$\mathrm{N}(\alpha) = \mathrm{N}(\beta) = p.$$

Ako pretpostavimo da je $\alpha = a + bi$, $a, b \in \mathbb{Z}$, onda bismo dobili $p = a^2 + b^2$, što je nemoguće jer je zbroj dva kvadrata uvijek kongruentan 0, 1 ili 2 modulo 4. Stoga je jedina moguća faktorizacija (do na varijante s pripadnim asociranim faktorima) od p u $\mathbb{Z}[i]$:

$p = p \cdot 1$. Zaključujemo da su svi prosti prirodni brojevi $p \equiv 3 \pmod 4$ i dalje prosti kao elementi prstena $\mathbb{Z}[i]$.

Slučaj $p \equiv 1 \pmod 4$: Pretpostavimo da je p prost u $\mathbb{Z}[i]$. Wilsonov teorem (teorem 3.13 iz [5]) kaže da za prost broj p vrijedi

$$(p-1)! \equiv -1 \pmod p.$$

Kako je u našem slučaju

$$(p-1)! \equiv \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \pmod p,$$

postoji cijeli broj a takav da je

$$a^2 \equiv -1 \pmod p.$$

Stoga p dijeli $a^2 + 1$ u $\mathbb{Z}$. Faktorizacijom izraza $a^2 + 1$ u obliku $(a+i)(a-i)$ nad $\mathbb{Z}[i]$, dobivamo da p dijeli umnožak $(a+i)(a-i)$. No, p ne dijeli ni $a+i$ ni $a-i$, dakle p nije Gaussov prost broj. Zbog toga postoje α i β, koji nisu jedinice, takvi da je $p = \alpha\beta$. Kako je $p^2 = \mathrm{N}(p) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$, nužno je $\mathrm{N}(\alpha) = p$ i stoga je $\pi = \alpha$ Gaussov prost broj. Nadalje, $p = \mathrm{N}(\pi) = \pi\overline{\pi}$.

Sve ovo što smo upravo pokazali rezimirat ćemo u sljedećoj propoziciji.

Propozicija 3.18. *Neka je π prost u $\mathbb{Z}[i]$. Tada vrijedi jedna od sljedeće tri tvrdnje:*

1. *π je pridružen (asociran) pozitivnom prostom broju p za koji vrijedi $p \equiv 3 \pmod 4$.*
2. *$N(\pi) = p$ gdje je p prost prirodan broj takav da vrijedi $p \equiv 1 \pmod 4$. U ovom slučaju svaki prost broj norme p je pridružen (asociran) točno jednom od π i $\overline{\pi}$.*
3. *π je pridružen (asociran) prostom broju $1+i$.*

Primjer 3.19. *Broj 7 je prost element prstena $\mathbb{Z}[i]$, jer je 7 prost broj iz $\mathbb{Z}$ i $7 \equiv 3 \pmod 4$. Njemu asocirani brojevi -7, $7i$ i $-7i$ su također prosti u $\mathbb{Z}[i]$.*

Broj 5 nije prost element prstena $\mathbb{Z}[i]$ iako je 5 prost broj iz $\mathbb{Z}$. Naime,

$$5 = (2+i)(2-i).$$

Uočimo da je $2+i$ prost broj u $\mathbb{Z}[i]$. Naime, u suprotnom bi vrijedilo da je $2+i = \alpha\beta$ pri čemu $\alpha, \beta \in \mathbb{Z}[i]$ nisu jedinice. No, tada je $5 = N(2+i) = N(\alpha)N(\beta)$ što znači da je jedan od elemenata α, β jedinica u $\mathbb{Z}[i]$. Analogno, $2-i$ je također prost broj. Uočimo da oni

nisu asocirani, to jest $2 + i \neq u(2 - i)$ *za* $u \in \{\pm 1, \pm i\}$. *Nadalje, uočimo da broj* 5 *možemo rastaviti i kao*

$$5 = (1 + 2i)(1 - 2i).$$

No, iz ovog rastava nismo dobili nove proste brojeve već asocirane prostima $2 + i$ *i* $2 - i$.

Primjer 3.20. *Faktorizirajmo* $\alpha = -133 - 119i$ *u prstenu* $\mathbb{Z}[i]$.

Rješenje. Najprije izračunajmo normu te ju faktorizirajmo u $\mathbb{N}$:

$$\mathrm{N}(\alpha) = (-113)^2 + (-119)^2 = 31850 = 2 \cdot 5^2 \cdot 7^2 \cdot 13.$$

S obzirom da 2 dijeli normu $\mathrm{N}(\alpha)$, znamo da $1 + i$ dijeli α. Znamo da je broj 7 prost u $\mathbb{Z}[i]$ jer vrijedi $7 \equiv 3 \pmod 4$, pa mora vrijediti da 7 dijeli α. Da bismo odredili što se događa s prostim brojevima čija norma iznosi 5 ili 13, moramo odrediti koji su to prosti brojevi. Imamo

$$5 = (2 + i)(2 - i)$$

i

$$13 = (3 + 2i)(3 - 2i).$$

Kako bismo završili faktorizaciju, moramo odrediti koji od prostih faktora broja 13 dijeli α te dijeli li jedan ili oba prosta faktora broja 5, broj α. Može se odrediti da $2 + i$ i $3 + 2i$ dijele α, stoga je α djeljiv sljedećim prostim faktorima i njihovim potencijama:

$$1 + i,\ (2 + i)^2,\ 7,\ 3 + 2i.$$

Konačno dobivamo

$$-133 - 119i = i \cdot (1 + i) \cdot (2 + i)^2 \cdot 7 \cdot (3 + 2i).$$

□

Propozicija 3.21. *Pozitivan racionalan prost broj* p *može se zapisati u obliku* $x^2 + y^2$ *sa* $x, y \in \mathbb{Z}$ *ako i samo ako se* p *faktorizira u* $\mathbb{Z}[i]$.

Dokaz. Pretpostavimo da je $p = x^2 + y^2$. Tada se p može faktorizirati u obliku $p = (x + yi)(x + yi)$ i lako se vidi da ni jedan od faktora nije jedinica (invertibilan element); stoga možemo zaključiti da se p može faktorizirati u $\mathbb{Z}[i]$.

Obratno, ako se p može faktorizirati u $\mathbb{Z}[i]$, primjerice u obliku $p = \alpha\beta$, tada vrijedi $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = p$. Ako je $\alpha = x + yi$, tada možemo zaključiti da je $p = x^2 + y^2$, čime smo dokazali obrat. □

Korolar 3.22. *Prirodni prost broj p može se zapisati u obliku $p = x^2 + y^2$ sa $x, y \in \mathbb{N}$ ako i samo ako vrijedi da $p = 2$ ili $p \equiv 1 \pmod 4$. Nadalje, ovaj prikaz je jedinstven do na poredak brojeva x i y.*

Dokaz. Jasno, $2 = 1^2 + 1^2$, a neparni prost broj $p \in \mathbb{N}$ je prost broj u $\mathbb{Z}[i]$ ako i samo ako $p \equiv 3 \pmod 4$. Stoga se prosti brojevi iz $\mathbb{N}$ oblika $p \equiv 1 \pmod 4$ mogu faktorizirati pa tvrdnja dalje slijedi iz propozicije 3.21.

Dokaz jedinstvenosti prikaza može se naći u [5], propozicija 5.6. □

3.4 Eisensteinovi cijeli brojevi

Skup *Eisensteinovih cijelih brojeva* je

$$\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\},$$

pri čemu je

$$\omega = \frac{-1 + \sqrt{-3}}{2} = \frac{-1 + i\sqrt{3}}{2} = e^{i2\pi/3} \in \mathbb{C},$$

primitivni kubni korijen broja 1. Stoga $\omega^3 - 1 = 0$. No, kako je $\omega \neq 1$, zaključujemo da je

$$\omega^2 + \omega + 1 = 0. \tag{3.7}$$

Eisensteinovi cijeli brojevi čine komutativni prsten algebarskih cijelih brojeva u algebarskom polju brojeva $\mathbb{Q}(\omega)$.

Želimo odrediti proste elemente i jedinice (invertibilne elemente) ovog prstena. U tu svrhu, proučimo normu u $\mathbb{Z}[\omega]$. Neka je $\alpha = a + b\omega \in \mathbb{Z}[\omega]$. Tada je norma $\mathrm{N}(\alpha)$ pozitivan cijeli broj određen s

$$\mathrm{N}(\alpha) = \alpha\overline{\alpha} \tag{3.8}$$

gdje je $\overline{\alpha}$ kompleksno konjugirani α. Uočimo da je $\overline{\alpha} \in \mathbb{Z}[\omega]$. Zaista,

$$\overline{\alpha} = a + b\overline{\omega} = a + b\frac{-1 - i\sqrt{3}}{2} = a - b - b\frac{-1 + i\sqrt{3}}{2} = a - b - b\omega.$$

Sada je za $\alpha = a + b\omega$

$$\mathrm{N}(\alpha) = (a + b\omega)(a - b - b\omega) = a^2 - ab - b^2\omega - b^2\omega^2.$$

Prema (3.7) je $\omega^2 = -\omega - 1$ pa dobivamo

$$\mathrm{N}(\alpha) = a^2 - ab - b^2\omega - b^2(-\omega - 1) = a^2 - ab + b^2.$$

Zbog (3.8) je jasno da je norma multiplikativna, odnosno da za $\alpha, \beta \in \mathbb{Z}[\omega]$, vrijedi $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$. Nadalje, u $\mathbb{Z}[\omega]$ vrijedi teorem analogan teoremu o dijeljenju ostatkom, što znači da je $\mathbb{Z}[\omega]$ Euklidova domena.

Teorem 3.23. *Za dane $\alpha, \beta \in \mathbb{Z}[\omega], \beta \neq 0$, postoje $\gamma, \delta \in \mathbb{Z}[\omega]$ takvi da vrijedi*

$$\alpha = \gamma\beta + \delta, \quad N(\delta) < N(\beta).$$

Dokaz. Jasno je da se funkcija norme $\mathrm{N}(\alpha) = \alpha\overline{\alpha}$ može definirati za $\alpha \in \mathbb{Q}(\omega) = \{r + s\omega : r, s \in \mathbb{Q}\}$ te da vrijedi $\mathrm{N}(uv) = \mathrm{N}(u)\mathrm{N}(v)$ za $u, v \in \mathbb{Q}(\omega)$.

Pokažimo najprije da je $\alpha/\beta \in \mathbb{Q}(\omega)$ za $\alpha, \beta \in \mathbb{Z}[\omega], \beta \neq 0$. Zaista,

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \frac{\alpha\overline{\beta}}{\mathrm{N}(\beta)} = \underbrace{\frac{1}{\mathrm{N}(\beta)}}_{\in\mathbb{Q}} \cdot \underbrace{\alpha}_{\in\mathbb{Z}[\omega]} \cdot \underbrace{\overline{\beta}}_{\in\mathbb{Z}[\omega]} \in \mathbb{Q}(\omega).$$

Stoga postoje $r, s \in \mathbb{Q}$ za koje je

$$\frac{\alpha}{\beta} = r + s\omega.$$

Neka su r_1, s_1 (racionalni) cijeli brojevi takvi da vrijedi

$$|r - r_1| \leq \frac{1}{2} \text{ i } |s - s_1| \leq \frac{1}{2}.$$

Sada definiramo

$$\gamma = r_1 + s_1\omega \text{ i } \delta = \alpha - \gamma\beta.$$

Uočimo da su γ, δ brojevi iz $\mathbb{Z}[\omega]$ za koje vrijedi

$$\alpha = \gamma\beta + \delta.$$

Preostalo je još pokazati da je $\mathrm{N}(\delta) < \mathrm{N}(\beta)$. Neka je

$$\epsilon = \frac{\alpha}{\beta} - \gamma = (r - r_1) + (s - s_1)\omega.$$

Tada je

$$\delta = \alpha - \gamma\beta = \beta\left(\frac{\alpha}{\beta} - \gamma\right) = \beta\epsilon.$$

S obzirom da je norma multiplikativna, dovoljno je pokazati da je $\mathrm{N}(\epsilon) < 1$. Raspišimo $\mathrm{N}(\epsilon)$ po formuli norme $\mathrm{N}(a + b\omega) = a^2 - ab + b^2$:

$$\mathrm{N}(\epsilon) = \mathrm{N}((r - r_1) + (s - s_1)\omega) = (r - r_1)^2 - (r - r_1)(s - s_1) + (s - s_1)^2,$$

odnosno

$$\mathrm{N}(\epsilon) = ((r - r_1) - (s - s_1))^2 + (r - r_1)(s - s_1).$$

Koristeći $|r - r_1|, |s - s_1| \leq \frac{1}{2}$ dobivamo željenu nejednakost. □

Teorem 3.23 povlači da je $\mathbb{Z}[\omega]$ Euklidova domena (jer je očito integralna domena). Stoga je i ovom prstenu faktorizacija na ireducibilne, odnosno proste faktore jedinstvena (do na asociranost).

Korolar 3.24. *Prsten Eisensteinovih cijelih brojeva je domena jedinstvene faktorizacije.*

Želimo opisati sve proste Eisensteinove brojeve i sve jedinice iz prstena $\mathbb{Z}[\omega]$.

Propozicija 3.25.

(i) Element $\alpha \in \mathbb{Z}[\omega]$ je jedinica ako i samo ako je norma $N(\alpha) = 1$.

(ii) Jedinice prstena $\mathbb{Z}[\omega]$ su $\left\{\pm 1, \pm\omega, \pm\omega^2\right\}$.

Dokaz. (i) Ako je $\mathrm{N}(\alpha) = 1$, tada vrijedi da $\alpha\overline{\alpha} = 1$ što znači da je α jedinica jer je $\overline{\alpha} \in \mathbb{Z}[\omega]$.

Ako je α jedinica, tada postoji β takav da vrijedi $\alpha\beta = 1$. Stoga vrijedi da je $\mathrm{N}(\alpha)\mathrm{N}(\beta) = 1$. S obzirom da su $\mathrm{N}(\alpha)$ i $\mathrm{N}(\beta)$ pozitivni cijeli brojevi, slijedi da je $\mathrm{N}(\alpha) = 1$.

(ii) Odredimo sve jedinice prstena $\mathbb{Z}[\omega]$. Pretpostavimo da je $\alpha = a + b\omega$, $a, b \in \mathbb{Z}$, jedinica. Tada vrijedi da je $\mathrm{N}(\alpha) = 1$, odnosno

$$a^2 - ab + b^2 = 1.$$

Množenjem prethodne relacije s 4, imamo

$$4a^2 - 4ab + 4b^2 = 4,$$

što možemo zapisati kao

$$(2a - b)^2 + 3b^2 = 4.$$

S obzirom da su $a, b \in \mathbb{Z}$, mogući su sljedeći slučajevi:

(a) $2a - b = \pm 1,\ b = \pm 1.$

(b) $2a - b = \pm 2,\ b = 0.$

Rješavanjem ovih linearnih sustava dobivamo rješenja:

(a) $(a, b) \in \{(1, 1), (0, -1), (0, 1), (-1, -1)\}$

(b) $(a, b) \in \{(1, 0), (-1, 0)\}$.

Stoga u prstenu $\mathbb{Z}[\omega]$ postoji ukupno šest jedinica:

$$1+\omega, -\omega, \omega, -1-\omega, 1, -1.$$

S obzirom da je $\omega^2+\omega+1=0$, vrijedi da je $\pm(1+\omega)=\mp\omega^2$.

□

Sljedeća lema će nam biti korisna za određivanje prostih elemenata od $\mathbb{Z}[\omega]$.

Lema 3.26. *Ako je $\alpha \in \mathbb{Z}[\omega]$ takav da je $N(\alpha)$ prost broj u $\mathbb{Z}$, tada je α prost element u $\mathbb{Z}[\omega]$.*

Dokaz. Pretpostavimo da α nije prost u $\mathbb{Z}[\omega]$. S obzirom da je $\mathbb{Z}[\omega]$ domena glavnih ideala, to znači da je α reducibilan. Dakle, $\alpha=\beta\gamma$ i $\mathrm{N}(\beta), \mathrm{N}(\gamma) > 1$. No, tada $\mathrm{N}(\alpha)=\mathrm{N}(\beta)\mathrm{N}(\gamma)$ ne može biti prost u $\mathbb{Z}$, što je u suprotnosti s pretpostavkom leme. □

Lema 3.27. *Ako je $\alpha \in \mathbb{Z}[\omega]$ prost, tada α dijeli neki prost broj p iz $\mathbb{Z}$ te vrijedi da je $N(\alpha)=p$ ili $N(\alpha)=p^2$.*

Dokaz. Budući da je α prost $\mathbb{Z}[\omega]$ i da dijeli cijeli broj $\mathrm{N}(\alpha)=\alpha\overline{\alpha}$, postoji prost broj p u $\mathbb{Z}$ takav da $\alpha \mid p$. No, tada $\mathrm{N}(\alpha) \mid \mathrm{N}(p)=p^2$ pa je $\mathrm{N}(\alpha) \in \{p, p^2\}$. □

Sada možemo odrediti sve proste elemente u $\mathbb{Z}[\omega]$.

Propozicija 3.28. *Neka je p prost broj u $\mathbb{Z}$. Tada:*

(i) Ako je $p=3$, tada je $3=-\omega^2(1-\omega)^2$ i $1-\omega$ prost u $\mathbb{Z}[\omega]$.

(ii) Ako je $p \equiv 1 \pmod 3$, tada postoji prost $\pi \in \mathbb{Z}[\omega]$ takav da je $p=\pi\overline{\pi}$ te su prosti π i $\overline{\pi}$ pridruženi (asocirani) u $\mathbb{Z}[\omega]$.

(iii) Ako je $p \equiv 2 \pmod 3$, tada p ostaje prost u $\mathbb{Z}[\omega]$.

Nadalje, svaki prost element u $\mathbb{Z}[\omega]$ je pridružen (asociran) jednom od prostih u (i), (ii) ili (iii).

Dokaz. (i) Računski provjerimo da je $3=-\omega^2(1-\omega)^2$. Nadalje, kako je $\mathrm{N}(1-\omega)=3$ što je prost broj u $\mathbb{Z}$, lema 3.26 povlači da je $1-\omega$ prost u $\mathbb{Z}[\omega]$.

(ii) Neka je $p \equiv 1 \pmod 3$ prost u $\mathbb{Z}$. Tvrdnja slijedi iz činjenice da je -3 kvadratni ostatak modulo p za $p \equiv 1 \pmod 3$ iz čega se može pokazati da p dijeli a^2-a+1, odnosno $(a+\omega)(a+\overline{\omega})$. Dalje je sve analogno kao za Gaussove cijele brojeve (u slučaju $p \equiv 1 \pmod 4$).

(iii) Uočimo da je $\mathrm{N}(a + b\omega) = a^2 - ab + b^2 \equiv 0, 1 \pmod 3$ za $a, b \in \mathbb{Z}$. Ako je α prost broj koji dijeli p, onda zaključujemo da je jedino moguće $\mathrm{N}(\alpha) = p^2$, tj. $\alpha = p$.

Preostalo nam je dokazati da su svi prosti elementi u $\mathbb{Z}[\omega]$ pridruženi (asocirani) jednom od prostih u (i), (ii) ili (iii). Nazovimo za ovaj dokaz proste elemente u (i)-(iii) "poznati prosti elementi" od $\mathbb{Z}[\omega]$ te neka je α bilo koji prost element u $\mathbb{Z}[\omega]$. Tada je $\mathrm{N}(\alpha) = \alpha\overline{\alpha}$ cijeli broj i može se faktorizirati na cijele proste brojeve. Ali (i)-(iii) implicira da je bilo koji cijeli prost broj umnožak "poznatih prostih elemenata" u $\mathbb{Z}[\omega]$, stoga je $\mathrm{N}(\alpha) = \alpha\overline{\alpha}$ također umnožak "poznatih prostih elemenata".

□

3.5 Nejedinstvena faktorizacija

U prethodnim odjeljcima pokazali smo da u prstenima $\mathbb{Z}[i]$ i $\mathbb{Z}[\omega]$ imamo jedinstvenu faktorizaciju na ireducibilne, odnosno proste faktore. Ovdje ćemo dati nekoliko primjera prstena kvadratnih polja u kojima nemamo jedinstvenu faktorizaciju. Najprije iskažimo jednostavnu lemu koja će nam biti veoma korisna pri faktorizaciji i pronalaženju ireducibilnih brojeva.

Lema 3.29. *Neka je R potprsten nekog polja K tako da je norma $N(\alpha)$ cijeli broj za svaki $\alpha \in R$. Neka su α i β elementi od R takvi da α dijeli β u R. Tada $N(\alpha)$ dijeli $N(\beta)$ u $\mathbb{Z}$. Specijalno, ako je $N(\alpha)$ prost broj u $\mathbb{Z}$, tada je α ireducibilan u R. Također, α je jedinica (invertibilan element) samo ako je $N(\alpha) = \pm 1$.*

Prsten $\mathbb{Z}[\sqrt{-3}]$

Lema 3.30. *Jedinice prstena $\mathbb{Z}[\sqrt{-3}]$ su 1 i -1.*

Dokaz. Neka je $\alpha = a + b\sqrt{-3}$ jedinica u prstenu $\mathbb{Z}[\sqrt{-3}]$. Tada vrijedi da je norma $\mathrm{N}(\alpha) = 1$ iz čega slijedi da je $a^2 + 3b^2 = 1$, što ima cjelobrojna rješenja samo za $a = \pm 1$ i $b = 0$. Zaključujemo da su jedinice prstena ± 1. □

Prsten $\mathbb{Z}[\sqrt{-3}]$ nije domena jedinstvene faktorizacije. U to se možemo uvjeriti na temelju sljedećeg primjera.

Primjer 3.31. *Broj 4 se u prstenu $\mathbb{Z}[\sqrt{-3}]$ faktorizira na dva različita načina*

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Rješenje. Pokažimo najprije da su 2, $1 + \sqrt{-3}$ i $1 - \sqrt{-3}$ ireducibilni u $\mathbb{Z}[\sqrt{-3}]$.

Pretpostavimo da je broj 2 reducibilan. Tada vrijedi

$$2 = xy,$$

gdje x i y nisu jedinice, odnosno norma od x i y je veća od 1. Kako je norma prethodnog izraza jednaka

$$4 = \mathrm{N}(x)\mathrm{N}(y),$$

zaključujemo da su obje norme od x i y jednake 2. No, uočimo da u prstenu $\mathbb{Z}[\sqrt{-3}]$ ne postoji element čija je norma jednaka 2. Zaista, jednadžba

$$\mathrm{N}(a + b\sqrt{-3}) = a^2 + 3b^2 = 2,\ a, b \in \mathbb{Z},$$

nema rješenja u $\mathbb{Z}$. Stoga je 2 ireducibilan u $\mathbb{Z}[\sqrt{-3}]$.

Pretpostavimo da je broj $1 + \sqrt{-3}$ reducibilan, odnosno da je

$$1 + \sqrt{-3} = xy,$$

gdje x i y nisu jedinice, tj. norma im je veća od 1. Kako je norma prethodnog izraza jednaka

$$4 = \mathrm{N}(x)\mathrm{N}(y),$$

analogno kao u prethodnom slučaju zaključujemo da je $1 - \sqrt{-3}$ ireducibilan u $\mathbb{Z}[\sqrt{-3}]$.

Konačno, očito 2, $1 + \sqrt{-3}$ i $1 - \sqrt{-3}$ nisu asocirani, pa se broj 4 faktorizira na dva različita načina kao $2 \cdot 2$ i $(1 + \sqrt{-3})(1 - \sqrt{-3})$. □

Prsten $\mathbb{Z}[\sqrt{-5}]$

Lema 3.32. *Jedinice prstena* $\mathbb{Z}[\sqrt{-5}]$ *su* 1 *i* -1.

Dokaz. Neka je $\alpha = a + b\sqrt{-5}$ jedinica u prstenu $\mathbb{Z}[\sqrt{-5}]$. Tada vrijedi da je norma $\mathrm{N}(\alpha) = 1$ iz čega slijedi da je $a^2 + 5b^2 = 1$, što ima cjelobrojna rješenja samo za $a = \pm 1$ i $b = 0$. Zaključujemo da su jedinice prstena ± 1. □

Prsten $Z[\sqrt{-5}]$ nije domena jedinstvene faktorizacije što se može zaključiti iz sljedećeg primjera.

Primjer 3.33. *Broj* 6 *se u* $\mathbb{Z}[\sqrt{-5}]$ *faktorizira na dva različita načina:*

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

pri čemu su svi faktori ireducibilni u $\mathbb{Z}[\sqrt{-5}]$.

Rješenje. Pretpostavimo da je broj 2 reducibilan. Tada vrijedi

$$2 = xy$$

gdje x i y nisu jedinice, odnosno norma je veća od 1. Promatrajući normu dobivamo

$$4 = \mathrm{N}(x)\mathrm{N}(y)$$

što bi značilo da su obje norme od x i y jednake 2. Kada bi norma nekog broja iz prstena $\mathbb{Z}[\sqrt{-5}]$ bila jednaka 2, tada bi vrijedilo $\mathrm{N}(a + b\sqrt{-5}) = a^2 + 5b^2 = 2$ što nema rješenja u $\mathbb{Z}$. Stoga, ne postoji broj u prstenu $\mathbb{Z}[\sqrt{-5}]$ čija je norma jednaka 2. Ovime smo dokazali da je broj 2 ireducibilan u $\mathbb{Z}[\sqrt{-5}]$.

Pretpostavimo da je broj 3 reducibilan. Tada vrijedi

$$3 = xy$$

gdje x i y nisu jedinice, odnosno norma svakog od njih je veća od 1. Iz

$$9 = \mathrm{N}(x)\mathrm{N}(y)$$

slijedi da su obje norme od x i y jednake 3. Kada bi norma nekog broja iz prstena $\mathbb{Z}[\sqrt{-5}]$ bila jednaka 3, tada bi vrijedilo $\mathrm{N}(a + b\sqrt{-5}) = a^2 + 5b^2 = 3$ što nema rješenja u $\mathbb{Z}$. Stoga, ne postoji broj u prstenu $\mathbb{Z}[\sqrt{-5}]$ čija je norma jednaka 3. Ovime smo dokazali da je broj 3 ireducibilan u $\mathbb{Z}[\sqrt{-5}]$.

Pretpostavimo da je broj $1 + \sqrt{-5}$ reducibilan. Tada vrijedi

$$1 + \sqrt{-5} = xy$$

gdje x i y nisu jedinice, odnosno norma je veća od 1. Zbog

$$6 = \mathrm{N}(x)\mathrm{N}(y)$$

zaključujemo da su norme od x i y jednake 2 ili 3. No, već smo pokazali da u našem prstenu ne postoji broj čija je norma jednaka 2 ili 3. Ovime smo dokazali da je broj $1 + \sqrt{-5}$ ireducibilan u $\mathbb{Z}[\sqrt{-5}]$. Analogno vrijedi i za broj $1 - \sqrt{-5}$.

Očito brojevi 2 i 3 nisu asocirani brojevima $1 + \sqrt{-5}$ i $1 - \sqrt{-5}$, pa možemo zaključiti da broj 6 u našem prstenu ima dvije različite faktorizacije na ireducibilne elemente. □

Poznati matematičar L. Carlitz je 1960. godine pokazao da je duljina faktorizacije jedinstvena, odnosno ako se neki broj u prstenu $\mathbb{Z}[\sqrt{-5}]$ ili u prstenu $\mathbb{Z}[\sqrt{-3}]$ može faktorizirati na dva različita načina, tada je duljina obiju faktorizacija ista, tj. obje faktorizacije će imati jednak broj faktora. To smo mogli vidjeti i u prethodnim primjerima nejedinstvene faktorizacije, 3.31 i 3.33.

Bibliografija

[1] M. Barrus, W. Edwin Clark, *The Gaussian Integers*, https://math.libretexts.org/Bookshelves/Combinatorics_and_Discrete_Mathematics/Elementary_Number_Theory_(Barrus_and_Clark)/01%3A_Chapters/1.13%3A_The_Gaussian_Integers

[2] A. K. Bhuniya, *Chapter 7: Factorizations in Integral Domains, Module 2 : Prime and irreducible elements*, https://epgp.inflibnet.ac.in/epgpdata/uploads/epgp_content/S000025MS/P001533/M017004/ET/1527145666E-textofChapter7Module2.pdf

[3] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc. 11, 1960.

[4] D.A. Cox, *Primes of the form* $x^2 + ny^2$, Wiley

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

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

[7] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, 1990.

[8] D. A. Marcus, *Number Fields*, Springer, 1977.

[9] B. Širola, *Algebarske strukture*, skripta, https://web.math.pmf.unizg.hr/nastava/alg_prof/predavanja/ASpred.pdf

[10] T. Weston, *Algebraic Number Theory*, https://people.math.umass.edu/~weston/cn/notes.pdf

Sažetak

Neka je m cijeli broj koji nije potpuni kvadrat. Skup oblika $\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}$, uz standardne operacije zbrajanja i množenja u $\mathbb{C}$, čini polje i naziva se kvadratno polje. U radu se bavimo prstenima cijelih brojeva kvadratnih polja, to jest skupovima oblika $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$, za $m \equiv 2$ ili $3 \pmod 4$ i $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] = \left\{\frac{a+b\sqrt{m}}{2} : a, b \in \mathbb{Z},\ a \equiv b \pmod 2\right\}$, za $m \equiv 1 \pmod 4$, te problemom faktorizacije na ireducibilne faktore u tim prstenima.

Summary

Let m be an integer that is not a perfect square. A set of the form $\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}$, with standard addition and multiplication in $\mathbb{C}$, forms a field and is called a quadratic field. In the thesis, we deal with rings of integers of quadratic fields, that is, sets of the form $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \ : \ a, b \in \mathbb{Z}\}$, for $m \equiv 2$ or $3 \pmod 4$ and $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] = \left\{\frac{a+b\sqrt{m}}{2} \ : \ a, b \in Z,\ a \equiv b \pmod 2\right\}$, for $m \equiv 1 \pmod 4$, and with the factorization problem in these rings.

Životopis

Lucia Kurilovčan rođena je 26. kolovoza 1997. godine u Zagrebu u Republici Hrvatskoj. Pohađala je Osnovnu školu Velika Mlaka nakon čega upisuje IV. gimnaziju u Zagrebu. Tijekom školovanja pokazuje veliki interes za matematiku, fiziku i kemiju. 2016. godine upisuje integrirani sveučilišni studij Matematika i fizika; smjer nastavnički na Prirodoslovno-matematičkom fakultetu Sveučilišta u Zagrebu. Tijekom školovanja volonterski daje instrukcije. Od studenog 2023. godine radi kao nastavnik u Osnovoj školi Velika Mlaka. U slobodno vrijeme bavi se umjetničkim stvaralaštvom i proučavanjem psihologije.