Osnovne algebarske strukture i proširenja polja

Babok, Ema

Sveučilište Josipa Jurja Strossmayera u Osijeku

Fakultet primijenjene matematike i informatike

Sveučilišni diplomski studij Matematika
modul: financijska matematika i statistika

Osnovne algebarske strukture i proširenja polja

Diplomski rad

Mentor:
izv. prof. dr. sc. Ivan Soldo

Student:
Ema Babok

Osijek, 2024.

Sadržaj

1 | Uvod

Algebarske strukture su skupovi elemenata na kojima je definirana barem jedna operacija te su zadovoljena određena svojstva. Kada spominjemo operacije na skupovima, najprije se sjetimo operacije zbrajanja i množenja. Uzmemo li naizgled jednostavnu kvadratnu jednadžbu

$$y = x^2 + 1,$$

zanima nas kojem skupu pripadaju njena rješenja. Faktorizacija te jednadžbe

$$y = (x + \sqrt{-1})(x - \sqrt{-1})$$

daje motivaciju za proučavanje polja algebarskih brojeva.
Na početku naše razrade, objasnit ćemo osnovne algebarske strukture: grupe, prstene, ideale i polja. U trećem poglavlju definirat ćemo proširenje polja i veću pozornost posvetiti kvadratnom proširenju kao glavom cilju ovog rada. Kvadratno proširenje polja nastaje dodavanjem kvadratnog korijena nekog elementa polja. Centar našeg istraživanja bit će kvadratno proširenje polja racionalnih brojeva, to jest $\mathbb{Q}(\sqrt{d})$.
Nakon toga definirat ćemo algebarske brojeve i algebarske cijele brojeve. Pokazat ćemo da se traženje invertibilnih elemenata u realnim kvadratnim poljima svodi na rješavanje Pellovih jednadžbi. Definirat ćemo skalarne funkcije normu i trag koje će biti korisne u faktorizaciji algebarskih cijelih brojeva. Jedinstvenost faktorizacije svest će se na provedbu Euklidovog algoritma.

2 | Osnovne algebarske strukture

U ovom poglavlju definirat će se osnovni pojmovi potrebni za daljnju analizu. Definicije prstena, grupe, polja i ideala temelj su algebre, ali i ostalih grana matematike.

2.1 Grupe

Grupe su jednostavne, ali moćne strukture koje omogućuju razumijevanje složenijih matematičkih koncepata. Pojavljuju se u gotovo svim granama matematike, a najznačajniji utjecaj imaju u području algebre i teorije brojeva.

Definicija 1. *Neka je V neprazan skup. Binarna operacija na V je funkcija koja svakom uređenom paru elemenata iz V pridružuje element iz V, to jest*

$$(u, v) \mapsto u * v \in V, \quad \text{za sve } u, v \in V.$$

Kažemo da je V zatvoren s obzirom na operaciju $*$ i uređeni par $(V, *)$ nazivamo grupoid.

Primjer 1. *Uređen par $(\mathbb{N}, \cdot)$ je grupoid uz binarnu operaciju standardnog množenja. $(\mathbb{N}, -)$ nije grupoid jer razlika dva prirodna broja ne mora biti prirodan broj.*

Definicija 2. *Polugrupa je grupoid V u kome je zadana binarna operacija asocijativna.*

Primjer 2. *$(\mathbb{N}, +)$ je grupoid. $(\mathbb{Z}, -)$ je grupoid, ali nije polugrupa.*

Lijeva jedinica u grupoidu V je svaki element u za koji vrijedi $uc = c$, za sve $c \in V$. Desna jedinica u grupoidu V je svaki element v takav da je $cv = b$, za sve $c \in V$.

Propozicija 1 (vidjeti [9])**.** *Neka je V grupoid. Označimo s $\mathcal{L}(V)$ skup svih lijevih jedinica u V te s $\mathcal{R}(V)$ skup svih desnih jedinica u V. Pretpostavimo da je $\mathcal{L}(V) \neq \emptyset$ i $\mathcal{R}(V) \neq \emptyset$. Tada je $\mathcal{L}(V) = \mathcal{R}(V)$ i $|\mathcal{L}(V)| = 1$.*

Dokaz. Uzmimo dva elementa tako da vrijedi $u \in \mathcal{L}(V)$ i $v \in \mathcal{R}(V)$. Tada vrijedi $uv = u$ i $uv = v$ što implicira $u = v$, to jest $\mathcal{L}(V) = \mathcal{R}(V)$. Dakle, svaka lijeva ili desna jedinica istovremeno je i obostrana jedinica ili samo jedinica. Neka su $u_1, u_2 \in \mathcal{L}(V)$. Tada vrijedi $u_1 u_2 = u_2$ i $u_1 u_2 = u_1$ iz čega slijedi da je $u_1 = u_2$ pa zaključujemo da je $|\mathcal{L}(V)| = 1$. □

Jedini element skupa $\mathcal{L}(V) = \mathcal{R}(V)$ naziva se neutralni element, jedinica ili jedinični element grupoida V. Označava se s $1, e$ ili 0.

Definicija 3. *Monoid je polugrupa V s jedinicom, to jest neutralnim elementom.*

Ukoliko imamo multiplikaciju, inverz od $u \in V$ označavamo s u^{-1} dok u slučaju aditivne notacije inverz od u označavamo s $-u$.
Element $u \in V$ je invertibilan ukoliko ima inverz, to jest ako postoji u^{-1} takav da je $uu^{-1} = u^{-1}u = e$.

Definicija 4. *Grupa je monoid V u kojem je svaki element invertibilan.*

Komutativnu grupu nazivamo i Abelova grupa.

Primjer 3. *Promotrimo skup $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$. Pokazat ćemo da je $(\mathbb{Q}^*, \cdot)$ grupa.*

1. *Neka su $u, v \in \mathbb{Q}^*$. Tada je $u \cdot v \in \mathbb{Q}^*$. Budući da je $u \neq 0$ i $v \neq 0$, za njihov produkt također vrijedi $u \cdot v \neq 0$. Dakle, $u \cdot v \in \mathbb{Q}^*$, što znači da je skup $\mathbb{Q}^*$ zatvoren na standardnu operaciju množenja.*

2. *Za sve $u, v, w \in \mathbb{Q}^*$ vrijedi*

$$(u \cdot v) \cdot w = u \cdot (v \cdot w),$$

   što znači da je množenje u skupu $\mathbb{Q}^*$ asocijativno.

3. *Neutralni element za množenje u skupu $\mathbb{Q}^*$ je $1 \in \mathbb{Q}^*$ te vrijedi*

$$1 \cdot u = u \cdot 1 = u,$$

   za svaki $u \in \mathbb{Q}^*$.

4. *Za svaki element $u \in \mathbb{Q}^*$ postoji inverzni element takav da vrijedi*

$$u \cdot \frac{1}{u} = \frac{1}{u} \cdot u = 1.$$

   Dakle, svaki element iz $\mathbb{Q}^*$ ima svoj inverzni element iz $\mathbb{Q}^*$.

Uređen par $(\mathbb{Q}^*, \cdot)$ je grupa jer zadovoljava svojstva zatvorenosti, asocijativnosti te postojanja neutralnog i inverznog elementa. Kako za svaka dva elementa $u, v \in \mathbb{Q}^*$ vrijedi i komutativnost, to jest

$$u \cdot v = v \cdot u,$$

grupa $(\mathbb{Q}^*, \cdot)$ je i Abelova grupa.

Primjer 4. *Pogledajmo sada cijeli skup racionalnih brojeva $\mathbb{Q}$. Uređen par $(\mathbb{Q}, \cdot)$ nije grupa. Naime, svojstvo postojanja neutralnog elementa zahtijeva da svaki element u skupu mora imati inverzni element koji je također iz toga skupa. U skupu racionalnih brojeva, 0 nema svoj inverzni element, to jest, multiplikativni inverz.*

2.2 Prsteni

Prsteni su matematičke strukture koje proširuju koncept grupa tako što sadrže dodatne operacije koje omogućuju zbrajanje i množenje elemenata unutar iste strukture.

Definicija 5. *Neprazan skup V na kojem su definirane binarne operacije zbrajanja*

$$(u, v) \in V \times V \mapsto u + v,$$

i množenja

$$(u, v) \in V \times V \mapsto uv,$$

zovemo prsten ukoliko vrijede sljedeća svojstva:

1. *u odnosu na zbrajanje, V je Abelova grupa. Neutralni element u odnosu na zbrajanje označavamo s 0 i zovemo nula (ili nula prstena V);*
2. *u odnosu na množenje, V je polugrupa (množenje je asocijativno);*
3. *množenje slijeva i zdesna je distributivno u odnosu na zbrajanje, dakle za sve $u, v, w \in V$ vrijedi*

$$u \cdot (v + w) = u \cdot v + u \cdot w, \quad (u + v) \cdot w = u \cdot w + v \cdot w.$$

Kažemo da je prsten komutativan ukoliko je množenje u njemu komutativno.

V je prsten s jedinicom ukoliko je V u odnosu na množenje monoid, to jest postoji element $1 \in V$ takav da je $u \cdot 1 = 1 \cdot u$, za svaki element $u \in V$. Takav element je jedinstven i nazivamo ga jedinica prstena V.
U prstenu V vrijedi $0 = 1$ ako i samo ako je $V = 0$. Tada se V naziva trivijalni prsten.

Primjer 5 (vidjeti [2, Zadatak 2.1.1.]). *Pokažimo da je $(\mathbb{Z}, \oplus, \otimes)$, uz binarne operacije zbrajanja i množenja definirane s $u \oplus v = u + v + 1$ i $u \otimes v = u + v + uv$, komutativan prsten:*

- *zatvorenost vrijedi za obje operacije zbog zatvorenosti zbrajanja i množenja cijelih brojeva,*
- *za $u, v, w \in \mathbb{Z}$ vrijedi $(u \oplus v) \oplus w = u \oplus (v \oplus w)$, a to možemo pokazati raspisujući najprije lijevu pa desnu stranu:*

$$(u \oplus v) \oplus w = (u + v + 1) \oplus w = u + v + 1 + w + 1 = u + v + w + 2,$$

$$u \oplus (v \oplus w) = u \oplus (v + w + 1) = u + v + w + 1 + 1 = u + v + w + 2.$$

  Oba izraza daju isti rezultat $u + v + w + 2$, što pokazuje da je zbrajanje asocijativno.

- *za bilo koje elemente $u, v \in \mathbb{Z}$ zadovoljena je komutativnost zbrajanja, to jest vrijedi*

$$u \oplus v = u + v + 1 = v + u + 1 = v \oplus u,$$

- *kako bi bilo zadovoljeno postojanje neutralnog elementa, iz* $u \oplus e = u + e + 1$ *slijedi da je* $e = -1 \in \mathbb{Z}$ *desni neutralni element za zbrajanje. Zbog komutativnosti,* $e = -1 \in \mathbb{Z}$ *je ujedno i lijevi neutralni element za zbrajanje. Dakle,* $u \oplus e = e \oplus u = u$ *pa je* $e = -1 \in \mathbb{Z}$ *neutralni element za zbrajanje,*

- *iz* $-1 = u \oplus v = u + v + 1$ *slijedi da je* $v = -u - 2 \in \mathbb{Z}$ *desni inverz od* u*. Kako je zadovoljeno svojstvo komutativnosti,* $v = -u - 2 \in \mathbb{Z}$ *također je i lijevi inverz od* u*. Imamo* $e = u \oplus v = v \oplus u$*, što znači da je* $v = -u - 2 \in \mathbb{Z}$ *inverzni element od* $u \in \mathbb{Z}$*,*

- *za* $u, v, w \in \mathbb{Z}$ *vrijedi* $(u \otimes v) \otimes w = u \otimes (v \otimes w)$*, a to možemo pokazati raspisujući izraze:*

$$u \otimes (v \otimes w) = u \otimes (v + w + vw) = u + v + w + vw + uv + uw + uvw,$$

$$(u \otimes v) \otimes w = (u + v + uv) \otimes w = u + v + uv + w + uw + vw + uvw.$$

  Oba izraza daju isti rezultat što znači da je asocijativnost množenja zadovoljena,

- *za bilo koje elemente* $u, v \in \mathbb{Z}$ *zadovoljena je komutativnost množenja, to jest vrijedi*

$$u \otimes v = u + v + uv = v + u + uv = v \otimes u,$$

- *za* $u, v, w \in \mathbb{Z}$ *vrijedi distributivnost zdesna*

$$(u \oplus v) \otimes w = (u + v + 1) \otimes w = u + v + 1 + uw + vw + w,$$

  $u \otimes w \oplus v \otimes w = (u + w + uw) \oplus (v + w + vw) = u + w + uw + v + w + vw + 1.$

  Obzirom da je zadovoljena komutativnost množenja, vrijedi i distributivnost slijeva.

Pokazali smo da su zadovoljena sva svojstva iz Definicije 5 te zaključujemo da je $(\mathbb{Z}, \oplus, \otimes)$ *komutativan prsten. Da bi* $e \in \mathbb{Z}$ *bio jedinica prstena, mora vrijediti* $u \otimes e = e \otimes u = u$*. Lako zaključimo da je* $e = 0 \in \mathbb{Z}$ *jedinica prstena* $(\mathbb{Z}, \oplus, \otimes)$*.*

Primjer 6. *Pokažimo da skup* $\mathcal{S} = \{m + n\sqrt{2} + k\sqrt{3} : m, n, k \in \mathbb{Z}\}$ *nije prsten uz standardne binarne operacije zbrajanja i množenja realnih brojeva. Da bismo pokazali da skup* $\mathcal{S}$ *nije zatvoren na binarnu operaciju množenja, uzmimo neka dva elementa iz skupa* $\mathcal{S}$

$$u = 1 + \sqrt{2},$$
$$v = 1 + \sqrt{3}.$$

Pogledajmo njihov umnožak

$$u \cdot v = (1 + \sqrt{2})(1 + \sqrt{3}) = 1 + \sqrt{2} + \sqrt{3} + \sqrt{6}.$$

Rezultat $1 + \sqrt{2} + \sqrt{3} + \sqrt{6}$ *nije oblika* $m + n\sqrt{2} + k\sqrt{3}$ *jer sadrži broj* $\sqrt{6}$ *koji se ne može zapisati kao linearna kombinacija brojeva* $\sqrt{2}$ *i* $\sqrt{3}$ *sa cjelobrojnim koeficijentima. Budući da umnožak dva elementa skupa* $\mathcal{S}$ *ne pripada skupu* $\mathcal{S}$*, zaključujemo da* $\mathcal{S}$ *nije zatvoren na binarnu operaciju množenja. Stoga,* $\mathcal{S}$ *ne može biti prsten.*

Definicija 6. *Neka je V komutativan prsten s nulom 0_V. Pretpostavimo da postoji prirodan broj n takav da je $nu = 0$, za svaki element $u \in V$. Najmanji takav prirodan broj zovemo karakteristika prstena V i označavamo s $char(V)$. Ukoliko takav n ne postoji, kažemo da se radi o prstenu karakteristike nula, $char(V)$=0.*

Primjer 7. *Prsteni $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ imaju karakteristiku 0.*

Primjer 8. *Pogledajmo karakteristiku prstena $(\mathbb{Z}_4, +_4, \cdot_4)$ s elementima $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Karakteristika prstena $\mathbb{Z}_4$ je 4 jer je to najmanji broj za koji vrijedi $n \cdot u = 0$, za svaki $u \in \mathbb{Z}_4$. Općenito, za svaki $n \geq 2$, vrijedi $char(\mathbb{Z}_n) = n$.*

2.3 Ideali

Ideali su podskupovi prstena s posebnim svojstvima. Alat su za dublju analizu strukture prstena te omogućuju konstrukciju novih prstenova povezanih s originalnim. U ovom dijelu pretpostavlja se da je svaki prsten komutativan prsten s jedinicom.

Definicija 7. *Aditivna podgrupa I prstena V je lijevi ideal u prstenu V ako za $u \in I$ i $v \in V$ vrijedi $vu \in I$ dok za desni ideal vrijedi $uv \in I$. Ukoliko je I i lijevi i desni ideal u prstenu V, kažemo da je I obostrani ideal u V ili jednostavnije, samo ideal u V.*

Činjenicu da je I ideal u prstenu V označavamo s

$$I \trianglelefteq V.$$

Primjer 9. *Pokazat ćemo da skup svih parnih brojeva $2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}$ čini obostrani ideal u prstenu $\mathbb{Z}$. Neka je $u \in \mathbb{Z}$ i $v \in 2\mathbb{Z}$. Tada $u \cdot v$ pripada skupu $2\mathbb{Z}$ jer je umnožak cijelog broja i parnog broja ponovo paran broj. Na sličan način možemo zaključiti da je i $v \cdot u \in 2\mathbb{Z}$. Dolazimo do zaključka da je skup $2\mathbb{Z}$ obostrani ideal u $\mathbb{Z}$.*

Uvedimo pojam normalne podgrupe.

Definicija 8. *Neka je J grupa. Podgrupa $I \subseteq J$ naziva se normalna podgrupa ukoliko vrijedi $uI = Iu$, za sve $u \in J$.*

Najjednostavniji primjeri normalnih podgrupa su trivijalna podgrupa $\{e\}$ i cijela grupa J jer ove dvije podgrupe automatski zadovoljavaju uvjet komutativnosti sa svim elementima grupe.
U kontekstu prstena V, ideal I se može promatrati kao podgrupa aditivne grupe $(V, +)$. Po definiciji, ideal je zatvoren na zbrajanje i sadrži aditivne inverze što znači da zadovoljava uvjete podgrupe. Također, budući da ideal zadovoljava uvjete za lijevi i desni ideal on je automatski i normalna podgrupa aditivne grupe $(V, +)$. Na primjer, u prstenu $\mathbb{Z}$, ideal $2\mathbb{Z}$ je normalna podgrupa aditivne grupe $(\mathbb{Z}, +)$ jer je zatvoren na zbrajanje i sadrži aditivne inverze, to jest negacije parnih brojeva.
Uvedimo pojam lijeve i desne kongruencije modulo H, pri čemu je H podgrupa. One nam omogućuju uspoređivanje elemenata grupe na temelju njihovih odnosa prema podgrupi H te će nam biti ključne za definiranje kvocijentnih grupa.

Definicija 9. *Neka je G grupa i H podgrupa grupe G. Neka su $u, v \in G$. Kažemo da je u desno kongruentan v modulo H ako je*

$$v^{-1}u \in H.$$

Pišemo $u \sim_H v$.

Definicija 10. *Neka je G grupa i H podgrupa grupe G. Neka su $u, v \in G$. Kažemo da je u lijevo kongruentan v modulo H ako je*

$$uv^{-1} \in H.$$

Pišemo $u \ {}_H\!\sim v$.

Sljedeći teorem povezuje gornje relacije kongruencije s pojmom ekvivalencije i strukturom klase.

Teorem 1 (vidjeti [9, Normalne podgrupe i kvocijente grupe])**.** *Neka je H podgrupa grupe G.*

1. *"Biti desno kongruentan modulo H" je relacija ekvivalencije na G;*
2. *ako klasu ekvivalencije elemenata $u \in G$ označimo s $[u]$, tada je*

$$[u] = \{uh : h \in H\} = uH.$$

Pokažimo da su zadovoljena svojstva klase ekvivalencije:

- simetričnost: ako je $u \sim_H v$, tada je i $u \ {}_H\!\sim v$ jer $v^{-1}u \in H$ povlači $u^{-1}v \in H$;
- refleksivnost: svaki element $u \in G$ je desno kongruentan samom sebi jer je $u^{-1}u = e \in H$, gdje je e neutralni element grupe;
- tranzitivnost: neka su $u, v, w \in G$. Ako je $u \sim_H v$ i $v \sim_H w$, tada je $u \sim_H w$ jer je
$$(v^{-1}u) \cdot (w^{-1}v) = (w^{-1}u) \in H.$$

Analogno, relacija *biti lijevo kongruentan modulo H* također je relacija ekvivalencije na G.
Klase ekvivalencije $[u] = uH$, za $u \in G$, nazivaju se desne klase u G u odnosu na podgrupu H ili skraćeno desne H–klase u G. Grupa G jednaka je disjunktnoj uniji svih svojih desnih H-klasa. Klase ekvivalencije elemenata $u \in G, [u] = Hu$, nazivaju se lijeve H-klase u G. Također, može se reći da je grupa G disjunktna unija svih svojih lijevih H-klasa.
Neka je G grupa i H normalna podgrupa od G, a G/H skup svih H-klasa u G. Na skupu G/H definiramo binarnu operaciju kao

$$(uH)(vH) = uvH, \quad uv \in G. \tag{2.1}$$

Da bismo pokazali da je ova binarna operacija dobro definirana, moramo dokazati da rezultat uvH ne ovisi o odabiru predstavnika H-klasa. Uzmimo po dva predstavnika iz iste H-klase:

$$uH = u_1H,$$

$$vH = v_1H.$$

Tada postoje $h_1, h_2 \in H$ takvi da je $u^{-1}u_1 = h_1$ i $v^{-1}v_1 = h_2$. Slijedi $u_1 = uh_1$ i $v_1 = vh_2$. Provjerimo je li $uvH = u_1v_1H$:

$$u_1v_1 = uh_1vh_2 = uvv^{-1}h_1vh_2.$$

H je normalna podgrupa od G pa slijedi $v^{-1}h_1v \in H$ te postoji $h_3 \in H$ takav da je

$$u_1v_1 = uv(h_3h_2). \tag{2.2}$$

Kako su h_2, h_3 iz H, njihov produkt također mora biti iz H. Pomnožimo li slijeva jednakost (2.2) s $(uv)^{-1}$ dobivamo

$$(uv)^{-1}(u_1v_1) = h_3h_2,$$

to jest

$$(uv)^{-1}(u_1v_1) \in H.$$

Po Definiciji 9 slijedi $u_1v_1 \sim_H uv$ pa je $uvH = u_1v_1H$ što znači da binarna operacija ne ovisi o izboru predstavnika. Obzirom na ovakvo definiranu binarnu operaciju (2.1), skup G/H postaje grupa. Potrebno je još pokazati da su zadovoljena svojstva grupe:

- zatvorenost: za sve $uH, vH \in G/H$ vrijedi $uvH \in G/H$.
- asocijativnost: za sve $uH, vH, wH \in G/H$ vrijedi

$$\begin{aligned}((uH)(vH))(wH) &= (uvH)(wH)\\ &= uvwH\\ &= (uH)(vwH)\\ &= (uH)((vH)(wH)).\end{aligned}$$

- postojanje neutralnog elementa: neutralni element u G/H postoji i to je $eH = \{eh : h \in H\} = \{h : h \in H\} = H$ takav da vrijedi

$$(eH)(uH) = (uH)(eH) = (uH)H = uH, \quad \text{za svaki } uH \in G/H.$$

- postojanje inverznog elementa: za svaki $uH \in G/H$ postoji $(uH)^{-1} = u^{-1}H \in G/H$ takav da vrijedi

$$(uH)(uH)^{-1} = (uH)^{-1}(uH) = eH.$$

Definicija 11. *Grupa G/H naziva se kvocijentna grupa grupe G po normalnoj podgrupi H.*

Formirajmo kvocijentnu grupu V/I čiji su elementi skupovi oblika $\{u + I = u + v : v \in I\}$. Zbrajanje se definira kao $(u + I) + (v + I) = u + v + I, u, v \in V$, a množenje kao $(u + I)(v + I) = uv + I, u, v \in V$. Tako definirano množenje posjeduje svojstvo asocijativnosti i distributivnosti u odnosu na zbrajanju. Prema

tome, V/I čini prsten koji se naziva kvocijentni prsten prstena V po idealu I. Ukoliko je V prsten s jedinicom 1, onda je i V/I prsten s jedinicom $1+I$. Kvocijentni prsten V/I predstavlja novu strukturu koja zadržava osnovne operacije i osobine prstena, ali istovremeno *smanjuje* prsten V po idealu I. Ovakva struktura omogućuje rad s elementima prstena tako da uzima u obzir određene *izgubljene* elemente ili svojstva kroz ideal.

Primjer 10 (vidjeti [6, 3.7. Kvocijentna grupa]). *Neka je $G=\mathbb{Z}$ i $H=m\mathbb{Z}$, gdje je $m\in\mathbb{N}$. Koristeći činjenicu da je $m\mathbb{Z}$ normalna podgrupa od $\mathbb{Z}$ te da je $\mathbb{Z}$ Abelova grupa, možemo definirati kvocijentnu grupu $\mathbb{Z}/m\mathbb{Z}$ koja se naziva grupa klasa ostataka modulo m. Elementi te grupe su klase oblika*

$$\begin{aligned}[r] &= \{l\in\mathbb{Z} : l\equiv r \pmod m\}\\ &= \{l\in\mathbb{Z} : l-r \text{ djeljivo s } m\}\\ &= \{l\in\mathbb{Z} : l-r\in m\mathbb{Z}\}\\ &= \{l\in\mathbb{Z} : l\in r+m\mathbb{Z}\}\\ &= r+m\mathbb{Z},\end{aligned}$$

pri čemu je $r\in\mathbb{Z}$. Među klasama ima samo m različitih

$$\begin{aligned}[0] &= m\mathbb{Z}\\ [1] &= 1+m\mathbb{Z}\\ &\vdots\\ [m-1] &= (m-1)+m\mathbb{Z}.\end{aligned}$$

To možemo objasniti na sljedeći način

$$\begin{aligned}[m] &= m+m\mathbb{Z} = m(1+\mathbb{Z}) = m\mathbb{Z} = [0],\\ [m+1] &= (m+1)+m\mathbb{Z} = 1+(m+m\mathbb{Z}) = 1+m\mathbb{Z} = [1],\\ [-1] &= -1+m\mathbb{Z} = (m-1)-m+m\mathbb{Z} = (m-1)+m(-1\mathbb{Z})\\ &= (m-1)+m\mathbb{Z} = [m-1].\end{aligned}$$

Ovim postupkom pokazuje se da svi cijeli brojevi pripadaju jednoj od m različitih klasa $[0],[1],\ldots,[m-1]$ jer se svi ostali brojevi svode na jedan od ovih ostataka modulo m. Dakle, kvocijentna grupa je oblika

$$\mathbb{Z}/m\mathbb{Z} = \{m\mathbb{Z}, 1+m\mathbb{Z},\ldots,(m-1)+m\mathbb{Z}\} = \{[0],[1],\ldots,[m-1]\}.$$

Binarna operacija zbrajanja definirana je s

$$(u+m\mathbb{Z})+(v+m\mathbb{Z}) = u+v+m\mathbb{Z}, \text{ za sve } u,v\in\mathbb{Z}.$$

Definicija 12. *Neka je V prsten i I neki ideal. Skup $G\subseteq V$ je skup generatora od I ako je*

$$I = \langle G\rangle = (G) := \bigcap_{\substack{J\trianglelefteq V\\ G\subseteq J}} J,$$

odnosno I je najmanji ideal u V koji sadrži skup G.

Ukoliko gledamo skup generatora kao ideal, svaki element u tom idealu može se izraziti kao linearna kombinacija elemenata iz tog skupa generatora, pomnoženih odgovarajućim elementima prstena. Skup definiran na ovakav način, omogućuje reprezentaciju ideala pomoću manjeg broja elemenata što pojednostavljuje analizu i manipulaciju idealima u prstenu.

Primjer 11. *Primjer skupa generatora u prstenu može se ilustrirati kroz ideal od parnih brojeva unutar skupa cijelih brojeva. Neka je* $V = \mathbb{Z}$ *i* $I = 2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}$. *S* $G = \{2\}$ *označimo skup generatora od* I. *Možemo zapisati*

$$I = \langle G \rangle = (G) = 2\mathbb{Z}.$$

Ideal I *je najmanji ideal u* V *koji sadrži* G, *jer se svaki parni broj može zapisati kao umnožak broja* 2 *i nekog cijelog broja* k. *Dakle,* $2\mathbb{Z}$ *je ideal generiran skupom* G *koji sadrži samo jedan element* 2.

Definicija 13. *Ideal* I *u prstenu* V *je prost ideal ako je* $I \neq V$ *te iz* $u \cdot v \in I$ *slijedi* $u \in I$ *ili* $v \in I$.

U ovom svojstvu uočava se zatvorenost u odnosu na množenje. Ukoliko produkt dva elementa prstena V pripada idealu I, tada barem jedan od tih elemenata pripada idealu I. U daljnjem radu vidjet će se da ovaj pojam dobro generalizira pojam prostog broja.

Primjer 12. *U prstenu cijelih brojeva* $V = \mathbb{Z}$, *ideal* $I = 3\mathbb{Z}$ *je prost ideal. Pretpostavimo da su* u *i* v *neki cijeli brojevi, te da je* $uv \in 3\mathbb{Z}$. *Kako ideal* $3\mathbb{Z}$ *sadrži sve višekratnike broja* 3, *barem jedan od brojeva* u *i* v *mora biti djeljiv s* 3.

Primjer 13. *Neka je dan prsten cijelih brojeva,* $V = \mathbb{Z}$, *i ideal koji se sastoji od svih cijelih brojeva koji su djeljivi s 12, dakle* $I = 12\mathbb{Z}$. *Iz* $3 \cdot 8 = 24 \in (12)$, *slijedi* $3 \notin (12)$ *i* $8 \notin (12)$. *Zaključujemo da* $12\mathbb{Z}$ *nije prost ideal u prstenu* $\mathbb{Z}$.

Definicija 14. *Ideal* I *u prstenu* V *je glavni ideal ako postoji* $u \in V$ *takav da je* $I = (u)$.

Suštinski, ako postoji element unutar prstena čija linearna kombinacija sa svim elementima iz prstena gradi taj ideal, taj ideal se naziva glavnim idealom.

Primjer 14. *Pogledajmo ideal generiran brojem 5 u prstenu* $\mathbb{Z}$. *On je oblika*

$$(5) = \{5l : l \in \mathbb{Z}\}.$$

Ideal (5) *je glavni ideal u prstenu cijelih brojeva jer se može generirati jednim elementom, u ovom slučaju brojem 5. U prstenu* $\mathbb{Z}$ *svi ideali su glavni jer se svaki ideal može generirati nekim brojem* $l \in \mathbb{Z}$.

Sljedeća definicija govori o najvećem idealu u prstenu.

Definicija 15. *Ideal* I *u prstenu* V *je maksimalan ako je* $I \neq V$ *te ako ne postoji ideal* J *u prstenu* V *takav da je* $I \subsetneq J \subsetneq V$.

Jednostavnije rečeno, maksimalan ideal najveći je mogući ideal u odnosu na druge ideale, osim samog prstena V.

Primjer 15. *Pogledajmo prsten* $(\mathbb{Z}_{12}, +_{12}, \cdot_{12})$ *s elementima* $\mathbb{Z}_{12} = \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]\}$. *U prstenu* $\mathbb{Z}_{12}$ *maksimalni ideali su:*

- $(2) = \{[0], [2], [4], [6], [8], [10]\}$,
- $(3) = \{[0], [3], [6], [9]\}$,
- $(4) = \{[0], [4], [8]\}$.

Dakle, ideali (2), (3) *i* (4) *su generirani brojevima 2, 3 i 4, koji su djelitelji broja 12. U tom smislu, ne postoje drugi manji ideali koji ih mogu proširiti osim cijelog prstena* $\mathbb{Z}_{12}$. *Brojevi 5, 7 i 11 su relativno prosti s 12, što znači da je njihov najveći zajednički djelitelj s 12 jednak 1. Međutim, ovi brojevi ne mogu generirati ideale koji bi proširili postojeće maksimalne ideale* (2), (3) *i* (4) *jer ne obuhvaćaju elemente koje ti ideali sadrže. Tako, na primjer, ideal* (5) *sadrži samo elemente oblika* $\{5l : l \in \mathbb{Z}\}$ *i ne može obuhvatiti elemente ideala* (2), (3) *ili* (4).

Propozicija 2 (vidjeti [7, Korolar 3.1.]). *Svaki maksimalan ideal I u prstenu V je prost.*

Dokaz. Pretpostavimo suprotno, neka je I maksimalan ideal koji nije prost. Slijedi da postoje $u, v \in V, u \neq I, v \neq I$ takvi da je $uv \in I$. $I + (u), I + (v)$ su također ideali u V. Za $x \in I$ vrijedi $x = x + 0 \in I + (u)$ pa je $I \subseteq (u)$. Kako je $u = 0 + u \in I + (u)$, slijedi da je $u \in I + (u)$, ali zbog $u \neq I$ slijedi $I \subsetneq I + (u)$. I je maksimalan ideal pa imamo $I + (u) = V$. Analogno se zaključi $I + (v) = V$. Zbog komutativnosti iz V i $uv \in I$ slijedi

$$\begin{aligned}(u)(v) &= \{(ur_1)(ur_2) : r_1, r_2 \in V\} \\ &= \{(uv)r_1r_2 : r_1, r_2 \in V\} \subseteq \{(uv)r : r \in V\} \\ &= (uv) \subseteq I.\end{aligned}$$

Kako je $1 \in V$ te za svaki $r \in V$ vrijedi $r = r \cdot 1 \subset \{r_1r_2 : r_1, r_2 \in V\} = V \cdot V$, dobiva se $V \cdot V = V$. Slijedi

$$V = V \cdot V = (I + (u))(I + (v)) \subseteq I \cdot I + (u) \cdot I + I \cdot (v) + (u)(v) \subseteq I + I + I + I \subseteq I,$$

iz čega je $I = V$, što nije moguće. Slijedi da je maksimalan ideal I prost. □

Obrat prethodne propozicije ne vrijedi. Možemo uzeti $(0) \subset \mathbb{Z}$ što je prost ideal koji nije maksimalan.

2.4 Polja

Za početak ovog poglavlja podsjetimo se pojma invertibilnosti. Element u iz prstena s jedinicom V je invertibilan ukoliko postoji $v \in V$ takav da je $u \cdot v = v \cdot u = 1$. $V^\times$ označava grupu invertibilnih elemenata u V.

Definicija 16. *Komutativan prsten s jedinicom V je polje ako je svaki njegov ne-nul element invertibilan.*

Primjer 16. *Primjeri polja jesu polje realnih brojeva* $\mathbb{R}$*, polje kompleksnih brojeva* $\mathbb{C}$*, polje racionalnih brojeva* $\mathbb{Q}$*, uz standardne operacije zbrajanja i množenja, te polje algebarskih brojeva s kojim ćemo se susreti u daljnem radu. Skup* $\mathbb{Z}$ *nije polje. Polje zahtijeva da za svaki element postoji inverz u odnosu na množenje, što znači da svaki ne-nul element ima multiplikativni inverz. Primjerice, broj 3 nema multiplikativni inverz u skupu cijelih brojeva.*

Definicija 17. *Neka je* V *komutativan prsten s jedinicom* 1*,* $1 \neq 0$*. Element* $u \in V$*,* $u \neq 0$*, je djelitelj nule ako postoji* $v \in V$*,* $v \neq 0$*, takav da je* $u \cdot v = 0$*.*

Primjer 17. *2 i 5 su djelitelji nule u prstenu* $\mathbb{Z}_{10}$ *jer je* $2 \cdot_{10} 5 = 0$*.*

Definicija 18. *Komutativan prsten s jedinicom* 1*,* $1 \neq 0$*, u kojem ne postoje djelitelji nule naziva se integralna domena.*

$\mathbb{Z}_n$, pri čemu je n složeni broj, nije integralna domena, a to je pokazano u Primjeru 17 za $n = 10$. Broj n može se zapisati u obliku $n = k \cdot q$ gdje je $1 < k, q < n$ te vrijedi $k \cdot_n q = 0$ pri čemu su k i q djelitelji nule u $\mathbb{Z}_n$. Prsten cijelih brojeva $\mathbb{Z}$ je integralna domena jer ukoliko za dva cijela broja u i v vrijedi $u \cdot v = 0$ tada je $u = 0$ ili $v = 0$.
Uočimo sada razlike između prstena i integralne domene. U prstenu koji nije integralna domena ne možemo zaključiti da iz $u \cdot v = 0$ slijedi $u = 0$ ili $v = 0$.

Primjer 18. *Pogledajmo prsten* $\mathbb{Z}/6\mathbb{Z}$*. Elementi prstena su* $\{[0], [1], [2], [3], [4], [5]\}$*, gdje je svaki element klasa ekvivalencije cijelih brojeva modulo 6. Uzmimo* $[2]$ *i* $[3]$*:*

$$[2] \cdot [3] = [6] = [0] \in \mathbb{Z}/6\mathbb{Z}.$$

Imamo $[2] \cdot [3] = [0]$*, ali ni* $[2]$ *ni* $[3]$ *nisu nul-elementi u* $\mathbb{Z}/6\mathbb{Z}$*.*

Također, ne možemo zaključiti da iz $u \cdot v = uw, u \neq 0$, slijedi $v = w$. Ovo se događa jer u prstenu koji nije integralna domena može postojati u koje dijeli oba člana $u \cdot v$ i $u \cdot w$, ali v i w ne moraju biti jednaki.

Primjer 19. *Elementi prstena* $\mathbb{Z}/4\mathbb{Z}$ *su* $\{[0], [1], [2], [3]\}$*, pri čemu svaki element predstavlja klasu ekvivalencije cijelih brojeva modulo 4. Pogledajmo sljedeće:*

$$[2] \cdot [1] = [2],$$
$$[2] \cdot [3] = [2].$$

Iako smo množenjem dobili isti rezultat, klase ekvivalencije $[1]$ *i* $[3]$ *nisu jednake.*

Neka su sada u, v, w elementi neke integralne domene, $u \neq 0$, takvi da je $u \cdot v = u \cdot w$. Slijedi $u \cdot v - u \cdot w = 0$ pa jedino može biti $v - w = 0$, to jest $v = w$. Ovime se pokazalo da u integralnoj domeni možemo skraćivati.

Teorem 2 (vidjeti [9])**.** *Svaka konačna integralna domena je polje.*

Dokaz. Dokazat ćemo da svaki ne-nul element iz V ima multiplikativni inverz, a to povlači da je V polje. Neka je V neka konačna integralna domena i neka su $u_1, u_2, \ldots, u_n$ elementi iz V. Za fiksni $u \in V, u \neq 0$, promotrimo produkte $uu_1, uu_2, \ldots, uu_n$. Kako je $u \neq 0$, slijedi da je $u_i - u_j = 0$, to jest $u_i = u_j$. Zaključujemo da je svaki element u V oblika uu_i pa je tada i $1 = uu_i$, za neki $1 \leq i \leq n$, gdje 1 predstavlja jedinicu u V. Po definiciji, množenje u integralnoj domeni je komutativno pa vrijedi $u_i u = 1$, što znači da je u_i multiplikativni inverz od u. Slijedi da elementi prstena V čine Abelovu grupu obzirom na množenje te zaključujemo da je V polje. □

2.5 Faktorizacija u komutativnim prstenovima

Istražit ćemo mogućnosti rastavljanja elemenata prstena na jednostavnije komponente. U tom kontekstu, ireducibilni elementi zauzimaju značajno mjesto, budući da predstavljaju one elemente koji se ne mogu dodatno faktorizirati.

Definicija 19. *Neka je V komutativan prsten te $u, v \in V, u \neq 0$. Kaže se da u dijeli v i piše $u|v$ ako postoji $x \in V$ takav da je $v = ux$. Ukoliko vrijedi da $u|v$ i $v|u$ tada su elementi $u, v \in V$ asocirani.*

Primjer 20. *Uzmimo komutativan prsten $V = \mathbb{Z}$. Neka je $u = 4$ i $v = 12$. Da bi provjerili dijeli li 4 broj 12, tražimo $x \in \mathbb{Z}$ takav da je $12 = 4 \cdot x$. Očito je $x = 3$ pa slijedi da 4 dijeli 12. Da bi 12 bio djeljiv s 4, treba vrijediti $4 = 12 \cdot y$, za neki $y \in \mathbb{Z}$. U skupu cijelih brojeva, ne postoji broj y koji bi zadovoljavao tu jednadžbu. Dakle, 12 ne dijeli 4. Zaključujemo da brojevi $u = 4$ i $v = 12$ nisu asocirani.*

Definicija 20. *Neka je V komutativan prsten s jedinicom 1, $1 \neq 0$. Element $w \in V$ je ireducibilan ako vrijedi:*

- *w je različit od nule i w nije invertibilan,*
- *ako je $w = uv$ za neke $u, v \in V$, tada je ili u invertibilan ili v invertibilan.*

Ova definicija naglašava da se ireducibilni elementi ne mogu dalje rastaviti u faktore unutar prstena osim u slučajevima kada su ti faktori invertibilni. Za element koji nije ireducibilan kaže se da je reducibilan, što implicira da se može rastaviti na manje faktore. Drugim riječima, element iz prstena je ireducibilan ako nema faktorizaciju.

Primjer 21. *U polju cijelih brojeva $\mathbb{Z}$ izaberimo broj $w = 2$. Vrijedi $2 \neq 0$ te ne postoji $x \in \mathbb{Z}$ takav da je $2 \cdot x = 1$. Ako je $2 = uv, u, v \in \mathbb{Z}$, treba pokazati da je ili u ili v invertibilan. Moguće dekompozicije broja 2 u skupu $\mathbb{Z}$ su*

- $2 = 2 \cdot 1$ *(1 je invertibilan),*
- $2 = (-1) \cdot (-2)$ *(-1 je invertibilan),*
- $2 = 1 \cdot 2$ *(1 je invertibilan).*

Budući da se 2 može izraziti kao umnožak u i v gdje je barem jedan od njih invertibilan, zaključujemo da je 2 ireducibilan element u $\mathbb{Z}$. Općenito, u prstenu cijelih brojeva, ireducibilni elementi su prosti brojevi, budući da se oni ne mogu rastaviti na manje faktore. Broj 6 je reducibilan u prstenu cijelih brojeva $\mathbb{Z}$ jer ga možemo faktorizirati u obliku $6 = 2 \cdot 3$, pri čemu niti jedan od faktora nije invertibilan u skupu $\mathbb{Z}$.

Definicija 21. *Neka su $u_1, u_2, \ldots, u_n \in V$ takvi da je $u_i \neq 0$ barem za jedan $i \in 1, 2, \ldots, n$. Najveći zajednički djelitelj elemenata $u_1, u_2, \ldots, u_n$ je element $c \in V$ za koji vrijedi:*

- *c dijeli u_i, za sve $i \in \{1, 2, \ldots, n\}$,*
- *ako je $d \in V$ takav da d dijeli u_i za sve $i \in \{1, 2, \ldots, n\}$, tada d dijeli c.*

U daljnjem radu, najveći zajednički djelitelj brojeva označavat ćemo s $(u_1, u_2, \ldots, u_n)$.

Primjer 22. *Najveći zajednički djelitelji brojeva 5, 10 i 15 u prstenu $\mathbb{Z}$ je 5, što možemo zapisati kao $(5, 10, 15) = 5$. Općenito, najveći zajednički djelitelj elemenata koji nisu svi jednaki nuli jedinstven je do na množenje invertibilnim elementima, što znači da predstavlja klasu asociranosti. Ova klasa asociranosti za neki element c uključuje sve elemente koji su asocirani s c i označava se kao $\{uc : u \in V^\times\}$. Dakle, za naš konkretan slučaj možemo pisati $(5, 10, 15) = 5$, uz napomenu da je broj -5 asociran s brojem 5. Standardno se uzima samo pozitivni broj kao reprezentativni najveći zajednički djelitelj.*

Definirajmo sada prosti element, jednu od ključnih osobina u teoriji brojeva i algebri.

Definicija 22. *Neka je V komutativan prsten s jedinicom 1, $1 \neq 0$. Element $p \in V$ je prost ako vrijedi:*

- *p je različit od nule i p nije invertibilan,*
- *ako $p|uv$ za neke $u, v \in V$, tada $p|u$ ili $p|v$.*

Primjer 23. *Ukoliko imamo prost broj p, $p \in \mathbb{Z}$, tada su p i $-p$ ireducibilni i prosti elementi u tom prstenu. U prstenu $\mathbb{Z}_{10}$ vrijedi $5 =_{10} 3 \cdot 5$. 5 je prost broj, ali niti 5 niti 3 nisu invertibilni u $\mathbb{Z}_{10}$.*

Sljedeći teorem opisuje odnos između prostih i ireducibilnih elemenata u integralnoj domeni kao i njihovu povezanost s idealima.

Teorem 3 (vidjeti [9]). *Neka su p i c ne-nul elementi u integralnoj domeni V. Tada vrijedi:*

1. *element p je prost ako i samo ako je (p) prost ideal, pri čemu je (p) glavni ideal generiran elementom p, to jest $(p) = \{p \cdot v : v \in V\}$,*
2. *element c je ireducibilan ako i samo ako je ideal (c) maksimalan u skupu glavnih ideala u V,*
3. *svaki prost element u V je ireducibilan,*

4. *ako je V domena glavnih ideala, element p je prost ako i samo ako je reducibilan.*

Dokaz. 1. Pretpostavimo da je p prost broj te neka su u i v iz V takvi da vrijedi $uv \in (p)$. To znači da možemo zapisati $uv = px$, za neki $x \in V$, to jest da p dijeli uv. Budući da je p prost, slijedi da p dijeli u ili p dijeli v. Pretpostavimo sada da je ideal (p) prost. Ako p dijeli uv, tada vrijedi $uv \in (p)$. Budući da je (p) prost ideal, slijedi da je $u \in (p)$ ili $v \in (p)$, to jest da p dijeli u ili p dijeli v. Slijedi da je element p prost.

2. Neka je c ireducibilan element, a J glavni ideal koji sadrži (c). Potrebno je dokazati da vrijedi ili $J = (c)$ ili $J = V$. Budući je J glavni ideal, postoji element $d \in V$ takav da je $J = (d)$. Iz $(c) \subseteq (d)$ slijedi $c \in (d)$ pa možemo pisati $c = dx$, za neki $x \in V$. Kako je c ireducibilan, to povlači da je ili d invertibilan ili x invertibilan. Ako je d invertibilan, slijedi $I = (d) = V$. Ukoliko je x invertibilan, tada je $d = cx^{-1}$, što znači da su elementi c i d asocirani. Dakle, $(c) = (d) = J$.
   Sada pokažimo obrnutu tvrdnju. Pretpostavimo da je ideal (c) maksimalan ideal u skupu glavnih ideala u V i neka vrijedi $c = uv$. Tada je $c \in (u)$ i $c \in (v)$ pa iz toga slijedi $(c) \subseteq (u)$ i $(c) \subseteq (v)$. Ako u nije invertibilan, tada je $(u) \neq V$, što znači $(c) = (u)$ i $u \in (c)$. Dakle, postoji element $x \in V$ takav da je $u = cx$. Uvrstimo li ovaj izraz u $c = uv$, dobivamo $c = cxv$, što dalje implicira da je $xv = 1$ (V integralna domena). Iz toga slijedi da je v invertibilan, što znači da je c ireducibilan.

3. Neka je p prost element i neka vrijedi $p = uv$. Kako je $uv = p \cdot 1$ slijedi da p dijeli uv. Po definiciji prostog elementa, p dijeli u ili p dijeli v. Pretpostavimo da p dijeli u. To znači da postoji je $x \in V$ takav da je $u = px$. Zamjenom u jednadžbu $p = uv$, dobivamo $p = pxv$, što dalje implicira da je $xv = 1$. Dakle, v je invertibilan, što pokazuje da je p ireducibilan.

4. Budući da je domena glavnih ideala integralna domena, prvi smjer je već dokazan u dijelu 3.
   Dokažimo sada suprotni smjer. Pretpostavimo da je p ireducibilan element. Kako je V domena glavnih ideala, iz točke 2. slijedi da je ideal (p) maksimalan. Kao maksimalan ideal, (p) je ujedno i prost. Po točki 1., zaključujemo da je i element p prost.

□

Teorem 3 uspostavlja ključne veze između prostih i ireducibilnih elemenata u integralnim domenama, posebno u domenama glavnih ideala, gdje se pokazuje da su prosti elementi ekvivalentni ireducibilnim. Važnost Teorema 3 nadopunjuje sljedeća definicija koja uspostavlja jedinstvenost faktorizacije u integralnim domenama. Ova definicija naglašava da svaki neinvertibilni element može biti razložen na proizvode ireducibilnih elemenata, a ta razgradnja je jedinstvena, osim do permutacija i množenja invertibilnim elementima.

Definicija 23. *Integralna domena V je faktorijalan prsten ili domena jedinstvene faktorizacije ako vrijede sljedeća dva svojstva:*

- *svaki neinvertibilni element* $u \in V, u \neq 0$, *može se prikazati u obliku* $u = c_1c_2\cdots c_n$, *gdje su* $c_1, c_2, \ldots, c_n$ *ireducibilni,*
- *gornja faktorizacija jedinstvena je do na množenje pojedinih faktora invertibilnim elementima.*

Prvi dio prethodne definicije podrazumijeva da svaki ne-nul neinvertibilni element možemo prikazati u obliku produkta ireducibilnih elemenata. U prstenu $\mathbb{Z}$ rastavimo broj 15:

$$15 = 3 \cdot 5 = 5 \cdot 3 = (-3) \cdot (-5) = (-5) \cdot (-3).$$

Zbog permutacije iz definicije omogućena nam je zamjena poretka elemenata dok je veza pojedinih faktora ostvarena množenjem invertibilnim elementima.
Drugi dio Definicije 23 daje jedinstvenost takvog prikaza. Naime, ukoliko je $u = c_1c_2\cdots c_n$ i $u = d_1d_2\cdots d_m$, gdje su svi c_i, d_j ireducibilni, tada je $n = m$ te postoji permutacija $\sigma \in S_n$ takva da su c_i i $d_{\sigma(i)}$ asocirani za sve $i = 1, 2, \ldots, n$.

2.6 Faktorizacija u prstenima polinoma

Elementi prstena polinoma su polinomi i promatrat ćemo njihovu faktorizaciju. Prsten polinoma, poput $V[x]$, gdje je V komutativni prsten, omogućuje nam analizu i razlaganje polinoma na proste faktore, što igra ključnu ulogu u rješavanju algebarskih jednadžbi.

Neka je V proizvoljni komutativni prsten s jedinicom. Skup svih nizova $a = (a_0, a_1, \ldots)$ u V takvih da postoji n_0 pri čemu je $a_n = 0$, za sve $n \geq n_0$ označimo s $\mathcal{P}$. Zbrajanje i množenje na $\mathcal{P}$ definiramo kao

$$\begin{aligned}(a_o, a_1, a_2, \ldots) + (b_o, b_1, b_2, \ldots) &= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots),\\ (a_o, a_1, a_2, \ldots) \cdot (b_o, b_1, b_2, \ldots) &= (c_0, c_1, c_2, \ldots),\end{aligned}$$

gdje je

$$c_n = a_0b_n + a_1b_{n-1} + \cdots + a_{n-1}b_1 + a_nb_0 = \sum_{i=0}^{n} a_ib_{n-i}.$$

Ukoliko sa x označimo niz $(0, 1, 0, 0, \ldots)$, tada x nazivamo varijablom nad V. Neka je sada $a \in \mathcal{P}$ te uzmimo $n \in \mathbb{N}$ tako da je $a_k = 0$ za $k > n$. Tada je

$$\begin{aligned}a &= (a_0, a_1, \ldots, a_n, 0, 0, \ldots) = (a_0, a_1, \ldots, a_{n-1}, 0, 0, \ldots) + a_nx^n\\ &= \cdots = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n.\end{aligned}$$

Gornji prikaz elementa a je jedinstven. Naime, ukoliko imamo $a = b_0 + b_1x + \cdots + b_mx^m$, tada je $a_i = b_i = 0$ ako je $i > min(n, m)$ i $a_i = b_i$ za $i = 0, 1, \ldots, min(n, m)$, gdje su n i m stupnjevi polinoma a, to jest b.
Prsten $\mathcal{P}$ nazivamo prsten polinoma nad V u jednoj varijabli i označavamo ga s $V[x]$. Elemente prstena $V[x]$ nazivamo polinomima. Nula u prstenu $V[x]$ je nulpolinom $0 = (0, 0, \ldots)$, a jedinica je $1 = (1, 0, 0, \ldots)$. Nadalje, V će označavati faktorijalan prsten.

Napomena 1. *Prsten polinoma u više varijabli definira se induktivno.* $V[x_1, x_2] = (V[x_1])[x_2]$ *je prsten polinoma u dvije varijable. Može se promatrati kao polinom u varijabli* x_2 *čiji su koeficijenti polinomi u varijabli* x_1.

Svojstva kao što su djeljivost i invertibilnost u prstenima polinoma zapravo su direktno povezana s osobinama elemenata u komutativnom prstenu iz kojeg su polinomi sastavljeni. Možemo reći da se ova svojstva *nasljeđuju* kroz strukturu polinoma.

Definicija 24. *Polinom* $g \in V$ *dijeli polinom* $a \in V[x]$, *ako postoji polinom* $h \in V[x]$ *takav da je* $a = gh$.

Kažemo da je g djelitelj od a, a a da je višekratnik od g.

Primjer 24. *Neka je* $V = \mathbb{Z}[x]$ *te neka su* $g(x) = x - 3$ *i* $a(x) = x^2 - 9$ *iz* $\mathbb{Z}[x]$. *Polinom a možemo zapisati u obliku* $a(x) = x^2 - 9 = (x-3)(x+3)$. *Uočavamo da postoji polinom* $h(x) = (x+3) \in \mathbb{Z}[x]$ *takav da vrijedi* $a = g \cdot h$. *Dakle, polinom g dijeli polinom a.*

Definicija 25. *Polinom p je invertibilan u prstenu V ako postoji polinom q takav da je* $p \cdot q = 1$.

Primjer 25. *Prsten* $\mathbb{Z}_5[x]$ *je prsten polinoma s koeficijentima iz* $\mathbb{Z}_5$ *što znači da su svi koeficijenti polinoma elementi ostataka modulo 5. Polinom* $p(x) = 2$ *je invertibilan jer postoji polinom* $q(x) = 3$ *takav da vrijedi*

$$p(x) \cdot q(x) = 2 \cdot 3 = 6 \equiv 1 \pmod 5.$$

Sada ćemo bez dokaza navesti dva važna teorema u kojima su navedena neka svojstva prstena polinoma $V[x]$.

Teorem 4. (***Teorem o dijeljenju s ostatkom***) [*vidjeti* [5, *Teorem 11.1.*]]
Neka je V proizvoljno polje te neka su a *i* $g \neq 0$ *polinomi iz* $V[x]$. *Tada postoje jedinstveni polinomi* $q, r \in V[x]$ *takvi da je*

$$a = g \cdot q + r$$

i

$$\deg r < \deg g.$$

Primjer 26. *Pokažimo Teorem o dijeljenju s ostatkom na konkretnom primjeru. Neka je* $a(x) = 2x^2 - 5x - 1$ *i* $g(x) = x - 3$. *Podijelimo ova dva polinoma:*

$$\begin{array}{r} (\ 2x^2 - 5x - 1) \div (x-3) = 2x + 1 + \dfrac{2}{x-3} \\ \underline{-2x^2 + 6x} \\ x - 1 \\ \underline{-x + 3} \\ 2 \end{array}$$

Iz gornjeg računa može se iščitati da je $q(x) = 2x + 1$ *i* $r(x) = 2$. *Vrijedi* $\deg r = 0 < 1 = \deg g$ *što potvrđuje Teorem o dijeljenju s ostatkom.*

Teorem 5 (vidjeti [5, Teorem 11.3.]). *Neka je V polje i $a_1, a_2 \in V[x]$. Tada postoje $b_1, b_2 \in V[x]$ takvi da je*

$$b = b_1 a_1 + b_2 a_2$$

jedinstveni normirani najveći zajednički djelitelj od a_1 i a_2.

Najveći zajednički djelitelj dvaju polinoma možemo pronaći uzastopnom primjenom Teorema o dijeljenju s ostatkom za polinome (vidi Teorem 4). Dobiva se niz ostataka koji su polinomi sa sve manjim stupnjevima, a nakon konačnog broja koraka dolazimo do ostatka koji je nul-polinom. Tada se, slično kao u slučaju cijelih brojeva, može pokazati da je najveći zajednički djelitelj posljednji ostatak koji nije nul-polinom.

Primjer 27. *Želimo naći najveći zajednički djelitelj polinoma $a_1(x) = x^3 - 2x + 1$ i $a_2(x) = x^2 - 1$. Prvi korak je podijeliti $a_1(x)$ sa $a_2(x)$. Dobivamo:*

$$\begin{array}{r} (\quad x^3 - 2x + 1) \div (x^2 - 1) = x + \dfrac{-x+1}{x^2-1}. \\ \underline{-x^3 \quad + x} \\ \qquad -x + 1 \end{array}$$

Dakle, prvi ostatak je $r_1(x) = -x + 1$. U drugom koraku dijelimo $a_2(x)$ s $r_1(x)$:

$$\begin{array}{r} (\quad x^2 \qquad - 1) \div (-x + 1) = -x - 1. \\ \underline{-x^2 + x} \\ \qquad x - 1 \\ \underline{\qquad -x + 1} \\ \qquad 0 \end{array}$$

Drugi ostatak je $r_2(x) = 0$ i tu naš algoritam staje. Najveći zajednički djelitelj polinoma a_1 i a_2 je polinom $-x + 1$, to jest $(a_1(x), a_2(x)) = x - 1$.

Definicija 26. *Neka je $a \in V[x]$, $a = \sum_{i=0}^{n} u_i x^i$. Sadržaj polinoma a je najveći zajednički djelitelj koeficijenata $u_0, u_1, \ldots, u_n$. Označavamo ga s $C(a)$.*

Primjer 28. *Neka je dan polinom $a(x) = 12x^3 + 4x - 8 \in \mathbb{Z}[x]$. Sadržaj polinoma je $C(a) = 4$ ili $C(a) = -4$.*

Ukoliko koeficijenti polinoma nemaju pravog zajedničkog djelitelja, to jest ako su relativno prosti, kaže se da je polinom primitivan.

Primjer 29. *Polinom $b(x) = x^4 - 2x^3 + 3x - 5 \in \mathbb{Z}[x]$ je primitivan polinom jer su koeficijenti polinoma relativno prosti.*

Sljedeći teorem opisuje vezu između polinoma, kao prstena glavnih ideala, i faktorizacije.

Teorem 6 (vidjeti [9]). *Ako je V polje, onda je prsten polinoma $V[x]$ prsten glavnih ideala.*

Dokaz. Najprije ćemo pokazati da se svaki element iz $V[x]$ može prikazati u obliku produkta ireducibilnih elemenata. Neka je $f \in V[x]$. Ukoliko je f polinom stupnja nula, onda ova tvrdnja odmah slijedi jer je V faktorijalan prsten.
Uzmimo sada da je f polinom pozitivnog stupnja. Možemo ga prikazati kao $f = C(f)f_1$, gdje je $f_1 \in V[x]$ primitivan polinom. Kako je V faktorijalan prsten, tada je ili $C(f)$ invertibilan ili je $C(f_1) = c_1c_2 \cdots c_m$, gdje su svi elementi $c_1c_2 \cdots c_m$ ireducibilni u V. Tada su svi ti elementi ireducibilni i u $V[x]$ jer c_i možemo prikazati u obliku $a \cdot b, a, b \in V[x]$ pa a i b moraju biti polinomi stupnja nula. Dakle, $a, b \in V$ pa jedan od njih mora biti invertibilan.
Neka je K polje kvocijenata od V. Tada je $K[x]$ faktorijalan prsten i postoje ireducibilni elementi $p_1^*, p_2^*, \ldots, p_n^* \in K[x]$ takvi da je $f_1 = p_1^* p_2^* \cdots p_n^*$. Svaki $p_i^*, i = 1, 2, \ldots, n$, može se prikazati u obliku

$$p_i^* = \frac{a_i}{b_i} p_i,$$

gdje su $a_i, b_i \in V, b_i \neq 0$, a p_i je primitivan polinom iz $V[x]$. Pokažimo sada da je polinom p_i ireducibilan u $K[x]$. Pretpostavimo suprotno, neka p_i nije ireducibilan. Tada postoje $g, h \in K[x]$ koji nisu invertibilni takvi da je $p_i = g \cdot h, g, h \in V[x]$. Oba polinom g i h su stupnja barem 1 iz čega slijedi $p_i^* = \frac{a_i}{b_i} gh$, što nije moguće jer je p_i^* ireducibilan, a $\frac{a_i}{b_i} g$ i h su polinomi pozitivnog stupnja iz $K[x]$ koji nisu invertibilni. □

Kako je $V[x]$ prsten glavnih ideala, svaki ideal može biti rastavljen na temelju polinoma koji ga generira što nam omogućava faktorizaciju polinoma na proste faktore. Faktorizacija osigurava da se svaka komponenta, to jest faktor, može analizirati kao ideal čime se stvara izravna veza između razlaganja polinoma i strukture ideala.

Sljedeći teorem omogućuje da se svojstva sadržaja polinoma očuvaju tijekom množenja.

Teorem 7 (**Gaussova lema za polinome**). [*vidjeti* [5, *Teorem 11.4*]]
Ako su $u, v \in V[x]$, *tada je* $C(u \cdot v) = C(u)C(v)$. *Posebno, produkt primitivnih polinoma je primitivan.*

Dokaz. Zapišemo polinome u i v u obliku $u = C(u)u_1, v = C(v)v_1$, pri čemu su $u_1, v_1 \in V[x]$ primitivni polinomi. Tada vrijedi

$$C(u \cdot v) = C(C(u)C(v)u_1v_1) = C(u)C(v)C(u_1v_1),$$

što znači da je za dokaz dovoljno dokazati $C(u_1v_1) = 1$, to jest da je polinom u_1v_1 primitivan. Neka je

$$u_1 = \sum_{i=0}^{n} a_i x^i, \quad v_1 = \sum_{j=0}^{m} b_j x^j.$$

Tada je $u_1v_1 = \sum_{k=0}^{m+n} c_k x^k$, pri čemu je $c_k = u_0v_k + u_1v_{k-1} + \cdots + u_kv_0$. Pretpostavimo da u_1v_1 nije primitivan polinom. Tada $C(u_1v_1)$ nije invertibilan te se u

faktorijalnoj domeni V može prikazati kao produkt ireducibilnih elemenata koji su također i prosti elementi. Za $C(u_1v_1)$ odaberemo jednog predstavnika klase asociranosti najveće zajedničke mjere koeficijenata od u_1v_1. To znači da postoji ireducibilan element $p \in V$ takav da $p|c_k$ za sve $k = 0, 1, 2, \ldots, m+n$. u_1 je primitivan pa $p \nmid C(u_1)$ i postoji $i \in \{0, 1, \ldots, n\}$ takav da $p \nmid a_i$. Neka je s najmanji takav broj za koji vrijedi $p \nmid a_s$. Dakle, $p|a_0, a_1, \ldots, a_{s-1}$ i $p \nmid a_s$. Istim razmišljanjem dolazimo do zaključka da postoji $t \in \{0, 1, \ldots, m\}$ takav da $p|b_0, b_1, \ldots, b_{t-1}$ i $p \nmid b_t$. Primijetimo sljedeće:

$$c_{s+t} = a_0b_{s+t} + \cdots + a_{s-1}b_{t+1} + a_sb_t + a_{s+1}b_{t-1} + \cdots + a_{s+t}b_0.$$

Iz činjenice $p|a_0, \ldots, a_{s-1}$, slijedi da $p|a_0b_{s+t}, \ldots, a_{s-1}b_{t+1}$. Kako $p|b_0, \ldots, b_{t-1}$, slijedi da $p|a_{s+1}b_{t-1}, \ldots, a_{s+t}b_0$. Zaključujemo da $p|c_{s+t}$ što znači da p mora dijeliti i a_sb_t. Kako je p prost, mora vrijediti da $p|a_s$ ili $p|b_t$, što nije moguće te zaključujemo da je polinom u_1v_1 primitivan. □

Primjer 30. *Uzmimo polinome $u(x) = 2x + 4$ i $v(x) = 3x + 6$ iz prstena $\mathbb{Z}[x]$. Odredimo sadržaj oba polinoma:*

$$C(u) = 2, \quad C(v) = 3.$$

Dakle, ni u ni v nisu primitivni jer im sadržaji nisu jednaki 1. Pomnožimo polinome u i v:

$$w(x) = u(x) \cdot v(x) = (2x + 4)(3x + 6) = 6x^2 + 24x + 24.$$

Sadržaj produkta je $C(w) = 6$ što znači da produkt također nije primitivan, ali je ispunjeno $C(uv) = C(u)C(v)$.

Uvedimo sada definiciju ireducibilnosti za polinome.

Definicija 27. *Neka je V integralna domena. Za polinom $a \in V[x]$ kažemo da je reducibilan nad V ako se može prikazati u obliku $a = gh$, gdje su $g, h \in V[x] \setminus V$. Ukoliko nekonstantan polinom nije reducibilan, kažemo da je ireducibilan nad V.*

Primjer 31. *Polinom $a(x) = x^2 - 3$ ireducibilan je nad poljem $\mathbb{Q}$ jer se ne može faktorizirati u produkt polinoma nižeg stupnja s koeficijentima iz $\mathbb{Q}$. S druge strane, polinom je reducibilan nad polje $\mathbb{R}$ jer ga možemo zapisati kao $a(x) = (x - \sqrt{3})(x + \sqrt{3})$. U ovom rastavu, $\sqrt{3}$ i $-\sqrt{3}$ su realni brojevi pa je faktorizacija moguća unutar polja $\mathbb{R}$.*

Definicija 28. *Neka je V integralna domena. Za $\alpha \in V$ kažemo da je korijen ili nul-točka polinoma $a \in V[x]$ ako je $a(\alpha) = 0$.*

Ukoliko ovu definiciju povežemo s Teoremom o dijeljenju s ostatkom za polinome (vidi Teorem 4), slijedi da je α korijen od a ako i samo ako $(x - \alpha)$ dijeli $a(x)$.

Primjer 32. *Uzmimo polinom $a(x) = x^2 - 5x + 6$ iz $\mathbb{Z}[x]$. Faktorizacijom pronađimo nultočke polinoma $a(x)$:*

$$a(x) = x^2 - 5x + 6 = (x - 2)(x - 3).$$

Prema Teoremu o dijeljenju s ostatkom za polinome možemo zaključiti da $(x-2)$ *i* $(x-3)$ *dijele polinom a. Zaista, podijelimo li polinom a s polinomima* $(x-2)$ *i* $(x-3)$*, u oba slučaja dobivamo ostatak 0:*

$$\begin{array}{r} (\quad x^2-5x+6) \div (x-2) = x-3, \\ \underline{-x^2+2x} \\ \quad -3x+6 \\ \quad \underline{3x-6} \\ \quad\quad 0 \end{array}$$

$$\begin{array}{r} (\quad x^2-5x+6) \div (x-3) = x-2. \\ \underline{-x^2+3x} \\ \quad -2x+6 \\ \quad \underline{2x-6} \\ \quad\quad 0 \end{array}$$

Definicija 29. *Neka je* $a \in V[x]$*. Kažemo da je* $\alpha \in V$ *korijen kratnosti* $k \geq 1$ *od a ako* $(x-\alpha)^k$ *dijeli a u* $V[x]$*, ali* $(x-\alpha)^{k+1}$ *ne dijeli a u* $V[x]$*.*

Primjer 33. *Neka je* $a(x) = x^4 - 14x^3 + 60x^2 - 104x + 64$ *iz* $\mathbb{Z}[x]$*. Faktorizirajmo polinom*

$$\begin{aligned} a(x) &= x^4 - 14x^3 + 60x^2 - 104x + 64 = (x-2)^3(x-8) \\ &= (x-2)(x-2)(x-2)(x-8). \end{aligned}$$

Broj $\alpha = 2$ *je korijen polinoma a te pokažimo da mu je kratnost jednaka 3. Treba pokazati da* $(x-2)^3$ *dijeli a, ali* $(x-2)^4$ *ne dijeli a. Polinom a sadrži faktor* $(x-2)^3$ *pa zaključujemo da* $(x-2)^3$ *dijeli a. S druge strane, polinom a ne sadrži faktor* $(x-2)^4$ *jer postoje samo tri faktora* $(x-2)$ *pa* $(x-2)^4$ *ne dijeli a.*

Ekvivalent prostih brojeva u prstenima polinoma jesu ireducibilni polinomi. Svaki polinom pozitivnog stupnja $a \in V[x]$ možemo prikazati kao

$$a(x) = c(x-\alpha_1)^{n_1} \cdot \ldots \cdot (x-\alpha_k)^{n_k}, \tag{2.3}$$

gdje su $\alpha_1, \ldots, \alpha_k$ različiti korijeni, a $n_1, \ldots, n_k$ njihove kratnosti. c predstavlja konstantni koeficijent iz polja V kojeg zovemo vodeći koeficijent.

Definicija 30. *Polje* V *je algebarski zatvoreno ukoliko svaki polinom u* $V[x]$ *pozitivnog stupnja ima barem jednu nultočku u polju V.*

Iz Definicije 30 slijedi da je V algebarski zatvoreno polje ako i samo ako su ireducibilni polinomi u $V[x]$ upravo polinomi stupnja 1. Tada polinom $a \in V[x]$ ima točno $n_1 + \ldots + n_k = deg\, a$ korijena, uz uvjet da svaki korijen brojimo onoliko puta kolika mu je kratnost. Rastav (2.3) naziva se kanonski rastav polinoma a u prstenu $V[x]$.

Primjer 34. *Polje* $\mathbb{R}$ *nije algebarski zatvoreno. Primjerice, polinom* $a(x) = x^2 + 3$ *nema korijen u* $\mathbb{R}$*.*

Definirajmo sada polje ostataka modulo p.
Neka je p prost broj. S $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ definira se polje ostataka modulo p uz operacije zbrajanja i množenja modulo p. Za $u \in V$ definira se $\overline{u} \in \mathbb{F}_p$ takav da je $u \equiv \overline{u} \pmod{p}$. Neka je $a(x) = u_0 + u_1 x + \cdots + u_n x^n \in V[x]$ te neka je $\overline{a}$ redukcija od a modulo p, to jest polinom $\overline{a}(x) = \overline{u_0} + \overline{u_1} x + \cdots + \overline{u_n} x^n \in \mathbb{F}_p[x]$. Redukcijom polinoma a smanjuju se koeficijenti polinoma a na elemente polja ostataka modulo p.
Ova konstatacija potrebna nam je za sljedeći teorem koji govori o određenim svojstvima ireducibilnosti polinoma i vezi između ostataka pri dijeljenju polinoma s prostim brojevima.

Teorem 8 (**Schönemann**). [*vidjeti* [5, *Teorem 11.14.*]]
Neka je $a = g^n + ph \in \mathbb{Z}[x]$ normirani polinom gdje je n prirodan broj, p prost broj te $g, h \in \mathbb{Z}[x]$. Pretpostavimo da je $\overline{g}$ ireducibilan u $\mathbb{F}_p[x]$ te da $\overline{g}$ ne dijeli $\overline{h}$ u $\mathbb{F}_p[x]$. Tada je polinom a ireducibilan u $\mathbb{Z}[x]$.

Dokaz. Pretpostavimo da je $a = a_1 a_2$ netrivijalna faktorizacija od a u $\mathbb{Z}[x]$. Neka su polinomi a_1, a_2 normirani. Tada je $\overline{a} = \overline{a_1} \cdot \overline{a_2} \in \mathbb{F}_p[x]$. Polinomi $\overline{a} = \overline{g}^n$ i $\overline{g}$ ireducibilni su u $\mathbb{F}_p[x]$ pa postoje $u, v \in \mathbb{N}$ takvi da je $u + v = n$ te polinomi $h_1, h_2 \in \mathbb{Z}[x]$ tako da vrijedi

$$a_1 = g^u + ph_1, \quad a_2 = g^v + ph_2.$$

Iz $a = g^n + ph = (g^u + ph_1)(g^v + ph_2)$ slijedi da je

$$h = g^u h_2 + g^v h_1 + ph_1 h_2. \tag{2.4}$$

Pretpostavimo da je $u \leq v$. Tada izraz (2.4) postaje

$$h = g^u h_3 + ph_1 h_2, \tag{2.5}$$

pri čemu je $h_3 = h_2 + g^{v-u} h_1 \in \mathbb{Z}[x]$. Promotrimo sada redukciju izraza (2.5) modulo p,

$$\overline{h} = \overline{g}^u \cdot \overline{h_3}.$$

Zaključujemo da $\overline{g}$ dijeli $\overline{h}$ u $\mathbb{F}_p[x]$ što je u suprotnosti sa pretpostavkom teorema. □

Schönemannov teorem daje uvid u to kako transformacije na polinomima mogu očuvati svojstva ireducibilnosti. Važno je naglasiti da teorem vrijedi za prstene polinoma koji su nad poljem karakteristike 0.

Primjer 35. *Neka je dan polinom $a(x) = (x^2+1)^3 + 3(x+2) \in \mathbb{Z}[x]$ koji odgovara obliku polinoma iz Schönemannovog teorema. Pogledajmo kako se polinom $g(x) = x^2 + 1$ ponaša u polju $\mathbb{Z}_3[x]$. U polju $\mathbb{Z}_3[x]$ imamo $\overline{g}(x) = x^2 + 1$ jer je $1 = 1 \mod 3$. Polinom $\overline{g}$ je ireducibilan u polju $\mathbb{Z}_3[x]$ jer se ne može faktorizirati u polinome nižeg stupnja iz $\mathbb{Z}_3[x]$. Dalje, u polju $\mathbb{Z}_3[x]$ imamo $\overline{h}(x) = x + 2$. Polinom $\overline{g}$ ne dijeli polinom $\overline{h}$ u $\mathbb{Z}_3[x]$ jer je $\deg \overline{h} < \deg \overline{g}$. Prema postavljenim uvjetima, zaključujemo da je polinom $a(x) = (x^2+1)^3 + 3(x+2) \in \mathbb{Z}[x]$ ireducibilan u $\mathbb{Z}[x]$.*

Sljedeći kriterij jedan je od najpoznatijih i najkorisnijih kriterija za identifikaciju ireducibilnosti polinoma sa cjelobrojnim koeficijentima.

Teorem 9 (**Eisensteinov kriterij**). [*vidjeti* [5, *Teorem 11.15*]]
Neka je

$$a(x) = x^n + u_{n-1}x^{n-1} + \ldots + u_1x + u_0$$

normirani polinom s koeficijentima iz skupa $\mathbb{Z}$ *te neka je* p *prost broj za koji vrijedi da* p *dijeli* $u_0, u_1, \ldots, u_{n-1}$, *ali* p^2 *ne dijeli* u_0. *Tada je* a *ireducibilan polinom u* $\mathbb{Z}[x]$.

Dokaz. Polinom a možemo zapisati koristeći Schönemannov teorem (vidi Teorem 8) na sljedeći način

$$a = g^n + ph,$$

gdje je

$$g(x) = x, \quad h(x) = \frac{1}{p}(u_{n-1}x^{n-1} + \ldots + u_1x + u_0).$$

Time su zadovoljene pretpostavke Schönemannovog teorema, to jest $\frac{u_0}{p} \not\equiv 0 \pmod{p}$ i $\overline{g}(x) = x$ ne dijeli $\overline{h}(x)$. Zaključujemo da je a ireducibilan u $\mathbb{Z}[x]$. □

Primjer 36. *Pokažimo da polinom* $a(x) = x^3 + 6x^2 + 9x + 12$ *zadovoljava Eisensteinov kriterij. Prost broj* $p = 3$ *dijeli koeficijente* $6, 9$ *i* 12, *to jest dijeli sve koeficijente osim vodećeg. Kvadrat broja* p, $p^2 = 9$, *ne dijeli* 12, *to jest koeficijent uz slobodan član. Zaključujemo da je polinom* a *ireducibilan u* $\mathbb{Z}[x]$. *Zaista, prisjetimo li se definicije ireducibilnog polinoma, vidimo da se polinom* a *ne može faktorizirati u produkt polinoma nižeg stupnja s koeficijentima iz* $\mathbb{Z}[x]$. *To znači da je* a, *po Definiciji 27, ireducibilan u* $\mathbb{Z}[x]$.

3 | Proširenja polja

U Poglavlju 2 definiran je pojam polja kao jedno od najznačajnijih objekata u algebri. Ovo poglavlje objasnit će proširenje polja te na posljetku definirati kvadratno proširenje. Proširenje polja je koncept u algebri koji se odnosi na stvaranje većeg polja tako što se postojećem polju dodaju novi elementi. Ono omogućava rješavanje određenih problema čije rješenje nije bilo moguće unutar početnog polja.

3.1 Općenito o proširenjima polja

Definicija 31. *Neka su V i L polja, $V \subseteq L$, uz iste operacije. Tada je polje L proširenje polja V te je V potpolje od L. Ukoliko su V, L i M polja, $V \subseteq L \subseteq M$, uz iste operacije, kaže se da je L međupolje.*

Proširenja polja mogu se klasificirati prema različitim kriterijima, kao što su stupanj proširenja, algebarska i transcendentalna proširenja, te konačna i beskonačna proširenja. Ako je L proširenje polja V, tada L možemo promatrati kao vektorski prostor nad poljem V. Elementi polja L (vektori) čine Abelovu grupu obzirom na zbrajanje. Svaki vektor $a \in L$ možemo pomnožiti sa skalarom $\alpha \in V$ pri čemu je $\alpha a \in L$.
Algebarska proširenja nastaju dodavanjem korijena polinoma sa koeficijentima iz V, dok transcendentalna proširenja uključuju elemente koji nisu korijeni niti jednog polinoma iz V.

Definicija 32. *Neka je L proširenje polja V. Ukoliko je L konačnodimenzionalan vektorski prostor nad V, L je konačno proširenje polja V. Dimenzija tog vektorskog prostora naziva se stupanj proširenja i označava s $[L : V]$. Ukoliko L nije konačno proširenje polja V, piše se $[L : V] = \infty$.*

Primjer 37. *Polje kompleksnih brojeva $\mathbb{C}$ je proširenje polja $\mathbb{R}$ te je $[\mathbb{C} : \mathbb{R}] = 2$ budući da skup $\{1, i\}$ tvori jednu bazu od $\mathbb{C}$ nad $\mathbb{R}$. S druge strane, proširenje polja realnih brojeva nad racionalnim brojevima je beskonačno, to jest $[\mathbb{R} : \mathbb{Q}] = \infty$. Polje $\mathbb{R}$ sadrži beskonačno mnogo elemenata koji se ne mogu izraziti kao linearne kombinacije racionalnih brojeva, primjerice brojevi $\pi, e, \sqrt{3}, \ldots$. Dakle, ne postoji konačan skup elemenata iz $\mathbb{R}$ koji bi mogao tvoriti bazu za $\mathbb{R}$ nad $\mathbb{Q}$.*

Teorem 10 (vidjeti [7, Teorem 4.4.])**.** *Ako je L konačno proširenje polja V i M konačno proširenje polja L, tada je M konačno proširenje polja V i vrijedi*

$$[M : V] = [M : L][L : V].$$

Dokaz. Neka je $\{u_i : i \in I\}$ baza za L/M i $\{v_i : i \in J\}$ baza za M/L. Treba pokazati da skup $\{u_i v_j : i \in I, j \in J\}$ čini bazu proširenja za M/V. Neka je

$$x = \sum_j \alpha_j v_j,$$

pri čemu je $\alpha_j \in L$ i postoji konačno mnogo elemenata v_j različitih od nule. Možemo pisati

$$\alpha_j = \sum_i \gamma_{ij} u_i,$$

za neke ne-nul elemente $\gamma_{ij} \in V$. Kombiniranjem ova dva izraza dobivamo

$$x = \sum_j \left(\sum_i \gamma_{ij} u_i \right) v_j = \sum_i \sum_j \gamma_{ij} u_i v_j.$$

što znači da se $x \in M$ može izraziti kao linearna kombinacija vektora iz baze $\{a_i b_j\}$, a to povlači da skup $\{a_i b_j\}$ pokriva M nad V.
Pretpostavimo sada da je $\sum_{i,j} \gamma_{ij} u_i v_j = 0$, $\gamma_{ij} \in V$. Kako je $\{v_j\}$ baza za K/L, a time i linearno nezavisna nad L, slijedi da je $\sum_i \gamma_{ij} u_i = 0$, za svaki fiksni j. Tada koeficijent α_{ij} mora biti jednak nuli za sve i i j. Zbog nezavisnosti $u_i v_j$ nad V, oni kreiraju bazu za K/L. Imamo

$$[M : V] = |\{a_i b_j : i \in I, j \in J\}| = |\{u_i : i \in I\}| \cdot |\{v_i : i \in J\}| = [M : L] \cdot [L : V].$$

□

Za specijalni slučaj $[L : V] = 2$ kaže se da je to kvadratno proširenje. Ukoliko je $[L : V] = 3$ imamo kubno proširenje i tako dalje.

Kvadratno proširenje polja je proširenje polja koje nastaje dodavanjem kvadratnog korijena nekog elementa polja. Formalno, ako je V polje, i d element koji nije kvadrat u V, kvadratno proširenje dobije se tako da dodamo element $\sqrt{d}$ u polje V. Proširenje polja V koje je nastalo dodavanjem $\sqrt{d}$ u polje V, označava se s $V(\sqrt{d})$ te se sastoji od elemenata koji su oblika

$$V(\sqrt{d}) = \{u + v\sqrt{d} : u, v \in V\}. \tag{3.1}$$

Primjer 38. *Polje $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ je proširenje polja $\mathbb{Q}$ nastalo dodavanjem elemenata $\sqrt{2}$ i $\sqrt{3}$. Zanima nas kako izgledaju elementi tog polja te koliko iznos stupanj proširenja. Možemo pisati*

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}(\sqrt{2})\}. \tag{3.2}$$

Kako su $a, b \in \mathbb{Q}(\sqrt{2})$, oni su oblika $a = c + d\sqrt{2}, b = e + f\sqrt{2}$. Uvrstimo a i b u izraz (3.2):

$$a + b\sqrt{3} = c + d\sqrt{2} + (e + f\sqrt{2})\sqrt{3} = c + d\sqrt{2} + e\sqrt{3} + f\sqrt{6}.$$

Dakle, elementi polja $\mathbb{Q}(\sqrt{2},\sqrt{3})$ *su oblika*

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \{c + d\sqrt{2} + e\sqrt{3} + f\sqrt{6} : a,b,c,d \in \mathbb{Q}\}.$$

Stupanj proširenja je $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$ *jer je baza od* $\mathbb{Q}(\sqrt{2},\sqrt{3})$ *nad* $\mathbb{Q}$ $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$.

Sljedeća definicija opisuje klasu kvadratnog proširenja polja koja zauzima glavni interes u algebarskoj teoriji brojeva.

Definicija 33. *Svako međupolje* $\mathbb{Q} \subseteq V \subseteq \mathbb{C}$ *takvo da je* $[V : \mathbb{Q}]$ *konačno, zovemo polje algebarskih brojeva.*

Početak razvijanja algebarske teorije brojeva započeo je u 19. stoljeću iako su pojmovi ove teorije bili poznati i ranije. U ovom poglavlju definirat ćemo algebarske brojeve te ih primijeniti za rješavanje diofanskih jednadžbi.

Definicija 34. *Kompleksni broj* α *naziva se algebarski broj ako postoji polinom* $P(x)$ *s racionalnim koeficijentima, različit od nul-polinoma, takav da je* $P(\alpha) = 0$. *Ukoliko* α *nije algebarski, kažemo da je transcedentan.*

Ukoliko je svaki element iz L algebarski nad V, kažemo da je L algebarsko proširenje polja V.

U prethodnoj definiciji nužno je da P bude nekonstantan polinom jer bi za $P = 0$ vrijedilo $P(\alpha) = 0$ za svaki $\alpha \in L$. Također, polje V je algebarsko proširenje samog sebe jer je za $\alpha \in V$ polinom $P = x - \alpha \in V[x]$ i $P(\alpha) = 0$.

Primjer 39. *Realan broj* $\sqrt{3}$ *je algebarski nad poljem* $\mathbb{Q}$ *jer za polinom* $P = x^2 - 3 \in \mathbb{Q}(x)$ *vrijedi* $P(\sqrt{3}) = 0$.
Polje realnih brojeva $\mathbb{R}$ *nije algebarsko proširenje polja racionalnih brojeva* $\mathbb{Q}$ *jer možemo izabrati brojeve* π *ili* e *koji su transcedentni nad* $\mathbb{Q}$.
Polje kompleksnih brojeva $\mathbb{C}$ *je algebarsko proširenje polja realnih brojeva* $\mathbb{R}$. *Možemo uzeti neki kompleksni broj* $z = a + bi \in \mathbb{C}, a, b \in \mathbb{R}$ *i polinom* $P = (x-a)^2 + b^2 \in \mathbb{R}[x]$ *pri čemu će vrijediti* $P(z) = 0$.

Teorem 11 (vidjeti [1, Teorem 0.3.])**.** *Ako je proširenje polja* $[L : V]$ *konačno, onda je ono i algebarsko proširenje.*

Dokaz. Neka je $\alpha \in V$ proizvoljan i neka je $[V : K] = n, n \in \mathbb{N}$. Treba pokazati da postoji polinom $q(x) \in K[x]$ takav da vrijedi $q(\alpha) = 0$. Kako je V polje, vrijedi $1, a, a^2, \ldots, a^n \in V$. Također, $1, a, a^2, \ldots, a^n$ je skup od $n+1$ vektora koji se nalaze u n-dimenzionalnom vektorskom prostoru i oni su međusobno linearno zavisni nad K. To jest, postoje neki $k_0, k_1, \ldots, k_m \in K, m \leq n$ i $k_m \neq 0$, takvi da vrijedi

$$k_0 + k_1\alpha + \cdots + k_n\alpha^n = 0.$$

Dakle, proizvoljan broj α je algebarski nad K i time je propozicija dokazana. □

Definicija 35. *Polje* L *je konačno generirano proširenje polja* V *ako postoji* $n \in \mathbb{N}$ *te* $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ *takvi da je* $L = V(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Prethodna definicija sugerira da su elementi $\alpha_1, \alpha_2, \ldots, \alpha_n$ dovoljni da generiraju cijelo proširenje L iz V što znači da nema potrebe za dodavanjem dodatnih elemenata izvan njihove kombinacije. Također kaže da je proširenje L najmanje polje koje sadrži V i sve kombinacije elemenata $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Primjer 40. *Neka je $V = \mathbb{Q}$ i $L = \mathbb{Q}(\sqrt{3})$ proširenje polja generirano dodavanjem kvadratnog korijena broja 3. To znači da se L može zapisati kao $L = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$. Trebamo pokazati da postoji konačan skup elemenata u L čije linearne kombinacije s koeficijentima iz V tvore L. Budući da L sadrži samo elemente oblika $a + b\sqrt{3}$, gdje su a i b racionalni brojevi, možemo uzeti konačan skup $\mathcal{S} = \{1, \sqrt{3}\}$. Svaki element x iz L je oblika $x = a + b\sqrt{3}$. Također se može zapisati kao $x = 1 \cdot a + b \cdot \sqrt{3}$ što daje linearnu kombinaciju elemenata iz skupa $\mathcal{S}$ s koeficijentima iz $\mathbb{Q}$. Skup L je očito zatvoren za zbrajanje i množenje. Još je potrebno provjeriti da svaki element iz L ima inverz u L.*

$$\begin{aligned}(a + b\sqrt{3})^{-1} &= \frac{1}{a + b\sqrt{3}} = \frac{1}{a + b\sqrt{3}} \cdot \frac{a - b\sqrt{3}}{a - b\sqrt{3}} = \frac{a - b\sqrt{3}}{a^2 - 3b^2} \\ &= \frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{3}.\end{aligned}$$

Dakle, $(a + b\sqrt{3})^{-1}$ je oblika $x + y\sqrt{3}$, gdje su $x = \dfrac{a}{a^2 - 3b^2}$ i $y = \dfrac{b}{a^2 - 3b^2}$ iz polja $\mathbb{Q}$.

Na kraju ovog dijela navedimo i dokažimo rezultat koji povezuje konačna i algebarska proširenja polja.

Teorem 12 (vidjeti [7, Teorem 4.5.])**.** *Proširenje L polja V je konačno ako i samo ako je to proširenje algebarsko i konačno generirano.*

Dokaz. Neka je L konačno proširenje polja V te neka je $\alpha \in L$. Vektorski prostor L nad poljem V je konačnodimenzionalan pa skup $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ ne može biti linearno nezavisan za svaki $n \in \mathbb{N}$. Dakle, postoji prirodan broj n za koji je skup $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ linearno nezavisan. To znači da postoje koeficijenti $a_0, a_1, \ldots, a_n \in V$, gdje nisu svi jednaki nuli, tako da vrijedi

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0.$$

Dakle, za polinom $P = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 \in V[x]$ vrijedi $P \neq 0$ i $P(\alpha) = 0$ što implicira da je α algebarski nad V, a L algebarsko proširenje polja V. Neka je sada $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ baza vektorskog prostora L nad V. Tada je $V(\alpha_1, \alpha_2, \ldots, \alpha_m) \subseteq L$ jer je $V \cup \{\alpha_1, \alpha_2, \ldots, \alpha_m\} \subseteq L$. Kako je $L = \{a_1\alpha_1 + a_2\alpha_2 + \cdots + a_m\alpha_m : a_1, a_2, \ldots, a_m \in V\}$ te $\{a_1\alpha_1 + a_2\alpha_2 + \cdots + a_m\alpha_m : a_1, a_2, \ldots, a_m \in V\} \subseteq V(\alpha_1, \alpha_2, \ldots, \alpha_m)$ slijedi da je $L = V(\alpha_1, \alpha_2, \ldots, \alpha_m)$ pa je L konačno generirano proširenje polja V.
Pokažimo obrnuti smjer. Neka je sada L algebarsko i konačno generirano proširenje polja V te $\alpha_1, \alpha_2, \ldots, \alpha_m \in L$ takvi da je $L = V(\alpha_1, \alpha_2, \ldots, \alpha_m)$. Definiramo $V_0 = V, V_1 = V(\alpha_1)$ i $V_j = V(\alpha_1, \alpha_2, \ldots, \alpha_m)$, pri čemu je $j = 2, \ldots, m$. Tada je $V = V_0 \subseteq V_1 \subseteq V_2 \subseteq \cdots \subseteq V_{m-1} = L$ te

$$[L : V] = [V_m : V_{m-1}] \cdot [V_{m-1} : V_{m-2}] \cdots [V_2 : V_1] \cdot [V_1 : V_0].$$

Primijetimo da za svaki $j \in \{1, 2, \ldots, m\}$ vrijedi $V_j = V_{j-1}(\alpha_j)$. Kako je α_j algebarski nad V, a $V \subseteq V_{j-1}$, slijedi da je α_j također algebarski nad V_{j-1} što znači da je V_j konačno proširenje od V_{j-1}, to jest $[V_j : V_{j-1}] < \infty$. Prema tome, i $[L : V] < \infty$ pa je L konačno proširenje polja V. □

Primjer 41. *Pogledajmo proširenje polja* $\mathbb{Q}(\sqrt{2})$ *nad* $\mathbb{Q}$ *dobiveno dodavanjem elementa* $\sqrt{2}$ *polju* $\mathbb{Q}$. *Element* $\sqrt{2}$ *je algebarski nad poljem* $\mathbb{Q}$ *jer je korijen polinoma* $P(x) = x^2 - 2$ *iz prstena* $\mathbb{Q}[x]$. *Kako je svaki element iz* $\mathbb{Q}(\sqrt{2})$ *algebarski nad* $\mathbb{Q}$, *slijedi da je* $\mathbb{Q}(\sqrt{2})$ *algebarsko proširenje nad* $\mathbb{Q}$. *Proširenje polja je konačno jer je stupanj proširenja konačan, to jest* $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. *Također, proširenje je konačno generirano jer se može generirati jednim elementom* $\sqrt{2}$. *Dakle, polje* $\mathbb{Q}(\sqrt{2})$ *je konačno generirano proširenje polja* $\mathbb{Q}$.

3.2 Kvadratna proširenja

Kako je predmet izučavanja ovog rada proširenje polja, u daljnjem radu analizirat ćemo proširenja polja koja uključuju kvadratne korijene, što je važno u kontekstu algebarske teorije brojeva.
U okviru ovog poglavlja objasnili smo da je kvadratno proširenje polja V nastalo dodavanjem polju kvadratnog korijena nekog elementa iz tog polja te da su ti elementi oblika $\{u + v\sqrt{d} : u, v \in V\}$ (vidi (3.1)). Baza takvog kvadratnog proširenja polja V može se prikazati kao $\{1, \sqrt{d}\}$, gdje je d kvadratni korijen elementa d iz polja V.
Pokažimo kako se od kvadratnog proširenja može doći do kvadratnog polinoma koji nam je potreban za daljnju analizu.
Neka je $[L : V]$ proizvoljno kvadratno proširenje te neka 1 označava jedinicu u poljima L i V. Tada za bilo koji element $w \in L \backslash V$ imamo bazu $\{1, w\}$ od L kao vektorski prostor nad poljem V. Posebno je

$$L = \{a + bw | a, b \in V\}.$$

Kako je $w \in L$, onda je i $w^2 \in L$ pa postoje neki $a_0, b_0 \in V$ takvi da vrijedi

$$w^2 = a_0 + b_0 w$$

što povlači

$$w^2 - b_0 w - a_0 = 0.$$

Zaključuje se da je w nultočka polinoma $q(X) \in V[X]$ definiranog s

$$q(X) = X^2 - b_0 X - a_0.$$

Ovim se postupkom od kvadratnog proširenja dolazi do kvadratno polinoma.
Konstatirajmo obrnuti smjer. Ukoliko je dano polje realnih brojeva i kvadratni polinom $X^2 + 1 = 0$ čiji korijeni nisu realni brojevi, možemo proširiti polje realnih brojeva tako da dodamo imaginarnu jedinicu i kao korijen kvadratnog polinoma. Na taj način dobivamo prošireno polje kompleksnih brojeva $\overline{\mathbb{C}}$.
Ovaj primjer motivacija je za vrlo važan teorem koji se ovdje neće dokazivati.

Teorem 13 (**Osnovni teorem algebre**). [*vidjeti* [10, *Teorem 37.10.*]] *Neka je* $f(X) = a_n X^n + \cdots + a_1 X + a_0$ *polinom u prstenu* $\mathbb{C}[X]$ *stupnja* $n \geq 1$. *Tada postoji barem jedna nultočka tog polinoma u* $\mathbb{C}$.

Direktna posljedica Teorema 13 je ta da je polje kompleksnih brojeva algebarski zatvoreno.

Definicija 36. *Proširenje L polja V se naziva algebarskim zatvaračem polja V ako je proširenje L algebarsko nad V, a istovremeno je i algebarski zatvoreno.*

Drugim riječima, to je najmanje polje koje sadrži polje V i sve korijene svih polinoma s koeficijentima iz polja V. To znači da algebarski zatvarač sadrži sve elemente potrebne za rješavanje svih algebarskih jednadžbi nad V, bez dodavanja suvišnih elemenata. Standardna oznaka je $\overline{V}$.

Primjer 42. *Polje kompleksnih brojeva* $\mathbb{C}$ *algebarski je zatvarač polja realnih brojeva* $\mathbb{R}$, *a to opet znači da je* $\mathbb{C}$ *proširenje polja* $\mathbb{R}$. *Možemo pisati* $\mathbb{C} = \overline{\mathbb{R}}$.
Polja realnih $\mathbb{R}$ *i racionalnih brojeva* $\mathbb{Q}$ *nisu algebarski zatvorena, što znači da postoje polinomi sa koeficijentima iz tih polja koji nemaju rješenja unutar istih. Primjerice, polinom* $x^2 + 2 = 0$ *nema rješenje u* $\mathbb{R}$ *jer ne postoji realni broj čiji je kvadrat jednak* -2. *Da bi riješili ovu jednadžbu, potrebno je proširiti polje* $\mathbb{R}$.

Primjer 43. *Za primjer polinoma koji je ireducibilan nad poljem* $\mathbb{R}$ *ponovno možemo uzeti* $a(x) = x^2 + 1$ *jer nema nultočke u polju* $\mathbb{R}$. *Dakle, po definiciji, polinom a je ireducibilan. Nasuprot tome, kvadratni polinom* $b(x) = x^2 - 25$ *je reducibilan jer su mu nultočke 5 i -5 iz polja* $\mathbb{R}$.

3.3 Algebarski brojevi

Objasnili smo da su kvadratna proširenja posebna vrsta proširenja koja se formiraju dodavanjem polju korijena kvadratnog polinoma, čime se stvara nova algebarska struktura koja sadrži algebarske brojeve. Kroz analizu kvadratnih proširenja, istražit ćemo kako se algebarski brojevi mogu klasificirati prema njihovim karakteristikama, poput djeljivosti i normi.

U prethodnom poglavlju dana je definicija algebarskog broja (Definicija 34). Sljedeći teorem povezuje algebarske brojeve i polinome te osigurava da za svaki algebarski broj postoji jedinstveni minimalni polinom koji ga definira. Teorem također govori da se svaki algebarski broj može napisati kao nultočka određenog polinoma s cjelobrojnim koeficijentima te da taj polinom ima neka važna svojstva koja osiguravaju njegovu jedinstvenost i minimalnost.

Teorem 14 (vidjeti [5, Teorem 12.1.]). *Za svaki algebarski broj* α *postoji jedinstveni polinom*

$$P(x) = a_n x^n + \cdots + a_1 x + a_0 \tag{3.3}$$

sa svojstvima:

- $P(x) \in \mathbb{Z}[x]$,

- $a_n > 0$ *i* $(a_0, a_1, \ldots, a_n) = 1$,
- $P(\alpha) = 0$,
- *ako je* $P_0(x) \in \mathbb{Q}[x]$ *takav da je* $P_0(\alpha) = 0$, *onda* $P(x)$ *dijeli* $P_0(x)$ *u* $\mathbb{Q}[x]$,
- $P(x)$ *je ireducibilan nad* $\mathbb{Q}$.

Primjer 44. *U Primjeru 41 pokazali smo da je element* $\alpha = \sqrt{2}$ *algebarski nad poljem* $\mathbb{Q}(\sqrt{2})$ *jer je korijen normiranog polinoma* $P(x) = x^2 - 2 \in \mathbb{Z}[x]$. *Korijen polinoma* $P_0(x) = x^2 - 2 \in \mathbb{Q}[x]$ *je također element* $\sqrt{2}$ *što znači da polinom* $P(x)$ *dijeli polinom* $P_0(x)$ *jer su oni jednaki. Polinom* $P(x) = x^2 - 2$ *je ireducibilan nad poljem* $\mathbb{Q}$ *jer se ne može faktorizirati kao produkt polinoma prvog stupnja s racionalnim koeficijentima. Zadovoljeni su svi uvjeti iz Teorema 14, što znači da je* $P(x) = x^2 - 2$ *jedinstveni polinom za algebarski broj* α.

Definicija 37. *Cjelobrojni minimalni polinom algebarskog broja* α *je polinom* $P(x)$ *opisan u Teoremu 14. Minimalni polinom od* α *je polinom* $g(x) = \frac{1}{a_n}P(x)$, *dakle to je ireducibilni normirani polinom s racionalnim koeficijentima takav da je* $g(\alpha) = 0$. *Stupanj algebarskog broja je stupanj njegovog minimalnog polinoma.*

Drugim riječima, minimalni polinom je polinom najnižeg stupnja koji ima rješenje α.

Primjer 45. *U Primjeru 44 pronašli smo jedinstveni polinom* $P(x) = x^2 - 2$ *za algebarski broj* $\alpha = \sqrt{2}$. *Budući da je vodeći član promatranog polinoma* $a_n = 1$, *nije ga potrebno normirati, to jest, polinom* g *iz definicije odgovara polinomu* $P(x) = x^2 - 2$. *Od sada ćemo takav polinom zvati minimalni polinom algebarskog broja* α. *Stupanj algebarskog broja* α *je stupanj njegovog minimalnog polinoma. Dakle, vrijedi* $\deg P = 2$.

U ovom dijelu bit će definirano i dokazano ključno svojstvo skupa algebarskih brojeva, a to je da on čini polje. Za dokaz ovog teorema navest ćemo sljedeći teorem, koji ovdje neće biti dokazan.

Teorem 15 (vidjeti [5, Korolar 11.22.])**.** *Neka su* u *i* v *polinomi nad poljem* V *stupnja* n, *to jest* k, *te neka su* $\alpha_1, \ldots, \alpha_n$, *odnosno* $\beta_1, \ldots, \beta_k$ *njihovi korijeni. Tada su*

$$h_1(x) = \prod_{j=1}^{k}\prod_{i=1}^{n}(x - \alpha_i - \beta_j),$$

$$h_2(x) = \prod_{j=1}^{k}\prod_{i=1}^{n}(x - \alpha_i\beta_j),$$

polinomi s koeficijentima iz V.

Teorem 15 kaže da se mogu konstruirati novi polinomi, h_1 i h_2, s koeficijentima iz polja V ukoliko znamo korijene polinoma u i v.

Teorem 16 (vidjeti [5, Korolar 12.2.])**.** *Skup svih algebarskih brojeva čini polje.*

Dokaz. Neka su α i $\beta \neq 0$ algebarski brojevi. Potrebno je dokazati da su $\alpha + \beta, \alpha\beta, -\beta$ i β^{-1} također algebarski brojevi. Neka su $u(x)$ i $v(x)$ minimalni polinomi od α, to jest β. Direktnom primjenom Teorema 15 na polinome $u(x)$ i $v(x)$ zaključuje se da su $\alpha + \beta$ i $\alpha\beta$ algebarski brojevi jer su korijeni polinoma $h_1(x)$ i $h_2(x)$ čiji su koeficijenti iz $\mathbb{Q}$. Broj $-\beta$ je algebarski jer je korijen polinoma $v(-x)$, dok je broj β^{-1} algebarski jer je korijen polinoma $x^m v(\frac{1}{x})$, pri čemu je m stupanj polinoma v. Budući da su svi algebarski brojevi zatvoreni na operacije zbrajanja, množenja, negacije i inverzije, zaključujemo da skup svih algebarskih brojeva čini polje. □

3.4 Algebarski cijeli brojevi

Prije daljnje analize uvodimo definiciju za kvadratno slobodan broj koja će nam trebati u nastavku rada.

Definicija 38. *Za prirodan broj a kažemo da je kvadratno slobodan ako je 1 najveći kvadrat koji ga dijeli.*

Primjer 46. *Kvadratno slobodni brojevi su* $\pm 1, \pm 2, \pm 3, \pm 5, \pm 7$. *Primjeri brojeva koji nisu kvadratno slobodni su* $\pm 12, \pm 18, \pm 45, \pm 72$.

Definicija 39. *Algebarski broj α je algebarski cijeli broj ako njegov minimalni polinom ima cjelobrojne koeficijente, to jest ako je njegov minimalni polinom normiran.*

Drugim riječima, algebarski cijeli broj je algebarski broj koji je rješenje neke algebarske jednadžbe s cijelim koeficijentima, ali je istovremeno i cijeli broj.

Propozicija 3 (vidjeti [5, Propozicija 12.3.])**.** *U skupu racionalnih brojeva, jedini algebarski cijeli brojevi su cijeli brojevi.*

Dokaz. Svaki $z \in \mathbb{Z}$ je algebarski cijeli broj jer je korijen polinoma $u(x) = x - z$. Ukoliko imamo algebarski cijeli broj $\frac{z}{q}$, gdje je $(z, q) = 1$, tada je

$$\left(\frac{z}{q}\right)^n + a_{n-1}\left(\frac{z}{q}\right)^{n-1} + \cdots + a_0 = 0,$$

$$z^n + a_{n-1}qz^{n-1} + \cdots + a_0 q^n = 0.$$

Dakle, $q | z^n$, pa iz $(z, q) = 1$ slijedi da je $q = \pm 1$ što znači da je $\frac{z}{q} \in \mathbb{Z}$. □

Možemo reći da je skup algebarskih cijelih brojeva podskup algebarskih brojeva te da su oni također cijeli brojevi.
U Poglavlju 2.5 objasnili smo faktorizaciju u komutativnim prstenima. Kako smo se ograničili samo na kvadratna proširenja polja, postavlja se pitanje koje prstene analogne prstenu cijelih brojeva treba razmatrati u daljnjem radu. Odgovor na to pitanje daje nam sljedeća definicija.

Definicija 40. *Kvadratno polje $\mathbb{Q}(\sqrt{d})$ je skup svih brojeva oblika $u + v\sqrt{d}, u, v \in \mathbb{Q}$ uz standardne operacije zbrajanja i množenja kompleksnih brojeva pri čemu je d kvadratno slobodan cijeli broj i $d \neq 1$.*

U daljnjem tekstu opisat ćemo kada su dva kvadratna polja jednaka.

Propozicija 4 (vidjeti [4, Propozicija 2.]). *Neka su $V_1 = \mathbb{Q}(\sqrt{d_1})$ i $V_2 = \mathbb{Q}(\sqrt{d_2})$ kvadratna polja. Tada vrijedi $V_1 = V_2$ ako i samo ako je $\frac{d_1}{d_2}$ kvadrat nekog racionalnog broja.*

Dokaz. Ako je $V_1 = V_2$, onda je $\sqrt{d_1} \in V_2 = \mathbb{Q}(\sqrt{d_2})$ pa možemo pisati $\sqrt{d_1} = u + v\sqrt{d_2}, u, v \in \mathbb{Q}$. Kvadriramo li tu jednakost, dobivamo

$$d_1 = u^2 + 2uv\sqrt{d_2} + v^2 d_2.$$

Dakle, mora vrijedi

$$d_1 = u^2 + v^2 d_2, \quad 2uv = 0.$$

Slijedi da je ili $u = 0$ ili $v = 0$. Ukoliko je $v = 0$ dobivamo $d_1 = u^2$, a to je kontradikcija s pretpostavkom da d_1 nije potpun kvadrat. Ostaje nam slučaj $u = 0$ te vrijedi $\frac{d_1}{d_2} = v^2$.
Pokažimo obrat. Ako je $\frac{d_1}{d_2} = v^2, v \in \mathbb{Q}$, onda je $d_1 = v^2 d_2$. Korjenujemo li prethodni izraz, dobivamo

$$\sqrt{d_1} = v\sqrt{d_2}, \quad \sqrt{d_2} = \frac{1}{v}\sqrt{d_1}.$$

Dakle,

$$e + f\sqrt{d_1} = e + yf\sqrt{d_2}, \quad s + t\sqrt{d_2} = s + \frac{t}{v}\sqrt{d_1}.$$

Slijedi da je $V_1 \subseteq V_2$ i $V_2 \subseteq V_1$ što povlači jednakost polja V_1 i V_2. □

Primjer 47. *Neka su $d_1 = 1$ i $d_2 = 9$. Tada imamo*

$$\frac{d_1}{d_2} = \frac{1}{9} = \left(\frac{1}{3}\right)^2.$$

Obzirom da je $\frac{d_1}{d_2}$ kvadrat racionalnog broja, možemo pisati

$$V_1 = \mathbb{Q}(\sqrt{1}) = \mathbb{Q}(1) = \mathbb{Q},$$
$$V_2 = \mathbb{Q}(\sqrt{9}) = \mathbb{Q}(9) = \mathbb{Q}.$$

Dakle, u polje $\mathbb{Q}$ ne dodajemo nove elemente jer se i 1 i 9 već nalaze unutar polja $\mathbb{Q}$ i zato je $V_1 = V_2$.

Definicija 41. *Funkcija $N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ definirana s*

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

naziva se norma u $\mathbb{Q}(\sqrt{d})$.

Kako je $\alpha = u + v\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, element $\overline{\alpha} = u - v\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ naziva se konjugirani element od α.

Definicija 42. *Funkciju* $Tr : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ *definiranu s*

$$Tr(\alpha) = \alpha + \overline{\alpha}$$

zovemo trag u $\mathbb{Q}(\sqrt{d})$.

Teorem 17 (vidjeti [5, Teorem 12.5.])**.** *Vrijedi sljedeće:*

1. $N(\alpha\beta) = N(\alpha)N(\beta)$,
2. $N(\alpha) = 0$ *ako i samo ako je* $\alpha = 0$,
3. *ako je* α *algebarski cijeli broj u* $\mathbb{Q}(\sqrt{d})$, *onda je* $N(\alpha) \in \mathbb{Z}$,
4. *algebarski cijeli broj* $\epsilon \in \mathbb{Q}(\sqrt{d})$ *je jedinica ako i samo ako je* $N(\epsilon) = \pm 1$.

Dokaz. 1. Neka je $\alpha = u + v\sqrt{d}, \beta = m + n\sqrt{d}$. Tada je

$$\begin{aligned}\overline{\alpha\beta} &= \overline{(um + vnd + (un + vm)\sqrt{d})} = um + vnd - (un + vm)\sqrt{d} \\ &= (u - v\sqrt{d})(m - n\sqrt{d}) \\ &= \overline{\alpha} \cdot \overline{\beta}\end{aligned}$$

Imamo

$$N(\alpha\beta) = \alpha\beta\overline{\alpha}\overline{\beta} = \alpha\beta\overline{\alpha}\overline{\beta} = (\alpha\overline{\alpha})(\beta\overline{\beta}) = N(\alpha)N(\beta).$$

2. Ako je $\alpha = 0$, tada je i $\overline{\alpha} = 0$ i $N(\alpha) = 0$. Ukoliko je $N(\alpha) = 0$, onda je $\alpha\overline{\alpha} = 0$, što povlači $\alpha = 0$ ili $\overline{\alpha} = 0$. Iz $\overline{\alpha} = 0$ slijedi $\alpha = 0$.

3. Neka je $\alpha = u + v\sqrt{d}, u, v \in \mathbb{Q}$ algebarski cijeli broj. Tada je on rješenje kvadratne jednadžbe $x^2 + px + q = 0$, gdje su $p, q \in \mathbb{Z}$. Norma od α je oblika $N(\alpha) = \alpha \cdot \overline{\alpha} = u^2 - dv^2$. Želimo pokazati da je $N(\alpha)$ cijeli broj. Prema Osnovnom teoremu algebre znamo da navedeni polinom ima dvije nultočke, α i $\overline{\alpha}$. To znači

$$x^2 + px + q = (x - (u + v\sqrt{d}))(x + (u + v\sqrt{d})),$$

iz čega slijedi

$$p = -2u, \quad q = u^2 - dv^2.$$

Budući da je p cijeli broj, tada je i $2u \in \mathbb{Z}$. Kako je $q \in \mathbb{Z}$ i $u \in \mathbb{Z}$, i dv^2 mora biti cijeli broj. Znamo da je d kvadratno slobodan broj, a tada iz $dv^2 \in \mathbb{Z}$ slijedi $v^2 \in \mathbb{Z}$, to jest $v \in \mathbb{Z}$. Zaključujemo da je norma od α cijeli broj.

4. Ukoliko je ϵ jedinica, tada je $N(\epsilon)N(\frac{1}{\epsilon}) = N(1) = 1$. Kako su $N(\epsilon)$ i $N(\frac{1}{\epsilon})$ cijeli brojevi, to povlači da je ϵ jedinica.
Obratno, ako je $N(\epsilon) = \pm 1$, tada je $\epsilon\overline{\epsilon} = \pm 1$, pa je $\frac{1}{\epsilon} = \pm\overline{\epsilon}$ algebarski cijeli broj, a to opet znači da je ϵ jedinica.

□

Primjer 48. *Pokažimo svojstvo $N(\alpha\beta) = N(\alpha)N(\beta)$ na konkretnom primjeru. Neka su $\alpha = 1+\sqrt{2}$ i $\beta = 2-\sqrt{2}$. Izračunajmo norme brojeva α i β:*

$$N(\alpha) = \alpha \cdot \overline{\alpha} = (1+\sqrt{2})(1-\sqrt{2}) = 1^2 - (\sqrt{2})^2 = 1-2 = -1,$$

$$N(\beta) = \beta \cdot \overline{\beta} = (2-\sqrt{2})(2+\sqrt{2}) = 2^2 - (\sqrt{2})^2 = 4-2 = 2.$$

Pogledajmo produkt $\alpha\beta$:

$$\alpha\beta = (1+\sqrt{2})(2-\sqrt{2}) = 2-\sqrt{2}+2\sqrt{2}-(\sqrt{2})^2 = \sqrt{2}.$$

Sada izračunajmo normu od $\alpha\beta = \sqrt{2}$:

$$N(\alpha\beta) = (\sqrt{2})(-\sqrt{2}) = -2.$$

Dakle, $N(\alpha)N(\beta) = -1 \cdot 2 = -2$, što je jednako $N(\alpha\beta) = -2$.

Primjer 49. *Pokažimo da je norma algebarskog cijelog broja α u kvadratnom proširenju $\mathbb{Q}(\sqrt{d})$ cijeli broj. Neka je $d = 2$ i $\alpha = 5+\sqrt{2}$ algebarski cijeli broj u proširenju $\mathbb{Q}(\sqrt{2})$. Izračunajmo mu normu:*

$$N(\alpha) = (5+\sqrt{2})(5-\sqrt{2}) = 5^2 - (\sqrt{2})^2 = 25-2 = 23.$$

Dakle, norma broja α je $N(\alpha) = 23$, što je cijeli broj.

Propozicija 5 (vidjeti [4, Propozicija 4.]). *Ako je $\alpha \in \mathbb{Q}(\sqrt{d})$, tada su $N(\alpha)$ i $Tr(\alpha)$ cijeli brojevi.*

Dokaz. Kako je α algebarski cijeli broj, postoje brojevi $a_i \in \mathbb{Z}$ takvi da je

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n = 0.$$

Konjugiramo li prethodni izraz, dobivamo da je i $\overline{\alpha}$ algebarski cijeli broj. Iz činjenice da su zbroj i produkt dva algebarska cijela broja daje ponovno algebarski cijeli broj slijedi da su $N(\alpha) = \alpha \cdot \overline{\alpha}$ i $Tr(\alpha) = \alpha + \overline{\alpha}$ algebarski cijeli brojevi. Prema Propoziciji 3 vrijedi tvrdnja da su norma i trag cijeli brojevi. □

Specifično polje $\mathbb{Q}(\sqrt{-1})$ naziva se polje Gaussovih brojeva. Njegovi elementi su oblika $u+vi$ te vrijedi $N(\alpha) = u^2+v^2$.

Teorem 18 (vidjeti [5, Teorem 12.4.]). *Ako je $d \equiv 2$ ili $3 \pmod 4$, onda su algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ oblika $u+v\sqrt{d}$, $u,v \in \mathbb{Z}$. Ako je $d \equiv 1 \pmod 4$, onda su algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ oblika $s+t\cdot\dfrac{1+\sqrt{d}}{2}, s,t \in \mathbb{Z}$.*

Dokaz. Neka je $\alpha = u+v\sqrt{d}$ algebarski cijeli broj u $\mathbb{Q}(\sqrt{d})$ te neka je $a = 2u, b = 2v, c = N(\alpha) = u^2 - dv^2$. Slijedi da je α nultočka polinoma $f(x) = x^2 - ax + c$. Dakle, racionalni brojevi a i c moraju biti cijeli. Iz $db^2 = a^2 - 4c$ i činjenice da je d kvadratno slobodan broj, slijedi da je i $b \in \mathbb{Z}$.
Uzmimo sada $d \equiv 2$ ili $3 \pmod 4$. Iz $a^2 \equiv b^2 d \pmod 4$, $a^2 \equiv 0$ ili $1 \pmod 4$, $b^2 d \equiv 0, 2$ ili $3 \pmod 4$, slijedi da su a i b parni brojevi te da su $u, v \in \mathbb{Z}$.
Ukoliko je $d \equiv 1 \pmod 4$, iz $a^2 \equiv b^2 \pmod 4$ slijedi da su a i b iste parnosti. Tada je broj $u - v = \frac{1}{2}(a-b)$ cijeli broj. Uvedemo li oznake $s = u - v, t = 2v$, dobivamo da su $s, t \in \mathbb{Z}$ i $u + v\sqrt{d} = s + t \cdot \frac{1+\sqrt{d}}{2}$. □

Primjer 50. *Primjerice, za broj 7 vrijedi* $7 \equiv 3 \pmod 4$. *Stoga su algebarski cijeli brojevi u* $\mathbb{Q}(\sqrt{7})$ *oblika* $u + v\sqrt{7}$, *gdje su* $u, v \in \mathbb{Z}$. *Primjeri algebarskih cijelih brojeva u ovom proširenju uključuju, na primjer, brojeve* $3 + 2\sqrt{7}$ *i* $-1 + 4\sqrt{7}$. *Analogno, uzmimo* $d = 13 \equiv 1 \pmod 4$. *Algebarski cijeli brojevi u* $\mathbb{Q}(\sqrt{13})$ *imaju oblik* $s + t \cdot \dfrac{1+\sqrt{d}}{2}, s, t \in \mathbb{Z}$. *Primjeri algebarskih cijelih brojeva u* $\mathbb{Q}(\sqrt{13})$ *su* $5 + 7 \cdot \dfrac{1+\sqrt{13}}{2}$ *i* $4 \cdot \dfrac{1+\sqrt{13}}{2}$.

Može se reći da su svi algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ oblika $u + v\sqrt{d}$, $u, v \in \mathbb{Z}$, a ako je $d \equiv 1 \pmod 4$, tada su to još i brojevi oblika $\dfrac{u + v\sqrt{d}}{2}$, pri čemu su u, v neparni.

Definicija 43. *Invertibilni element u* $\mathbb{Q}(\sqrt{d})$ *je algebarski cijeli broj* ϵ *za koji vrijedi da je* $\frac{1}{\epsilon}$ *također algebarski cijeli broj.*

Kvadratno polje $\mathbb{Q}(\sqrt{d})$ je realno ako je $d > 0$, a imaginarno ukoliko je $d < 0$.

Teorem 19 (vidjeti [5, Teorem 12.6.])**.** *Neka je* d *negativan kvadratno slobodan cijeli broj. Kvadratno polje* $\mathbb{Q}(\sqrt{d})$ *ima jedinice* ± 1 *i to su jedine jedinice osim u slučajevima kada je* $d = -1$ *i* $d = -3$. *Jedinice u* $\mathbb{Q}(i)$ *su* $\pm 1, \pm i$, *a u* $\mathbb{Q}(\sqrt{-3})$ *su* $\pm 1, \dfrac{1 \pm \sqrt{-3}}{2}, \dfrac{-1 \pm \sqrt{-3}}{2}$.

Dokaz. Trebamo pronaći sve algebarske cijele brojeve α za koje vrijedi $N(\alpha) = \pm 1$. Ukoliko je $d \equiv 2$ ili $3 \pmod 4$, tada α ima oblik $\alpha = x + y\sqrt{d}, x, y \in \mathbb{Z}$. Treba riješiti diofantsku jednadžbu $x^2 - dy^2 = \pm 1$. Kako je d negativan, odbacujemo slučaj $x^2 - dy^2 = -1$. Ako je $d \leq -2$, tada je dy^2 najmanje dvostruko veće od y^2, to jest $x^2 - dy^2 \geq x^2 + 2y^2 \geq 2y^2$. Jedina rješenja su $(x, y) = (\pm 1, 0)$ pa je $\alpha = \pm 1$. Ako je $d = -1$, rješenja (x, y) jednadžbe $x^2 + y^2 = 1$ su dana s $x = \pm 1, y = 0$ i $x = 0, y = \pm 1$, to jest $\alpha = \pm 1, \pm i$.
Uzmimo sada $d \equiv 1 \pmod 4$. Tada je α oblika $x + y\frac{1+\sqrt{d}}{2}$, iz čega slijedi da je norma $N(\alpha) = (x + \frac{y}{2})^2 - \frac{1}{4}dy^2$. Zbog $d < 0$, jednadžba $N(\alpha) = -1$ nema rješenja. Ukoliko je $d \leq -7$, tada $(x + \frac{y}{2})^2 - \frac{1}{4}dy^2 \geq \frac{7}{4}y^2$, pa iz $N(\alpha) = 1$ slijedi $y = 0, x = \pm 1$, to jest $\alpha = \pm 1$. Za $d = -3$ imamo jednadžbu

$$\left(x + \frac{y}{2}\right)^2 + \frac{3}{4}y^2 = 1. \tag{3.4}$$

Nakon sređivanja izraza, dobivamo

$$x^2 + xy + y^2 = 1.$$

Iz izraza (3.4) zaključujemo da je $|y| \leq 1$. Ukoliko stavimo da je $y = 0$, dobivamo $x = \pm 1$ iz čega slijedi $\alpha = \pm 1$. Ako je $y = 1$, tada je $x = 0$ ili $x = -1$ pa slijedi $\alpha = \frac{1+\sqrt{-3}}{2}$ ili $\alpha = \frac{-1+\sqrt{-3}}{2}$. Uvrstimo li $y = -1$, dobivamo $x = 0$ ili $x = 1$ iz čega slijedi $\alpha = \frac{-1-\sqrt{-3}}{2}$ ili $\alpha = \frac{1-\sqrt{-3}}{2}$. □

Problem pronalaska invertibilnih elemenata u realnim kvadratnim poljima usko je povezan s Pellovim jednadžbama. Jedinice polja $\mathbb{Q}(\sqrt{d})$ imaju oblik $u+v\sqrt{d}$, a njihova norma, definirana kao $N(u+v\sqrt{d}) = u^2 - dv^2$, iznosi 1. Nas će zanimati svi elementi koji zadovoljavaju jednadžbu $u^2 - dv^2 = \pm 1$.

Definicija 44. *Diofanska jednadžba*

$$u^2 - dv^2 = 1, \tag{3.5}$$

pri čemu prirodan broj d nije potpun kvadrat nekog broja naziva se Pellova jednadžba.

Kada bi d bio potpun kvadrat, $d = g^2, g \in \mathbb{Z}$, imali bi

$$u^2 - dv^2 = (u+gv)(u-gv) = 1.$$

Slijedi da je

$$(u+gv) = (u-gv) = \pm 1.$$

U tom bi slučaju imali trivijalna rješenja $u = \pm 1, v = 0$.

Definicija 45. *Diofantsku jednadžbu*

$$u^2 - dv^2 = N,$$

gdje je d prirodan broj koji nije potpun kvadrat i N cijeli broj različit od 0, zovemo pellovska jednadžba.

Najmanje rješenje Pellove jednadžbe (3.5) u skupu prirodnih brojeva naziva se fundamentalno rješenje.

Pellovom jednadžbom često se nazivaju četiri jednadžbe oblika $u^2 - dv^2 = \pm 1, \pm 4$. Vrijedi sljedeće:

- ako je $d \equiv 2$ ili $3 \pmod 4$, tada je $u+v\sqrt{d}$ invertibilan u $\mathbb{Q}(\sqrt{d})$ ako i samo ako vrijedi $u^2 - dv^2 = \pm 1$,
- ako je $d \equiv 1 \pmod 4$, onda je $\frac{u+v\sqrt{d}}{2}$ invertibilan u $\mathbb{Q}(\sqrt{d})$ ako i samo ako je zadovoljeno $u^2 - dv^2 = \pm 4$.

Generatori grupe invertibilnih elemenata u realnom kvadratnom polju su oni elementi koji mogu proizvesti sve ostale elemente te grupe. Generiranje novih elemenata podrazumijeva korištenje operacija potenciranja i množenja s generatorom kako bi se dobili svi preostali invertibilni elementi u polju.

Korolar 1 (vidjeti [5, Korolar 12.8.]). *Grupa jedinica u realnom kvadratnom polju $\mathbb{Q}(\sqrt{d})$ ima dva generatora, -1 i ζ_d, gdje je*

$$\zeta_d = u+v\sqrt{d} \quad ili \quad \zeta_d = \frac{u+v\sqrt{d}}{2},$$

dok je $u+v\sqrt{d}$ fundamentalno rješenje jedne od Pellovih jednadžbi $u^2 - dv^2 = \pm 1, \pm 4$. Dakle, svaka se jedinica može napisati u obliku $\pm\zeta_d^n, n \in \mathbb{Z}$. Generator ζ_d naziva se fundamentalna jedinica kvadratnog polja $\mathbb{Q}(\sqrt{d})$. Ako je $u_1 + v_1\sqrt{d}$ fundamentalno rješenje Pellove jednadžbe $u^2 - dv^2 = 1$, onda je $u_1 + v_1\sqrt{d} = (u+v\sqrt{d})^\nu$, gdje je $\nu \in \{1,2,3,6\}$.

Pronalazak fundamentalnog rješenja nije uvijek jednostavno. Ponekad rješenje lako možemo pronaći uvrštavanjem brojeva za y i provjeravanjem je li $dv^2 + 1$ potpuni kvadrat.
Uzmimo sada za primjer $d = 61$. Fundamentalno rješenje za Pellovu jednadžbu $u^2 - 61v^2 = 1$ iznosi $u = 1766319049, v = 226153980$. Vidimo da za izbor relativno malog d-a dobivamo vrlo veliko fundamentalno rješenje. Nameće se pitanje kako onda pronaći fundamentalno rješenje Pellove jednadžbe. Osnovna metoda je razvoj broja $\sqrt{d}$ u verižni razlomak. Više detalja o ovoj temi može se naći u [5].

Teorem 20 (vidjeti [5, Teorem 12.7.]). *U svakom realnom kvadratnom polju postoji beskonačno mnogo jedinica.*

Dokaz. Neka su $\alpha = u + v\sqrt{d}, u, v \in \mathbb{Z}$ algebarski cijeli brojevi iz $\mathbb{Q}(\sqrt{d})$. Njihova norma iznosi $N(\alpha) = u^2 - dv^2$. Ukoliko je $u^2 - dv^2 = 1$, tada je α jedinica. Kako je $u^2 - dv^2 = 1$ Pellova jednadžba, ona za kvadratno slobodan broj $d > 1$ ima beskonačno mnogo rješenja. □

Podsjetimo se kako glasi jedan od najpoznatijih teorema općenito u matematici.

Teorem 21 (**Veliki Fermatov teorem**). [*vidjeti* [*8, Teorem 6.8.*]]
Za prirodne brojeve $n > 2$ ne postoje prirodni brojevi a, b, c takvi da vrijedi

$$a^n + b^n = c^n.$$

Iako nam ovaj teorem nije potreban u razradi ove teme, pokušaj njegovog dokazivanja imao je ogroman utjecaj na teoriju brojeva, konkretno na jedinstvenost faktorizacije. Dokazujući Fermatov teorem za polinome trećeg stupnja, Euler je, bez dokaza, primijenio svojstvo: *ako su brojevi relativno prosti i njihov umnožak je kub, onda je svaki od njih kub*. Njegovo razmišljanje bilo je pogrešno jer je implicitno pretpostavio jedinstvenu faktorizaciju, to jest da se svaki broj može na jedinstven način rastaviti na proste faktore, kao što je to slučaj u skupu cijelih brojeva $\mathbb{Z}$. Međutim, ovo svojstvo ne vrijedi u svim proširenjima polja, kao što je slučaj sa proširenjem $\mathbb{Q}(\sqrt{-3})$. U prstenu $\mathbb{Q}(\sqrt{-3})$ postoji broj 4 koji ima dvije različite faktorizacije

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

Ova konstatacija objašnjava koliko je zapravo jedinstvena faktorizacija važna. Kako bi se nosili s nedostatkom jedinstvenosti faktorizacije u promatranim prstenima, matematičari su usmjerili pažnju prema drugim matematičkim strukturama u kojima je ona jedinstvena. Tu nastupa pojam koji smo već objasnili u ovom radu, a to je pojam ideala.
Prosti ideal generalizira koncept prostog broja tako što omogućuje analizu faktorizacije elemenata prstena na način koji odgovara svojstvima prostih brojeva u cjelobrojnom prstenu.
Iako smo u Poglavlju 2.5 definirali pojmove prostog, ireducibilnog i asociranog broja, sljedeća definicija opisuje ova svojstva u terminima algebarskog cijelog broja.

Definicija 46. *Za algebarske cijele brojeve $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$ kažemo da α dijeli β, pišemo $\alpha|\beta$, ako postoji algebarski cijeli broj $\gamma \in \mathbb{Q}(\sqrt{d})$ takav da je $\beta = \alpha\gamma$. Jedinice su upravo djelitelji broja 1. α i β su asocirani ako je količnik $\frac{\alpha}{\beta}$ jedinica.*

Za algebarski cijeli broj $\alpha \in \mathbb{Q}(\sqrt{d})$ koji nije nula niti jedinica u $\mathbb{Q}(\sqrt{d})$, kažemo da je ireducibilan ako je djeljiv samo s jedinicama i sebi asociranim brojevima.
Algebarski cijeli broj $\pi \in \mathbb{Q}(\sqrt{d})$ je prost ako π nije nula niti jedinica u $\mathbb{Q}(\sqrt{d})$ te ako π ima svojstvo da ukoliko $\pi|\beta\gamma$, pri čemu su β, γ algebarski cijeli brojevi iz $\mathbb{Q}(\sqrt{d})$, onda $\pi|\beta$ ili $\pi|\gamma$.

Primijetimo da je svaki prosti broj ujedno i ireducibilan. U skupu cijelih brojeva $\mathbb{Z}$ vrijedi i obrat, ali općenito ireducibilan broj ne mora biti prost.

Primjer 51. *Uzmimo kvadratno polje $\mathbb{Q}(\sqrt{-5})$. Broj 3 je ireducibilan u tom polju jer ga možemo zapisati kao $3 = \beta\gamma$. Slijedi $N(\beta)N(\gamma) = \pm 9$. Jednadžbe $x^2 + 5y^2 = \pm 3$ nemaju cjelobrojih rješenja pa slijedi da je $N(\beta) = \pm 1$ ili $N(\gamma) = \pm 1$ što znači da jedan od brojeva β ili γ mora biti jedinica. Međutim, 3 nije prost u $\mathbb{Q}(\sqrt{-5})$ jer 3 dijeli $(1+\sqrt{-5})(1-\sqrt{-5}) = 6$, ali 3 ne dijeli ni $(1+\sqrt{-5})$ niti $(1-\sqrt{-5})$ jer $N(1-\sqrt{-5}) = N(1+\sqrt{-5}) = 6$ i $N(3) = 9$, a 9 ne dijeli 6.*

Teorem 22 (vidjeti [5, Teorem 12.9.])**.** *Ukoliko je norma algebarskog cijelog broja α u $\mathbb{Q}(\sqrt{d})$ jednaka $\pm p$, pri čemu je p prost broj, onda je α ireducibilan.*

Dokaz. Neka je $\alpha = \beta\gamma$, pri čemu su β i γ cijeli brojevi u $\mathbb{Q}(\sqrt{d})$. Po Teoremu 17 znamo da je $N(\alpha) = N(\beta)N(\gamma)$. U skladu s tim imamo $N(\beta)N(\gamma) = \pm p$. Kako su $N(\beta)$ i $N(\gamma)$ cijeli brojevi, jedan od njih mora biti jednak ± 1. To bi značilo da je jedan od brojeva β i γ jedinica, a drugi je asociran s α. □

Primjer 52. *Uzmimo algebarski cijeli broj $\alpha = 3 + \sqrt{2}$ iz $\mathbb{Q}(\sqrt{2})$. Njegova norma je*

$$N(\alpha) = \alpha \cdot \overline{\alpha} = (3+\sqrt{2})(3-\sqrt{2}) = 3^2 - (\sqrt{2})^2 = 7.$$

Budući da je 7 prost broj, prema tvrdnji Teorema 22, α je ireducibilan u $\mathbb{Q}(\sqrt{2})$. Neka je $\beta = 4 + 2\sqrt{2}$ algebarski cijeli broj iz istog polja $\mathbb{Q}(\sqrt{2})$. Njegova norma je

$$N(\beta) = \beta \cdot \overline{\beta} = (4+2\sqrt{2})(4-2\sqrt{2}) = 4^2 - (2\sqrt{2})^2 = 8.$$

Kako 8 nije prost broj, ne možemo tvrditi da je β ireducibilan u $\mathbb{Q}(\sqrt{2})$.

Teorem 23 (vidjeti [5, Teorem 12.10.])**.** *Svaki algebarski cijeli broj α u $\mathbb{Q}(\sqrt{d})$, koji nije nula ni jedinica, može se prikazati kao produkt ireducibilnih brojeva u $\mathbb{Q}(\sqrt{d})$.*

Dokaz. Pretpostavimo da α nije ireducibilan. Tada ga možemo rastaviti na produkt $\beta\gamma$, pri čemu β i γ nisu jedinice. Nastavljamo postupak faktorizirajući β i γ ukoliko nisu ireducibilni. Proces faktorizacije u jednom trenutku mora stati jer bismo inače dobili α u obliku $\beta_1\beta_2\ldots\beta_n$, gdje je n proizvoljno velik, a niti jedan od β_j nije jedinica. Ako su β_j ireducibilni, njihova norma je barem 2. U tom slučaju, produkt normi bit će barem 2^n. Dobili bi

$$|N(\alpha)| = \prod_{j=1}^{n} |N(\beta_j)| \geq 2^n,$$

a to je kontradikcija s početnom pretpostavkom. □

Primjer 53. *Promotrimo broj 6 u polju* $\mathbb{Q}(\sqrt{-5})$*:*

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

Broj 6 ima dvije faktorizacije, a brojevi $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ *su ireducibilni u* $\mathbb{Q}(\sqrt{-5})$*. Ako algebarski broj* $\alpha \in \mathbb{Q}(\sqrt{-5})$ *nije 0 ni jedinica, onda je norma oblika*

$$N(\alpha) = N(u + v\sqrt{-5}) = (u + v\sqrt{-5})(u - v\sqrt{-5}) = u^2 - (v\sqrt{-5})^2 = u^2 + 5v^2.$$

Kako α *ne može biti jedinica, najmanja vrijednost norme od* α *je 4. Također,* $N(\alpha)$ *ne može biti 2,3 ili 6 jer ne postoji kombinacija u i v u* $\mathbb{Q}$ *koja bi zadovoljila jednakost* $u^2 + 5v^2 = 2, 3, 6$*. Pogledajmo slijedeće mogućnost:*

- *iz* $2 = \alpha\beta$ *i* $N(\alpha)N(\beta) = 4$ *slijedi* $N(\alpha) = \pm 1$ *ili* $N(\beta) = \pm 1$*;*
- *ako je* $3 = \alpha\beta$ *i* $N(\alpha)N(\beta) = 9$*, onda je* $N(\alpha) = \pm 1$ *ili* $N(\beta) = \pm 1$*;*
- *iz* $1 \pm \sqrt{-5} = \alpha\beta$ *i* $N(\alpha)N(\beta) = 6$ *slijedi* $N(\alpha) = \pm 1$ *ili* $N(\beta) = \pm 1$*.*

Kako algebarski cijeli broj, po Teoremu 23, nije 0 niti jedinica, naši slučajevi nisu mogući te zaključujemo da 6 nema jedinstvenu faktorizaciju na ireducibilne elemente u $\mathbb{Q}(\sqrt{-5})$*.*

Dokazali smo da faktorizacija na ireducibilne faktore u $\mathbb{Q}(\sqrt{d})$ uvijek postoji, ali ona ne mora biti jedinstvena. Postavlja se pitanje za koje sve vrijednosti d postoji jedinstvena faktorizacija. Odgovor na to pitanje povezano je s Euklidovim algoritmom.

Definicija 47. *Kažemo da kvadratno polje* $\mathbb{Q}(\sqrt{d})$ *ima svojstvo jedinstvene faktorizacije ako se svaki algebarski cijeli broj u* $\mathbb{Q}(\sqrt{d})$*, koji nije nula ni jedinica, može faktorizirati na ireducibilne faktore jednoznačno, do na poredak faktora i zamjenu faktora asociranim elementima.*

Definicija 48. *Kvadratno polje je euklidsko ako je za algebarske cijele brojeve u* $\mathbb{Q}(\sqrt{d})$ *moguće provesti analogon Euklidova algoritma, to jest ako za algebarske brojeve* α, β *u* $\mathbb{Q}(\sqrt{d}), \beta \neq 0$*, postoje algebarski cijeli brojevi* γ *i* δ *u* $\mathbb{Q}(\sqrt{d})$ *takvi da je* $\alpha = \beta\gamma + \delta$ *i* $|N(\delta)| < |N(\beta)|$*.*

Teorem 24 (vidjeti [5, Teorem 12.11.])**.** *Svako euklidsko kvadratno polje ima svojstvo jedinstvene faktorizacije.*

Dokaz. Najprije ćemo pokazati da ako su α i β algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ koji nemaju zajedničkih djelitelja osim jedinice. Tada postoje algebarski cijeli brojevi $\mu_0, \lambda_0 \in \mathbb{Q}(\sqrt{d})$ takvi da je

$$\alpha\lambda_0 + \beta\mu_0 = 1.$$

Definiramo skup

$$\mathcal{N} = \{\alpha\lambda_0 + \beta\mu_0 : \lambda_0, \mu_0 \in \mathbb{Q}(\sqrt{d})\}.$$

Brojevi $|N(\alpha\lambda+\beta\mu)|$ su nenegativni cijeli brojevi. Izaberemo element $\psi=\alpha\lambda_1+\beta\mu_1$ iz skupa $\mathcal{N}$ tako da $|N(\psi)|$ ima najmanju pozitivnu vrijednost među brojevima $|N(\alpha\lambda+\beta\mu)|$. Primijenimo Euklidov algoritam na brojeve α i ψ. Dobivamo

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

Tada je $\delta=\alpha-\gamma(\alpha\lambda_1+\beta\mu_1)=\alpha(1-\gamma\mu_1)+\beta(-\gamma\mu_1)\in\mathcal{M}$. Iz definicije od ψ imamo $N(\delta)=0$, iz čega slijedi da je $\delta=0$. Dakle, $\alpha=\psi\gamma$ i $\psi|\alpha$ pa je ψ jedinica. Analogno se pokaže da $\psi|\beta$. Sada je i ψ^{-1} jedinica pa imamo

$$1=\psi^{-1}\psi=\psi^{-1}(\alpha\lambda_1+\beta\mu_1)=\alpha(\psi^{-1}\lambda_1)+\beta(\psi^{-1}\mu_1)=\alpha\mu_0+\beta\mu_0.$$

Pokažimo sada da ako je π ireducibilan u $\mathbb{Q}(\sqrt{d})$, tada je on i prost. Dakle, treba pokazati ako $\pi|\alpha\beta$, onda $\pi|\alpha$ ili $\pi|\beta$. Naime, ako je $\pi\nmid\alpha$, tada π i α nemaju zajedničkog djelitelja osim jedinica, pa postoje algebarski cijeli brojevi λ_0 i μ_0 takvi da vrijedi $\pi\lambda_0+\alpha\mu_0=1$. Tada je $\beta=\pi\beta\lambda_0+\alpha\beta\mu_0$, što znači da $\pi|\beta$. Indukcijom slijedi da ako $\pi|(\alpha_1\cdot\ldots\cdot\alpha_n)$, tada π dijeli neki α_j.
Pretpostavimo sada da algebarski cijeli broj β ima dvije faktorizacije na ireducibilne faktore, to jest neka je

$$\beta=\rho_1\rho_2\cdots\rho_m=\nu_1\nu_2\cdots\nu_n. \tag{3.6}$$

Ukoliko je $m=1$, tada je β ireducibilan i mora vrijediti da je $n=1$ i $\beta=\nu_1$. Uzmimo da je $m>1$. Kako je ρ_1 prost, iz $\rho_1|\nu_1\nu_2\cdots\nu_n$ slijedi da ρ_1 dijeli neki ν_j. Uzmimo da $\rho_1|\nu_1$. Znamo da je ν_1 ireducibilan, a to znači da je ρ_1 njemu asociran broj, to jest

$$\nu_1=\psi\rho_1,$$

gdje je ψ invertibilan element. Ukoliko prethodnu jednakost uvrstimo u (3.6) i podijelimo s ρ_1, dobivamo

$$\rho_2\rho_3\cdots\rho_m=\psi\nu_2\nu_3\cdots\nu_n.$$

Ponavljanjem postupka, dobili bi jedinstvenu faktorizaciju na ireducibilne elemente. □

Primjer 54 (vidjeti [5, Primjer 12.2.]). *Pokažimo da su kvadratna polja $\mathbb{Q}(\sqrt{d})$ za $d=2,3,-1,-2$ euklidska.*
Neka su α i $\beta\neq0$ algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{d})$. Tada je $\frac{\alpha}{\beta}=u+v\sqrt{d}, u,v\in\mathbb{Q}$. Uzmimo $x,y\in\mathbb{Z}$ takve da je

$$0\leq|u-x|\leq\frac{1}{2}, \quad 0\leq|v-y|\leq\frac{1}{2}.$$

Uvedimo oznake $x+y\sqrt{d}=\delta, \alpha-\beta\gamma=\delta$. γ i δ su cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ i vrijedi

$$\begin{aligned}N(\delta)&=N(\alpha-\beta\gamma)\\&=N(\beta)N\left(\frac{\alpha}{\beta}-\gamma\right)\\&=N(\beta)N\left((u-x)+(v-y)\sqrt{d}\right)\\&=N(\beta)\left((u-x)^2-d(v-y)^2\right),\end{aligned}$$

iz čega slijedi

$$|N(\delta)| = |N(\beta)| \cdot |(u-x)^2 - d(v-y)^2)|. \tag{3.7}$$

Ukoliko je $d > 0$*, tada je*

$$-\frac{d}{4} \leq (u-x)^2 - d(v-y)^2 \leq \frac{1}{4},$$

a ako je $d < 0$*, onda je*

$$0 \leq (u-x)^2 - d(v-y)^2 \leq \frac{1}{4} + \frac{1}{4}(-d).$$

Ako uzmemo $d = 2, 3, -1, -2$*, tada iz* (3.7) *slijedi* $|N(\delta)| < |N(\beta)|$ *pa je za te vrijednosti d polje* $\mathbb{Q}(\sqrt{d})$ *euklidsko.*

Euklidska polja nisu jedina polja s jedinstvenom faktorizacijom. Matematičari Kurt Heegner, Alan Baker i Harold Stark pokazali su da ako je $d < 0$, onda za $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$, kvadratno polje $\mathbb{Q}(\sqrt{d})$ ima svojstvo jedinstvene faktorizacije. Godine 1952. Heegner dokazuje da je ovaj popis potpun, ali se smatralo da je njegov dokaz pogrešan. Stark je 1967. godine usavršio dokaz koji je na kraju prihvaćen. Ukoliko je $d > 0$, pretpostavlja se da takvih polja ima beskonačno mnogo.

Literatura

[1] A. K. Bhuniya, *Abstract algebra*, Department of Mathematics, Visva-Bharati, Santiniketan, West Bengal, dostupno na https://epgp.inflibnet.ac.in/epgpdata/uploads/epgp_content/S000025MS/P001533/M017010/ET/1468559390E-textofChapter8Module3.pdf

[2] D. Brajković, *Algebra kroz primjere, priručnik za vježbe*, Sveučilište J. J. Strossmayera u Osijeku, Odjel za matematiku, Osijek, 2018.

[3] R. Chapman, *Notes on algebraic numbers*, dostupno na https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=d6c065e71c1f53516e5a0e330c8ddffbb7dac737

[4] K. Conrad, *Factoring in quadratic fields*, dostupno na https://kconrad.math.uconn.edu/blurbs/gradnumthy/quadraticgrad.pdf

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

[6] K. Horvatić, *Linearna algbra*, Golden marketing - Tehnička knjiga, Zagreb, 2004.

[7] H. Kraljević, *Algebra*, Odjel za matematiku, Osijek, 2007., dostupno na https://web.math.pmf.unizg.hr/~hrk/nastava/2006-07/algebra_Osijek_2006_7.pdf

[8] J. S. Milne, *Algebraic number theory*, dostupno na https://www.jmilne.org/math/CourseNotes/ANT.pdf

[9] I. Matić, *Osnovne algebarske strukture*, nastavni materijal, dostupno na https://www.mathos.unios.hr/wp-content/uploads/2014/09/Algebra_predavanja.pdf

[10] Š. Ungar, *Matematička analiza 4*, nastavni materijal, dostupno na https://web.math.pmf.unizg.hr/~ungar/NASTAVA/MA/Analiza4.pdf

[11] I. Stewart, D. Tall, *Algebrain number theory and Fermat's last theorem*, A. K. Peters, LTD, Natick, 2002.

Sažetak

U ovom radu proučavali smo osnovne algebarske strukture i kvadratna proširenja polja racionalnih brojeva. Počevši od osnovnih definicija i pojmova iz algebre, istražujemo kako se formiraju proširenja polja, s posebnim naglaskom na kvadratna proširenja. Nakon što smo konstruirali polje $\mathbb{Q}(\sqrt{d})$, definirali smo pojmove algebarskog broja i algebarskog cijelog broja. Daljnje analize uključuju primjere kvadratnih proširenja i njihovu primjenu u teoriji brojeva. Rad naglašava važnost kvadratnih proširenja u razumijevanju dubljih algebarskih struktura i njihovih svojstava.

Ključne riječi

algebarske strukture, kvadratna polja, algebarski cijeli brojevi, ireducibilnost, prosti brojevi, jedinstvenost faktorizacije

Basic algebraic structures and field extensions

Summary

In this final paper, we consider basic algebraic structures and quadratic extensions of rational numbers. Starting from basic definitions and concepts from algebra, we explore how field extensions are formed, with a particular emphasis on quadratic extensions. After constructing the field $\mathbb{Q}(\sqrt{d})$, we define the concepts of algebraic numbers and algebraic integers, highlighting their key characteristics.
Further analysis includes examples of quadratic extensions and their applications in number theory. We also examine how algebraic integers can serve as a foundation for studying algebraic structures within these extensions. In the context of these definitions, we particularly focus on how the solutions to quadratic equations can be interpreted within the extended fields. Finally, the thesis emphasizes the importance of quadratic extensions in understanding deeper algebraic structures and their properties.

Keywords

algebraic structures, quadratic fields, algebraic integers, irreducibility, prime numbers, unique factorization

Životopis

Rođena sam 24. kolovoza 1996. godine u Osijeku. Nakon završene osnovne škole u Ladimirevcima, upisala sam opću gimnaziju u Srednjoj školi Valpovo koju sam završila 2015. godine. Iste godine upisala sam prijediplomski studij Matematika na Odjelu za matematiku, današnjem Fakultetu primijenjene matematike i informatike u sastavu Sveučilišta Josipa Jurja Strossmayera u Osijeku. Prijediplomski studij završila sam 2021. godine s temom završnog rada *Nizovi i redovi realnih brojeva* koji je izrađen pod mentorstvom prof. dr. sc. Dragane Jankov Maširević. Te godine, na istom fakultetu, upisala sam diplomski studij, modul: financijska matematika i statistika.