Hiperbolički brojevi

Crnjak, Maria

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Maria Crnjak

HIPERBOLIČKI BROJEVI

Diplomski rad

Voditelj rada:
Izv. prof. dr. sc. Zvonko Iljazović

Zagreb, srpanj, 2020.

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

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

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Zahvalu upućujem svima koji su direktno ili indirektno bili uključeni u proces dostizanja ovog cilja - naizgled iz nekog drugog svijeta. Međutim, očigledno postoji izomorfizam među svjetovima, jer inače danas ovog rada ne bi bilo!

Sadržaj

Uvod

U ovom radu će se proučavati strukture skupova prirodnih, cijelih i racionalnih brojeva, te određene algebarske strukture koje proširuju polje realnih brojeva. Između ostalog, proučavat će se kvaternioni i hiperbolički brojevi.
U prvom poglavlju proučavamo grupe i prstene, a definirat će se i potpuno uređeno polje.
U drugom poglavlju definiramo prirodne, cijele i racionalne brojeve unutar fiksiranog polja realnih brojeva.
U trećem poglavlju proučavamo potprstene i potpolja.
U četvrtom poglavlju definiramo polje kompleksnih brojeva $\mathbb{C}$, zatim proučavamo određeno potpolje od $\mathbb{C}$ izomorfno s $\mathbb{R}$ te na kraju definiramo morfizam uređenih skupova.
U petom poglavlju definiramo i proučavamo svojstva tijela kvaterniona $\mathbb{H}$, proučavamo morfizme i izomorfizme prstenova, te razmatramo određeno polje u $\mathbb{H}$ koje je izomorfno sa $\mathbb{C}$.
U šestom, konačnom, poglavlju definiramo prsten hiperboličkih brojeva $\mathbb{D}$, te proučavamo određeno polje u $\mathbb{D}$ koje je izomorfno sa $\mathbb{R}$.

Poglavlje 1

Potpuno uređena polja

1.1 Grupe i prsteni

Definicija 1. *Neka je S skup. Za bilo koju funkciju sa $S \times S$ u S kažemo da je* ***binarna operacija*** *na S.*

Ako je $f : S \times S \to S$ tj. f je binarna operacija na S, onda ćemo za $x, y \in S$, umjesto $f(x, y)$ pisati xfy.

Binarne operacije na skupu S obično označavamo sa $\cdot$, $+$, $*$, i sl., pa ćemo za $x, y \in S$ vrijednost binarne operacije na uređenom paru (x, y) označavati sa $x \cdot y$, $x + y$, $x * y$, ...

Definicija 2. *Neka je $\cdot$ binarna operacija na skupu S. Kažemo da je $\cdot$* ***komutativna*** *binarna operacija, ako za $\forall x, y \in S$ vrijedi $x \cdot y = y \cdot x$.*

Definicija 3. *Neka je $\cdot$ binarna operacija na skupu S. Kažemo da je $\cdot$* ***asocijativna*** *binarna operacija ako za $\forall x, y, z \in S$ vrijedi $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.*

Definicija 4. *Za uređeni par $(S, \cdot)$, gdje je $\cdot$ asocijativna binarna operacija na skupu S, kažemo da je* ***polugrupa****.*

Definicija 5. *Neka je $\cdot$ binarna operacija na skupu S, te neka je $e \in S$. Kažemo da je e* ***neutralni element*** *za binarnu operaciju $\cdot$, ako za $\forall x \in S$ vrijedi $x \cdot e = x$ i $e \cdot x = x$.*

Napomena 6. *Neutralni element za binarnu operaciju, ako postoji, mora biti jedinstven.*

Naime, pretpostavimo da je $\cdot$ binarna operacija na skupu S te da su e_1 i e_2 neutralni elementi za binarnu operaciju $\cdot$. Znamo da je po definiciji neutralnog elementa, $e_1 \cdot x = x$, za $\forall x \in S$. Posebno vrijedi $e_1 \cdot e_2 = e_2$.

S druge strane, iz činjenice da je e_2 neutralni element za binarnu operaciju $\cdot$ slijedi da je $x \cdot e_2 = x$, za $\forall x \in S$, pa je posebno $e_1 \cdot e_2 = e_1$.

Dakle, $e_1 \cdot e_2 = e_2$ i $e_1 \cdot e_2 = e_1$, pa je očito $e_1 = e_2$.

Definicija 7. *Neka je* $(S, \cdot)$ *polugrupa. Pretpostavimo da binarna operacija* $\cdot$ *ima neutralni element. Tada za* $(S, \cdot)$ *kažemo da je* ***monoid****.*

Napomena 8. *Ako je* $(S, \cdot)$ *monoid, onda ćemo za neutralni element za binarnu operaciju* $\cdot$ *reći da je neutralni element u monoidu* $(S, \cdot)$ *i obično ćemo ga označavati sa* e*.*

Definicija 9. *Neka je* $(S, \cdot)$ *monoid te neka je* $x \in S$*. Za* $y \in S$ *kažemo da je* ***inverzni element od*** x *u monoidu* $(S, \cdot)$ *ako je* $x \cdot y = e$ *i* $y \cdot x = e$*.*

Napomena 10. *Inverzni element nekog elementa u monoidu, ako postoji, mora biti jedinstven.*

Naime, pretpostavimo da je $(S, \cdot)$ monoid, $x \in S$ te da su y_1 i y_2 inverzni elementi od x. Koristeći $x \cdot y_2 = e$ i $y_1 \cdot x = e$ dobivamo:

$$y_1 = y_1 \cdot e = y_1 \cdot (x \cdot y_2) = (y_1 \cdot x) \cdot y_2 = e \cdot y_2 = y_2$$

Dakle, $y_1 = y_2$.

Napomena 11. *Ako je* $(S, \cdot)$ *monoid i* $x \in S$ *element koji ima inverzni element, onda ćemo inverzni element od* x *obično označavati sa* x^{-1}*.*

Definicija 12. *Neka je* $(S, \cdot)$ *monoid. Pretpostavimo da svaki element od* S *ima inverzni element u monoidu* $(S, \cdot)$*. Tada za* $(S, \cdot)$ *kažemo da je* ***grupa****.*

Definicija 13. *Za grupu* $(S, \cdot)$ *kažemo da je* ***komutativna*** *ili* ***Abelova*** *ako je binarna operacija* $\cdot$ *komutativna.*

Lema 14. *Neka je* S *skup te neka su* $+$ *i* $\cdot$ *binarne operacije na* S*. Za uređenu trojku* $(S, +, \cdot)$ *kažemo da je* ***prsten*** *ako vrijedi sljedeće:*

1. $(S, +)$ *je Abelova grupa.*
2. $(S, \cdot)$ *je polugrupa.*
3. *za* $\forall x, y, z \in S$ *vrijedi:*

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z) \tag{1.1}$$
$$(x + y) \cdot z = (x \cdot z) + (y \cdot z)$$

U tom slučaju za binarnu operaciju $+$ *kažemo da je zbrajanje u prstenu* $(S, +, \cdot)$*, a za binarnu operaciju* $\cdot$ *da je množenje u prstenu* $(S, +, \cdot)$*.*

Napomena 15. *Ako je* $(S, +, \cdot)$ *prsten, onda ćemo kao i inače podrazumijevati prilikom korištenja oznaka* $+$ *i* $\cdot$ *da množenje ima veći prioritet od zbrajanja. Tako ćemo na primjer umjesto* (1.1) *pisati naprosto* $x \cdot (y + z) = x \cdot y + x \cdot z$*.*

Napomena 16. *Ako je* $(S, +, \cdot)$ *prsten, onda ćemo neutralni element za operaciju* $+$ *zvati* ***nula u prstenu*** $(S, +, \cdot)$ *i obično označavati sa* 0.

Nadalje, za $x \in S$ *ćemo sa* $-x$ *označavati inverzni element od* x *u* $(S, +)$. *Dakle,* $x + (-x) = 0$ *i* $(-x) + x = 0$.

Lema 17. *Neka je* $(G, \cdot)$ *grupa.*

1. *Neka su* $a, b, c \in G$ *tako da je* $a \cdot b = a \cdot c$. *Tada je* $b = c$.

2. *Neka su* $a, b \in G$ *tako da je* $a \cdot b = a$. *Tada je* $b = e$.

Dokaz.

1. Iz $a \cdot b = a \cdot c$ slijedi $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c)$, pa je
   $(a^{-1} \cdot a) \cdot b = (a^{-1} \cdot a) \cdot c$, tj. $e \cdot b = e \cdot c$.
   Dakle, $b = c$.

2. Iz $a \cdot b = a$ slijedi $a \cdot b = a \cdot e$, pa iz tvrdnje 1. slijedi $b = e$.

□

Propozicija 18. *Neka je* $(S, +, \cdot)$ *prsten te neka je* $x \in S$. *Tada je* $x \cdot 0 = 0$ *i* $0 \cdot x = 0$.

Dokaz. Vrijedi:

$$x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0. \tag{1.2}$$

Definirajmo $a = x \cdot 0$. Iz (1.2) slijedi $a = a + a$, pa prema lemi 17. 2. vrijedi $a = 0$, odnosno $x \cdot 0 = 0$.

Analogno se dokaže da je $0 \cdot x = 0$. □

Definicija 19. *Za prsten* $(S, +, \cdot)$ *kažemo da je komutativan ako je binarna operacija* $\cdot$ *komutativna.*

Definicija 20. *Neka je* $(S, +, \cdot)$ *prsten. Kažemo da je* $(S, +, \cdot)$ ***prsten s jedinicom*** *ako binarna operacija* $\cdot$ *ima neutralni element. U tom slučaju, taj neutralni element obično označavamo sa* 1 *i zovemo* ***jedinica u prstenu*** $(S, +, \cdot)$.

Definicija 21. *Za prsten* $(S, +, \cdot)$ *kažemo da je* ***integralna domena*** *ako za* $\forall x, y \in S$ *takve da su* $x, y \neq 0$ *vrijedi* $x \cdot y = 0$.

Napomena 22. *Neka je* $(S, +, \cdot)$ *prsten. Pretpostavimo da je* $(S, \cdot)$ *grupa. Tada za* $\forall x \in S\ \exists y \in S$ *tako da vrijedi* $x \cdot y = 1$ *i* $y \cdot x = 1$.

Posebno, za $x = 0\ \exists y \in S$ *tako da vrijedi* $0 \cdot y = 1$ *i* $y \cdot 0 = 1$.

Iz propozicije 18. slijedi da je $0 \cdot y = 0$. Stoga je $0 = 1$. Neka je $x \in S$ neki element iz S. Imamo $x = x \cdot 1 = x \cdot 0 = 0$. Dakle, $x = 0$, $\forall x \in S$, tj. $S = \{0\}$.

Zaključak: Ako je $(S, +, \cdot)$ prsten takav da je $(S, \cdot)$ grupa, onda je $S = \{0\}$, tj. prsten $(S, +, \cdot)$ je trivijalan.

Napomena 23. *Za prsten $(S, +, \cdot)$ kažemo da je trivijalan ako je S jednočlan skup. Inače kažemo da je prsten netrivijalan.*

Napomena 24. *Neka je $(S, +, \cdot)$ prsten s jedinicom. Tada je $(S, +, \cdot)$ trivijalan prsten ako i samo ako je $0 = 1$.*

Naime, ako je $(S, +, \cdot)$ trivijalan prsten, onda je očito $0 = 1$. Obratno, ako je $0 = 1$, onda kao u napomeni 16. vidimo da je $(S, +, \cdot)$ trivijalan prsten.

Definicija 25. *Neka je $(S, +, \cdot)$ netrivijalan prsten s jedinicom. Pretpostavimo da za $\forall x \in S$ td. je $x \neq 0$ vrijedi da x ima inverzni element u monoidu $(S, \cdot)$, odnosno $\exists y \in S$ td. $x \cdot y = 1$ i $y \cdot x = 1$. Tada za $(S, +, \cdot)$ kažemo da je **tijelo**.*

Propozicija 26. *Neka je $(S, +, \cdot)$ tijelo. Tada je $(S, +, \cdot)$ integralna domena.*

Dokaz. Neka su $x, y \in S$ takvi da $x \neq 0$ i $y \neq 0$. Pretpostavimo da je $x \cdot y = 0$.

Obzirom da je $(S, +, \cdot)$ tijelo, x ima inverzni element u $(S, \cdot)$ [oznake x^{-1}]. Slijedi $x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0$. Nadalje, vrijedi $(x^{-1} \cdot x) \cdot y = 0$, tj. $1 \cdot y = 0$, pa je $y = 0$. To je u kontradikciji s početnom pretpostavkom da je $y \neq 0$.

Zaključak: $x \cdot y \neq 0$.

Slijedi da je $(S, +, \cdot)$ integralna domena. □

Definicija 27. *Neka je $(S, +, \cdot)$ tijelo. Pretpostavimo da je binarna operacija $\cdot$ komutativna. Tada za $(S, +, \cdot)$ kažemo da je **polje**.*

1.2 Uređeni prsteni i polja

Definicija 28. *Neka je S skup te neka je $\rho \subseteq S \times S$. Tada za ρ kažemo da je **binarna relacija** na S. Ako je ρ binarna relacija na skupu S te ako su $x, y \in S$ td. je $(x, y) \in \rho$, onda pišemo $x \rho y$.*

Definicija 29. *Neka je $\leq$ binarna relacija na S.*

1. *Kažemo da je $\leq$ **refleksivna relacija** na S ako je $x \leq x$, $\forall x \in S$.*
2. *Kažemo da je $\leq$ **antisimetrična relacija** na S ako za $\forall x, y \in S$ td. je $x \leq y$ i $y \leq x$, vrijedi $x = y$.*

3. *Kažemo da je* $\leq$ ***tranzitivna relacija*** *na* S *ako za* $\forall x, y, z \in S$ *td. je* $x \leq y$ *i* $y \leq z$*, vrijedi* $x \leq z$*.*

Za binarnu relaciju na skupu S *koja je refleksivna, antisimetrična i tranzitivna kažemo da je* ***parcijalni uređaj*** *na skupu* S*.*

Definicija 30. *Neka je* $\leq$ *parcijalni uređaj na skupu* S*. Pretpostavimo da za* $\forall x, y \in S$ *vrijedi* $x \leq y$ *ili* $y \leq x$*. Tada za* $\leq$ *kažemo da je* ***uređaj*** *na* S*.*

Napomena 31. *Parcijalni uređaj ne mora biti uređaj.*

Naime, neka je S skup svih podskupova od $\mathbb{R}$. Na S definiramo binarnu relaciju $\leq$ sa $A \leq B$ ako je $A \subseteq B$. Budući da za $\forall A \in S$ vrijedi $A \subseteq A$, tj. $A \leq A$, imamo da je $\leq$ refleksivna relacija na S.

Nadalje, ako su $A, B \in S$ td. $A \leq B$ i $B \leq A$, onda je $A \subseteq B$ i $B \subseteq A$, pa je $A = B$. Dakle, relacija $\leq$ je antisimetrična na S.

Lako vidimo da je $\leq$ tranzitivna relacija na S.

Dakle, $\leq$ je parcijalni uređaj na S. No, $\leq$ nije uređaj na S jer za $A = \{1, 2\}$ i $B = \{3, 4\}$ imamo $A, B \in S$, ali ne vrijedi ni $A \leq B$ ni $B \leq A$.

Definicija 32. *Neka je* $(S, +, \cdot)$ *prsten te neka je* $\leq$ *uređaj na* S *td. za* $\forall x, y, z \in S$ *vrijedi sljedeće:*

1. *Ako je* $x \leq y$*, onda je* $x + z \leq y + z$*.*

2. *Ako je* $0 \leq x$ *i* $0 \leq y$*, onda je* $0 \leq x \cdot y$*.*

Tada za uređenu četvorku $(S, +, \cdot, \leq)$ *kažemo da je* ***uređeni prsten****.*

Definicija 33. *Za uređeni prsten* $(S, +, \cdot, \leq)$ *kažemo da je* ***uređeno polje****, ako je* $(S, +, \cdot)$ *polje.*

Definicija 34. *Neka je* $\leq$ *uređaj na skupu* S*. Tada za uređeni par* $(S, \leq)$ *kažemo da je* ***uređen skup****.*

Definicija 35. *Neka je* $(S, \leq)$ *uređen skup. Pretpostavimo da za sve neprazne podskupove* $A, B \in S$ *td. je* $x \leq y$ *za* $\forall x \in A$ *i* $\forall y \in B$ *postoji* $z \in S$ *td. je* $x \leq z$ *za* $\forall x \in A$ *i* $z \leq y$ *za* $\forall y \in B$*.*

Tada za $(S, \leq)$ *kažemo da je* ***potpuno uređen skup****.*

Definicija 36. *Neka je* $(S, +, \cdot, \leq)$ *uređeno polje takvo da je* $(S, \leq)$ *potpuno uređen skup. Tada za* $(S, +, \cdot, \leq)$ *kažemo da je* ***potpuno uređeno polje*** *ili* ***polje realnih brojeva****.*

Poglavlje 2

Skupovi $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$

Od sad pa nadalje, neka je $(\mathbb{R}, +, \cdot, \leq)$ jedno fiksirano polje realnih brojeva.

2.1 Skup prirodnih brojeva

Definicija 37. *Neka je $S \subseteq \mathbb{R}$. Kažemo da je S* ***induktivan skup*** *ako vrijedi sljedeće:*

1. $1 \in S$.

2. *Ako je $x \in S$, onda je $x + 1 \in S$.*

Očito je $\mathbb{R}$ induktivan skup.

S druge strane, skup $S = \{1\}$ nije induktivan. Naime, tada bi vrijedilo $1 + 1 \in S$, tj. $1 + 1 = 1$, iz čega prema lemi 17.2. slijedi da je $1 = 0$. No, $(\mathbb{R}, +, \cdot)$ je netrivijalan prsten (jer je polje, pa je i tijelo), pa prema napomeni 24. vrijedi $1 \neq 0$.

Dakle, S nije induktivan skup.

Definicija 38. *Definirajmo $\mathbb{N} = \{x \in \mathbb{R} \mid x \in S$, za svaki induktivni skup $S\}$.*

Uočimo da je $1 \in \mathbb{N}$. Nadalje, pretpostavimo da je $x \in \mathbb{N}$. Tada je $x \in \mathbb{R}$ i $x \in S$ za svaki induktivni skup S. Iz definicije induktivnog skupa slijedi da je $x + 1 \in S$, za svaki induktivni skup S. Očito je $x + 1 \in \mathbb{R}$, pa iz toga slijedi da je $x + 1 \in \mathbb{N}$.

Zaključujemo da je $\mathbb{N}$ induktivni skup.

Uočimo da iz definicije od $\mathbb{N}$ slijedi da je $\mathbb{N} \subseteq S$, za svaki induktivni skup S.

Propozicija 39. *Neka je $S \subseteq \mathbb{N}$ tako da vrijedi:*

1. $1 \in S$.

2. *Ako je $x \in S$, onda je $x + 1 \in S$.*

Tada je $S = \mathbb{N}$.

Dokaz. Očito je S induktivan skup, pa je $\mathbb{N} \subseteq S$. S druge strane, prema pretpostavci propozicije, vrijedi $S \subseteq \mathbb{N}$, pa je $S = \mathbb{N}$. □

Propozicija 40. *Za sve* $x, y \in \mathbb{N}$ *vrijedi* $x + y \in \mathbb{N}$.

Dokaz. Neka je $x_0 \in \mathbb{N}$. Dokažimo da je $x_0 + y \in \mathbb{N}$, za svaki $y \in \mathbb{N}$.

Neka je $S = \{y \in \mathbb{N} \mid x_0 + y \in \mathbb{N}\}$. Očito je $S \subseteq \mathbb{N}$. Imamo $1 \in \mathbb{N}$ i $x_0 + 1 \in \mathbb{N}$, jer je $\mathbb{N}$ induktivan skup. Slijedi, $1 \in S$.

Pretpostavimo da je $y \in S$, tada je $y \in \mathbb{N}$ i $x_0 + y \in \mathbb{N}$. Iz činjenice da je $\mathbb{N}$ induktivan skup slijedi da je $y + 1 \in \mathbb{N}$ i $(x_0 + y) + 1 \in \mathbb{N}$, odnosno $x_0 + (y + 1) \in \mathbb{N}$. Zaključujemo kako je $y + 1 \in S$.

Dakle, ako je $y \in S$, onda je $y + 1 \in S$.

Iz propozicije 39. slijedi da je $S = \mathbb{N}$. Dakle, za svaki $y \in \mathbb{N}$ vrijedi $x_0 + y \in \mathbb{N}$, pa je stoga tvrdnja ove propozicije dokazana. □

Propozicija 41. *Za sve* $x, y \in \mathbb{N}$ *vrijedi* $x \cdot y \in \mathbb{N}$.

Dokaz. Neka je $x_0 \in \mathbb{N}$. Dokažimo da je $x_0 \cdot y \in \mathbb{N}$, za svaki $y \in \mathbb{N}$.

Neka je $S = \{y \in \mathbb{N} \mid x_0 \cdot y \in \mathbb{N}\}$. Očito je $S \subseteq \mathbb{N}$. Vrijedi $1 \in \mathbb{N}$ i $x_0 \cdot 1 \in \mathbb{N}$, pa je $1 \in S$.

Pretpostavimo da je $y \in S$. Tada vrijedi da je $y \in \mathbb{N}$ i $x_0 \cdot y \in \mathbb{N}$. Imamo $y + 1 \in \mathbb{N}$ i $x_0 \cdot (y + 1) = x_0 \cdot y + x_0$, pa iz propozicije 40. slijedi da je $x_0 \cdot (y + 1) \in \mathbb{N}$. Stoga je $y + 1 \in S$.

Iz propozicije 39. slijedi da je $S = \mathbb{N}$, čime je tvrdnja ove propozicije dokazana. □

Propozicija 42. *Za svaki* $x \in \mathbb{N}$ *vrijedi* $1 \leq x$.

Kako bi dokazali ovu propoziciju, potrebne su nam još neke činjenice koje ćemo dokazati u nastavku, nakon čega ćemo provesti dokaz ove tvrdnje.

Napomena 43. *Neka je* $(P, +, \cdot)$ *prsten. Tada za* $\forall a \in P$ *vrijedi* $-(-a) = a$.

To slijedi iz $(-a) + a = 0$ dodavanjem $-a$ lijevoj i desnoj strani.

Propozicija 44. *Neka je* $(P, +, \cdot)$ *prsten te neka su* $x, y \in P$. *Tada vrijedi:*

1. $(-x) \cdot y = -(x \cdot y)$
2. $x \cdot (-y) = -(x \cdot y)$
3. $(-x) \cdot (-y) = x \cdot y$

Dokaz.

1. Vrijedi $(-x) \cdot y + x \cdot y = (-x + x) \cdot y = 0 \cdot y = 0$, što slijedi iz propozicije 18. Dakle, $(-x) \cdot y + x \cdot y = 0$, pa je tvrdnja 1. dokazana.

2. Tvrdnju 2. dokazujemo posve analogno.

3. Iz prethodno dokazanih tvrdnji 1. i 2. te napomene 43. slijedi:

$$(-x) \cdot (-y) = -(x \cdot (-y)) = -(-(x \cdot y)) = x \cdot y$$

□

Definicija 45. *Neka je $(P, +, \cdot)$ prsten. Za $x, y \in P$ definiramo $x - y = x + (-y)$.*
Očito je $x - x = 0$ za $\forall x \in P$.

Propozicija 46. *Neka je $(P, +, \cdot)$ prsten te neka su $x, y, z, \in P$. Tada vrijedi:*

1. $x \cdot (y - z) = x \cdot y - x \cdot z$

2. $(x - y) \cdot z = x \cdot z - y \cdot z$

Dokaz. Koristeći propoziciju 44. dobivamo:

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

2. Tvrdnju dokazujemo analogno.

□

Napomena 47. *Neka je $\leq$ uređaj na skupu S, te neka su $x, y \in S$. Pišemo:*

1. $x \not\leq y$, *ako ne vrijedi* $x \leq y$.

2. $x < y$, *ako vrijedi* $x \leq y$ *i* $x \neq y$.

3. $x \not< y$, *ako ne vrijedi* $x < y$.

Propozicija 48. *Neka je $(P, +, \cdot, \leq)$ uređeni prsten, pri čemu je $(P, +, \cdot)$ prsten s jedinicom. Tada je* $0 \leq 1$.

Dokaz. Budući da je $\leq$ uređaj na P, vrijedi $0 \leq 1$ ili $1 \leq 0$.

Pretpostavimo da $0 \not\leq 1$.

Tada je $1 \leq 0$, pa iz definicije uređenog prstena slijedi $(-1) + 1 \leq -1$, tj. $0 \leq -1$. Sada iz definicije uređenog prstena slijedi $0 \leq (-1) \cdot (-1)$.

Iz propozicije 44. 3. slijedi $(-1) \cdot (-1) = 1 \cdot 1 = 1$, dakle $0 \leq 1$, što je u kontradikciji s pretpostavkom da $0 \not\leq 1$. Prema tome, $0 \leq 1$. □

Korolar 49. *Neka je* $(P, +, \cdot, \leq)$ *uređeno polje. Tada je* $0 < 1$.

Dokaz. Prema definiciji polja vrijedi $0 \neq 1$, a prema propoziciji 48. vrijedi da je $0 \leq 1$. Stoga je $0 < 1$. □

Sada se možemo vratiti na dokazivanje propozicije 42.:

Dokaz. Definirajmo $S = \{x \in \mathbb{N} \mid 1 \leq x\}$. Dovoljno je dokazati da je $S = \mathbb{N}$.

Vrijedi $1 \leq 1$ jer je binarna operacija $\leq$ refleksivna. Prema tome, $1 \in S$.

Pretpostavimo da je $x \in S$. Tada je $1 \leq x$. Prema propoziciji 48. vrijedi da je $0 \leq 1$, pa slijedi $x \leq x + 1$. Nadalje, iz tranzitivnosti binarne operacije $\leq$ slijedi da je $1 \leq x + 1$. Dakle, $x + 1 \in S$.

Iz gore navedenoga slijedi kako za $\forall x \in S$ vrijedi $x + 1 \in S$. Tada iz propozicije 39. slijedi $S = \mathbb{N}$. □

Napomena 50. *Neka je* $\leq$ *uređaj na skupu* S. *Za* $\forall x \in S$ *očito vrijedi* $x \not< x$.
Nadalje, ako su $x, y \in S$, *onda ne može vrijediti i* $x \leq y$ *i* $y < x$. *Naime, u suprotnom bi antisimetričnost binarne operacije* $\leq$ *povlačila da je* $x = y$, *što je nemoguće zbog* $y < x$.
Analogno, ne može vrijediti i $x < y$ *i* $y \leq x$.

Napomena 51. *Neka je* $\leq$ *uređaj na skupu* S *te neka su* $x, y \in S$. *Tada je* $x < y$ *ili* $x = y$ *ili* $y < x$.

Naime, ako je $x = y$, tvrdnja je očita. U slučaju kada je $x \neq y$, zbog $x \leq y$ ili $y \leq x$ (što vrijedi po definiciji uređaja) imamo $x < y$ ili $y < x$.

Napomena 52. *Neka je* $\leq$ *uređaj na skupu* S. *Neka su* $x, y \in S$ *takvi da* $x \not< y$. *Tada je* $y \leq x$.

Naime, tvrdnja slijedi iz prethodno navedene napomene 51. Obratno, kada bi vrijedilo $x \not\leq y$, to bi povlačilo da je $y < x$, što također slijedi iz napomene 51.

Propozicija 53. *Neka je* $\leq$ *uređaj na skupu* S *te neka su* $x, y, z \in S$.

1. *Pretpostavimo da je* $x \leq y$ *i* $y < z$. *Tada je* $x < z$.

2. *Pretpostavimo da je* $x < y$ *i* $y \leq z$. *Tada je* $x < z$.

Dokaz.

1. Iz tranzitivnosti relacije $\leq$ slijedi $x \leq z$. Pretpostavimo da je $x = z$. Tada iz pretpostavke tvrdnje 1. slijedi $x \leq y$ i $y < x$, što je nemoguće prema napomeni 50. Prema tome, $x \neq z$, pa je $x < z$.

2. Tvrdnju 2. dokazujemo analogno.

□

Propozicija 54. *Neka je* $(P, +, \cdot, \leq)$ *uređeni prsten te neka su* $x, y, z \in P$. *Pretpostavimo da je* $x < y$. *Tada je* $x + z < y + z$.

Dokaz. Iz $x < y$ slijedi $x \leq y$, pa prema definiciji uređenog prstena vrijedi $x + z \leq y + z$. Još je potrebno pokazati da je $x + z \neq y + z$.

Pretpostavimo suprotno, tj. da je $x + z = y + z$. Slijedi $(x + z) + (-z) = (y + z) + (-z)$, pa dobivamo $x = y$, što je u kontradikciji s pretpostavkom da je $x < y$. Prema tome, $x + z \neq y + z$.

Zaključujemo, $x + z < y + z$. □

Korolar 55. *Za svaki* $x \in \mathbb{N}$ *vrijedi* $x \neq 0$.

Dokaz. Neka je $x \in \mathbb{N}$. Prema propoziciji 42. vrijedi $1 \leq x$. Iz korolara 49. slijedi da je $0 < 1$, a iz propozicije 53. 2. slijedi da je $0 < x$. Tada posebno vrijedi da je $x \neq 0$. □

Lema 56. *Vrijedi:*

$$\mathbb{N} = \{1\} \cup \{1 + k \mid k \in \mathbb{N}\}$$

Dokaz. Označimo $S = \{1\} \cup \{1 + k \mid k \in \mathbb{N}\}$. Očito je $S \subseteq \mathbb{N}$. Nadalje, očito je $1 \in S$.

Pretpostavimo da je $x \in S$. Tada je $x \in \mathbb{N}$, pa je očito $x + 1 \in S$. Shodno tome, iz propozicije 39. slijedi da je $S = \mathbb{N}$. □

Propozicija 57. *Ako su* $x, y \in \mathbb{N}$ *tako da je* $x < y$, *onda je* $x + 1 \leq y$.

Dokaz. Definirajmo S kao skup svih $x \in \mathbb{N}$ koji imaju sljedeće svojstvo - ako je $y \in \mathbb{N}$ tako da je $x < y$, onda je $x + 1 \leq y$.

Dokažimo da je $S = \mathbb{N}$. Očito je $S \subseteq \mathbb{N}$. Dokažimo da je $1 \in S$. Pretpostavimo da je $y \in \mathbb{N}$ tako da je $1 < y$. Slijedi $1 \neq y$, pa iz leme 56. zaključujemo da postoji $k \in \mathbb{N}$ tako da je $y = 1 + k$. Prema propoziciji 42. vrijedi $1 \leq k$, što povlači da je $1 + 1 \leq k + 1$, odnosno $1 + 1 \leq y$. Time smo dokazali da je $1 \in S$.

Pretpostavimo da je $x \in S$. Želimo dokazati da je $x + 1 \in S$. Pretpostavimo da je $y \in \mathbb{N}$ tako da je $x + 1 < y$. Zbog $x + 1 \in \mathbb{N}$ imamo da je $1 \leq x + 1$, pa slijedi $1 < y$. Iz leme 56. slijedi da postoji $k \in \mathbb{N}$ tako da je $y = k + 1$. Sada zbog $x + 1 < y$ imamo $x + 1 < k + 1$, pa iz propozicije 54. slijedi da je $(x + 1) + (-1) < (k + 1) + (-1)$, tj. $x < k$. Zbog toga što je $x \in S$ imamo da $x + 1 \leq k$. Slijedi $(x + 1) + 1 \leq k + 1$, tj. $(x + 1) + 1 \leq y$. Stoga je $x + 1 \in S$.

Iz propozicije 39. slijedi $S = \mathbb{N}$. Time je tvrdnja propozicije dokazana. □

Lema 58. *Neka je* $n \in \mathbb{N}$. *Tada je* $\mathbb{N} = \{x \in \mathbb{N} \mid x \leq n\} \cup \{n + k \mid k \in \mathbb{N}\}$.

Dokaz. Neka je $S = \{x \in \mathbb{N} \mid x \leq n\} \cup \{n + k \mid k \in \mathbb{N}\}$. Očito je $S \subseteq \mathbb{N}$. Imamo $1 \in \mathbb{N}$ i $1 \leq n$, pa je $1 \in S$. Pretpostavimo da je $x \in S$. Tada je $x \leq n$ ili $x \in \{n + k \mid k \in \mathbb{N}\}$.

1. $x \leq n$

   Ako je $x = n$, onda je $x + 1 = n + 1$, pa je očito $x + 1 \in S$.

   Pretpostavimo da je $x \neq n$. Tada imamo $x < n$, pa prema propoziciji 57. vrijedi $x + 1 \leq n$. Stoga je $x + 1 \in S$.

2. $x \in \{n + k \mid k \in \mathbb{N}\}$

   Tada postoji $k \in \mathbb{N}$ takav da je $x = n + k$. Vrijedi $x + 1 = (n + k) + 1 = n + (k + 1)$. Stoga je $x + 1 \in S$.

U oba slučaja smo dobili da je $x + 1 \in S$. Iz propozicije 39. slijedi da je $S = \mathbb{N}$. □

Korolar 59. *Neka su $m, n \in \mathbb{N}$ takvi da je $n < m$. Tada je $m - n \in \mathbb{N}$.*

Dokaz. Prema lemi 58. vrijedi $\mathbb{N} = \{x \in \mathbb{N} \mid x \leq n\} \cup \{n + k \mid k \in \mathbb{N}\}$. Stoga slijedi da je $m \in \{x \in \mathbb{N} \mid x \leq n\}$ ili $m \in \{n + k \mid k \in \mathbb{N}\}$. Međutim, zbog pretpostavke korolara i napomene 50. ne vrijedi $m \leq n$.

Prema tome, $m \in \{n + k \mid k \in \mathbb{N}\}$. Dakle, postoji $k \in \mathbb{N}$ takav da je $m = n + k$. Slijedi $m + (-n) = k$, tj. $m - n = k$, pa je očito $m - n \in \mathbb{N}$. □

Propozicija 60. *Neka je $(G, \cdot)$ monoid te neka su x i y invertibilni elementi u $(G, \cdot)$. Tada je $x \cdot y$ invertibilan element i vrijedi $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.*

Dokaz. Vrijedi:
$(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = ((x \cdot y) \cdot y^{-1}) \cdot x^{-1} = (x \cdot (y \cdot y^{-1})) \cdot x^{-1} = (x \cdot e) \cdot x^{-1} = x \cdot x^{-1} = e$.
Dakle, $(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = e$. Analogno dobivamo da je $(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = e$, pa slijedi da je $x \cdot y$ invertibilan i vrijedi $y^{-1} \cdot x^{-1} = (x \cdot y)^{-1}$. □

Korolar 61. *Neka je $(P, +, \cdot)$ prsten. Tada za $\forall x, y \in P$ vrijedi $-(x + y) = (-x) + (-y)$.*

2.2 Skup cijelih brojeva

Definicija 62. *Definirajmo $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-n \mid n \in \mathbb{N}\}$.*

Propozicija 63. *Neka su $x, y \in \mathbb{Z}$. Tada je $x + y \in \mathbb{Z}$.*

Dokaz. Tvrdnja je jasna ako je $x = 0$ ili $y = 0$. Pretpostavimo da je $x \neq 0$ i $y \neq 0$. Tada imamo 4 mogućnosti:

1. $x, y \in \mathbb{N}$

   Tada je $x + y \in \mathbb{N}$, pa je $x + y \in \mathbb{Z}$.

2. $x, y \in \{-n \mid n \in \mathbb{N}\}$

   Tada $\exists\, m, n \in \mathbb{N}$ takvi da je $x = -m$ i $y = -n$. Koristeći korolar 61. dobivamo $x + y = (-m) + (-n) = -(m + n)$. Dakle, $x + y = -(m + n)$, pa zbog $m + n \in \mathbb{N}$ imamo $x + y \in \mathbb{Z}$.

3. $x \in \mathbb{N}$, $y \in \{-n \mid n \in \mathbb{N}\}$

   Slijedi da postoji $n \in \mathbb{N}$ takav da je $y = -n$. Imamo $x + y = x + (-n) = x - n$. Imamo tri slučaja:

   a) $n < x$

      Prema korolaru 59. vrijedi $x - n \in \mathbb{N}$, pa je stoga $x + y \in \mathbb{Z}$.

   b) $x = n$

      Tada je $x - n = 0$, pa je $x + y \in \mathbb{Z}$.

   c) $x < n$

      Iz napomene 43. i korolara 61. slijedi:
      $x - n = -(-(x + (-n))) = -((-x) + (-(-n))) = -((-x) + n) = -(n - x)$.
      Dakle, $x + y = -(n - x)$. Ako je $x < n$, onda je prema korolaru 59. $n - x \in \mathbb{N}$, pa je $x + y \in \mathbb{Z}$.

4. $x \in \{-n \mid n \in \mathbb{N}\}$, $y \in \mathbb{N}$

   Analogno kao u slučaju 3. dobivamo da je $x + y \in \mathbb{Z}$.

Time je tvrdnja propozicije dokazana. □

Propozicija 64. *Neka su $x, y \in \mathbb{Z}$. Tada je $x \cdot y \in \mathbb{Z}$.*

Dokaz. Ako je $x = 0$ ili $y = 0$, onda je $x \cdot y = 0$, pa je očito $x \cdot y \in \mathbb{Z}$. Pretpostavimo da je $x \neq 0$ i $y \neq 0$. Imamo 4 mogućnosti:

1. $x, y \in \mathbb{N}$

   Tada je $x \cdot y \in \mathbb{N}$, pa je $x \cdot y \in \mathbb{Z}$.

2. $x \in \{-n \mid n \in \mathbb{N}\}$, $y \in \mathbb{N}$

   Tada je $x = -n$ za neki $n \in \mathbb{N}$. Iz propozicije 44. slijedi $x \cdot y = (-n) \cdot y = -(n \cdot y)$. Vrijedi $n \cdot y \in \mathbb{N}$, pa je $x \cdot y \in \mathbb{Z}$.

3. $x \in \mathbb{N}$, $y \in \{-n \mid n \in \mathbb{N}\}$

   Analogno kao u prethodnom slučaju dobijemo da je $x \cdot y \in \mathbb{Z}$.

4. $x, y \in \{-n \mid n \in \mathbb{N}\}$

   Tada je $x = -n$, $y = -m$ za neke $n, m \in \mathbb{N}$. Iz propozicije 44. slijedi $x \cdot y = (-n) \cdot (-m) = n \cdot m \in \mathbb{N}$, pa je $x \cdot y \in \mathbb{Z}$.

Time je tvrdnja propozicije dokazana. □

Propozicija 65. *Neka je $x \in \mathbb{Z}$. Tada je $-x \in \mathbb{Z}$.*

Dokaz.

1. Ako je $x \in \mathbb{N}$, onda je očito $-x \in \mathbb{Z}$.
2. Ako je $x = 0$, onda je $-x = 0$, pa je $-x \in \mathbb{Z}$.
3. Ako je $x \in \{-n \mid n \in \mathbb{N}\}$, onda je $x = -n$, za neki $n \in \mathbb{N}$. Iz napomene 43. slijedi $-x = -(-n) = n \in \mathbb{N}$. Stoga je $-x \in \mathbb{Z}$.

□

2.3 Skup racionalnih brojeva

Definicija 66. *Za $x, y \in \mathbb{R}$, $y \neq 0$ definiramo $\frac{x}{y} = x \cdot y^{-1}$.*

Propozicija 67. *Neka su $x, y, z, k, u, v \in \mathbb{R}$, pri čemu su $y \neq 0$, $k \neq 0$ i $v \neq 0$. Tada vrijedi:*

1. $\frac{x}{1} = x$
2. $\frac{x}{y} = \frac{kx}{ky}$
3. $\frac{x}{y} + \frac{z}{y} = \frac{x+z}{y}$
4. $\frac{x}{y} + \frac{u}{v} = \frac{xv+uy}{yv}$
5. $\frac{x}{y} \cdot \frac{u}{v} = \frac{xu}{yv}$

Dokaz.

1. Očito je $1^{-1} = 1$, pa je $\frac{x}{1} = x \cdot 1^{-1} = x \cdot 1 = x$.

2. Uz pomoć propozicije 60. dobivamo:

$$\begin{aligned}\frac{kx}{ky} &= (kx)\cdot(ky)^{-1} = (kx)\cdot(k^{-1}\cdot y^{-1}) = k(x\cdot(k^{-1}\cdot y^{-1})) = k((x\cdot k^{-1})\cdot y^{-1}) = \\ &= k((k^{-1}\cdot x)\cdot y^{-1}) = k(k^{-1}\cdot(x\cdot y^{-1})) = (k\cdot k^{-1})\cdot(x\cdot y^{-1}) = \\ &= 1\cdot(x\cdot y^{-1}) = x\cdot y^{-1} = \frac{x}{y}\end{aligned}$$

3. Vrijedi:

$$\frac{x}{y}+\frac{z}{y} = x\cdot y^{-1}+z\cdot y^{-1} = (x+z)\cdot y^{-1} = \frac{x+z}{y}$$

4. Koristeći prethodno dokazane tvrdnje 2. i 3. dobivamo:

$$\frac{x}{y}+\frac{u}{v} = \frac{x\cdot v}{y\cdot v}+\frac{u\cdot y}{v\cdot y} = \frac{xv+uy}{yv}$$

5. Koristeći propoziciju 60. dobivamo:

$$\frac{x}{y}\cdot\frac{u}{v} = (x\cdot y^{-1})\cdot(u\cdot v^{-1}) = (x\cdot u)\cdot(y^{-1}\cdot v^{-1}) = (x\cdot u)\cdot(y\cdot v)^{-1} = \frac{x\cdot u}{y\cdot v}$$

□

Definicija 68. *Definirajmo* $\mathbb{Q} = \left\{\frac{m}{n} \mid m\in\mathbb{Z}, n\in\mathbb{N}\right\}$.

Za svaki $m\in\mathbb{Z}$ vrijedi $m = \frac{m}{1}$, pa je $m\in\mathbb{Q}$. Dakle, $\mathbb{Z}\subseteq\mathbb{Q}$.

Propozicija 69. *Neka su* $r_1, r_2\in\mathbb{Q}$. *Tada je* $r_1+r_2\in\mathbb{Q}$ *i* $r_1\cdot r_2\in\mathbb{Q}$.

Dokaz. Imamo $r_1 = \frac{x}{y}$, gdje su $x\in\mathbb{Z}$, $y\in\mathbb{N}$ i $r_2 = \frac{u}{v}$, gdje su $u\in\mathbb{Z}$, $v\in\mathbb{N}$. Prema propoziciji 67. vrijedi

$$r_1+r_2 = \frac{xv+uy}{yv} \quad \text{i} \quad r_1\cdot r_2 = \frac{xu}{yv}$$

pa iz propozicija 40., 41., 63. i 64. slijedi $r_1+r_2\in\mathbb{Q}$ i $r_1\cdot r_2\in\mathbb{Q}$. □

Napomena 70. *Neka je* $(P,+,\cdot)$ *polje te neka je* $x\in P$, $x\neq 0$. *Tada je* $(-x)^{-1} = -x^{-1}$.

Naime, imamo $(-x)\cdot(-x^{-1}) = x\cdot x^{-1} = 1$, pri čemu smo koristili propoziciju 44. Dakle, $(-x)\cdot(-x^{-1}) = 1$, pa je očito $(-x)^{-1} = -x^{-1}$.

Propozicija 71. *Neka su* $x, y\in\mathbb{R}$, $y\neq 0$.

1. *Vrijedi:* $-\frac{x}{y} = \frac{-x}{y}$
2. *Vrijedi:* $-\frac{x}{y} = \frac{x}{-y}$
3. *Pretpostavimo da je* $x \neq 0$. *Tada je* $\frac{x}{y} \neq 0$ *te je* $\left(\frac{x}{y}\right)^{-1} = \frac{y}{x}$.

Dokaz.

1. Koristeći propoziciju 44. dobivamo:
$$-\frac{x}{y} = -(x \cdot y^{-1}) = (-x) \cdot y^{-1} = \frac{-x}{y}$$
2. Koristeći propoziciju 44. i napomenu 70. dobivamo:
$$-\frac{x}{y} = -(x \cdot y^{-1}) = x \cdot (-y^{-1}) = x \cdot (-y)^{-1} = \frac{x}{-y}$$
3. Imamo $\frac{x}{y} = x \cdot y^{-1}$, pa iz činjenice da je $(\mathbb{R}, +, \cdot)$ integralna domena slijedi da je $\frac{x}{y} \neq 0$. Prema propoziciji 60. vrijedi:
$$\left(\frac{x}{y}\right)^{-1} = (x \cdot y^{-1})^{-1} = (y^{-1})^{-1} \cdot x^{-1}$$
Iz definicije inverznog elementa u monoidu je očito da je $(y^{-1})^{-1} = y$. Stoga je:
$$\left(\frac{x}{y}\right)^{-1} = y \cdot x^{-1} = \frac{y}{x}$$

□

Propozicija 72. *Neka je* $r \in \mathbb{Q}$. *Tada je* $-r \in \mathbb{Q}$. *Nadalje, ako je* $r \neq 0$, *onda je* $r^{-1} \in \mathbb{Q}$.

Dokaz. Iz propozicije 71. 1. lako zaključujemo da je $-r \in \mathbb{Q}$.

Imamo $r = \frac{m}{n}$, gdje su $m \in \mathbb{Z}$ i $n \in \mathbb{N}$. Pretpostavimo da je $r \neq 0$. Tada je $m \neq 0$.

Iz propozicije 71. 3., napomene 43. i propozicije 71. 1. i 2. točno ovim redoslijedom slijedi:
$$r^{-1} = \frac{n}{m} = -\left(-\frac{n}{m}\right) = -\frac{n}{-m} = \frac{-n}{-m}$$
Dakle, $r^{-1} = \frac{n}{m}$ i $r^{-1} = \frac{-n}{-n}$. Iz $m \in \mathbb{Z}$ i $m \neq 0$ slijedi da je $m \in \mathbb{N}$ ili $m \in \{-k \mid k \in \mathbb{N}\}$.

Ako je $m \in \mathbb{N}$, onda iz $r = \frac{n}{m}$ slijedi da je $r^{-1} \in \mathbb{Q}$.

Ako je $m \in \{-k \mid k \in \mathbb{N}\}$, onda je $m = -k$, $k \in \mathbb{N}$, pa je prema napomeni 43., $-m = k$, odnosno, $-m \in \mathbb{N}$. Tada iz $r^{-1} = \frac{-n}{-m}$ slijedi da je $r^{-1} \in \mathbb{Q}$.

Time je tvrdnja propozicije dokazana. □

Poglavlje 3

Potprsteni i potpolja

3.1 Definicija i svojstva potprstena i potpolja

Definicija 73. *Neka su* $(A, +_A, \cdot_A)$ *i* $(B, +_B, \cdot_B)$ *prsteni. Kažemo da je* $(A, +_A, \cdot_A)$ ***potprsten*** *od* $(B, +_B, \cdot_B)$ *ako je* $A \subseteq B$ *te ako za* $\forall x, y \in A$ *vrijedi:*

$$x +_A y = x +_B y \quad i \quad x \cdot_A y = x \cdot_B y$$

Propozicija 74. *Neka je* $(A, +_A, \cdot_A)$ *potprsten od* $(B, +_B, \cdot_B)$*. Neka je* 0_A *nula u prstenu* $(A, +_A, \cdot_A)$ *te neka je* 0_B *nula u prstenu* $(B, +_B, \cdot_B)$*. Tada je* $0_A = 0_B$*.*

Dokaz. Odaberimo $x \in A$.

Imamo $0_A +_A x = x$, tj. $0_A +_B x = x$. Budući da je $(B, +_B, \cdot_B)$ prsten, postoji $y \in B$ takav da je $x +_B y = 0_B$.

Iz $0_A +_B x = x$ slijedi $(0_A +_B x) +_B y = x +_B y$, pa je $0_A +_B (x +_B y) = 0_B$, tj. $0_A +_B 0_B = 0_B$.

Obzirom da je 0_B nula u prstenu $(B, +_B, \cdot_B)$, slijedi da je $0_A +_B 0_B = 0_A$, pa je $0_A = 0_B$. □

Napomena 75. *Neka je* $(A, +_A, \cdot_A)$ *potprsten od* $(B, +_B, \cdot_B)$*. Neka je* $x \in A$*. Tada je inverzni element od* x *u* $(A, +_A)$ *jednak inverznom elementu u* $(B, +_B)$*.*

Naime, neka je 0 nula u prstenu $(A, +_A, \cdot_A)$. Prema prethodnoj propoziciji vrijedi da je 0 nula u prstenu $(B, +_B, \cdot_B)$. Neka je y inverzni element od x u $(A, +_A)$. Tada je $x +_A y = 0$ i $y +_A x = 0$, tj. $x +_B y = 0$ i $y +_B x = 0$. Iz ovoga zaključujemo da je y inverzni element od x u $(B, +_B)$.

Propozicija 76. *Neka je* $(B, +, \cdot)$ *prsten, te neka je* $A \subseteq B$*,* $A \neq \emptyset$*. Tada postoje binarne operacije* $+_A$ *i* $\cdot_A$ *na* A *tako da je* $(A, +_A, \cdot_A)$ *potprsten od* $(B, +, \cdot)$ *ako i samo ako za* $\forall x, y \in A$ *vrijedi* $x - y \in A$ *i* $x \cdot y \in A$*.*

Dokaz. Pretpostavimo da postoje binarne operacije $+_A$ i $\cdot_A$ na A takve da je $(A, +_A, \cdot_A)$ potprsten od $(B, +, \cdot)$.

Neka su $x, y \in A$. Imamo $x \cdot y = x \cdot_A y \in A$, dakle $x \cdot y \in A$.

Prema napomeni 75., inverzni element od y u $(A, +_A)$ jednak je inverznom elementu od y u $(B, +)$, tj. jednak je $-y$. Prema tome, $-y \in A$. Vrijedi:

$$x - y = x + (-y) = x +_A (-y) \in A$$

Dakle, $x - y \in A$.

Obratno, pretpostavimo da za $\forall x, y \in A$ vrijedi $x - y \in A$ i $x \cdot y \in A$. Odaberimo neki $x_0 \in A$. Tada je prema pretpostavci $x_0 - x_0 \in A$, tj. $0 \in A$.

Neka je $y \in A$. Imamo $0, y \in A$, pa prema pretpostavci vrijedi $0 - y \in A$, tj. $-y \in A$. Dakle, za $\forall y \in A$ vrijedi $-y \in A$.

Neka su $x, y \in A$. Slijedi $x - y \in A$, pa prema pretpostavci vrijedi $x - (-y) \in A$, tj. $x + (-(-y)) \in A$. Dakle, $x + y \in A$, za $\forall x, y \in A$.

Definirajmo binarne operacije $+_A$ i $\cdot_A$ na A sa $x +_A y = x + y$ i $x \cdot_A y = x \cdot y$. Tvrdimo da je $(A, +_A, \cdot_A)$ potprsten od $(B, +, \cdot)$. Dovoljno je dokazati da je $(A, +_A, \cdot_A)$ prsten.

Neka su $x, y, z \in A$. Vrijedi:

$$(x +_A y) +_A z = (x + y) + z = x + (y + z) = x +_A (y +_A z)$$

Prema tome, operacija $+_A$ je asocijativna na A. Analogno dobivamo da je operacija $\cdot_A$ asocijativna na A te da je $+_A$ komutativna operacija na A.

Vidjeli smo da je $0 \in A$. Za svaki $x \in A$ vrijedi $x +_A 0 = x + 0 = x$ i $0 +_A x = 0 + x = 0$. Prema tome, 0 je neutralni element za operaciju $+_A$.

Također smo vidjeli da za svaki $x \in A$ vrijedi da je $-x \in A$. Za svaki $x \in A$ vrijedi $x +_A (-x) = x + (-x) = 0$ i $(-x) +_A x = 0$.

Zaključak: $(A, +_A)$ je Abelova grupa. Nadalje, $(A, \cdot_A)$ je polugrupa. Neka su $x, y, z \in A$. Iz $x \cdot (y + z) = x \cdot y + x \cdot z$ neposredno slijedi $x \cdot_A (y +_A z) = x \cdot_A y +_A x \cdot_A z$. Analogno zaključujemo da je $(x +_A y) \cdot_A z = x \cdot_A z +_A y \cdot_A z$.

Prema tome, $(A, +_A, \cdot_A)$ je prsten. □

Definicija 77. *Neka su $(A, +_A, \cdot_A)$ i $(B, +_B, \cdot_B)$ polja. Kažemo da je $(A, +_A, \cdot_A)$* ***potpolje*** *od $(B, +_B, \cdot_B)$ ako je $(A, +_A, \cdot_A)$ potprsten od $(B, +_B, \cdot_B)$.*

Propozicija 78. *Neka je $(A, +_A, \cdot_A)$ potpolje od $(B, +_B, \cdot_B)$. Neka je 1_A jedinica u prstenu $(A, +_A, \cdot_A)$, te neka je 1_B jedinica u prstenu $(B, +_B, \cdot_B)$. Tada je $1_A = 1_B$.*

Dokaz. Prema propoziciji 74., nule u ova dva prstena se podudaraju. Odaberimo $x \in A$ tako da je $x \neq 0$. Neka je $y \in B$ inverzni element od x u $(B, \cdot_B)$.

Imamo $1_A \cdot_A x = x$, tj. $1_A \cdot_B x = x$, pa slijedi $(1_A \cdot_B x) \cdot_B y = x \cdot_B y$, tj. $1_A \cdot_B (x \cdot_B y) = 1_B$, odnosno $1_A \cdot_B 1_B = 1_B$.

Stoga je $1_A = 1_B$. □

Napomena 79. *Neka je* $(A, +_A, \cdot_A)$ *potpolje od* $(B, +_B, \cdot_B)$*. Neka je* $x \in A$, $x \neq 0_A$*, te neka je* $y \in A$ *inverzni element od* x *u* $(A, \cdot_A)$*. Tada je* y *inverzni element od* x *u* $(B, \cdot_B)$*.*

Naime, vrijedi $x \cdot_A y = 1_A$ i $y \cdot_A x = 1_A$, pa iz prethodne propozicije slijedi $x \cdot_B y = 1_B$ i $y \cdot_B x = 1_B$.

3.2 Prsten u prstenu. Polje u prstenu.

Definicija 80. *Neka je* $(B, +, \cdot)$ *prsten, te neka je* $A \subseteq B$*. Kažemo da je* A ***prsten u*** $(B, +, \cdot)$ *ako postoje binarne operacije* $+_A$ *i* $\cdot_A$ *na* A *tako da je* $(A, +_A, \cdot_A)$ *potprsten od* $(B, +, \cdot)$*.*

Definicija 81. *Neka je* $(B, +, \cdot)$ *prsten, te neka je* $A \subseteq B$*. Kažemo da je* A ***polje u*** $(B, +, \cdot)$ *ako postoje binarne operacije* $+_A$ *i* $\cdot_A$ *na* A *tako da je* $(A, +_A, \cdot_A)$ *potpolje od* $(B, +, \cdot)$*.*

Propozicija 82. *Neka je* $(B, +, \cdot)$ *polje, te neka je* $A \subseteq B$ *td.* A *ima barem* 2 *elementa. Tada je* A *polje u* $(B, +, \cdot)$ *ako i samo ako vrijedi:*

$$\begin{aligned} &x - y \in A \ \text{ i } \ x \cdot y \in A \ \text{ za } \ \forall x, y \in A \\ &\text{te } \ x^{-1} \in A \ \text{ za } \ \forall x \in A \ \text{ td. je } \ x \neq 0 \end{aligned} \tag{*}$$

Dokaz. Pretpostavimo da vrijedi (*).

Iz propozicije 76. slijedi da postoje binarne operacije $+_A$ i $\cdot_A$ iz A tako da je $(A, +_A, \cdot_A)$ potprsten od $(B, +, \cdot)$. Dokažimo da je $(A, +_A, \cdot_A)$ polje.

Budući da A ima barem 2 elementa, postoji $x \in A$ tako da je $x \neq 0$. Prema (*) vrijedi $x^{-1} \in A$, pa iz (*) zaključujemo da je $x \cdot x^{-1} \in A$, tj. $1 \in A$. Neka je $x \in A$. Imamo $x \cdot_A 1 = x \cdot 1 = x$, te analogno $1 \cdot_A x = x$. Prema tome, 1 je jedinica u prstenu $(A, +_A, \cdot_A)$.

Neka su $x, y \in A$. Imamo $x \cdot_A y = x \cdot y = y \cdot x = y \cdot_A x$. Prema tome, operacija $\cdot_A$ je komutativna pa slijedi da je $(A, +_A, \cdot_A)$ komutativan prsten.

Uočimo da prema propoziciji 74. vrijedi $0_A = 0$. Neka je $x \in A$, $x \neq 0_A$. Tada je $x \neq 0$, pa je prema (*) $x^{-1} \in A$. Imamo $x \cdot_A x^{-1} = x \cdot x^{-1} = 1$, te analogno $x^{-1} \cdot x = 1$. Zaključujemo da je $(A, +_A, \cdot_A)$ polje.

Prema tome, $(A, +_A, \cdot_A)$ je potpolje od $(B, +, \cdot)$. Time smo dokazali da je A polje u $(B, +, \cdot)$.

Obratno, pretpostavimo da je A polje u $(B, +, \cdot)$.

Tada postoje binarne operacije $+_A$ i $\cdot_A$ na A tako da je $(A, +_A, \cdot_A)$ potpolje od $(B, +, \cdot)$. Posebno, imamo da je $(A, +_A, \cdot_A)$ potprsten od $(B, +, \cdot)$, pa iz propozicije 76. slijedi da za svaki $x, y \in A$ vrijedi $x - y \in A$ i $x \cdot y \in A$.

Pretpostavimo da je $x \in A$, td. $x \neq 0$. Znamo da je $0_A = 0$ iz propozicije 74., pa je $x \neq 0_A$, što zajedno s činjenicom da je $(A, +_A, \cdot_A)$ polje povlači da postoji $y \in A$ takav da je

$x \cdot_A y = 1_A$ i $y \cdot_A x = 1_A$. Iz propozicije 78. slijedi da je $1_A = 1$, pa je $x \cdot y = 1$ i $y \cdot x = 1$, što znači da je $y = x^{-1}$. Prema tome, $x^{-1} \in A$.

Zaključujemo kako vrijedi (*). □

Primjer 83.

- *Imamo* $1 \in \mathbb{N}$*, no* $1 - 1 = 0$*,* a $0 \notin \mathbb{N}$ *prema korolaru 55. Stoga iz propozicije 76. slijedi da* $\mathbb{N}$ ***nije*** *prsten u* $(\mathbb{R}, +, \cdot)$.
- *Neka su* $x, y, z \in \mathbb{Z}$*. Iz propozcija 63., 64. i 65. slijedi da je* $x - y \in \mathbb{Z}$ *i* $x \cdot y \in \mathbb{Z}$*. Stoga iz propozicije 76. slijedi da je* $\mathbb{Z}$ *prsten u* $(\mathbb{R}, +, \cdot)$.
- *Neka su* $x, y \in \mathbb{Q}$*. Iz propozicija 69. i 72. slijedi da je* $x - y \in \mathbb{Q}$ *i* $x \cdot y \in \mathbb{Q}$*. Pretpostavimo da je* $x \neq 0$*. Prema propoziciji 74. vrijedi* $x^{-1} \in \mathbb{Q}$*. Iz propozicije 82. slijedi da je* $\mathbb{Q}$ *polje u* $(\mathbb{R}, +, \cdot)$.

Propozicija 84. *Neka je* $(P, +, \cdot, \leq)$ *uređeni prsten. Neka su* a, b, c, d *elementi od* P*.*

1. *Pretpostavimo da je* $a \leq b$ *i* $c \leq d$*. Tada je* $a + c \leq b + d$*.*
2. *Pretpostavimo da je* $a < b$*. Tada je* $a + c < b + c$*.*
3. *Pretpostavimo da je* $a < b$ *i* $c \leq d$*. Tada je* $a + c < b + d$*.*
4. *Pretpostavimo da je* $a < b$ *i* $c < d$*. Tada je* $a + c < b + d$*.*

Dokaz.

1. Iz $a \leq b$ i definicije uređenog prstena slijedi $a+c \leq b+c$. Nadalje, iz $c \leq d$ i definicije uređenog prstena slijedi $b + c \leq b + d$. Iz činjenice da je relacija $\leq$ tranzitivna slijedi da je $a + c \leq b + d$.
2. Iz $a < b$ slijedi $a \leq b$, pa je $a + c \leq b + c$. Pretpostavimo da je $a + c = b + c$. Tada je $(a + c) + (-c) = (b + c) + (-c)$, pa slijedi da je $a = b$ što je u kontradikciji s $a < b$. Dakle, $a + c \neq b + c$, pa je $a + c < b + c$.
3. Iz $a < b$ i tvrdnje 2. slijedi $a + c < b + c$. Iz $c \leq d$ slijedi $b + c \leq b + d$. Iz propozicije 53. slijedi $a + c < b + d$.
4. Slijedi direktno iz tvrdnje 3.

□

Propozicija 85. *Neka je* $(P, +, \cdot, \leq)$ *uređeno polje, te neka je* $x \in P$*.*

1. *Pretpostavimo da je* $0 < x$*. Tada je* $0 < x^{-1}$*.*

2. *Pretpostavimo da je* $x < 0$. *Tada je* $x^{-1} < 0$.

Dokaz.

1. Vrijedi $x^{-1} \leq 0$ ili $0 \leq x^{-1}$. Pretpostavimo da je $x^{-1} \leq 0$. Tada je $0 \leq -x^{-1}$. Iz toga i činjenice da je $0 \leq x$, što slijedi iz $0 < x$, te definicije uređenog prstena slijedi da je $0 \leq (-x^{-1}) \cdot x$.

   Iz propozicije 44.1. slijedi da je $0 \leq -(x^{-1} \cdot x)$, tj. $0 \leq -1$, pa slijedi $1 \leq 0$. Međutim, ovo je u kontradikciji s činjenicom da je $0 < 1$ (prema korolaru 49.). Prema tome, $0 \leq x^{-1}$.

   Kada bi vrijedilo $x^{-1} = 0$, onda bismo imali $1 = x \cdot x^{-1} = x \cdot 0 = 0$, što je nemoguće. Prema tome, $x^{-1} \neq 0$, pa vrijedi $0 < x^{-1}$.

2. Iz $x < 0$ slijedi $0 < -x$ (prema propoziciji 84.3.). Tada je prema tvrdnji 1. $0 < (-x)^{-1}$, tj. $0 < -(x^{-1})$ (prema napomeni 70.), pa slijedi $x^{-1} < 0$.

□

Napomena 86. *Neka je* $(P, +, \cdot, \leq)$ *uređeno polje. Neka su* $x, y \in P$ *td. je* $0 < x$ *i* $0 < y$. *Tada je* $0 < x \cdot y$.

Naime, imamo $0 \leq x$ i $0 \leq y$, pa iz definicije uređenog prstena slijedi da je $0 \leq x \cdot y$. Imamo $0 \neq x$ i $0 \neq y$, pa iz činjenice da je $(P, +, \cdot)$ integralna domena (prema propoziciji 26.) slijedi da je $0 \neq x \cdot y$. Stoga je $0 < x \cdot y$.

Propozicija 87. *Neka je* $(P, +, \cdot, \leq)$ *uređeno polje. Neka su* $a, b, c \in P$ *td. je* $a < b$ *i* $0 < c$. *Tada je* $ac < bc$.

Dokaz. Iz $a < b$ slijedi $0 < b + (-a)$, tj. $0 < b - a$. Iz napomene 86. slijedi da je $0 < (b-a)c$. Iz propozicije 46. zaključujemo da je $0 < bc - ac$, pa je $ac < bc$. □

Primjer 88. $\mathbb{Z}$ *nije polje u* $(\mathbb{R}, +, \cdot)$.

Definirajmo $2 := 1 + 1$. Očito je $2 \in \mathbb{N}$. Iz $0 < 1$ slijedi $1 < 1 + 1$, tj. $1 < 2$. Posebno vrijedi $0 < 2$, pa iz propozicije 85. slijedi da je $0 < 2^{-1}$. Ovo, uz činjenicu da je $1 < 2$ i propoziciju 87. povlači da je $2^{-1} < 1$. Za $\forall n \in \mathbb{N}$ vrijedi $1 \leq n$, pa slijedi $2^{-1} \notin \mathbb{N}$. Nadalje iz $0 < 2^{-1}$ slijedi $2^{-1} \neq 0$.

Neka je $n \in \mathbb{N}$. Tada je $0 < n$ pa je $-n < 0$, što povlači da $-n \neq 2^{-1}$. Iz definicije od $\mathbb{Z}$ slijedi da $2^{-1} \notin \mathbb{Z}$. Iz $2 \in \mathbb{Z}$ i propozicije 82. slijedi da $\mathbb{Z}$ nije polje u $\mathbb{R}$.

Definicija 89. *Neka je* $(P, +, \cdot)$ *prsten, te neka je* $x \in P$. *Definiramo* $x^2 = x \cdot x$.

Uočimo da je $(-x)^2 = (-x) \cdot (-x) = x \cdot x = x^2$, pri čemu smo koristili propoziciju 44. 3. Dakle, $(-x)^2 = x^2$.

Propozicija 90. *Neka je* $(P, +, \cdot, \leq)$ *uređeni prsten. Neka je* $x \in P$. *Tada je* $0 \leq x^2$.

Dokaz. Vrijedi $0 \leq x$ ili $x \leq 0$.

1. $0 \leq x$

   Iz definicije uređenog prstena slijedi da je $0 \leq x \cdot x$, tj. $0 \leq x^2$.

2. $x \leq 0$

   Tada je $0 \leq -x$, pa iz 1. slučaja imamo $0 \leq (-x)^2$, tj. $0 \leq x^2$.

   U oba slučaja smo dobili $0 \leq x^2$. Dakle, propozicija je dokazana.

□

Propozicija 91. *Neka je* $(P, +, \cdot, \leq)$ *uređen prsten takav da je* $(P, +, \cdot)$ *netrivijalan prsten s jedinicom. Tada ne postoji* $x \in P$ *takav da je* $x^2 = -1$.

Dokaz. Pretpostavimo da postoji $x \in P$ takav da je $x^2 = -1$.

Iz prethodne propozicije slijedi da je $0 \leq x^2$, dakle $0 \leq -1$. Stoga je $1 \leq 0$. S druge strane, prema propoziciji 48. vrijedi $0 \leq 1$. Zaključujemo da je $0 = 1$. Iz napomene 24. slijedi da je $(P, +, \cdot)$ trivijalan prsten, što je u kontradikciji s pretpostavkom propozicije. Dakle, ne postoji $x \in P$ takav da je $x^2 = -1$. □

Korolar 92. *Ne postoji* $x \in \mathbb{R}$ *takav da je* $x^2 = -1$.

Dokaz. Imamo da je $(\mathbb{R}, +, \cdot, \leq)$ uređeno polje. Dakle $(\mathbb{R}, +, \cdot)$ je netrivijalan prsten s jedinicom, pa tvrdnja slijedi iz prethodne propozicije. □

Poglavlje 4

Polje kompleksnih brojeva $\mathbb{C}$

4.1 Definicija i svojstva kompleksnih brojeva

Definicija 93. *Definirajmo $\mathbb{C} = \mathbb{R} \times \mathbb{R}$. Na skupu $\mathbb{C}$ definirajmo binarne operacije $+$ i $\cdot$ na način:*

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

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

Definirajmo $0_{\mathbb{C}} = (0, 0)$ i $1_{\mathbb{C}} = (1, 0)$.

Propozicija 94. *Vrijedi: $(\mathbb{C}, +, \cdot)$ je polje. Nula u polju $\mathbb{C}$ je $0_{\mathbb{C}}$, a jedinica je $1_{\mathbb{C}}$.*

Dokaz. Neka su $z_1, z_2, z_3 \in \mathbb{C}$. Tada je $z_1 = (a_1, b_1)$, $z_2 = (a_2, b_2)$, $z_3 = (a_3, b_3)$ za neke $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{R}$.

Imamo:

$$\begin{aligned}(z_1 + z_2) + z_3 &= (a_1 + a_2, b_1 + b_2) + (a_3, b_3)\\ &= ((a_1 + a_2) + a_3, (b_1 + b_2) + b_3)\\ &= (a_1 + (a_2 + a_3), b_1 + (b_2 + b_3))\\ &= (a_1, b_1) + (a_2 + a_3, b_2 + b_3)\\ &= z_1 + (z_2 + z_3)\end{aligned}$$

Dakle, $(\mathbb{C}, +)$ je polugrupa.

Neka su $z_1, z_2 \in \mathbb{C}$, $z_1 = (a_1, b_1)$, $z_2 = (a_2, b_2)$.

Imamo:

$$\begin{aligned}(z_1 + z_2) &= (a_1 + a_2, b_1 + b_2)\\ &= (a_2 + a_1, b_2 + b_1)\\ &= z_2 + z_1\end{aligned}$$

Prema tome, operacija $+$ je komutativna.

Neka je $z \in \mathbb{C}$, $z = (a, b)$.
Imamo:

$$\begin{aligned} z + 0_{\mathbb{C}} &= (a + b) + (0, 0) \\ &= (a, b) \\ &= z \end{aligned}$$

Zbog komutativnosti operacije + također vrijedi $0_{\mathbb{C}} + z = z$. Prema tome, $0_{\mathbb{C}}$ je neutralni element za operaciju +. Dakle, $(\mathbb{C}, +)$ je monoid.

Neka je $z \in \mathbb{C}$, $z = (a, b)$. Definirajmo $z' = (-a, -b)$. Tada je $z + z' = 0_{\mathbb{C}}$.

Zaključujemo da je $(\mathbb{C}, +)$ Abelova grupa.

Neka su $z_1, z_2, z_3 \in \mathbb{C}$, $z_1 = (a_1, b_1)$, $z_2 = (a_2, b_2)$, $z_3 = (a_3, b_3)$. Tada je:

$$\begin{aligned} (z_1 \cdot z_2) \cdot z_3 &= (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1) \cdot (a_3, b_3) \\ &= ((a_1a_2 - b_1b_2)a_3 - (a_1b_2 + a_2b_1)b_3, (a_1a_2 - b_1b_2)b_3 + (a_1b_2 + a_2b_1)a_3) \end{aligned}$$

S druge strane:

$$\begin{aligned} z_1 \cdot (z_2 \cdot z_3) &= (a_1, b_1) \cdot (a_2a_3 - b_2b_3, a_2b_3 + a_3b_2) \\ &= (a_1(a_2a_3 - b_2b_3) - b_1(a_2b_3 + a_3b_2), a_1(a_2b_3 + a_3b_2) + b_1(a_2a_3 - b_2b_3)) \end{aligned}$$

Koristeći asocijativnost zbrajanja i množenja na $\mathbb{R}$, distributivnost množenja u odnosu na zbrajanje na $\mathbb{R}$ te propoziciju 46., zaključujemo da je $(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$. Prema tome, $(\mathbb{C}, \cdot)$ je polugrupa.

Neka su $z_1, z_2 \in \mathbb{C}$. Imamo $z_1 = (a, b)$ i $z_2 = (c, d)$, gdje su $a, b, c, d \in \mathbb{R}$. Vrijedi:

$$z_1 \cdot z_2 = (a \cdot c - b \cdot d, a \cdot d + b \cdot c)$$

$$z_2 \cdot z_1 = (c \cdot a - d \cdot b, c \cdot b + d \cdot a)$$

Koristeći komutativnost operacija + i $\cdot$ na $\mathbb{R}$ zaključujemo da je $z_1 \cdot z_2 = z_2 \cdot z_1$. Stoga je operacija $\cdot$ na $\mathbb{C}$ komutativna.

Neka je $z \in \mathbb{C}$, $z = (a, b)$, gdje je $a, b \in \mathbb{R}$. Imamo:

$$\begin{aligned} 1_{\mathbb{C}} \cdot z &= (1, 0) \cdot (a, b) \\ &= (1 \cdot a - 0 \cdot b, 1 \cdot b - 0 \cdot a) \\ &= (a, b) \\ &= z \end{aligned}$$

Dakle, $1_{\mathbb{C}} \cdot z = z$, a zbog komutativnosti vrijedi $z \cdot 1_{\mathbb{C}} = z$. Dakle, $(\mathbb{C}, \cdot)$ je monoid, a $1_{\mathbb{C}}$ je neutralni element u tom monoidu.

Neka su $z_1, z_2, z_3 \in \mathbb{C}$, $z_1 = (a_1, b_1)$, $z_2 = (a_2, b_2)$, $z_3 = (a_3, b_3)$. Vrijedi:

$$\begin{aligned} z_1 \cdot (z_2 + z_3) &= (a_1, b_1) \cdot (a_2 + a_3, b_2 + b_3) \\ &= (a_1(a_2 + a_3) - b_1(b_2 + b_3), a_1(b_2 + b_3) + b_1(a_2 + a_3)) \\ &= (a_1a_2 + a_1a_3 - b_1b_2 - b_1b_3, a_1b_2 + a_1b_3 + b_1a_2 + b_1a_3) \end{aligned}$$

S druge strane:

$$\begin{aligned} z_1 \cdot z_2 + z_1 \cdot z_3 &= (a_1, b_1) \cdot (a_2, b_2) + (a_1, b_1) \cdot (a_3, b_3) \\ &= (a_1a_2 - b_1b_2, a_1b_2 + b_1a_2) + (a_1a_3 - b_1b_3, a_1b_3 + b_1a_3) \\ &= (a_1a_2 - b_1b_2 + a_1a_3 - b_1b_3, a_1b_2 + b_1a_2 + a_1b_3 + b_1a_3) \end{aligned}$$

Iz činjenice da je $(\mathbb{R}, +, \cdot)$ prsten, zaključujemo da je $z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3$.

Koristeći dokazano i komutativnost operacije $\cdot$ na $\mathbb{C}$ dobivamo $(z_1+z_2)\cdot z_3 = z_3 \cdot (z_1+z_2) = z_3 \cdot z_1 + z_3 \cdot z_2 = z_1 \cdot z_3 + z_2 \cdot z_3$, dakle $(z_1 + z_2) \cdot z_3 = z_1 \cdot z_3 + z_2 \cdot z_3$.

Zaključujemo da je $(\mathbb{C}, +, \cdot)$ komutativan prsten s jedinicom. Nula u prstenu je $0_{\mathbb{C}}$, a jedinica je $1_{\mathbb{C}}$.

Neka je $z \in \mathbb{C}$ takav da je $z \neq 0_{\mathbb{C}}$. Imamo $z = (a, b)$, $a, b \in \mathbb{R}$. Zbog $z \neq 0_{\mathbb{C}}$ vrijedi $a^2 + b^2 > 0$. Definirajmo:

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

Imamo:

$$\begin{aligned} z \cdot u &= (a, b) \cdot \left(\frac{a}{a^2 + b^2} \, , \, \frac{-b}{a^2 + b^2} \right) \\ &= \left(\frac{a^2}{a^2 + b^2} - \frac{b \cdot (-b)}{a^2 + b^2} \, , \, \frac{-ab}{a^2 + b^2} + \frac{ba}{a^2 + b^2} \right) \\ &= (1, 0) \\ &= 1_{\mathbb{C}} \end{aligned}$$

Dakle, $z \cdot u = 1_{\mathbb{C}}$, te zbog komutativnosti vrijedi i $u \cdot z = 1_{\mathbb{C}}$. Znači, svaki element od $\mathbb{C}$ različit od $0_{\mathbb{C}}$ ima inverzni element u $(\mathbb{C}, \cdot)$.

Zaključak: $(\mathbb{C}, +, \cdot)$ je polje. □

Napomena 95. *Neka su $a, b \in \mathbb{R}$. Tada u prstenu $(\mathbb{C}, +, \cdot)$ vrijedi $-(a, b) = (-a, -b)$. Naime, to slijedi iz dokaza prethodne propozicije. Iz istog dokaza slijedi i da za $(a, b) \neq (0, 0)$ vrijedi $(a, b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \right)$.*

Primjer 96. *Neka je $z = (0,1)$. Koristeći napomenu 95. dobivamo da je $z^2 = z \cdot z = (0,1) \cdot (0,1) = (-1,0) = -(1,0) = -1_{\mathbb{C}}$. Dakle, $z^2 = -1_{\mathbb{C}}$.*

Propozicija 97. *Ne postoji uređaj $\leq$ na $\mathbb{C}$ tako da je $(\mathbb{C}, +, \cdot, \leq)$ uređeno polje.*

Dokaz. Naime, to slijedi iz primjera 96. i propozicije 91. □

4.2 Realni brojevi u $\mathbb{C}$

Definicija 98. *Definirajmo $\mathbb{R}' = \{(x,0) \mid x \in \mathbb{R}\}$.*

Propozicija 99. *$\mathbb{R}'$ je polje u $(\mathbb{C}, +, \cdot)$.*

Dokaz. Neka su $z_1, z_2 \in \mathbb{R}'$. Tada postoje $x, y \in \mathbb{R}$ tako da je $z_1 = (x,0)$ i $z_2 = (y,0)$. Vrijedi $z_1 - z_2 = z_1 + (-z_2) = (x,0) + (-y,0) = (x-y,0)$, pa je očito $z_1 - z_2 \in \mathbb{R}'$.

Nadalje imamo $z_1 \cdot z_2 = (x,0) \cdot (y,0) = (x \cdot y, 0)$, pa je $z_1 \cdot z_2 \in \mathbb{R}'$.

Neka je $z \in \mathbb{R}'$ takav da je $z \neq 0_{\mathbb{C}}$. Imamo $z = (x,0)$, gdje je $x \in \mathbb{R}$ i $x \neq 0$. Koristeći napomenu 95., dobivamo:

$$z^{-1} = (x,0)^{-1} = \left(\frac{x}{x^2+0^2}, \frac{-0}{x^2+0^2}\right) = \left(\frac{x}{x^2}, 0\right) = (x^{-1}, 0)$$

jer je prema propoziciji 67.:

$$\frac{x}{x^2} = \frac{1 \cdot x}{x \cdot x} = \frac{1}{x} = x^{-1}$$

U svakom slučaju, vrijedi $z^{-1} \in \mathbb{R}'$. Iz propozicije 82. slijedi da je $\mathbb{R}'$ polje u $(\mathbb{C}, +, \cdot)$. □

Definicija 100. *Prema prethodnoj propoziciji, postoje binarne operacije $+'$ i $\cdot'$ na $\mathbb{R}'$ tako da je $(\mathbb{R}', +', \cdot')$ potpolje od $(\mathbb{C}, +, \cdot)$. Neka su $x, y \in \mathbb{R}$. Imamo:*

$$(x,0) +' (y,0) = (x,0) + (y,0) = (x+y, 0)$$

$$(x,0) \cdot' (y,0) = (x,0) \cdot (y,0) = (x \cdot y, 0)$$

Dakle,

$$(x,0) +' (y,0) = (x+y, 0)$$

$$(x,0) \cdot' (y,0) = (x \cdot y, 0)$$

Definicija 101. *Na $\mathbb{R}'$ definiramo binarnu operaciju $\leq'$ na sljedeći način:*

$$(x,0) \leq' (y,0) \text{ ako je } x \leq y$$

Propozicija 102. *Binarna operacija $\leq'$ je uređaj na $\mathbb{R}'$.*

Dokaz. Neka je $x \in \mathbb{R}$. Tada je $x \leq x$, pa je $(x,0) \leq' (x,0)$. Prema tome, $\leq'$ je refleksivna relacija na $\mathbb{R}'$.

Neka su $x, y \in \mathbb{R}$ takvi da je $(x,0) \leq' (y,0)$ i $(y,0) \leq' (x,0)$. Tada je $x \leq y$ i $y \leq x$, pa je $x = y$. Stoga je $(x,0) = (y,0)$. Dakle, $\leq'$ je antisimetrična relacija na $\mathbb{R}'$.

Na sličan način zaključujemo da je $\leq'$ tranzitivna relacija na $\mathbb{R}'$ te da je $\leq'$ uređaj na $\mathbb{R}'$. □

Propozicija 103. *$(\mathbb{R}', +', \cdot', \leq')$ je uređeno polje.*

Dokaz. Dovoljno je dokazati da je $(\mathbb{R}', +', \cdot', \leq')$ uređeni prsten. Neka su $a, b, c \in \mathbb{R}'$ td. $a \leq' b$. Tvrdimo da je $a +' c \leq' b +' c$.

Imamo $a = (x,0)$, $b = (y,0)$ i $c = (z,0)$ gdje su $x, y, z \in \mathbb{R}$. Slijedi $x \leq y$, pa je $x + z \leq y + z$. Vrijedi:

$$a +' c = (x,0) +' (z,0) = (x+z, 0)$$

$$b +' c = (y,0) +' (z,0) = (y+z, 0)$$

Stoga je $a +' c \leq' b +' c$.

Uočimo da je $(0,0)$ nula u prstenu $(\mathbb{R}', +', \cdot')$. Pretpostavimo da su $a, b \in \mathbb{R}'$ takvi da je $(0,0) \leq' a$ i $(0,0) \leq' b$. Imamo $a = (x,0)$ i $b = (y,0)$, gdje su $x, y \in \mathbb{R}$. Slijedi $0 \leq x$ i $0 \leq y$, pa je $0 \leq x \cdot y$. Vrijedi $a \cdot' b = (x,0) \cdot' (y,0) = (x \cdot y, 0)$. Stoga je $(0,0) \leq' a \cdot' b$.

Zaključujemo da je $(\mathbb{R}', +', \cdot', \leq')$ uređeni prsten. □

4.3 Morfizam uređenih skupova

Definicija 104. *Neka su $(S, \leq)$ i $(T, \leq')$ uređeni skupovi, te neka je $f : S \to T$. Kažemo da je f **morfizam** uređenih skupova $(S, \leq)$ i $(T, \leq')$ ako za $\forall x, y \in S$ td. je $x \leq y$ vrijedi $f(x) \leq' f(y)$.*

Napomena 105. *Neka su $(S, \leq)$ i $(T, \leq')$ uređeni skupovi te neka je $f : S \to T$ morfizam ovih uređenih skupova. Pretpostavimo da su $x, y \in S$ td. je $f(x) <' f(y)$. Tada je $x < y$.*

Naime, pretpostavimo suprotno. Tada je po napomeni 52. $y \leq x$, pa slijedi $f(y) \leq' f(x)$. Ovo je prema napomeni 50. u kontradikciji s $f(x) <' f(y)$.

Propozicija 106. *Neka su $(S, \leq)$ i $(T, \leq')$ uređeni skupovi, te neka je $f : S \to T$ morfizam ovih uređenih skupova. Pretpostavimo da je f surjekcija, te da je $(S, \leq)$ potpuno uređen skup. Tada je $(T, \leq')$ potpuno uređen skup.*

Dokaz. Pretpostavimo da su $A, B \subseteq T$ td. $A \neq \emptyset$ i $B \neq \emptyset$ te $a \leq' b$, $\forall a \in A$ i $\forall b \in B$. Želimo dokazati da postoji $c \in T$ td.

$$a \leq' c \leq' b, \ \forall a \in A, \forall b \in B \qquad (\bullet)$$

To je jasno ako je $A \cap B \neq 0$. Naime, u tom slučaju možemo odabrati neki $c \in A \cap B$. Budući da je $c \in A$, vrijedi $c \leq' b$, $\forall b \in B$, a budući da je $c \in B$, vrijedi $a \leq' c$, $\forall a \in A$. Dakle, vrijedi (•).

Pretpostavimo da je $A \cap B = \emptyset$. Tada za $\forall a \in A, \forall b \in B$ vrijedi $a <' b$ (jer je $a \neq b$ i $a \leq' b$). Tvrdimo da je $f^{-1}(A) \neq \emptyset$.

Naime, odaberimo neki $a \in A$ obzirom da je $A \neq \emptyset$. Budući da je f surjekcija, postoji $x \in S$ takav da je $f(x) = a$. Dakle, $f(x) \in A$, pa je $x \in f^{-1}(A)$. Prema tome, $f^{-1}(A) \neq \emptyset$.

Analogno vidimo da je $f^{-1}(B) \neq \emptyset$.

Neka su $x \in f^{-1}(A)$ i $y \in f^{-1}(B)$. Tada je $f(x) \in A$ i $f(y) \in B$, pa je $f(x) <' f(y)$. Prema napomeni 105. vrijedi $x < y$. Dakle, $f^{-1}(A)$ i $f^{-1}(B)$ su neprazni podskupovi od S takvi da je $x \leq y$ za $\forall x \in f^{-1}(A)$ i za $\forall y \in f^{-1}(B)$. Budući da je $(S, \leq)$ potpuno uređen skup, postoji $z \in S$ tako da vrijedi:

$$x \leq z \leq y, \ \forall x \in f^{-1}(A), \forall y \in f^{-1}(B) \qquad (\bullet\bullet)$$

Označimo $c = f(z)$. Tvrdimo da vrijedi (•). Uzmimo neki $a \in A$. Budući da je f surjekcija, postoji $x \in S$ takav da je $f(x) = a$. Očito je $x \in f^{-1}(A)$.

Iz (••) slijedi da je $x \leq z$. Budući da je f morfizam uređenih skupova $(S, \leq)$ i $(T, \leq')$ imamo $f(x) \leq' f(z)$, tj. $a \leq' c$. Uzmimo $b \in B$. Tada postoji $y \in S$ takav da je $f(y) = b$. Imamo $y \in f^{-1}(B)$, pa prema (••) vrijedi $z \leq y$. Slijedi $f(z) \leq' f(y)$, tj. $c \leq' b$. Dakle, vrijedi (•).

Zaključak: $(T, \leq')$ je potpuno uređen skup. □

Korolar 107. $(\mathbb{R}', +', \cdot', \leq')$ *je potpuno uređeno polje.*

Prema propoziciji 103. vrijedi da je $(\mathbb{R}', +', \cdot', \leq')$ uređeno polje. Stoga je dovoljno dokazati da je $(\mathbb{R}', \leq')$ potpuno uređen skup.

Definirajmo funkciju $f : \mathbb{R} \to \mathbb{R}'$ sa $f(x) = (x, 0)$. Očito je f surjekcija. Nadalje, f je očito morfizam uređenih skupova $(\mathbb{R}, \leq)$ i $(\mathbb{R}', \leq')$. Imamo da je $(\mathbb{R}, \leq)$ potpuno uređen skup, pa iz prethodne propozicije slijedi da je $(\mathbb{R}', \leq')$ potpuno uređen skup.

Napomena 108. *Neka je* $i = (0, 1)$. *Imamo* $i \in \mathbb{C}$ *i* $i^2 = -1_{\mathbb{C}}$ *prema primjeru 96. Neka je* $z \in \mathbb{C}$. *Tvrdimo da postoje jedinstveni* $a, b \in \mathbb{R}'$ *td.* $z = a + bi$.

Naime, imamo $z = (x, y)$, gdje su $x, y \in \mathbb{R}$. Definirajmo $a = (x, 0)$ i $b = (y, 0)$. Očito su $a, b \in \mathbb{R}'$. Nadalje vrijedi:

$$\begin{aligned} a + bi &= (x, 0) + (y, 0) \cdot (0, 1) \\ &= (x, 0) + (0, y) \\ &= (x, y) \\ &= z \end{aligned}$$

Dakle, $z = a + bi$.

Pretpostavimo da su $a', b' \in \mathbb{R}'$ takvi da je $z = a' + b'i$. Slijedi da postoje $x', y' \in \mathbb{R}$ takvi da je $a' = (x', 0)$ i $b' = (y', 0)$. Vrijedi:

$$\begin{aligned}(x, y) &= z \\ &= a' + b'i \\ &= (x', 0) + (y', 0) \cdot (0, 1) \\ &= (x', 0) + (0, y') \\ &= (x', y')\end{aligned}$$

Dakle, $(x, y) = (x', y')$, pa je $x = x'$ i $y = y'$. Prema tome, $a = a'$ i $b = b'$.

Poglavlje 5

Tijelo kvaterniona $\mathbb{H}$

5.1 Definicija i svojstva kvaterniona

Definicija 109. *Definirajmo* $\mathbb{H} = \mathbb{R}^4$. *Na* $\mathbb{H}$ *definirajmo binarne operacije* $+$ *i* $\cdot$ *na sljedeći način:*

$$(x_1, x_2, x_3, x_4) + (y_1, y_2, y_3, y_4) = (x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4)$$

$$\begin{aligned}(x_1, x_2, x_3, x_4) \cdot (y_1, y_2, y_3, y_4) = (&x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4, x_2y_1 + x_1y_2 - x_4y_3 + x_3y_4,\\ &x_3y_1 + x_4y_2 + x_1y_3 - x_2y_4, x_4y_1 - x_3y_2 + x_2y_3 + x_1y_4)\end{aligned}$$

Propozicija 110. *Neka je* $0_{\mathbb{H}} = (0, 0, 0, 0)$. *Neutralni element za operaciju* $+$ *je* $0_{\mathbb{H}}$. *Inverzni element od* $(x_1, x_2, x_3, x_4) \in \mathbb{H}$ *u monoidu* $(\mathbb{H}, +)$ *je* $(-x_1, -x_2, -x_3 - x_4)$. $(\mathbb{H}, +)$ *je Abelova grupa.*

Dokaz. Neka su $a, b, c, d \in \mathbb{H}$. Imamo $a = (x_1, x_2, x_3, x_4)$, $b = (y_1, y_2, y_3, y_4)$ i $c = (z_1, z_2, z_3, z_4)$. Vrijedi:

$$\begin{aligned}(a + b) + c &= (x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4) + (z_1, z_2, z_3, z_4)\\ &= ((x_1 + y_1) + z_1, (x_2 + y_2) + z_2, (x_3 + y_3) + z_3, (x_4 + y_4) + z_4)\\ &= (x_1 + (y_1 + z_1), x_2 + (y_2 + z_2), x_3 + (y_3 + z_3), x_4 + (y_4 + z_4))\\ &= a + (b + c)\end{aligned}$$

Dakle, $(a + b) + c = a + (b + c)$. Prema tome, operacija $+$ na $\mathbb{H}$ je asocijativna.

Očito je $a + 0_{\mathbb{H}} = 0_{\mathbb{H}} + a$, za $\forall a \in \mathbb{H}$. Prema tome, $(\mathbb{H}, +)$ je monoid i $0_{\mathbb{H}}$ je neutralni element u tom monoidu.

Neka je $a \in \mathbb{H}$. Imamo $a = (x_1, x_2, x_3, x_4)$. Definirajmo $b = (-x_1, -x_2, -x_3, -x_4)$. Tada je očito $a + b = 0_{\mathbb{H}} = b + a$. Prema tome, b je inverzni element od a u monoidu $(\mathbb{H}, +)$. Zaključak, $(\mathbb{H}, +)$ je grupa.

Kako je operacija + na $\mathbb{H}$ očito komutativna, $(\mathbb{H}, +)$ je Abelova grupa. □

Propozicija 111. $(\mathbb{H}, \cdot)$ *je polugrupa.*

Dokaz. Neka su $a, b, c, d \in \mathbb{H}$. Imamo $a = (x_1, x_2, x_3, x_4)$, $b = (y_1, y_2, y_3, y_4)$ i $c = (z_1, z_2, z_3, z_4)$. Vrijedi:

$$\begin{aligned}
(a \cdot b) \cdot c &= (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4, x_2y_1 + x_1y_2 - x_4y_3 + x_3y_4, x_3y_1 + \\
&\quad x_4y_2 + x_1y_3 - x_2y_4, x_4y_1 - x_3y_2 + x_2y_3 + x_1y_4) \cdot (z_1, z_2, z_3, z_4) \\
&= (x_1y_1z_1 - x_2y_2z_1 - x_3y_3z_1 - x_4y_4z_1 - (x_2y_1z_2 + x_1y_2z_2 - x_4y_3z_2 + x_3y_4z_2) - \\
&\quad (x_3y_1z_3 + x_4y_2z_3 + x_1y_3z_3 - x_2y_4z_3) - (x_4y_1z_4 - x_3y_2z_4 + x_2y_3z_4 + x_1y_4z_4), \\
&\quad x_2y_1z_1 + x_1y_2z_1 - x_4y_3z_1 + x_3y_4z_1 + x_1y_1z_2 - x_2y_2z_2 - x_3y_3z_2 - x_4y_4z_2 - \\
&\quad (x_4y_1z_3 - x_3y_2z_3 + x_2y_3z_3 + x_1y_4z_3) + x_3y_1z_4 + x_4y_2z_4 + x_1y_3z_4 - x_2y_4z_4, \\
&\quad x_3y_1z_1 + x_4y_2z_1 + x_1y_3z_1 - x_2y_4z_1 + x_4y_1z_2 - x_3y_2z_2 + x_2y_3z_2 + x_1y_4z_2 + \\
&\quad x_1y_1z_3 - x_2y_2z_3 - x_3y_3z_3 - x_4y_4z_3 - (x_2y_1z_4 + x_1y_2z_4 - x_4y_3z_4 + x_3y_4z_4), \\
&\quad x_4y_1z_1 - x_3y_2z_1 + x_2y_3z_1 + x_1y_4z_1 - (x_3y_1z_2 + x_4y_2z_2 + x_1y_3z_2 - x_2y_4z_2) + \\
&\quad x_2y_1z_3 + x_1y_2z_3 - x_4y_3z_3 + x_3y_4z_3 + x_1y_1z_4 - x_2y_2z_4 - x_3y_3z_4 - x_4y_2z_4)
\end{aligned}$$

S druge strane vrijedi:

$$\begin{aligned}
(a \cdot b) \cdot c &= (x_1, x_2, x_3, x_4) \cdot (y_1z_1 - y_2z_2 - y_3z_3 - y_4z_4, y_2z_1 + y_1z_2 - y_4z_3 + \\
&\quad y_3z_4, y_3z_1 + y_4z_2 + y_1z_3 - y_2z_4, y_4z_1 - y_3z_2 + y_2z_3 + y_1z_4) \\
&= (x_1y_1z_1 - x_1y_2z_2 - x_1y_3z_3 - x_1y_4z_4 - (x_2y_2z_1 + x_2y_1z_2 - x_2y_4z_3 + x_2y_3z_4) - \\
&\quad (x_3y_3z_1 + x_3y_4z_2 + x_3y_1z_3 - x_3y_2z_4) - (x_4y_4z_1 - x_4y_3z_2 + x_4y_2z_3 + x_4y_1z_4), \\
&\quad x_2y_1z_1 - x_2y_2z_2 - x_2y_3z_3 - x_2y_4z_4 + x_1y_2z_1 + x_1y_1z_2 - x_1y_4z_3 + x_1y_3z_4 - \\
&\quad (x_4y_3z_1 + x_4y_4z_2 + x_4y_1z_3 - x_4y_2z_4) + x_3y_4z_1 - x_3y_3z_2 + x_3y_2z_3 + x_3y_1z_4, \\
&\quad x_3y_1z_1 - x_3y_2z_2 - x_3y_3z_3 - x_3y_4z_4 + x_4y_2z_1 + x_4y_1z_2 - x_4y_4z_3 + x_4y_3z_4 + \\
&\quad x_1y_3z_1 + x_1y_4z_2 + x_1y_1z_3 - x_1y_2z_4 - (x_2y_4z_1 - x_2y_3z_2 + x_2y_2z_3 + x_2y_1z_4), \\
&\quad x_4y_1z_1 - x_4y_2z_2 - x_4y_3z_3 - x_4y_4z_4 - (x_3y_2z_1 + x_3y_1z_2 - x_3y_4z_3 + x_3y_3z_4) + \\
&\quad x_2y_3z_1 + x_2y_4z_2 + x_2y_1z_3 - x_2y_2z_4 + x_1y_4z_1 - x_1y_3z_2 + x_1y_2z_3 + x_1y_1z_4)
\end{aligned}$$

Lako zaključujemo da je $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Prema tome, $(\mathbb{H}, \cdot)$ je polugrupa. □

Propozicija 112. *Neka je* $1_{\mathbb{H}} = (1, 0, 0, 0)$. *Tada je* $1_{\mathbb{H}}$ *neutralni element za operaciju* $\cdot$ *na* $\mathbb{H}$.

Dokaz. Neka je $a \in \mathbb{H}$. Imamo $a = (x_1, x_2, x_3, x_4)$. Vrijedi:

$$\begin{aligned} a \cdot 1_{\mathbb{H}} &= (x_1, x_2, x_3, x_4) \cdot (1, 0, 0, 0) \\ &= (x_1, x_2, x_3, x_4) \\ &= a \end{aligned}$$

Dakle, $a \cdot 1_{\mathbb{H}} = a$.

Analogno, $1_{\mathbb{H}} \cdot a = a$. □

Propozicija 113. $(\mathbb{H}, +, \cdot)$ *je prsten.*

Dokaz. Neka su $x, y, z \in \mathbb{H}$. Imamo $x = (x_1, x_2, x_3, x_4)$, $y = (y_1, y_2, y_3, y_4)$ i $z = (z_1, z_2, z_3, z_4)$. Vrijedi:

$$\begin{aligned} x \cdot (y + z) &= (x_1, x_2, x_3, x_4) \cdot (y_1 + z_1, y_2 + z_2, y_3 + z_3, y_4 + z_4) \\ &= (x_1(y_1 + z_1) - x_2(y_2 + z_2) - x_3(y_3 + z_3) - x_4(y_4 + z_4), \\ &\quad x_2(y_1 + z_1) + x_1(y_2 + z_2) - x_4(y_3 + z_3) + x_3(y_4 + z_4), \\ &\quad x_3(y_1 + z_1) + x_4(y_2 + z_2) + x_1(y_3 + z_3) - x_2(y_4 + z_4), \\ &\quad x_4(y_1 + z_1) - x_3(y_2 + z_2) + x_2(y_3 + z_3) + x_1(y_4 + z_4)) \\ &= (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 + x_1z_1 - x_2z_2 - x_3z_3 - x_4z_4, \\ &\quad x_2y_1 + x_1y_2 - x_4y_3 + x_3y_4 + x_2z_1 + x_1z_2 - x_4z_3 + x_3z_4, \\ &\quad x_3y_1 + x_4y_2 + x_1y_3 - x_2y_4 + x_3z_1 + x_4z_2 + x_1z_3 - x_2z_4, \\ &\quad x_4y_1 - x_3y_2 + x_2y_3 + x_1y_4 + x_4z_1 - x_3z_2 + x_2z_3 + x_1z_4) \\ &= (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4, x_2y_1 + x_1y_2 - x_4y_3 + x_3y_4, \\ &\quad x_3y_1 + x_4y_2 + x_1y_3 - x_2y_4, x_4y_1 - x_3y_2 + x_2y_3 + x_1y_4) + \\ &\quad (x_1z_1 - x_2z_2 - x_3z_3 - x_4z_4, x_2z_1 + x_1z_2 - x_4z_3 + x_3z_4, \\ &\quad x_3z_1 + x_4z_2 + x_1z_3 - x_2z_4, x_4z_1 - x_3z_2 + x_2z_3 + x_1z_4) \\ &= (x_1, x_2, x_3, x_4) \cdot (y_1, y_2, y_3, y_4) + (x_1, x_2, x_3, x_4) \cdot (z_1, z_2, z_3, z_4) \\ &= xy + xz \end{aligned}$$

Dakle, $x(y + z) = xy + xz$.

Nadalje:

$$\begin{aligned}
(x+y)\cdot z &= (x_1+y_1, x_2+y_2, x_3+y_3, x_4+y_4)\cdot(z_1, z_2, z_3, z_4)\\
&= ((x_1+y_1)z_1 - (x_2+y_2)z_2 - (x_3+y_3)z_3 - (x_4+y_4)z_4,\\
&\quad (x_2+y_2)z_1 + (x_1+y_1)z_2 - (x_4+y_4)z_3 + (x_3+y_3)z_4,\\
&\quad (x_3+y_3)z_1 + (x_4+y_4)z_2 + (x_1+y_1)z_3 - (x_2+y_2)z_4,\\
&\quad (x_4+y_4)z_1 - (x_3+y_3)z_2 + (x_2+y_2)z_3 + (x_1+y_1)z_4)\\
&= (x_1z_1 - x_2z_2 - x_3z_3 - x_4z_4 + y_1z_1 - y_2z_2 - y_3z_3 - y_4z_4,\\
&\quad x_2z_1 + x_1z_2 - x_4z_3 + x_3z_4 + y_2z_1 + y_1z_2 - y_4z_3 + y_3z_4,\\
&\quad x_3z_1 + x_4z_2 + x_1z_3 - x_2z_4 + y_3z_1 + y_4z_2 + y_1z_3 - y_2z_4,\\
&\quad x_4z_1 - x_3z_2 + x_2z_3 + x_1z_4 + y_4z_1 - y_3z_2 + y_2z_3 + y_1z_4)\\
&= (x_1z_1 - x_2z_2 - x_3z_3 - x_4z_4, x_2z_1 + x_1z_2 - x_4z_3 + x_3z_4,\\
&\quad x_3z_1 + x_4z_2 + x_1z_3 - x_2z_4, x_4z_1 - x_3z_2 + x_2z_3 + x_1z_4) +\\
&\quad (y_1z_1 - y_2z_2 - y_3z_3 - y_4z_4, y_2z_1 + y_1z_2 - y_4z_3 + y_3z_4,\\
&\quad y_3z_1 + y_4z_2 + y_1z_3 - y_2z_4, y_4z_1 - y_3z_2 + y_2z_3 + y_1z_4)\\
&= (x_1, x_2, x_3, x_4)\cdot(z_1, z_2, z_3, z_4) + (y_1, y_2, y_3, y_4)\cdot(z_1, z_2, z_3, z_4)\\
&= xz + yz
\end{aligned}$$

Prema tome, $(x+y)z = xz + yz$.

Iz propozicija 110. i 111. slijedi da je $(\mathbb{H}, +, \cdot)$ prsten. □

Propozicija 114. *Neka je* $x \in \mathbb{H}$, $x \neq 0_{\mathbb{H}}$. *Tada postoji* $y \in \mathbb{H}$ *takav da je* $x \cdot y = 1_{\mathbb{H}}$.

Dokaz. Imamo $x = (x_1, x_2, x_3, x_4)$, gdje su $x_1, x_2, x_3, x_4 \in \mathbb{R}$ i pri čemu je $x_i \neq 0$ za bar jedan $i \in \{1, 2, 3, 4\}$. Neka su $y_1, y_2, y_3, y_4 \in \mathbb{R}$, te neka je $y = (y_1, y_2, y_3, y_4)$. Tada je $x \cdot y = 1_{\mathbb{H}}$ ako i samo ako vrijede sljedeće 4 jednakosti:

$$\begin{aligned}
x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 &= 1\\
x_2y_1 + x_1y_2 - x_4y_3 + x_3y_4 &= 0\\
x_3y_1 + x_4y_2 + x_1y_3 - x_2y_4 &= 0\\
x_4y_1 - x_3y_2 + x_2y_3 + x_1y_4 &= 0
\end{aligned}$$

Odnosno, prethodne 4 jednakosti vrijede ako i samo ako:

$$\underbrace{\overbrace{\begin{bmatrix} x_1 & -x_2 & -x_3 & -x_4\\ x_2 & x_1 & -x_4 & x_3\\ x_3 & x_4 & x_1 & -x_2\\ x_4 & -x_3 & x_2 & x_1 \end{bmatrix}}^{\star} \cdot \begin{bmatrix} y_1\\ y_2\\ y_3\\ y_4 \end{bmatrix} = \begin{bmatrix} 1\\ 0\\ 0\\ 0 \end{bmatrix}}_{\diamond}$$

Neka je $A = \begin{bmatrix} x_1 & -x_2 & -x_3 & -x_4 \\ x_2 & x_1 & -x_4 & x_3 \\ x_3 & x_4 & x_1 & -x_2 \\ x_4 & -x_3 & x_2 & x_1 \end{bmatrix}$.

Imamo:

$$\begin{aligned}
\det A &= x_1 \cdot \begin{vmatrix} x_1 & -x_4 & x_3 \\ x_4 & x_1 & -x_2 \\ -x_3 & x_2 & x_1 \end{vmatrix} + x_2 \cdot \begin{vmatrix} x_2 & -x_4 & x_3 \\ x_3 & x_1 & -x_2 \\ x_4 & x_2 & x_1 \end{vmatrix} - x_3 \cdot \begin{vmatrix} x_2 & x_1 & x_3 \\ x_3 & x_4 & -x_2 \\ x_4 & -x_3 & x_1 \end{vmatrix} + x_4 \cdot \begin{vmatrix} x_2 & x_1 & -x_4 \\ x_3 & x_4 & x_1 \\ x_4 & -x_3 & x_2 \end{vmatrix} \\
&= x_1 \left(x_1 \begin{vmatrix} x_1 & -x_2 \\ x_2 & x_1 \end{vmatrix} + x_4 \begin{vmatrix} x_4 & -x_2 \\ -x_3 & x_1 \end{vmatrix} + x_3 \begin{vmatrix} x_4 & x_1 \\ -x_3 & x_2 \end{vmatrix} \right) + \\
&\quad x_2 \left(x_2 \begin{vmatrix} x_1 & -x_2 \\ x_2 & x_1 \end{vmatrix} + x_4 \begin{vmatrix} x_3 & -x_2 \\ x_4 & x_1 \end{vmatrix} + x_3 \begin{vmatrix} x_3 & x_1 \\ x_4 & x_2 \end{vmatrix} \right) - \\
&\quad x_3 \left(x_2 \begin{vmatrix} x_4 & -x_2 \\ -x_3 & x_1 \end{vmatrix} - x_1 \begin{vmatrix} x_3 & -x_2 \\ x_4 & x_1 \end{vmatrix} + x_3 \begin{vmatrix} x_3 & x_4 \\ x_4 & -x_3 \end{vmatrix} \right) + \\
&\quad x_4 \left(x_2 \begin{vmatrix} x_4 & x_1 \\ -x_3 & x_2 \end{vmatrix} - x_1 \begin{vmatrix} x_3 & x_1 \\ x_4 & x_2 \end{vmatrix} - x_4 \begin{vmatrix} x_3 & x_4 \\ x_4 & -x_3 \end{vmatrix} \right) \\
&= x_1 \left[x_1 \left(x_1^2 + x_2^2 \right) + x_4 \left(x_1 x_4 - x_2 x_3 \right) + x_3 \left(x_2 x_4 + x_1 x_3 \right) \right] + \\
&\quad x_2 \left[x_2 \left(x_1^2 + x_2^2 \right) + x_4 \left(x_1 x_3 + x_2 x_4 \right) + x_3 \left(x_2 x_3 - x_1 x_4 \right) \right] - \\
&\quad x_3 \left[x_2 \left(x_1 x_4 - x_2 x_3 \right) - x_1 \left(x_1 x_3 + x_2 x_4 \right) + x_3 \left(-x_3^2 - x_4^2 \right) \right] + \\
&\quad x_4 \left[x_2 \left(x_2 x_4 + x_1 x_3 \right) - x_1 \left(x_2 x_3 - x_1 x_4 \right) - x_4 \left(-x_3^2 - x_4^2 \right) \right] \\
&= x_1 \left[x_1 \left(x_1^2 + x_2^2 \right) + x_1 x_4^2 - \cancel{x_2 x_3 x_4} + \cancel{x_2 x_3 x_4} + x_1 x_3^2 \right] + \\
&\quad x_2 \left[x_2 \left(x_1^2 + x_2^2 \right) + \cancel{x_1 x_3 x_4} + x_2 x_4^2 + x_2 x_3^2 - \cancel{x_1 x_3 x_4} \right] - \\
&\quad x_3 \left[\cancel{x_1 x_2 x_4} - x_2^2 x_3 - x_1^2 x_3 - \cancel{x_1 x_2 x_4} - x_3 \left(x_3^2 + x_4^2 \right) \right] + \\
&\quad x_4 \left[x_2^2 x_4 + \cancel{x_1 x_2 x_3} - \cancel{x_1 x_2 x_3} + x_1^2 x_4 + x_4 \left(x_3^2 + x_4^2 \right) \right] \\
&= x_1^2 \left(x_1^2 + x_2^2 \right) + x_1^2 x_4^2 + x_1^2 x_3^2 + x_2^2 \left(x_1^2 + x_2^2 \right) + x_2^2 x_4^2 + x_2^2 x_3^2 + \\
&\quad x_3^2 x_2^2 + x_1^2 x_3^2 + x_3^2 \left(x_3^2 + x_4^2 \right) + x_2^2 x_4^2 + x_1^2 x_4^2 + x_4^2 \left(x_3^2 + x_4^2 \right) \\
&= x_1^2 \left(x_1^2 + x_2^2 + x_3^2 + x_4^2 \right) + x_2^2 \left(x_1^2 + x_2^2 + x_3^2 + x_4^2 \right) + x_3^2 \left(x_1^2 + x_2^2 + x_3^2 + x_4^2 \right) + \\
&\quad x_4^2 \left(x_1^2 + x_2^2 + x_3^2 + x_4^2 \right) \\
&= \left(x_1^2 + x_2^2 + x_3^2 + x_4^2 \right) \cdot \left(x_1^2 + x_2^2 + x_3^2 + x_4^2 \right) \\
&= \left(x_1^2 + x_2^2 + x_3^2 + x_4^2 \right)^2
\end{aligned}$$

Dakle, $\det A = \left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right)^2$. Zaključujemo da je $\det A > 0$, pa stoga postoje jedinstveni $y_1, y_2, y_3, y_4 \in \mathbb{R}$ tako da vrijedi ($\diamond$).

Stoga postoji jedinstveni $y \in \mathbb{H}$ takav da je $x \cdot y = 1_{\mathbb{H}}$. □

Teorem 115. $(\mathbb{H}, +, \cdot)$ *je tijelo.*

Dokaz. Znamo da je $(\mathbb{H}, +, \cdot)$ netrivijalan prsten s jedinicom. Neka je $x \in \mathbb{H}$, $x \neq 0_{\mathbb{H}}$. Prema prethodnoj propoziciji, postoji $y \in \mathbb{H}$ takav da je $x \cdot y = 1_{\mathbb{H}}$.

Uočimo da je $y \neq 0_{\mathbb{H}}$, jer bi u suprotnom imali da je $x \cdot y = 0_{\mathbb{H}}$, što je nemoguće jer je $0_{\mathbb{H}} \neq 1_{\mathbb{H}}$. Stoga prema istoj propoziciji postoji $z \in \mathbb{H}$ takav da je $y \cdot z = 1_{\mathbb{H}}$. Iz $x \cdot y = 1_{\mathbb{H}}$ slijedi $(x \cdot y) \cdot z = 1_{\mathbb{H}} \cdot z$, tj. $x \cdot (y \cdot z) = z$, pa je $x \cdot 1_{\mathbb{H}} = z$, odnosno $x = z$. Stoga je $y \cdot x = 1_{\mathbb{H}}$. Prema tome, y je inverzni element od x u monoidu $(\mathbb{H}, \cdot)$.

Time je tvrdnja teorema dokazana. □

Napomena 116. $(\mathbb{H}, +, \cdot)$ *je nekomutativno tijelo, tj. operacija* $\cdot$ *nije komutativna.*

Naime, uzmimo $x = (0, 1, 0, 0)$ i $y = (0, 0, 1, 0)$. Tada lako dobivamo da je $x \cdot y = (0, 0, 0, 1)$, a $y \cdot x = (0, 0, 0, -1)$.

Prema tome, $x \cdot y \neq y \cdot x$.

Napomena 117. *Neka je* $x \in \mathbb{H}$, $x \neq 0_{\mathbb{H}}$, $x = (x_1, x_2, x_3, x_4)$. *Neka je* y *inverzni element od* x *u* $(\mathbb{H}, \cdot)$. *Imamo* $y = (y_1, y_2, y_3, y_4)$.

Iz dokaza propozicije 114. slijedi da je $\underbrace{A \cdot \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}}_{\diamond}$, gdje je A matrica definirana sa ($\star$) u prethodnoj propoziciji.

Neka je $\lambda = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Lako dobivamo da je $A \cdot A^\tau = \begin{bmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{bmatrix} = \lambda \cdot I$, gdje je I jedinična matrica, a A^τ transponirana matrica matrice A.

Stoga je $A \cdot \left(\frac{1}{\lambda} A^\tau\right) = I$, pa je $A^{-1} = \frac{1}{\lambda} A^\tau$. Iz ($\diamond$) slijedi da je $\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = A^{-1} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$, tj.

$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \frac{1}{\lambda} A^\tau \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$. Slijedi $(y_1, y_2, y_3, y_4) = \left(\frac{x_1}{\lambda}, -\frac{x_2}{\lambda}, -\frac{x_3}{\lambda}, -\frac{x_4}{\lambda}\right)$. Dakle,

$$\underbrace{x^{-1} = \left(\frac{x_1}{x_1^2+x_2^2+x_3^2+x_4^2}, -\frac{x_2}{x_1^2+x_2^2+x_3^2+x_4^2}, -\frac{x_3}{x_1^2+x_2^2+x_3^2+x_4^2}, -\frac{x_4}{x_1^2+x_2^2+x_3^2+x_4^2}\right)}_{\triangle}$$

Napomena 118. *Neka je $(P, +, \cdot)$ prsten s jedinicom. Pretpostavimo da x ima inverzni element u monoidu $(P, \cdot)$. Tada $-x$ ima inverzni element u monoidu $(P, \cdot)$, te vrijedi $(-x)^{-1} = -x^{-1}$.*

Naime, iz $x \cdot x^{-1} = 1$, $x^{-1} \cdot x = 1$ i propozicije 44. slijedi $(-x) \cdot (-x^{-1}) = 1$ i $(-x^{-1}) \cdot (-x) = 1$, dakle, tvrdnja vrijedi.

Definicija 119. *Neka je $i = (0, 1, 0, 0)$, $j = (0, 0, 1, 0)$ i $k = (0, 0, 0, 1)$. Iz definicije operacije $\cdot$ u $\mathbb{H}$ slijedi $i^2 = -1_{\mathbb{H}}$, $j^2 = -1_{\mathbb{H}}$, $k^2 = -1_{\mathbb{H}}$. Iz ($\triangle$) slijedi $i^{-1} = -i$, $j^{-1} = -j, k^{-1} = -k$.*

Vrijedi $i \cdot j = (0, 0, 0, 1)$, dakle $i \cdot j = k$. Stoga je $(i \cdot j)^{-1} = k^{-1}$, pa je $j^{-1} \cdot i^{-1} = k^{-1}$. Slijedi $(-j) \cdot (-i) = -k$. Stoga je $j \cdot i = -k$.

Iz $i \cdot j = k$ slijedi $(i \cdot j) \cdot j = k \cdot j$, pa je $i \cdot (-1_{\mathbb{H}}) = k \cdot j$, tj. $k \cdot j = -i$.

Invertiranjem i korištenjem napomene 118., dobijemo $j \cdot k = i$. Iz $i \cdot j = k$ množenjem slijeva s i slijedi $-j = i \cdot k$. Invertiranjem dobijemo $j = k \cdot i$.

Definicija 120. *Neka je $(P, +, \cdot)$ prsten, te $A \subseteq P$. Kažemo da je **A tijelo u** $(P, +, \cdot)$ ako postoje binarne operacije $+_A$ i $\cdot_A$ na A tako da je $(A, +_A, \cdot_A)$ tijelo i $x +_A y = x + y$, te $x \cdot_A y = x \cdot y$, $\forall x, y \in A$.*

Napomena 121. *Neka je $(P, +, \cdot)$ prsten i $A \subseteq P$. Tada je A polje u $(P, +, \cdot)$ ako i samo ako je A polje u $(P, +, \cdot)$ i $(P, +, \cdot)$ je polje.*

Tvrdnja slijedi iz prethodne definicije i definicije polja u prstenu (definicija 81.).

5.2 Morfizam prstenova

Definicija 122. *Neka su $(A, +_A, \cdot_A)$ i $(B, +_B, \cdot_B)$ prsteni. Za funkciju $f : A \to B$ kažemo da je **morfizam** ovih prstena ako za $\forall x, y \in A$ vrijedi:*

$$f(x +_A y) = f(x) +_B f(y)$$

$$f(x \cdot_A y) = f(x) \cdot_B f(y)$$

Ako je uz to f i bijekcija, onda za f kažemo da je ***izomorfizam*** *prstena $(A, +_A, \cdot_A)$ i $(B, +_B, \cdot_B)$.*

Propozicija 123. *Neka su $(A, +_A, \cdot_A)$ i $(B, +_B, \cdot_B)$ prsteni, te neka je $f : A \to B$ morfizam ovih prstena. Neka je 0_A nula u $(A, +_A, \cdot_A)$, te 0_B nula u $(B, +_B, \cdot_B)$. Tada je $f(0_A) = 0_B$.*

Dokaz. Označimo $y = f(0_A)$. Imamo $y = f(0_A) = f(0_A +_A 0_A) = f(0_A) +_B f(0_A) = y +_B y$. Dakle, $y = y +_B y$, tj. $y +_B 0_B = y +_B y$. Prema lemi 17. vrijedi $0_B = y$.

Time je tvrdnja propozicije dokazana. □

Propozicija 124. *Neka su $(A, +_A, \cdot_A)$ i $(B, +_B, \cdot_B)$ prsteni, te neka je $f : A \to B$ izomorfizam ovih prstena. Tada je $f^{-1} : B \to A$ izomorfizam prstena $(B, +_B, \cdot_B)$ i $(A, +_A, \cdot_A)$.*

Dokaz. Neka su $b_1, b_2 \in B$. Želimo dokazati da je $\underbrace{f^{-1}(b_1 +_B b_2) = f^{-1}(b_1) +_A f^{-1}(b_2)}_{\square}$.

Označimo $a = f^{-1}(b_1 +_B b_2)$ i $a' = f^{-1}(b_1) +_A f^{-1}(b_2)$. Da bismo dokazali da vrijedi (□), tj. $a = a'$, dovoljno je dokazati da je $f(a) = f(a')$ jer je f injekcija.

Imamo $f(a) = b_1 +_B b_2$ i $f(a') = f\left(f^{-1}(b_1)\right) +_B f\left(f^{-1}(b_2)\right)$. Dakle, $f(a) = f(a')$, pa vrijedi (□).

Posve analogno dobivamo da je $f^{-1}(b_1 \cdot_B b_2) = f^{-1}(b_1) \cdot_A f^{-1}(b_2)$.

Time je tvrdnja propozicije dokazana. □

Propozicija 125. *Neka su $(A, +_A, \cdot_A)$ i $(B, +_B, \cdot_B)$ prsteni, te neka je $f : A \to B$ izomorfizam ovih prstenova.*

1. *Pretpostavimo da je $(A, +_A, \cdot_A)$ komutativan prsten. Tada je $(B, +_B, \cdot_B)$ komutativan prsten.*

2. *Pretpostavimo da je 1_A jedinica u prstenu $(A, +_A, \cdot_A)$. Tada je $f(1_A)$ jedinica u prstenu $(B, +_B, \cdot_B)$.*

3. *Pretpostavimo da je $(A, +_A, \cdot_A)$ polje. Tada je $(B, +_B, \cdot_B)$ polje.*

Dokaz.

1. Neka su $b_1, b_2 \in B$. Tada postoje $a_1, a_2 \in A$ tako da je $f(a_1) = b_1$ i $f(a_2) = b_2$. Budući da je $(A, +_A, \cdot_A)$ komutativan prsten, vrijedi $a_1 \cdot_A a_2 = a_2 \cdot_A a_1$. Stoga je $f(a_1 \cdot_A a_2) = f(a_2 \cdot_A a_1)$, tj. $f(a_1) \cdot_B f(a_2) = f(a_2) \cdot_B f(a_1)$. Dakle, $b_1 \cdot_B b_2 = b_2 \cdot_B b_1$.

   Prema tome, $(B, +_B, \cdot_B)$ je komutativan prsten.

2. Želimo dokazati da je $f(1_A)$ neutralni element za operaciju $\cdot_B$. Neka je $b \in B$. Tada postoji $a \in A$ takav da je $f(a) = b$. Imamo $b \cdot_B f(1_A) = f(a) \cdot_B f(1_A) = f(a \cdot_A 1_A) = f(a) = b$. Dakle, $b \cdot_B f(1_A) = b$.

   Analogno dobivamo da je $f(1_A) \cdot_B b = b$. Time je tvrdnja 2. dokazana.

3. Prema tvrdnji 1. imamo da je $(B, +_B, \cdot_B)$ komutativan prsten. Nadalje, $(A, +_A, \cdot_A)$ je prsten s jedinicom, pa neka je 1_A jedinica u tom prstenu. Označimo $1_B = f(1_A)$. Prema tvrdnji 2., 1_B je jedinica u prstenu $(B, +_B, \cdot_B)$.

   Neka je 0_A nula u prstenu $(A, +_A, \cdot_A)$, te neka je 0_B nula u prstenu $(B, +_B, \cdot_B)$. Prema propoziciji 123. vrijedi $f(0_A) = 0_B$.

   Neka je $b \in B, b \neq 0_B$. Želimo dokazati da postoji $b' \in B$ takav da je $b \cdot_B b' = 1_B$ i $b' \cdot_B b = 1_B$ (zbog komutativnosti je dovoljno dokazati da vrijedi jedna od navedenih jednakosti, pa odaberimo prvu). Postoji $a \in A$ takav da je $f(a) = b$. Tada je $a \neq 0_A$, jer bi u suprotnom imali $f(a) = f(0_A) = 0_B$, što je nemoguće jer je $b \neq 0_B$.

   Budući da je $(A, +_A, \cdot_A)$ polje, postoji $a' \in A$ takav da je $a \cdot_A a' = 1_A$. Slijedi $f(a \cdot_A a') = f(1_A)$, tj. $f(a) \cdot_B f(a') = 1_B$. Ako definiramo $b' := f(a')$, onda imamo $b \cdot_B b' = 1_B$.

   Dakle, $(B, +_B, \cdot_B)$ je polje.

□

Propozicija 126. *Neka je $(A, +_A, \cdot_A)$ prsten, neka je B skup, te neka su $+_B$ i $\cdot_B$ binarne operacije na B. Pretpostavimo da je $f : A \to B$ bijekcija tako da za $\forall x, y \in A$ vrijedi:*

$$f(x +_A y) = f(x) +_B f(y) \tag{$\triangle$}$$

$$f(x \cdot_A y) = f(x) \cdot_B f(y) \tag{$\triangledown$}$$

Tada je $(B, +_B, \cdot_B)$ prsten (te je f izomorfizam prstena $(A, +_A, \cdot_A)$ i $(B, +_B, \cdot_B)$).

Dokaz. Neka su $b_1, b_2, b_3 \in B$. Tada postoje $a_1, a_2, a_3 \in A$ takvi da je $f(a_1) = b_1$, $f(a_2) = b_2$ i $f(a_3) = b_3$. Vrijedi $(a_1 +_A a_2) +_A a_3 = a_1 +_A (a_2 +_A a_3)$, pa je $f((a_1 +_A a_2) +_A a_3) = f(a_1 +_A (a_2 +_A a_3))$.

Iz ($\triangle$) slijedi $(b_1 +_B b_2) +_B b_3 = b_1 +_B (b_2 +_B b_3)$. Prema tome, $+_B$ je asocijativna binarna operacija.

Neka je 0_A nula u prstenu $(A, +_A, \cdot_A)$. Analogno dokazu propozicije 125. 2., dobije se da je $f(0_A)$ neutralni element za $+_B$. Analogno dokazu propozicije 125. 1. dobijemo da je $+_B$ komutativna operacija na B. Analogno dokazu propozicije 125. 3. dobijemo da za $\forall b \in B\ \exists b' \in B$ td. je $b +_B b' = f(0_A)$.

Stoga je $(B, +_B)$ Abelova grupa.

Dokaz da je $\cdot_B$ asocijativna binarna operacija je posve analogan dokazu da je $+_B$ asocijativna binarna operacija. Neka su $b_1, b_2, b_3 \in B$. Tada postoje $a_1, a_2, a_3 \in A$ takvi da je $f(a_1) = b_1$, $f(a_2) = b_2$ i $f(a_3) = b_3$. Vrijedi $a_1 \cdot_A (a_2 +_A a_3) = a_1 \cdot_A a_2 +_A a_1 \cdot_A a_3$. Koristeći ($\triangle$) i ($\triangledown$) dobijemo $b_1 \cdot_B (b_2 +_B b_3) = b_1 \cdot_B b_2 +_B b_1 \cdot_B b_3$.

Analogno dobijemo $(b_1 +_B b_2) \cdot_B b_3 = b_1 \cdot_B b_3 +_B b_2 \cdot_B b_3$.

Dakle, $(B, +_B, \cdot_B)$ je prsten. □

5.3 Kompleksni brojevi u $\mathbb{H}$

Definicija 127. *Definirajmo* $\mathbb{C}' = \{(x, y, 0, 0) \mid x, y \in \mathbb{R}\}$.

Propozicija 128. $\mathbb{C}'$ *je polje u* $(\mathbb{H}, +, \cdot)$.

Dokaz. Neka su $a, b \in \mathbb{C}'$. Tvrdimo da je $a + b \in \mathbb{C}'$ i $a \cdot b \in \mathbb{C}'$. Neka su $a_1, a_2, b_1, b_2 \in \mathbb{R}$ takvi da je $a = (a_1, a_2, 0, 0)$ i $b = (b_1, b_2, 0, 0)$.

Imamo $a + b = (a_1 + b_1, a_2 + b_2, 0, 0) \in \mathbb{C}'$, pa je $a + b \in \mathbb{C}'$. Nadalje,

$$\begin{aligned} a \cdot b &= (a_1 \cdot b_1 - a_2 \cdot b_2 - 0 \cdot 0 - 0 \cdot 0, a_2 \cdot b_1 + a_1 \cdot b_2 - 0 \cdot 0 + 0 \cdot 0, \\ &\quad 0 \cdot b_1 + 0 \cdot b_2 + a_1 \cdot 0 - a_2 \cdot 0, 0 \cdot b_1 - 0 \cdot b_2 + a_2 \cdot 0 + a_1 \cdot 0) \\ &= (a_1 \cdot b_1 - a_2 \cdot b_2, a_2 \cdot b_1 - a_1 \cdot b_2, 0, 0) \in \mathbb{C}' \end{aligned}$$

pa je $a \cdot b \in \mathbb{C}'$.

Definirajmo binarne operacije $+_{\mathbb{C}'}$ i $\cdot_{\mathbb{C}'}$ na $\mathbb{C}'$ za $\forall a, b \in \mathbb{C}'$ sa:

$$a +_{\mathbb{C}'} b = a + b$$

$$a \cdot_{\mathbb{C}'} b = a \cdot b$$

Tvrdimo da je $(\mathbb{C}', +_{\mathbb{C}'}, \cdot_{\mathbb{C}'})$ polje.

Definirajmo $f : \mathbb{C} \to \mathbb{C}'$ kao $f(x) = f((x_1, x_2)) = (x_1, x_2, 0, 0)$, za $x = (x_1, x_2) \in \mathbb{C}$.

Ako su $(x_1, x_2), (y_1, y_2) \in \mathbb{C}$ takvi da je $(x_1, x_2) \neq (y_1, y_2)$, onda je $x_1 \neq y_1$ ili $x_2 \neq y_2$, pa je očito $(x_1, x_2, 0, 0) \neq (y_1, y_2, 0, 0)$, tj. $f((x_1, x_2)) \neq f((y_1, y_2))$. Prema tome, f je injekcija.

Iz definicije od $\mathbb{C}'$ slijedi da je f surjekcija. Prema tome, f je bijekcija.

Neka su $x, y \in \mathbb{C}$ td. je $x = (x_1, x_2)$ i $y = (y_1, y_2)$ pri čemu su $x_1, x_2, y_1, y_2 \in \mathbb{R}$. Dokažimo:

$$f(x + y) = f(x) +_{\mathbb{C}'} f(y) \tag{$\ominus$}$$

$$f(x \cdot y) = f(x) \cdot_{\mathbb{C}'} f(y) \tag{$\oplus$}$$

Imamo:

$$\begin{aligned} f(x + y) &= f((x_1, x_2) + (y_1, y_2)) \\ &= f(x_1 + y_1, x_2 + y_2) \\ &= (x_1 + y_1, x_2 + y_2, 0, 0) \\ &= (x_1, x_2, 0, 0) + (y_1, y_2, 0, 0) \\ &= (x_1, x_2, 0, 0) +_{\mathbb{C}'} (y_1, y_2, 0, 0) \\ &= f(x) +_{\mathbb{C}'} f(y) \end{aligned}$$

Dakle, vrijedi ($\ominus$). Nadalje:

$$\begin{aligned} f(x \cdot y) &= f((x_1, x_2) \cdot (y_1, y_2)) \\ &= f(x_1y_1 - x_2y_2, x_1y_2 + x_2y_1) \\ &= (x_1y_1 - x_2y_2, x_1y_2 + x_2y_1, 0, 0) \end{aligned}$$

S druge strane:

$$\begin{aligned} f(x) \cdot_{\mathbb{C}'} f(y) &= (x_1, x_2, 0, 0) \cdot (y_1, y_2, 0, 0) \\ &= (x_1y_1 - x_2y_2 - 0 - 0, x_1y_2 + x_2y_1 - 0 + 0, 0 + 0 + 0 + 0, 0 - 0 + 0 + 0) \\ &= (x_1y_1 - x_2y_2, x_1y_2 + x_2y_1, 0, 0) \end{aligned}$$

Dakle, vrijedi ($\oplus$).

Iz činjenice da je f bijekcija, ($\ominus$), ($\oplus$) te propozicije 126., slijedi da je $(\mathbb{C}', +_{\mathbb{C}'}, \cdot_{\mathbb{C}'})$ prsten, a f izomorfizam prstenova $(\mathbb{C}, +, \cdot)$ i $(\mathbb{C}', +_{\mathbb{C}'}, \cdot_{\mathbb{C}'})$.

Iz propozicije 125.3. slijedi da je $(\mathbb{C}', +_{\mathbb{C}'}, \cdot_{\mathbb{C}'})$ polje. Time je tvrdnja propozicije dokazana. □

Poglavlje 6

Prsten hiperboličkih brojeva $\mathbb{D}$

6.1 Definicija i svojstva hiperboličkih brojeva

Definicija 129. *Definirajmo* $\mathbb{D} = \mathbb{R} \times \mathbb{R}$. *Neka su* $+_{\mathbb{D}}$ *i* $\cdot_{\mathbb{D}}$ *binarne operacije na* $\mathbb{D}$ *definirane sa:*

$$(x_1, x_2) +_{\mathbb{D}} (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$$
$$(x_1, x_2) \cdot_{\mathbb{D}} (y_1, y_2) = (x_1y_1 + x_2y_2, x_1y_2 + x_2y_1)$$

Također, definirajmo $0_{\mathbb{D}} = (0, 0)$ *i* $1_{\mathbb{D}} = (1, 0)$.

Teorem 130. $(\mathbb{D}, +_{\mathbb{D}}, \cdot_{\mathbb{D}})$ *je komutativan prsten s jedinicom. Nula u tom prstenu je* $0_{\mathbb{D}}$, *a jedinica je* $1_{\mathbb{D}}$.

Dokaz. Očito je $\mathbb{D} = \mathbb{C}$, $0_{\mathbb{D}} = 0_{\mathbb{C}}$ i $+_{\mathbb{D}} = +$, gdje je $+$ binarna operacija iz definicije 93. Prema propoziciji 94., $(\mathbb{C}, +, \cdot)$ je polje i $0_{\mathbb{C}}$ je nula u tom polju. Dakle, $(\mathbb{C}, +)$ je Abelova grupa i $0_{\mathbb{C}}$ je neutralni element za operaciju $+$. Prema tome, $(\mathbb{D}, +_{\mathbb{D}})$ je Abelova grupa, a $0_{\mathbb{D}}$ je neutralni element za operaciju $+_{\mathbb{D}}$.

Neka su $x, y, z \in \mathbb{D}$. Postoje $x_1, x_2, y_1, y_2, z_1, z_2 \in \mathbb{R}$ td. je $x = (x_1, x_2)$, $y = (y_1, y_2)$ i $z = (z_1, z_2)$. Tvrdimo da je $(x \cdot_{\mathbb{D}} y) \cdot_{\mathbb{D}} z = x \cdot_{\mathbb{D}} (y \cdot_{\mathbb{D}} z)$.

Imamo:

$$\begin{aligned}(x \cdot_{\mathbb{D}} y) \cdot_{\mathbb{D}} z &= (x_1y_1 + x_2y_2, x_1y_2 + x_2y_1) \cdot_{\mathbb{D}} (z_1, z_2) \\ &= ((x_1y_1 + x_2y_2)z_1 + (x_1y_2 + x_2y_1)z_2, (x_1y_1 + x_2y_2)z_2 + (x_1y_2 + x_2y_1)z_1)\end{aligned}$$

S druge strane:

$$\begin{aligned}x \cdot_{\mathbb{D}} (y \cdot_{\mathbb{D}} z) &= (x_1, x_2) \cdot_{\mathbb{D}} (y_1z_1 + y_2z_2, y_1z_2 + y_2z_1) \\ &= (x_1(y_1z_1 + y_2z_2) + x_2(y_1z_2 + y_2z_1), x_1(y_1z_2 + y_2z_1) + x_2(y_1z_1 + y_2z_2))\end{aligned}$$

Koristeći asocijativnost zbrajanja i množenja na $\mathbb{R}$, te distributivnost množenja u odnosu na zbrajanje na $\mathbb{R}$, zaključujemo da je $(x \cdot_{\mathbb{D}} y) \cdot_{\mathbb{D}} z = x \cdot_{\mathbb{D}} (y \cdot_{\mathbb{D}} z)$.

Prema tome, $(\mathbb{D}, \cdot_{\mathbb{D}})$ je polugrupa.

Neka su $x, y \in \mathbb{D}$. Postoje $x_1, x_2, y_1, y_2 \in \mathbb{R}$ td. $x = (x_1, x_2)$ i $y = (y_1, y_2)$. Tvrdimo da je $x \cdot_{\mathbb{D}} y = y \cdot_{\mathbb{D}} x$. Vrijedi:

$$\begin{aligned} x \cdot_{\mathbb{D}} y &= (x_1, x_2) \cdot_{\mathbb{D}} (y_1, y_2) \\ &= (x_1y_1 + x_2y_2, x_1y_2 + x_2y_1) \end{aligned}$$

Također vrijedi:

$$\begin{aligned} y \cdot_{\mathbb{D}} x &= (y_1, y_2) \cdot_{\mathbb{D}} (x_1, x_2) \\ &= (y_1x_1 + y_2x_2, y_1x_2 + y_2x_1) \end{aligned}$$

Dakle, vrijedi $x \cdot_{\mathbb{D}} y = y \cdot_{\mathbb{D}} x$.

Neka su $x, y, z \in \mathbb{D}$. Imamo $x = (x_1, x_2)$, $y = (y_1, y_2)$ i $z = (z_1, z_2)$, gdje su x_1, x_2, y_1, y_2, $z_1, z_2 \in \mathbb{R}$. Dokažimo da je $x \cdot_{\mathbb{D}} (y +_{\mathbb{D}} z) = x \cdot_{\mathbb{D}} y +_{\mathbb{D}} x \cdot_{\mathbb{D}} z$. Vrijedi:

$$\begin{aligned} x \cdot_{\mathbb{D}} (y +_{\mathbb{D}} z) &= (x_1, x_2) \cdot_{\mathbb{D}} (y_1 + z_1, y_2 + z_2) \\ &= (x_1(y_1 + z_1) + x_2(y_2 + z_2), x_1(y_2 + z_2) + x_2(y_1 + z_1)) \\ &= (x_1y_1 + x_1z_1 + x_2y_2 + x_2z_2, x_1y_2 + x_1z_2 + x_2y_1 + x_2z_1) \end{aligned}$$

S druge strane:

$$\begin{aligned} x \cdot_{\mathbb{D}} y +_{\mathbb{D}} x \cdot_{\mathbb{D}} z &= (x_1, x_2) \cdot_{\mathbb{D}} (y_1, y_2) +_{\mathbb{D}} (x_1, x_2) \cdot_{\mathbb{D}} (z_1, z_2) \\ &= (x_1y_1 + x_2y_2, x_1y_2 + x_2y_1) +_{\mathbb{D}} (x_1z_1 + x_2z_2, x_1z_2 + x_2z_1) \\ &= (x_1y_1 + x_2y_2 + x_1z_1 + x_2z_2, x_1y_2 + x_2y_1 + x_1z_2 + x_2z_1) \end{aligned}$$

Dakle, vrijedi $x \cdot_{\mathbb{D}} (y +_{\mathbb{D}} z) = x \cdot_{\mathbb{D}} y +_{\mathbb{D}} x \cdot_{\mathbb{D}} z$.

Budući da je $\cdot_{\mathbb{D}}$ komutativna binarna operacija, vrijedi i $(y +_{\mathbb{D}} z) \cdot_{\mathbb{D}} x = y \cdot_{\mathbb{D}} x +_{\mathbb{D}} z \cdot_{\mathbb{D}} x$. Slijedi, $(\mathbb{D}, +_{\mathbb{D}}, \cdot_{\mathbb{D}})$ je komutativan prsten.

Neka je $x \in \mathbb{D}$. Imamo $x = (x_1, x_2)$, gdje su $x_1, x_2 \in \mathbb{R}$. Vrijedi:

$$x \cdot_{\mathbb{D}} 1_{\mathbb{D}} = (x_1, x_2) \cdot_{\mathbb{D}} (1, 0) = (x_1 \cdot 1 + x_2 \cdot 0, x_1 \cdot 0 + x_2 \cdot 1) = (x_1, x_2) = x$$

Dakle, $x \cdot_{\mathbb{D}} 1_{\mathbb{D}} = x$. Zbog komutativnosti operacije $\cdot_{\mathbb{D}}$, vrijedi i $1_{\mathbb{D}} \cdot_{\mathbb{D}} x = x$.

Zaključujemo da je $(\mathbb{D}, +_{\mathbb{D}}, \cdot_{\mathbb{D}})$ komutativan prsten s jedinicom, pri čemu je $1_{\mathbb{D}}$ jedinica u tom prstenu. Time je tvrdnja teorema dokazana. □

Za $(\mathbb{D}, +_{\mathbb{D}}, \cdot_{\mathbb{D}})$ kažemo da je **prsten hiperboličkih brojeva**.

Lema 131. *Neka je $(P, +, \cdot)$ komutativan prsten, te neka su $x, y \in P$. Tada je $x^2 - y^2 = (x - y)(x + y)$.*

Dokaz. Imamo:

$$\begin{aligned}(x-y)(x+y) &= (x-y)\cdot x + (x-y)\cdot y \\ &\overset{\text{prop 46.}}{=} (x\cdot x - y\cdot x) + (x\cdot y - y\cdot y) \\ &= (x^2 + (-y\cdot x)) + (y\cdot x - y^2) \\ &= x^2 - y^2\end{aligned}$$

Dakle, tvrdnja vrijedi.

□

Propozicija 132. *Neka je $(P, +, \cdot)$ komutativan prsten s jedinicom. Pretpostavimo da postoji $x \in P$ takav da je $x \neq 1, x \neq -1$, te da je $x^2 = 1$. Tada $(P, +, \cdot)$ nije integralna domena.*

Dokaz. Iz $x^2 = 1$ slijedi $x^2 - 1 = 0$, tj. $x^2 - 1^2 = 0$. Iz leme 131. slijedi $(x - 1)(x + 1) = 0$.

Nadalje, iz $x \neq 1$ slijedi $x - 1 \neq 0$, a iz $x \neq -1$ slijedi $x + 1 \neq 0$. Stoga je jasno da $(P, +, \cdot)$ nije integralna domena. □

Definicija 133. *Definirajmo $j = (0, 1)$. Vrijedi:*

$$j^2 = j \cdot_{\mathbb{D}} j = (0,1) \cdot_{\mathbb{D}} (0,1) = (0\cdot 0 + 1\cdot 1, 0\cdot 1 + 1\cdot 0) = (1,0) = 1_{\mathbb{D}}$$

Uočimo:

Ako je $x \in \mathbb{D}$, $x = (x_1, x_2)$, onda je $-x = (-x_1, -x_2)$ u prstenu $(\mathbb{D}, +_{\mathbb{D}}, \cdot_{\mathbb{D}})$. Stoga je $-1_{\,D} = (-1, 0)$. Onda očito $j \neq 1_{\mathbb{D}}$ i $j \neq -1_{\mathbb{D}}$. Iz propozicije 132. slijedi da $(\mathbb{D}, +_{\mathbb{D}}, \cdot_{\mathbb{D}})$ nije integralna domena. Posebno, $(\mathbb{D}, +_{\mathbb{D}}, \cdot_{\mathbb{D}})$ nije polje.

Konkretno, neka je $u = (-1, 1)$ i $v = (1, 1)$. Očito je $u \neq 0_{\mathbb{D}}$ i $v \neq 0_{\mathbb{D}}$, a vrijedi:

$$u \cdot_{\mathbb{D}} v = (-1,1) \cdot_{\mathbb{D}} (1,1) = (-1+1, -1+1) = (0,0) = 0_{\mathbb{D}}$$

6.2 Realni brojevi u $\mathbb{H}$

Podsjetimo se definicije skupa: $\mathbb{R}' = \{(x, 0) \mid x \in \mathbb{R}\}$.

Propozicija 134. *$\mathbb{R}'$ je polje u $(\mathbb{D}, +_{\mathbb{D}}, \cdot_{\mathbb{D}})$.*

Dokaz. Neka su $x, y \in \mathbb{R}'$. Imamo $x = (x_1, 0)$ i $y = (y_1, 0)$, gdje su $x_1, y_1 \in \mathbb{R}$. Tvrdimo da je $x +_{\mathbb{D}} y \in \mathbb{R}'$ i $x \cdot_{\mathbb{D}} y \in \mathbb{R}'$.

Vrijedi:

$$x +_{\mathbb{D}} y = (x_1 + y_1, 0) \in \mathbb{R}'$$

i

$$x \cdot_{\mathbb{D}} y = (x_1, 0) \cdot_{\mathbb{D}} (y_1, 0) = (x_1 y_1 + 0, x_1 \cdot 0 + 0 \cdot y_1) = (x_1 y_1, 0) \in \mathbb{R}'$$

Definirajmo binarne operacije $+'$ i $\cdot'$ na $\mathbb{R}'$ sa:

$$x +' y = x +_{\mathbb{D}} y$$

$$x \cdot' y = x \cdot_{\mathbb{D}} y$$

Kako bi dokazali tvrdnju propozicije, dovoljno je dokazati da je $(\mathbb{R}', +', \cdot')$ polje.

Neka je $f : \mathbb{R} \to \mathbb{R}'$ td. $f(x) = (x, 0)$, za $\forall x \in \mathbb{R}$. Očito je f bijekcija. Neka su $x, y \in \mathbb{R}$. Imamo:

$$f(x + y) = (x + y, 0) = (x, 0) +' (y, 0) = f(x) +' f(y)$$

Dakle,

$$f(x + y) = f(x) +' f(y) \qquad (\therefore)$$

Nadalje,

$$f(x \cdot y) = (x \cdot y, 0) = (x, 0) \cdot' (y, 0) = f(x) \cdot' f(y)$$

Dakle,

$$f(x \cdot y) = f(x) \cdot' f(y) \qquad (\because)$$

Iz propozicije 126., $(\therefore)$, $(\because)$ i činjenice da je f bijekcija slijedi da je $(\mathbb{R}', +', \cdot')$ prsten, a f izomorfizam prstenova $(\mathbb{R}, +, \cdot)$ i $(\mathbb{R}', +', \cdot')$. Sada iz propozicije 125. 3. slijedi da je $(\mathbb{R}', +', \cdot')$ polje, čime smo dokazali tvrdnju propozicije. □

Napomena 135. *Za svaki $z \in \mathbb{D}$ postoje jedinstveni $a, b \in \mathbb{R}'$ tako da je $z = a +_{\mathbb{D}} b \cdot_{\mathbb{D}} j$.*

Do ove činjenice dolazimo analogno kao i u napomeni 108.

Bibliografija

[1] F. Catoni, D. Boccaletti, R. Cannata, V. Catoni, P. Zampetti, *Hyperbolic Numbers, Geometry of Minkowski Space–Time*, Springer, Berlin, Heidelberg, 2011.

[2] S. Mardešić, *Matematička analiza 1*, Školska knjiga, Zagreb, 1991.

[3] G. Sobczyk, *The Hyperbolic Number Plane*, dostupno na https://www.researchgate.net/publication/228559618_The_Hyperbolic_Number_Plane

Sažetak

U prvom smo poglavlju proučili općenito grupe i prstene, te smo definirali što je to potpuno uređeno polje. U drugom smo se poglavlju osvrnuli na prirodne, cijele i racionalne brojeve, te ih definirali unutar fiksiranog polja realnih brojeva. Zatim smo u trećem poglavlju proučili potprstene i potpolja. U četvrtom poglavlju smo definirali polje kompleksnih brojeva $\mathbb{C}$, nakon čega smo proučavali određeno potpolje od $\mathbb{C}$ izomorfno s $\mathbb{R}$. Pri kraju poglavlja smo definirali morfizam uređenih skupova. U petom poglavlju smo proučavali svojstva tijela kvaterniona $\mathbb{H}$, morfizme i izomorfizme prstenova. Također, razmotrili smo određeno polje u $\mathbb{H}$ koje je izomorfno sa $\mathbb{C}$. Na kraju rada, u šestom poglavlju smo definirali prsten hiperboličkih brojeva $\mathbb{D}$ i proučili određeno polje u $\mathbb{D}$ koje je izomorfno sa $\mathbb{R}$.

Summary

In the first chapter, we studied groups and rings in general, and defined what a totally ordered field is. In the second chapter, we looked at natural, integer, and rational numbers, and defined them within a fixed field of real numbers. Then, in the third chapter, we studied subrings and subfields. In the fourth chapter, we defined a field of complex numbers $\mathbb{C}$, after which we studied a certain subfield of $\mathbb{C}$ isomorphic to $\mathbb{R}$. At the end of the chapter, we defined morphism of ordered sets. In the fifth chapter, we studied the properties of a field of quaternions $\mathbb{H}$, morphisms, and ring isomorphisms. We also considered a particular field in $\mathbb{H}$ that is isomorphic to $\mathbb{C}$. At the end of the paper, in sixth chapter, we defined a ring of hyperbolic numbers $\mathbb{D}$ and studied a particular field in $\mathbb{D}$ that is isomorphic to $\mathbb{R}$.

Životopis

Rodih se u Zagrebu 29. travnja 1993. godine, a ostatak života živim u Kutini. Nakon završene osnovne škole Stjepana Kefelje u Kutini, upisujem matematičku gimnaziju Tina Ujevića, također u Kutini. Godine 2012. upisujem preddiplomski studij nastavničke matematike na PMF-u u Zagrebu, a 2017. godine upisujem diplomski studij nastavničke matematike na PMF-u u Zagrebu.