Algebarska svojstva važnih skupova brojeva

Šolić, Valentina

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:790360

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni diplomski studij matematike
Smjer: Financijska matematika i statistika

Valentina Šolić

Algebarska svojstva važnih skupova brojeva

Diplomski rad

Osijek, 2022.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni diplomski studij matematike
Smjer: Financijska matematika i statistika

Valentina Šolić

Algebarska svojstva važnih skupova brojeva

Diplomski rad

Mentor: prof.dr.sc. Ivan Matić

Osijek, 2022.

Sadržaj

1 Uvod **1**

2 Uređene integralne domene **2**

3 Prsten cijelih brojeva **7**

4 Polje kvocijenata. Polje racionalnih brojeva. **8**

5 Uređena polja. Polja realnih brojeva. **13**

6 Polje kompleksnih brojeva **16**

7 Kompleksni korijeni iz jedinice **20**

Literatura **24**

Sažetak **25**

Summary **26**

Životopis **27**

1 Uvod

O ovom diplomskom radu bavimo se poznatim brojevnim sustavima kao što su cijeli brojevi, racionalni brojevi, realni brojevi te kompleksni brojevi te ćemo vidjeti po čemu se oni razlikuju u smislu svojstava prstena ili polja. U narednim poglavljima vidjet ćemo kako su konstruirani pojedini brojevi i razloge zbog kojih uopće oni jesu konstrurirani. Također, navest ćemo i dokazat neka važna svojstva.

U drugom poglavlju nakon što navedemo osnovne definicije za grupu, prsten i polje, definirat ćemo uređenu integralnu domenu te dokazati neka svojstva koja ima uređena integralna domena. Dokazat ćemo i da uređena integralna domena sadrži potprsten izomorfan prstenu cijelih brojeva.

Nakon toga, u poglavlju Prsten cijelih brojeva, definirat ćemo dobro uređenu integralnu domenu te dokazati da je prsten cijelih brojeva zapravo jedinstevena dobro uređena integralna domena.

U poglavlju nakon toga dolazimo do polja racionalnih brojeva. Racionalne brojeve konstrirat ćemo pomoću klasa ekvivalencije uređenih parova cijelih brojeva te ćemo dokazat da je skup svih tih klasa ekvivalencija s pripadnim operacijima polje. Polje racionalnih brojeva je zapravo jedinstveno polje kvocijenata jedinstvene dobro uređene integralne domene.

Realne brojeve kao rješenje problema $x^2 = 2$ uvodimo u petom poglavlju. U tom poglavlju ćemo dokazati da je $\sqrt{2}$ iracionalan broj te ćemo reći što je to gornja odnosno donja granica uređenog polja.

U odlomku Polja kompleksnih brojeva realne brojeve proširujemo na kompleksne brojeve te ćemo iskazati osnovni teorem algebre. U tom odlomku ćemo konstruirati kompleksne brojeve pomoću klasa ekvivalencija uređenih parova realnih brojeva te ćemo dokazati da je skup tih uređenih parova polje. Reći ćemo što je to proširenje neko polje te kada je neki element algebarski nad nekim polje. Na kraju ćemo reći što je to algebarsko proširenje i algebarski zatvarač polja s pripadnim primjerima.

U posljednjem odlomku s teorije prelazimo na računanje. Vidjet ćemo kako prikazujemo kompleksne brojeve geormetrijski te na koji način potenciramo kompleksne brojeve. Na samom kraju dolazimo do rješenja problema $x^n = 1$.

2 Uređene integralne domene

U ovom poglavlju činimo prve korake prema karakterizaciji prstena cijelih brojeva. Kako bismo došli do defincije uređene integralne domene najprije ćemo definirati neke osnovne pojmove na temelju kojih dolazimo da spomenute definicije. Kao prvi pojam definirat ćemo pojam grupe.

Definicija 1. *Grupa je skup G zajedno sa binarnom operacijom $*$ tako da je zadovoljen svaki od sljedećih aksioma:*

Asocijativnost

$$a * (b * c) = (a * b) * c \quad \forall\ a, b, c \in G.$$

Postojanje neutralnog elementa

Postoji element $e \in G$ takav da je

$$a * e = e * a = a \quad \forall\ a \in G.$$

Postojanje inverznog elementa

Za svaki $a \in G$ postoji $b \in G$ takav da je

$$a * b = b * a = e.$$

Nakon definicije grupe možemo definirati i što je to Abelova grupa.

Definicija 2. *Grupa G je Abelova grupa ukoliko je grupa G komutativna odnosno $a * b = b * a \ \ \forall\ a, b \in G$.*

Prije same definicje uređene integralne domene potrebno je definirati što je integralna domena. Kako bismo nju definirali potrebna nam je definicja prstena koju navodimo u nastavku.

Definicija 3. *Prsten je skup R sa binarnom operacijom zbarajanja $(a + b)$ i operacijom množenja (ab) za koje vrijedi sljedeće*

- *obzirom na zbrajanje R je Abelova grupa odnosno vrijedi*

  asocijativnost zbrajanja

  $$a + (b + c) = (a + b) + c \ \ \forall\ a, b, c \in R,$$

  postoji $0 \in R$ takva da je

  $$a + 0 = 0 + a = a \ \ \forall\ a \in R,$$

  za svaki $a \in R$ postoji $-a \in R$ tako da vrijedi

  $$a + (-a) = (-a) + a = 0,$$

komutativnost zbrajanja

$$a + b = b + a \quad \forall\, a, b \in R,$$

- *množenje je asocijativno odnosno*

$$a(bc) = (ab)c \quad \forall\, a, b, c \in R,$$

- *množenje je distributativno u odnosu na zbrajanje*

$$a(b + c) = ab + ac \quad i \quad (a + b)c = ac + bc \quad \forall\, a, b, c \in R.$$

Za prsten R kažemo da je komutativan ukoliko je operacija množenja komutativna odnosno $ab = ba \quad \forall\, a, b \in R$.

Definicija 4. *U komutativnom prstenu R element $a \neq 0$ nazivamo djeljitelj nule u R ako postoji $b \neq 0$ takav da je $ab = 0$.*

Sada imamo sve što nam je potrebno da bismo definirali integralnu domenu.

Definicija 5. *Integralna domena je komutativni prsten s jedinicom $e \neq 0$ (element e je jedinica u prstenu R ako je $ea = ae = a \quad \forall\, a \in R$) i bez djeljitelja nule.*

Definicija 6. *Komutativni prsten u kojem skup elemenata različitih od nule čini grupu u odnosu na množenje nazivamo poljem.*

Definicija uređene integralne domene koju navodimo u nastavku odnosi se na skup cijelih brojeva, ali i na mnoge druge integralne domene.

Definicija 7. *Kažemo da je integralna domena D uređena ako postoji podskup D^p (zamišljamo ga kao skup cijelih brojeva) od D takav da je*

- *zatvoren obzirom na zbrajanje odnosno*

$$\text{ako je} \quad a, b \in D^p, \quad \text{onda je} \quad a + b \in D^p,$$

- *zatvoren obzirom na množenje*

$$\text{ako je} \quad a, b \in D^p, \quad \text{onda je} \quad ab \in D^p,$$

- *vrijedi zakon trihotomije*

$$\text{ako je} \quad a \in D^p, \quad \text{tada vrijedi točno jedno od idućeg}:$$

$$a = 0, \; a \in D^p \quad ili \quad -a \in D^p.$$

Elemente iz D^p nazivamo pozitivni elementi dok elemente koji su različiti od nula i nisu pozitivni nazivamo negativnima. U nastavku ovog poglavlja pretpostavit ćemo da je D uređena integralna domena s jedinicom e.

Lema 1. *([1, Lemma 28.1]) Ako je $a \in D$ i $a \neq 0$, onda je $a^2 \in D^p$.*

Dokaz:
Kako je $a \neq 0$ prema definiciji od D^p imamo da je $a \in D^p$ ili $-a \in D^p$. Dakle, razlikujemo dva slučaja

- $a \in D^p$:
  kako je D^p zatvoren obzirom na množenje slijedi da je $a \cdot a = a^2 \in D^p$.
- $-a \in D^p$:
  kako je D^p zatvoren obzirom na množenje slijedi da je $(-a) \cdot (-a) = (-a)^2 \in D^p$, ali u bilo kojem prstenu vrijedi da je $(-a)^2 = a^2$ pa je opet $a^2 \in D^p$.

□

Korolar 1. *Vrijedi $e \in D^p$.*

Dokaz:
Kako je $e \in D$ i $e \neq 0$ prema Lemi 1 slijedi da je $e^2 \in D^p$. Kako je $e^2 = e$ slijedi da je $e \in D^p$. □

Lema 2. *([1, Lemma 28.2]) Ako je $a \in D^p$ i n prirodan broj, tada je $na \in D^p$, pri čemu je $na = a + \cdots + a$ (n puta).*

Dokaz:
Dokaz provodimo matematičkom indukcijom po n.

1) Direktno iz definicije slijedi $1 \cdot a = a \in D^p$.
2) Pretpostavimo da je $ka \in D^p$. Kako je D^p zatvoren obzirom na zbrajanje, slijedi $(k+1)a = ka + a \in D^p$.

Dakle, za svaki prirodan broj n vrijedi $na \in D^p$. □

Kako bismo naveli jedno od svojstava uređene integralne domene prvo ćemo definirati karakteristiku prstena te zatim i potprsten.

Definicija 8. *Neka je R prsten. Ako postoji prirodan broj n takav da je $na = 0$ za svaki $a \in R$, onda najmanji takav n zovemo karakteristika prstena. Ako takav prirodan broj ne postoji, kažemo da je R prsten karakteristike nula.*

Definicija 9. *Potprsten prstena R je podskup S od R koji je i sam prsten u odnosu na zadane operacije.*

Podsjetimo se pojma izomorfizma prstena.

Definicija 10. *Neka su R i S prstenovi. Izomorfizam s R na S je preslikavanje $\theta : R \to S$ koje je bijektivno i za koje vrijedi*

$$\theta(a+b) = \theta(a) + \theta(b)$$

i

$$\theta(ab) = \theta(a)\theta(b)$$

za svaki $a, b \in R$. *Ukoliko postoji izomorfizam s* R *na* S *kažemo da su prstenovi* R *i* S *izomorfni.*

Teorem 1. *([1, Theorem 28.1]) Ako je* D *uređena integralna domena, tada je* D *karakteristike nula.*

Dokaz:
Prema Korolaru 1 i Lemi 2 vrijedi $e \in D^p$ i $ne \in D^p$ za svaki prirodan broj n. Kako su pozitivni elementi, odnosno elementi iz D^p, različiti do 0, slijedi da je $ne \neq 0$ za svaki prirodan broj n. Stoga karakteristika ne može biti $n \neq 0$. □

Korolar 2. *Ako je* D *uređena integralna domena, tada* D *sadrži potprsten izomorfan prstenu cijelih brojeva.*

Dokaz:
U dokazu koristimo prethodni teorem i činjenicu da integralna domena karakteristike nula sadrži potprsten izomorfan prstenu cijelih brojeva (vidi [1, Theorem 27.2]). □

Korolar 3. *Konačna integralna domena ne može biti uređena. Konkretno,* $\mathbb{Z}_p$ *(pri čemu je* p *prost broj) nije uređena integralna domena.*

Dokaz:
Slijedi iz prethodnog korolara. □

Definicija 11. *Neka je* D *uređena integrala domena i neka su* $a, b \in D$. *Označimo s* $a > b$ *ukoliko je* $a - b \in D^p$. *Ako je* $a > b$ *kažemo da je* a *veće od* b *te da je* b *manje od* a.

Za prsten cijelih brojeva kao i za prsten racionalnih ili realnih brojeva prethodna se definicija podudara sa standardnim značenjem od $>$. Kao i obično

$$b < a \text{ znači } a > b$$

$$a \geq b \text{ znači } a > b \text{ ili } a = b$$

$$a \leq b \text{ znači } b < a \text{ ili } a = b.$$

Sljedeći teorem nam daje mnoga svojstva relacije $>$.

Teorem 2. *([1, Theorem 28.2]) Neka je* D *uređena integralna domena i neka su* $a, b, c \in D$.

a) Ako je $a > 0$ *i* $b > 0$, *onda je* $a + b > 0$.

b) Ako je $a > 0$ *i* $b > 0$, *onda je* $ab > 0$.

c) Vrijedi točno jedno od sljedećeg: $a = b$, $a > b$ *ili* $b > a$.

d) Ako je $a > b$, *onda je* $a + c > b + c$.

e) Ako je $a > b$ *i* $c > 0$, *onda je* $ac > bc$.

f) Ako je $a \neq 0$, *onda je* $a^2 > 0$.

g) Ako je $a > b$ *i* $b > c$, *onda je* $a > c$.

Dokaz:

a) Kako je $a > 0$ i $b > 0$ prema definiciji od $>$ slijedi $a - 0 \in D^p$ i $b - 0 \in D^p$. Kako je D^p zatvoren obzirom na zbrajanje imamo $a + b - 0 \in D^p$ pa opet prema deifiniciji slijedi $a + b > 0$.

b) Kako je $a > 0$ i $b > 0$ prema definiciji od $>$ slijedi $a - 0 \in D^p$ i $b - 0 \in D^p$. Obzirom da je D^p zatvoren u odnosu na množenje imamo $(a - 0)(b - 0) \in D^p$. Iz toga slijedi da je $ab - 0 \in D^p$ što znači da je $ab > 0$.

c) Ova tvrdnja je direktna posljedica zakona trihotomije.

d) Prema definiciji od $>$ imamo $a-b \in D^p$. Dodamo li i oduzmeno c imamo $a+c-(b+c) \in D^p$ iz čega slijedi $a + c > b + c$.

e) Kako je $a > b$ i $c > 0$ prema definiciji slijedi $a - b \in D^p$ i $c \in D^p$. Pošto je D^p zatvoren obzirom na množenje imamo $(a - b)c = ac - bc \in D^p$ iz čega primjenom definicije slijedi $ac > bc$.

f) Slijedi direktno iz Leme 1.

g) Prema definiciji imamo da je $a - b \in D^p$ i $b - c \in D^p$. Zbog zatvorenosti D^p obzirom na zbrajanje slijedi $a - b + b - c = a - c \in D^p$ pa primjenom definicije slijedi $a > c$.

□

3 Prsten cijelih brojeva

Definicija 12. *Kažemo da je u podskupu S uređene integralne domene element a najmanji ako je $x > a$ za svaki $x \in S$ takav da je $x \neq a$.*

Definicija 13. *Kažemo da uređena integralna domena D dobro uređena ako svaki neprazan podskup od D^p ima najmanji element.*

Kako svaki neprazan podskup skupa prirodnih brojeva ima najmanji element slijedi da je integralna domena cijelih brojeva dobro uređena. Teorem koji navodimo u nastavku nam govori da jedino skup cijelih brojeva čini dobro uređenu integralnu domenu. Kako bismo lakše dokazali taj teorem prvo navodimo jednu lemu.

Lema 3. *([1, Lemma 29.1]) Ako je D dobro uređena integralna domena s jedinicom e, tada je e najmanji element od D^p.*

Dokaz:
Kako je D dobro uređena integralna domena D^p mora imati najmanji element, pretpostavimo da je to $a \neq e$. Budući da je prema Korolaru 1 $e \in D^p$ i prema našoj pretpostavci a je najmanji element slijedi da je $e > a$. Kako je $e > a$ i $a > 0$ prema Teoremu 2 (e) slijedi $a > a^2$. Međutim, prema Lemi 1 je $a^2 \in D^p$. Dakle, imamo da je $a^2 \in D^p$ i $a > a^2$ što je u kontradikciji s pretpostavkom da je a najmanji element od D^p . Slijedi da je e najmanji element od D^p. □

Teorem 3. *([1, Theorem 29.1]) Ako je D dobro uređena integralna domena, onda je D izomorfan prstenu cijelih brojeva.*

Dokaz:
Pretpostavimo da D dobro uređena integralna domena i definirajmo $\theta : \mathbb{Z} \to D$ s $\theta(n) = ne$ za svaki $n \in \mathbb{Z}$. Ovdje ćemo dokazati da je $\theta(\mathbb{Z}) = D$ jer se može pokazati da je θ izomorfizam sa $\mathbb{Z}$ na $\theta(\mathbb{Z})$ (dokaz se može naći u [1],Theorem 27.2). Pretpostavimo da to nije zadovoljeno i neka d označava element takav da je $d \in D$, ali $d \notin \theta(\mathbb{Z})$. Tada je također $-d \in D$ i $-d \notin \theta(\mathbb{Z})$. Ako je $-d \in \theta(\mathbb{Z})$, na primjer $\theta(m) = -d$, tada je $\theta(m) = me = -d$ te $\theta(-m) = (-m)e = -(me) = d$, što povlači da je $d \in \theta(\mathbb{Z})$, što je kontradikcija. Kako je $d \notin \theta(\mathbb{Z})$ i $-d \notin \theta(\mathbb{Z})$, bilo $d \in D^p$ ili $-d \in D^p$, zaključujemo da postoji pozitivan element u D koji nije u $\theta(\mathbb{Z})$. Stoga je skup elemenata koji su u D^p, a nisu u $\theta(\mathbb{Z})$ neprazan te budući da je D dobro uređen postoji najmanji takav element koji ćemo označit sa s. To je najmanji element od D^p koji nije u $\theta(\mathbb{Z})$. Jer je $\theta(1) = 1 \cdot e = e$ slijedi da je $e \in \theta(\mathbb{Z})$ tako da je $e \neq s$. Dakle, kako je e prema Lemi 3 najmanji element od D^p, mora biti $s > e$, $s - e > 0$ i $s - e \in D^p$. Kako je $e = s - (s - e) \in D^p$ vrijedi $s > s - e$ te budući da je s najmanji element od D^p koji nije u $\theta(\mathbb{Z})$ imamo $s - e \in \theta(\mathbb{Z})$. Ali ako je $\theta(k) = ke = s - e$ za $k \in \mathbb{Z}$, tada je $\theta(k + 1) = (k + 1)e = ke + e = s - e + e = s$ i zbog toga je $s \in \theta(\mathbb{Z})$, što je u kontradikciji s pretpostavkom da s nije u $\theta(\mathbb{Z})$. Dakle, $\theta(\mathbb{Z}) = D$. □

Dakle, prsten cijelih brojeva je jedinstvena dobro uređena integralna domena. Na primjer, kako skup pozitivnih racionalnih brojeva nema najmanji element integralna domena racionalnih brojeva nije dobro uređena.

4 Polje kvocijenata. Polje racionalnih brojeva.

Pogledamo li jednadžbu $ax = b$, gdje su a i b cijeli brojevi, ona možda nema rješenje u integralnoj domeni cijelih brojeva. Rješenja takva jednadžbe nalaze se u polju racionalnih brojeva koje je dovoljno veliko da sadrži sva takva rješenja. Naime, svaki racionalni broj ima oblik $a^{-1}b$, gdje su a i b cijeli brojevi i $a \neq 0$, pa je svaki racionalni broj rješenje jednadžbe $ax = b$. Ovdje ćemo dokazati da ako je D bilo koja integralna domena tada postoji jedinstveno najmanje polje koje sadrži D tako da svaka jednadžba $ax = b$ ima rješenje u tom polju koje nazivamo polje kvocijenata. Kako je polje kvocijenata integralne domene cijelih brojeva polje racionalnih brojeva jedinstevnost tog polja i već ranije spomenuta karakterizacija cijelih brojeva daje nam karakterizaciju racionalnih brojeva. Prije same konstrukcije polja kvocijenata navodimo osnovnu ideju koja se odnosi na cijele brojeve. Razlomak $\frac{a}{b}$ zamišljamo kako uređeni par (a, b) gdje je druga komponenta različita od 0. Kako različiti razlomci mogu predstavljati isti racionalni broj (na primjer $\frac{1}{3}, \frac{10}{30}$ i $\frac{-5}{-15}$) dolazimo do relacije ekvivalencije: parovi (a, b) i (c, d) su ekvivalentni ako su pripadni razlomci jednaki. Polje racionalnih brojeva dobivamo tako da na skupu kojeg tvore klase ekvivalencije definiramo dvije operacije. U daljnjem razmatranju D će označavati integralnu domenu s jedinicom e dok će D' označavati skup svih nenul elemenata od D. Za elemente (a, b) i (c, d) iz $D \times D' = \{(a, b) : a, b \in D, b \neq 0\}$ pišemo

$$(a, b) \sim (c, d) \quad \text{ako i samo ako} \quad ad = bc.$$

Lema 4. *([1, Lemma 30.1]) Relacija $\sim$ je relacija ekvivalencije na $D \times D'$.*

Dokaz: Da bismo dokazali da je $\sim$ relacija ekvivalencije moramo provjeriti je li ona simetrična, refleksivna i tranzitivna.

1) Refleksivnost
   Za svaki $(a, b) \in D \times D'$ je $(a, b) \sim (a, b)$ jer je $ab = ba$ tj. relacija $\sim$ je refleksivna.

2) Simetričnost
   Ovdje moramo pokazati da $(a, b) \sim (c, d)$ povlači $(c, d) \sim (a, b)$. Iz $(a, b) \sim (c, d)$ slijedi da je $ad = bc$. Kako u D vrijedi komutativnost imamo $da = cb$. Relacija $=$ je refleksivna relacija pa slijedi da je $cb = da$ odakle slijedi da je $(c, d) \sim (a, b)$.

3) Tranzitivnost
   Za dokaz tranzitivnosti pretpostavimo da je $(a, b) \sim (c, d)$ i $(c, d) \sim (f, g)$. Tada je $ad = bc$ i $cg = df$. Iz prve jednadžbe slijedi $adg = bdg$ dok iz druge $bcf = bdf$ te zaključujemo da je $adg = bdf$ odnosno $agd = bfd$ (D je komutativno). Kako je D integralna domena i $d \neq 0$ svojstvo poništenja zdesna daje nam $ag = bf$ (vidjeti [1, Theorem 25,1]). Dakle, $(a, b) \sim (f, g)$ čime je dokazana tranzitivnost relacije $\sim$.

□

Klasu ekvivalencije kojoj $(a,b) \in D \times D'$ pripada u odnosu na $\sim$ označavamo s $[a,b]$. Prema tome

$$[a,b] = \{(x,y) \in D \times D' : (x,y) \sim (a,b)\}.$$

S F_D označavamo skup svih gore navedenih klasa ekvivalencije te na tom skupu definiramo operacije množenja i dijeljenja na sljedeći način (prisjetimo se $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$)

$$[a,b] + [c,d] = [ad+bc, bd] \quad \text{i} \quad [a,b] \cdot [c,d] = [ac, bd] \tag{1}$$

za svaki $[a,b], [c,d] \in F_D$. Primjetimo da je $bd \in D'$, jer je $b \in D'$ i $d \in D'$ te D nema djelitelja nule.

Lema 5. *([1, Lemma 30.2]) Ako je $[a_1,b_1] = [a_2,b_2]$ i $[c_1,d_1] = [c_2,d_2]$, onda je*

$$[a_1d_1 + b_1c_1, b_1d_1] = [a_2d_2 + b_2c_2, b_2d_2]$$

i

$$[a_1c_1, b_1d_1] = [a_2c_2, b_2d_2]$$

odnosno gore navedene operacije zbrajanja i množenja su dobro definirane.

Dokaz:
Iz $[a_1,b_1] = [a_2,b_2]$ znamo da je $(a_1,b_1) \sim (a_2,b_2)$ odnosno

$$a_1b_2 = b_1a_2. \tag{2}$$

Slično, iz $[c_1,d_1] = [c_2,d_2]$ znamo da je

$$c_1d_2 = d_1c_2. \tag{3}$$

Trebamo dokazati da je

$$[a_1d_1 + b_1c_1, b_1d_1] = [a_2d_2 + b_2c_2, b_2d_2]$$

odnosno

$$(a_1d_1 + b_1c_1)(b_2d_2) = (b_1d_1)(a_2d_2 + b_2c_2).$$

Koristeći (2) i (3) te svojstvo komutativnosti od D dobivamo sljedeće:

$$\begin{aligned}(a_1d_1 + b_1c_1)(b_2d_2) &= a_1d_1b_2d_2 + b_1c_1b_2d_2 \\ &= a_1b_2d_1d_2 + b_1b_2c_1d_2 \\ &= b_1a_2d_1d_2 + b_1b_2d_1c_2 \\ &= b_1d_1a_2d_2 + b_1d_1b_2d_2 \\ &= (b_1d_1)(a_2d_2 + b_2c_2).\end{aligned}$$

Sljedeće dokazujemo

$$[a_1c_1, b_1d_1] = [a_2c_2, b_2d_2]$$

odnosno

$$a_1c_1b_2d_2 = a_2c_2b_1d_1.$$

Koristeći opet svojstvo komutativnosti i (2) i (3) dolazimo do

$$\begin{aligned} a_1c_1b_2d_2 &= a_1b_2c_1d_2 \\ &= b_1a_2d_1c_2 \\ &= a_2c_2b_1d_1. \end{aligned}$$

□

Lako se pokaže da ako je $c \in D'$ i $[a,b] \in F_D$ tada je $[a,b] = [ca,cb] = [ac,bc]$.

Lema 6. *([1, Lemma 30.3]) F_D s operacijama definiranim kao u (1) je polje. Nula je $[0,e]$, suprotni element od $[a,b]$ je $[-a,b]$, jedinica je $[e,e]$ i inverz od $[a,b] \neq [0,e]$ je $[b,a]$.*

Dokaz:
Prvo ćemo pokazati da je F_D Abelova grupa.

- Asocijativnost zbrajanja
  Za $[a,b],[c,d],[f,g] \in F_D$ vrijedi $[a,b]+([c+d]+[f,g]) = [a,b]+([cg+df,dg]) = [a(dg)+b(cg+df),b(dg)] = [(ad+bd)g+(bd)f,(bd)g] = [ab+bc,bd]+[f,g] = ([a,b]+[c,d])+[f,g]$.

- Postojanje nule
  Za $[a,b] \in F_D$ je $[a,b]+[0,e] = [ae+b\cdot 0,be] = [ae,be] = [a,b]$ i $[0,e]+[a,b] = [0\cdot b+ea,eb] = [ea,eb] = [a,b]$.

- Postojanje suprotnog elementa
  $[a,b]+[-a,b] = [ab-ab,b^2] = [0,b^2]$

- Komutativnost zbrajanja
  Za $[a,b],[c,d] \in F_D$ vrijedi $[a,b]+[c,d] = [ad+bc,bd] = [bc+ad,db] = [c,d]+[a,b]$.

Sljedeće dokazujemo da je množenje asocijativno odnosno

$$\begin{aligned} &[a,b]([c,d][f,g]) = [a,b]([cf,dg]) = [a(cf),b(dg)] = \\ &= [(ac)f,(bd)g] = ([ac,bd])[f,g] = ([a,b][c,d])[f,g]. \end{aligned}$$

Dokažimo sad distributivnost množenja u odnosu na zbrajanje.

$$\begin{aligned} [a,b]([c,d]+[f,g]) &= [a,b][cg+df,dg] \\ &= [acg+adf,bdg] \\ &= [b(acg+adf),b(bdg)] \\ &= [(ac)(bg)+(bd)(af),(bd)(bg)] \\ &= [ac,bd]+[af,bg] \\ &= [a,b][c,d]+[a,b][f,g]. \end{aligned}$$

$$\begin{aligned}([a,b]+[c,d])[f,g] &= [ad+bc,bd][f,g] \\ &= [adf+bcf,bdg] \\ &= [(adf+bcf)g,(bdg)g] \\ &= [(af)(dg)+(cf)(bg),(bg)(dg)] \\ &= [af,bg]+[cf,dg] \\ &= [a,b][f,g]+[c,d][f,g].\end{aligned}$$

Za $[a,b],[c,d] \in F_D$ je

$$[a,b][c,d] = [ac,bd] = [ca,db] = [c,d][a,b]$$

čime je dokazana komutativnost množenja.
Preostaje nam pokazati da je $[e,e]$ jedinica te da je inverzni element $[b,a]$. Da bi $[e,e]$ bilo jedinica mora vrijediti $[a,b][e,e] = [e,e][a,b] = [a,b]$. Za $[a,b] \in F_D$ imamo

$$[a,b][e,e] = [ae,be] = [a,b] \quad \text{i} \quad [e,e][a,b] = [ea,eb] = [a,b].$$

Pretpostavimo da je $[a,b] \neq [0,e]$. Tada je $b \neq 0$, a iz $[a,b] \neq [0,e]$ slijedi $ae \neq b0$ odnosno $a \neq 0$. Tada je $[b,a] \in F_D$ što je inverzni element u odnosu na množenje:

$$[a,b][b,a] = [ab,ba] = [e,e] \quad \text{jer je} \quad ab = ba \neq 0.$$

□

Lema 7. *([1, Lemma 30.4]) Neka D_1 označava podskup od F_D koji se sastoji od svih $[a,e]$ za $a \in D$. Tada je D_1 potprsten od F_D i D i D_1 su izomorfni.*

Dokaz:
Definiramo preslikavanje $\theta : D \to F_D$ s $\theta(a) = [a,e]$ za svaki $a \in D$. Dokazat ćemo da je θ izomorfizam odakle će slijediti da je D_1 potprsten te da su D i D_1 izomorfni.
Jasno je da je slika od θ upravo D_1. Ako je $\theta(a_1) = \theta(a_2)$, onda je $[a_1,e] = [a_2,e]$ odakle slijedi $a_1e = ea_2$ te je $a_1 = a_2$.
Neka su $a,b \in D$. Tada je $\theta(a+b) = [a+b,e] = [ae+be,ee] = [a,e]+[b,e] = \theta(a)+\theta(b)$ i $\theta(ab) = [ab,e] = [ab,ee] = [a,e][b,e] = \theta(a)\theta(b)$. □

Polje F_D konstruirano iz integralne domene D na gore naveden način nazivamo polje kvocijenata od D. Ukoliko prsten R sadrži potprsten izomorfan prstenu S kažemo da se S može uložiti u R. Uz tu terminologiju, pokazali smo da se svaka integralna domena može uložiti u njeno polje kvocijenata. Općenito integralna domena može biti uložena u više polja. Na primjer, integralna domena cijelih brojeva može biti uložena u polje racionalnih brojeva, ali i u polje realnih brojeva.

Teorem 4. *([1, Theorem 30.1]) Ako je D integralna domena, tada postoji polje kvocijenata F_D takvo da*

(a) F_D *sadrži integralnu domenu izomorfnu* D*,*

(b) ako je K *bilo koje polje koje sadrži integralnu domenu izomorfnu* D*, onda* K *sadrži polje izomorfno* F_D*.*

Dokaz:
Lema 4 dokazuje da je F_D polje dok Lema 6 dokazuje svojstvo pod (a).
Za dokaz svojstva pod (b) pretpostavit ćemo da je D zapravo potprsten od K. Zbog načina na koje je polje kvocijenata F_D konstruirano od elemenata iz D imamo prirodnu korespodenciju između elemenata $ab^{-1} \in K$, za $a, b \in D$ i $b \neq 0$ i elemenata $[a, b] \in F_D$. Ako svaki element iz F_D identificiramo s odgovarajućim elementom $([a, b] \leftrightarrow ab^{-1})$, tada možemo F_D zamisliti kako potprsten od K, a to je ono što nam tvdi svojstvo pod (b). □

Polje racionalnih brojeva je jedinstveno polje kvocijenata jedinstvene dobro uređene integralne domene. Ako je K polje karateristike nula, onda K sadržava potprsten izomorfan prstenu cijelih brojeva. To slijedi iz činjenice da integralna domena karakteristike nula sadrži potprsten izomorfan prstenu cijelih brojeva (vidjeti [1, Theorem 27.2]). Osim toga, polje K sadrži potpolje izomorfno polju racionalnih brojeva što nam govori sljedeći korolar.

Korolar 4. *Ako je* K *polje karakteristike nula, onda sadrži potpolje izomorfno polju racionalnih brojeva.*

5 Uređena polja. Polja realnih brojeva.

Nakon što smo iz integralne domene cijelih brojeva prešli na polje racionalnih brojeva dobili smo rješenja svih jednadžbi obilka $ax = b$ (a i b cijeli brojevi, $b \neq 0$). No, pogledamo li jednadžbu $x^2 = 2$ ne postoji racionalan broj x koji je rješenje te jednadžbe. Pokazat ćemo da je $\sqrt{2}$, što je rješenje spomenute jednadžbe, iracionalan. Pitagorejci su prvi otkrili u geometrijskom obliku da ne postoji racionalan broj koji će mjeriti hipotenuzu pravokutnog trokuta kojemu je svaka kateta duljine jedan. U terminima brojevnog pravca to znači da ako odabranemo dvije točke označene s 0 i 1 te druge točke postavimo tako da odgovaraju racionalnim brojevima, neće postojati broj koji će odgovarati točki $\sqrt{2}$ jedinica od 0 u pozitivnom smjeru. Zapravo, mnogo točaka neće odgovarati racionalnim brojevima. Ovaj problem se može riješiti tako da umjesto racionalnih brojeva koristimo realne brojeve. U nastavku, umjesto oznake uređenog para (a, b) i klase ekivivalencije $[a, b]$ koristit ćemo oznaku $\frac{a}{b}$.

Teorem 5. *([1, Theorem 31.1]) Ne postoji racionalan broj x takav da je $x^2 = 2$.*

Dokaz:
Pretpostavimo da vrijedi suprotno, odnosno pretpostavimo da postoje cijeli brojevi a, b i $b \neq 0$ takvi da je $\left(\frac{a}{b}\right)^2 = 2$. Također, pretpostavimo da a i b nemaju zajedničkih djeljitelja osim ± 1. Iz $\left(\frac{a}{b}\right)^2 = 2$ slijedi $a^2 = 2b^2$. Kako je $2b^2$ parno slijedi da je i a^2 parno odnosno a mora biti parno. Dakle, a je oblika $a = 2k$ za neki cijeli broj k. Uvršavanjem $a = 2k$ u $a^2 = 2b^2$ dobivamo $(2k)^2 = 2b^2$ odnosno $2k^2 = b^2$. Kako je $2k^2$ paran, b^2 je paran pa je i b paran. Zaključili smo da su a i b parni te im je 2 zajednički faktor što je u kontradikciji s našom pretpostavkom. □

Prethodnim teoremom smo dokazali da je $\sqrt{2}$ iracionalan broj.

Teorem 6. *[1, Theorem 31.2]) Neka $\mathbb{Q}$ označava polje racionalnih brojeva, a $\mathbb{Q}^p$ skup svih elemenata iz $\mathbb{Q}$ s prikazom $\frac{a}{b}$ tako da je $ab > 0$. Tada je $\mathbb{Q}$ uređeno polje s $\mathbb{Q}^p$ kao skupom pozitivnih elemenata.*

Dokaz:
Prvo ćemo provjeriti je li uvjet ($ab > 0$) da element iz $\mathbb{Q}$ bude u $\mathbb{Q}^p$ neovisan o odabiru. Pretpostavimo da je $\frac{a}{b} = \frac{c}{d}$. Tada je $ad = bc$ te kako je $b^2 > 0$ i $d^2 > 0$ zajedno sa svojstvima relacije $>$ zaključujemo ako je $ab > 0$ tada je

$$abd^2 > 0$$
$$adbd > 0$$
$$bcbd > 0$$
$$cdb^2 > 0$$
$$cd > 0.$$

Slično, ako je $cd > 0$, onda je $ab > 0$. Stoga, $ab > 0$ ako i samo ako $cd > 0$.
Preostaje nam provjeriti svojstva iz definicije uređene integralne domene.

- Zatvorenost obzirom na zbrajanje
  Ako su $\frac{a}{b}$ i $\frac{c}{d}$ iz $\mathbb{Q}^p$, onda je $ab > 0$ i $cd > 0$ pa samim time i $abd^2 > 0$ te $cdb^2 > 0$. To povlači da je $(ad + bc)bd = abd^2 + cdb^2 > 0$ odnosno $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \in \mathbb{Q}^p$.
- Zatvorenost obzirom na množenje
  Ako su $\frac{a}{b}$ i $\frac{c}{d}$ iz $\mathbb{Q}^p$, onda je $ab > 0$ i $cd > 0$ pa slijedi $(ac)(bd) = (ab)(cd) > 0$ odnosno $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in \mathbb{Q}^p$.
- Zakon trihotomije
  Ako je $\frac{a}{b} \in \mathbb{Q}$ element različit od nule, onda je $a \neq 0$ i $b \neq 0$, dakle $ab \neq 0$. Stoga je $ab > 0$ ili $0 > ab$ pa prema tome $\frac{a}{b} \in \mathbb{Q}^p$ ili $-\left(\frac{a}{b}\right) = \frac{-a}{b} \in \mathbb{Q}^p$.

□

Kažemo da je element u uređenog polja F gornja (donja) granica za podskup S od F ako je $u \geq x$ ($u \leq x$) za svaki $x \in S$. Na primjer, svaki pozitivan racionalan broj je gornja granica za skup svih negativnih racionalnih brojeva. Skup cijelih brojeva nema gornju granicu u polju racionalnih brojeva niti u bilo kojem drugom polju.
Kažemo da je element u uređenog polja F najmanja gornja (najveća donja) granica za podskup S od F ako je zadovoljeno

1) u je gornja (donja) granica za S,

2) ako je $v \in F$ gornja (donja) granica, tada je $v \geq u$ ($v \leq u$).

Stoga, najmanja gornja granica za skup negativnih racionalnih brojeva je 0.
Ako S označava skup svih racionalnih brojeva r takvih da je $r^2 < 2$, tada S ima gornju granicu, ali ne i najmanju gornju granicu u polju racionalnih brojeva. Najmanju gornju granicu S ima u polju realnih brojeva.

Definicija 14. *Kažemo da je uređeno polje F potpuno ukoliko svaki neprazan podskup od F koji ima gornju granicu u F ima najmanju gornju granicu u F.*

Teorem 7. *[1, Theorem 31.3] Postoji potpuno uređeno polje. Bilo koja dva takva polja su izomorfna i svako takvo polje sadrži potpolje izomorfno polju racionalnih brojeva.*

Polje realnih brojeva je potpuno uređeno polje. Prethodni teorem nam pokazuje da takvo polje postoji i da je ono jedinstveno, a iz rezultata prethodnih poglavlja slijedi činjenica da sadrži potpolje izomorfno polju racionalnih brojeva.
Realni brojevi se u primjenama smatraju brojevim koji imaju decimalni zapis. Primjeri takvih brojeva su (vidi [1, str. 148.])

$$\begin{array}{ll} \frac{1}{2} = 0.5 & \frac{1}{3} = 0.\overline{3} \\ -12.138 & \frac{11}{7} = 1.\overline{571428} \\ \sqrt{2} = 1.414213\ldots & \pi = 3.141592\ldots \end{array}$$

gdje crta iznad brojeva označava da se ti brojevi stalno ponavljaju. Može se pokazati da periodičan decimalan broj predstavlja racionalan broj. Brojevi π i e su iracionalni, ali dokaz toga je puno teži od dokaza iracionalnosti $\sqrt{2}$.

6 Polje kompleksnih brojeva

Kako je kvadrat bilo kojeg nenul elementa uređene integralne domene pozitivan ne postoji realan broj x takav da je $x^2 = -1$ (Lema 1). Ovaj problem rješavamo uvođenjem polja kompleksnih brojeva koje kao potpolje sadrži polje realnih brojeva.

Teorem 8. ***(Osnovni teorem algebre)****([1, Theorem 32.1])*
Svaka polinomijalna jednadžba

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{4}$$

stupnja barem jedan i čiji su koeficijenti $a_n, a_{n-1}, \ldots, a_1, a_0$ kompleksni brojevi ima barem jedno rješenje u polju kompleksnih brojeva.

Kroz prethodna poglavlja smo vidjeli da smo za rješavanje određenih jednadžbi cijele brojeve proširili na racionalne dok smo racionalne proširili na realne. U ovom poglavlju realne brojeve proširujemo na kompleksne brojeve. Ono što nam osnovni teorem algebre kaže je da neće biti potrebe za daljnim proširenjem jer svaka jednadžba s kompleksnim brojevima kao koeficijentima imat će rješenje u polju kompleksnih brojeva. Kao što smo vidjeli, racionalni brojevi su konstruirani pomoću klasa ekvivalencije uređenih parova cijelih brojeva. Kompleksne brojeve ćemo konstruirati pomoću klasa ekvivalencije uređenih parova realnih brojeva.

Teorem 9. *([1, Theorem 32.2]) Neka $\mathbb{C}$ označava skup svih uređenih parova (a, b) gdje su $a, b \in \mathbb{R}$. Definiramo operaciju zbrajanja i množenja parova na sljedeći način:*

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

za sve $a, b, c, d \in \mathbb{R}$. S tako definiranim operacijama $\mathbb{C}$ je polje. Podskup od $\mathbb{C}$ koji se sastoji od svih $(a, 0)$ za $a \in \mathbb{R}$ tvori potpolje od $\mathbb{C}$ izomorfno $\mathbb{R}$.

Dokaz:
Koristeći definiciju zbrajanja i množenja te svojstva realnih brojeva za $(a, b), (c, d), (e, f) \in \mathbb{C}$ imamo sljedeće:

1) Asocijativnost zbrajanja

$$\begin{aligned}(a, b) + [(c, d) + (e, f)] &= (a, b) + (c + e, d + f) \\ &= (a + (c + e), b + (d + f)) \\ &= ((a + c) + e, (b + d) + f) \\ &= (a + c, b + d) + (e, f) \\ &= [(a, b) + (c, d)] + (e, f).\end{aligned}$$

2) Postojanje neutralnog elementa za zbrajanje

$$(a, b) + (0, 0) = (a + 0, b + 0) = (a, b) \quad \text{i} \quad (0, 0) + (a, b) = (0 + a, 0 + b) = (a, b).$$

3) Postojanje suprotnog elemenata

$$(a,b)+(-a,-b)=(a+(-a),b+(-b))=(0,0)$$

$$(-a,-b)+(a,b)=(-a+a,-b+b)=(0,0).$$

4) Komutativnost zbrajanja

$$(a,b)+(c,d)=(a+c,b+d)=(c+a,d+b)=(c,d)+(a,b).$$

5) Asocijativnost množenja

$$\begin{aligned}(a,b)[(c,d)(e,f)] &= (a,b)(ce-df,cf+de)\\ &= (a(ce-df)-b(cf+de),a(cf+de)+b(ce-df))\\ &= (ace-adf-bcf-bde,acf+ade+bce-bdf)\\ &= ((ac-bd)e-(ad+bc)f,(ac-bd)f+(ad+bc)e)\\ &= (ac-bd,ad+bc)(e,f)\\ &= [(a,b)(c,d)](e,f).\end{aligned}$$

6) Distributivnost množenja u odnosu na zbrajanje

$$\begin{aligned}(a,b)[(c,d)+(e,f)] &= (a,b)(c+e,d+f)\\ &= (a(c+e)-b(d+f),(a(d+f)+b(c+e))\\ &= (ac+ae-bd-bf,ad+af+bc+be)\\ &= (ac-bd+ae-bf,ad+bc+af+be)\\ &= (ac-bd,ad+bc)+(ae-bf,af+be)\\ &= (a,b)(c,d)+(a,b)(e,f)\end{aligned}$$

$$\begin{aligned}[(a,b)+(c,d)](e,f) &= (a+c,b+d)(e,f)\\ &= ((a+c)e-(b+d)f,(a+c)f+(b+d)e)\\ &= (ae+ce-bf-df,af+cf+be+de)\\ &= (ae-bf+ce-df,af+be+cf+de)\\ &= (ae-bf,af+be)+(ce-df,cf+de)\\ &= (a,b)(e,f)+(c,d)(e,f).\end{aligned}$$

7) Komutativnost množenja

$$\begin{aligned}(a,b)(c,d) &= (ac-bd,ad+bc)\\ &= (ca-db,cd+da)\\ &= (c,d)(a,b).\end{aligned}$$

8) Postojanje neutralnog elementa za množenje

$$(a,b)(1,0) = (1,0)(a,b) = (a\cdot 1 - b\cdot 0, a\cdot 0 + b\cdot 1) = (a,b).$$

9) Postojanje inverznog elemnat
Pretpostavimo da je $(a,b) \neq (0,0)$. Tada je $a \neq 0$ ili $b \neq 0$ tako da je $a^2 > 0$ ili $b^2 > 0$ i $a^2 + b^2 > 0$. Prema tome, element $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$ je element iz $\mathbb{C}$ i to je inverz od (a,b) u odnosu na množenje:

$$(a,b)\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)(a,b) = \left(\frac{a^2+b^2}{a^2+b^2}, \frac{-ab+ba}{a^2+b^2}\right).$$

Dakle, dokazali smo da je $\mathbb{C}$ polje. Kako bismo dokazali da je $\{(a,0) : a \in \mathbb{R}\}$ potpolje izomorfno $\mathbb{R}$ pogledajmo preslikavanje $\theta : \mathbb{R} \to \mathbb{C}$ dano sa $\theta(a) = (a,0)$ za svaki $a \in \mathbb{R}$. Dano preslikavanje čuva obje operacije:

$$\theta(a+b) = (a+b,0) = (a+b, 0+0) = (a,0) + (b,0) = \theta(a) + \theta(b)$$

i

$$\theta(ab) = (ab,0) = (a,0)(b,0) = \theta(a)\theta(b)$$

za svaki $a, b \in \mathbb{R}$. Također, ako je $\theta(a) = \theta(b)$, onda je $(a,0) = (b,0)$ odnosno $a = b$. Dakle, θ je izomorfizam sa $\mathbb{R}$ na $\{(a,0) : a \in \mathbb{R}\}$. □

Prirodno je element $a \in \mathbb{R}$ identificirati s $(a,0) \in \mathbb{C}$. Na taj način $\mathbb{R}$ postaje podskup od $\mathbb{C}$ pa je svaki realan broj ujedno i kompleksan broj. Element $(0,1) \in \mathbb{C}$ obično označavamo s i te svaki element $(0,b) \in \mathbb{C}$ s bi. To nas dovodi do oznake $a+bi$ za element $(a,b) \in \mathbb{C}$. Za $a, b, c, d \in \mathbb{R}$

$$a + bi = c + di \quad \text{ako i samo ako} \quad a = c \ \text{ i } \ b = d.$$

Pravila za zabrajanje i množenje tada su:

$$(a+bi) + (c+di) = (a+c) + (b+di)$$

i

$$(a+bi)(c+di) = (ac-bd) + (ad+bc)i.$$

Posebno, $i^2 = (0+1\cdot i)(0+1\cdot i) = -1+0\cdot i = -1$, pa je stoga i rješenje jednadžbe $x^2 = -1$. Za računanje elemenata iz $\mathbb{C}$ koristimo razne asocijativna, komutativne i distributivne zakone, zamjenjimo $i^2 = -1$ gdje je potrebno te se tako svaki izraz s kompleksnim brojevima svodi na oblik $a+bi$ za $a, b \in \mathbb{R}$. Kada je $a = 0$ kažemo da je takav broj čisto imaginaran.

Primjer 1. *([1, Example 32.1])*

a) $(1+i)^2 = 1 + 2i + i2 = 1 + 2i - 1 = 2i$

b) $i^4 = (i^2)^2 = (-1)^2 = 1$

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

d) $i(1-i) + 2(3+i) = i - i^2 + 6 + 2i = i - (-1) + 6 + 2i = i + 1 + 6 + 2i = 7 + 3i.$

Broj $a - bi$ zovemo kompleksno konjugirani broj od $a + bi$. Kako bismo pojednostavnili razlomke s kompleksnim brojem u nazivniku, množimo i brojnik i nazivnik sa kompleksno konjugiranim brojem nazivnika koristeći $(a + bi)(a - bi) = a^2 - (bi)^2 = a^2 + b^2$.

Primjer 2. *([1, Example 32.2])*

a) $\dfrac{1}{1+i} = \dfrac{1}{1+i}\dfrac{1-i}{1-i} = \dfrac{1-i}{2} = \dfrac{1}{2} - \dfrac{1}{2}i$

b) $\dfrac{2+i}{2-i} = \dfrac{2+i}{2-i}\dfrac{2+i}{2+i} = \dfrac{4+4i-1}{4+1} = \dfrac{3}{5} + \dfrac{4}{5}i$

Ako su E i F polja, tada kažemo da je E proširenje polja F ako E sadrži potpolje izomorfno polju F. Stoga, polje realnih brojeva je proširenje polja raconalnih brojeva, a polje kompleksnih brojeva proširenje polja realnih i racionalnih brojeva. Svako polje je proširenje samog sebe.

Neka je E proširenje polje F. Za element $a \in E$ kažemo da je algebarski nad F ukoliko je a rješenje neke polinomijalne jednadžbe (4) s koeficijentima u F.
Polje E je algebarsko proširenje polja F ako je svaki element $a \in E$ algebarsko nad F.

Na primjer, $\sqrt{2}$ je algebarski nad $\mathbb{Q}$ jer je rješenje jednadžbe $x^2 - 2 = 0$. Kako π i e nisu algebarski nad $\mathbb{Q}$ slijedi da $\mathbb{R}$ nije algebarsko proširenje od $\mathbb{Q}$. Polje kompleksnih brojeva je algebersko proširenje polja realnih brojeva.

Kažemo da je polje F algebarski zatvoreno ako svaka jednadžba (4) s koeficijentima u F ima rješenje u F. Prema osnovnom teoremu algebre slijedi da je $\mathbb{C}$ alglebarski zatvoreno, dok ni $\mathbb{Q}$ ni $\mathbb{R}$ nisu algebarski zatvoreni.
Polje E je algebarski zatvarač polja F ukoliko je :

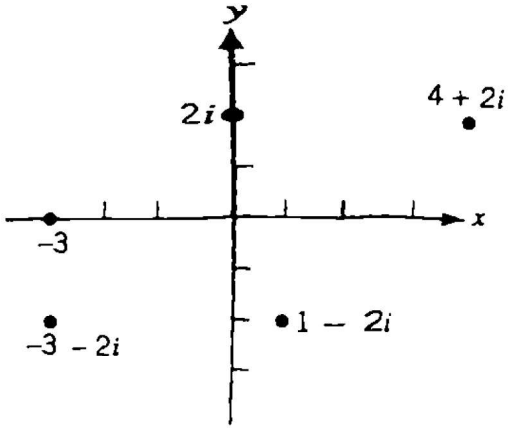
1) E algebarsko proširenje polja F,

2) E je algebarski zatvoreno.

Može se pokazati da svako polje ima algebarski zatvarač. Ako su E_1 i E_2 algebarski zatvarači polja F, tada su E_1 i E_2 izomorfni. Kako je $\mathbb{C}$ algebarsko proširenje od $\mathbb{R}$ te je $\mathbb{C}$ algebarski zatvoreno slijedi da je $\mathbb{C}$ algebarski zatvarač od $\mathbb{R}$. Dakle, polje kompleksnih brojeva je jedinstveni algebarski zatvarač potpuno uređenog polja. Kako $\mathbb{R}$ nije algebarski zatvoreno te $\mathbb{C}$ nije algebarsko proširenje od $\mathbb{Q}$ oni nisu algebarski zatvarači od $\mathbb{Q}$. Algebarski zatvarač od $\mathbb{Q}$ je potpolje od $\mathbb{C}$ koje je poznato kao polje algebarskih brojeva. To polje se sastoji od elemenata iz $\mathbb{C}$ koji su algebarski nad $\mathbb{Q}$.

7 Kompleksni korijeni iz jedinice

U prethodnim poglavljima bavili smo se nekim općim svojstvima. U ovom poglavlju bavit ćemo se računanjem. Promatrat ćemo načine reprezentacija kompleksnih brojeva te kako se oni mogu koristiti u određivanju rješenja jednadžbe oblika $x^n = 1$. Kao što za geometrijski prikaz realnih brojeva koristimo točke na pravcu, tako za geometrijski prikaz kompleksnih brojeva koristimo točke u ravnini. U pravokutnom koordinatnom sustavu svaki kompleksni broj $a + bi$ prikazan je točkom (a, b). Na slici možemo vidjeti neke primjere prikaza kompleksnih brojeva.



Slika 1: Prikaz kompleksnih brojeva (vidi [1, Figure 33.1])

Zbrajanje kompleksnih brojeva odgovara vektorskom zbrajanju točaka u ravnini odnosno

$$(a + bi) + (c + di) = (a + c) + (b + d)i \leftrightarrow (a + c, b + d) = (a, b) + (c, d).$$

Za geometrijski opis množenja kompleksnih brojeva prelazimo na polarne koordinate. Prisjetimo se da je (r, θ) polarni prikaz točke (a, b), gdje je r udaljenost između iskodišta i dane točke, a θ označava kut od pozitivne x-osi do polupravca iz ishodišta kroz danu točku, s pozitivnim smjerom suprotnim od smjera kazaljke na satu (Slika 2).

Prema tome,

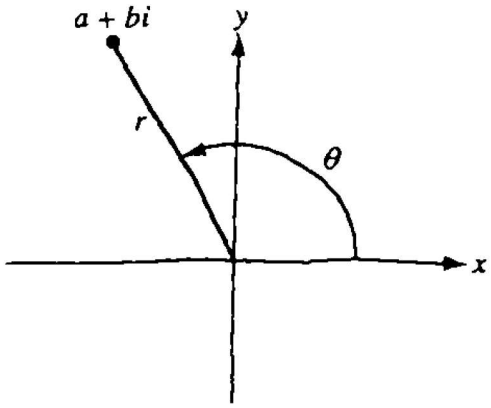
$$r = \sqrt{a^2 + b^2},$$

$$a = r \cos \theta,$$

$$b = r \sin \theta,$$

$$a + bi = r(\cos \theta + i \sin \theta).$$

To zovemo polarni ili trigonometrijski prikaz od $a+bi$. Nenegativni broj r nazivamo apsolutna vrijednost ili modul od $a + bi$ i označavamo s $|a + bi|$ te je on jedinstven. Kut θ nazivamo argument kompleksnog broja $a+bi$. Ako je θ argument, onda je i $\theta+2n\pi$ također argument za bilo koji prirodan broj n odnosno argument kompleksnog broja nije jedinstven. Ukoliko θ ograničimo tako da je $0 \leq \theta < 2\pi$, tada svaki kompleksni broj ima jedinstveni argument.



Slika 2: Polarne koordinate (vidi [1, Figure 33.2])

Primjer 3. *([1, Example 33.1]) Odredimo trigonometrijski prikaz broja* $-2+2i$.
Apsolutna vrijednost od $-2+2i$ *je* $r = |-2+2i| = \sqrt{(-2)^2+2^2} = 2\sqrt{2}$, *a najmanji pozitivni argument je* $\theta = \frac{3\pi}{4} = 135°$.
Trigonometrijski prikaz broja $-2+2i$ *je tada oblika* $2\sqrt{2}(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4})$.

Trigonometrijski oblik kompleksnog broja je prikladan za množenje kompleksnih brojeva što nam govori sljedećih teorem.

Teorem 10. *([1, Theorem 33.1]) Ako je* $z = r(\cos\theta + i\sin\theta)$ *i* $w = s(\cos\phi + i\sin\phi)$, *tada je*

$$zw = rs(\cos(\theta+\phi) + i\sin(\theta+\phi)).$$

Apsolutna vrijednost umnoška kompleksnih brojeva je umnožak apsolutnih vrijednosti, a argument umnoška je suma argumenata.

Dokaz:
U dokazu koristimo sljedeće dvije formule:

$$\cos(\theta+\phi) = \cos\theta\cos\phi - \sin\theta\sin\phi$$

i

$$\sin(\theta+\phi) = \sin\theta\cos\phi + \cos\theta\sin\phi.$$

Korištenjem gornjih formula dobivamo

$$\begin{aligned} zw &= r(\cos\theta + i\sin\theta)\cdot s(\cos\phi + i\sin\phi) \\ &= rs[(\cos\theta\cos\phi - \sin\theta\sin\phi) + i(\sin\theta\cos\phi + \cos\theta\sin\phi)] \\ &= rs(\cos(\theta+\phi) + i\sin(\theta+\phi). \end{aligned}$$

□

De Moivreov teorem. *([1, str. 156]) Neka je* n *prirodan broj i* $z = r(\cos\theta + i\sin\theta)$. *Tada je* $z^n = r^n(\cos(n\theta) + i\sin(n\theta))$.

Dokaz:
Dokaz provodimo matematičkom indukcijom po n.

1) Za $n = 1$ rezultat je očit.

2) Pretpostavimo da je teorem točan za $n = k$. Koristeći prethodni teorem za množenje kompleksnih brojeva za $w = z^k$ imamo

$$\begin{aligned} z^{k+1} &= zz^k = r(\cos\theta + i\sin\theta)r^k(\cos(k\theta) + i\sin(k\theta)) \\ &= r^{k+1}(\cos((k+1)\theta) + i\sin((k+1)\theta)). \end{aligned}$$

□

Primjer 4. *Izračunajmo* $(-2+2i)^5$.
Kao što vidimo $-2+2i$ *je kompleksni broj iz Primjera 3 pa već imamo njegov trigonometrijski zapis koji je oblika* $2\sqrt{2}(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4})$. *Primjenjujući sad De Moivreov teorem imamo:*

$$\begin{aligned} (-2+2i)^5 &= (2\sqrt{2})^5\left(\cos\frac{5\cdot 3\pi}{4} + i\sin\frac{5\cdot 3\pi}{4}\right) \\ &= 128\sqrt{2}\left(\cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4}\right) \\ &= 128\sqrt{2}\left(\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right) \\ &= 128 - 128i. \end{aligned}$$

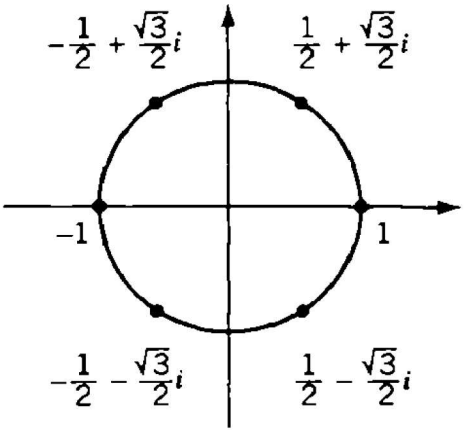
Za svaki prirodni broj $n \geq 1$ postoji najviše n različitih kompleksnih brojeva koji su rješenja jednadžbe $x^n = 1$. Zapravo postoji točno n rješanja koja nazivamo kompleksni n-ti jedinični korijen te se oni mogu odrediti koristeći De Moivreovu formulu.

Teorem 11. *Za svaki prirodni broj* $n \geq 1$, n *različitih vrijednosti* n*-tog korijena iz jedinice su oblika*

$$\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \quad k = 0, 1, \ldots, n-1. \tag{5}$$

Dokaz:
Prema De Moivreovom teoremu argument n-te potencije svakog broja iz (5) je $n\frac{2k\pi}{n} = 2k\pi$, a apsolutna vrijednost je $1^n = 1$. Stoga je svaki od brojeva n-ti jedinični korijen. Brojevi u (5) su različiti jer su $\frac{2k\pi}{n}$ različiti te je $0 \leq \frac{2k\pi}{n} < 2\pi$ za $k = 0, 1, \ldots, n-1$. Prema tome, brojevi u (5) predstavljaju sve n-te korijene iz jedinice. □

Geometrijski gledano, n-ti korijen iz jedinice predstavljen je s n jednako razmaknutih točaka na jediničnoj kružnici sa središtem u ishodištu, pri čemu je jedna od točaka jedinica. Na slici 3 možemo vidjeti geometrijski prikaz za $n = 6$.



Slika 3: Geometrijski prikaz rješenja $\sqrt[6]{1}$ (vidi [1, Figure 33.3])

Može se pokazati da su n-ti korijeni kompleksnog broja $z = r(\cos\theta + i\sin\theta)$ dani s

$$\sqrt[n]{r}\left(\cos\frac{\theta+2k\pi}{n} + i\sin\frac{\theta+2k\pi}{n}\right), \quad k = 0, 1, \ldots, n-1.$$

Literatura

[1] J. R. Durbin, *Modern Algebra: An Introduction*, Sixth Edition, The University of Texas at Austin, 2008.

[2] T. W. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.

Sažetak

U ovom diplomskom radu bavit ćemo se brojevnim sustavima te njihovim razlikama u smislu svojstava koje imaju kao prsten ili polje. Kroz poglavlja navest ćemo razloge zbog kojih uvodimo pojedine brojeve kao i sami način konstrukcije tih brojeva. Uz osnovne pojmove, iskazat ćemo i dokazati neka svojstva koja vrijede za pojedina polja i prstene. Osim teorije, također ćemo dati neke primjere.
Ključne riječi: prsten, integralna domena, polje

Algebraic properties of important sets of numbers

Summary

In this thesis, we will deal with number systems and their differences in the terms of the properties they have as a ring or a field. Through the chapters, we will specify the reasons for which we introduce individual numbers as well as the very method of construction of those numbers. In addition to the basic concepts, we will state and prove some properties that are valid for individual fields and rings. Besides the theory, we will also provide some examples.

Keywords: ring, integral domain, field

Životopis

Rođena sam 18. srpnja 1998. godine u Požegi. Nakon završene osnovne škole upisujem Gimnaziju u Požegi, prirodoslovno - matematički smijer. Po završetku srednje škole 2017. godine upisujem preddiplomski studij matematike na Odjelu za matematiku u Osijeku. Preddiplomski studij završavam 2020. godine sa završnim radom na temu Newtonova metoda za rješavanje nelinearnih jednadžbi pod mentorstvom izv. prof. dr. sc. Tomislava Marošević. Iste godine upisujem diplosmki studij matematike, smjer Financijska matematika i statistika.