Aksiomi kompleksnih brojeva

Kralj, Lana

Master's thesis / Diplomski rad

2018

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:003509

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO–MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Lana Kralj

AKSIOMI KOMPLEKSNIH BROJEVA

Diplomski rad

Voditelj rada:
dr.sc. Zvonko Iljazović,
izvanredni profesor

Zagreb, rujan, 2018.

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. _____

Ovaj moj let kroz godine bio je predivan. Bilo je uspona, bilo je turbulencija a bilo je i padova. No svi putnici mog aviona bili su tu, svaki ispit i svaki moj uspon slavili a plakali sa mnom uz svaki moj pad. Ovaj diplomski rad stoga posvećujem svima njima. Prije svega mojoj obitelji, mom nepresušnom izvoru ljubavi i snage, bez kojih nikada ne bih dospjela tu, gdje sam sada. Zatim mojim prijateljima koji su uporno i neumorno gurali me naprijed i poticali da nikada ne odustanem. Veliko hvala mom profesoru, mentoru Zvonku Iljazoviću koji me tako strpljivo i pozitivno sve ove mjesece učio i naučio da sve što hoću, to i mogu. Najveće hvala Njemu što nikada nije dozvolio da se predam i padnem jer moj avion zbog Njega i dalje leti i ja se ničega ne bojim.

Sadržaj

Uvod

U ovom diplomskom radu proučavamo polje kompleksnih brojeva kao jednu apstraktnu algebarsku strukturu. U prvom poglavlju definirali smo neke osnovne pojmove kao što su binarne relacije i operacije te proučavali koncepte različitih algebarskih struktura. U drugom poglavlju definirali smo skupove prirodnih, cijelih i racionalnih brojeva kao podskupove jednog potpuno uređenog polja te proučavali neka zanimljiva svojstva operacija nad njima. Također smo definirali i potpolja. U trećem poglavlju definirali smo polje kompleksnih brojeva, zatim izomorfizam polja te smo promatrali proširenje polja realnih brojeva do polja kompleksnih brojeva.

Poglavlje 1

Uređeni prsteni

1.1 Binarne relacije i operacije

Neka je S skup te neka je $\sim$ podskup Kartezijevog produkta $S \times S$. Tada za $\sim$ kažemo da je **binarna relacija** na S. Ako je $\sim$ binarna relacija na skupu S te ako su $x, y \in S$ takvi da je $(x, y) \in \sim$ onda pišemo $x \sim y$, a ako su $x, y \in S$ takvi da $(x, y) \notin \sim$, onda pišemo $x \nsim y$. Npr. ako je S bilo koji skup te $\sim = S \times S$, onda je $\sim$ binarna relacija na S te za sve $x, y \in S$ vrijedi $x \sim y$. Ako je S bilo koji skup te $\sim = \emptyset$, onda je $\sim$ binarna relacija na S te za sve $x, y \in S$ vrijedi $x \nsim y$.

Neka je $\sim$ binarna relacija na skupu S. Kažemo da je $\sim$ **refleksivna relacija** na skupu S ako je

$$x \sim x$$

za svaki $x \in S$. Kažemo da je $\sim$ **antisimetrična relacija** na S ako za sve $x, y \in S$ vrijedi: $x \sim y$ i $y \sim x \Rightarrow x = y$.

Kažemo da je $\sim$ **tranzitivna relacija** na S ako za sve $x, y, z \in S$ vrijedi:$x \sim y$ i $y \sim z \Rightarrow x \sim z$. Kažemo da binarna relacija $\sim$ ima **svojstvo usporedivosti** na S ako za sve $x, y \in S$ vrijedi $x \sim y$ ili $y \sim x$. Za binarnu relaciju na skupu S koja je refleksivna, antisimetrična i tranzitivna te ima svojstvo usporedivosti kažemo da je **uređaj** na skupu S.

Primjer 1.1.1. *Neka je S skup svih podksupova od $\mathbb{R}$ te neka je $\sim$ binarna relacija na Sdefinirana sa*

$$A \sim B$$

ako je $A \subseteq B$. Za svaki skup A vrijedi $A \subseteq A$ pa je relacija $\sim$ refleksivna na S. Nadalje, ako su A i B skupovi takvi da je $A \subseteq B$ i $B \subseteq A$, onda je $A = B$, dakle relacija $\sim$ je antisimetrična.

Ako su A, B, C skupovi takvi da je $A \subseteq B$ i $B \subseteq C$, onda je $A \subseteq C$, što znači da je relacija $\sim$ tranzitivna. No, $\sim$ nije uređaj na S jer nema svojstvo usporedivosti.

Naime, za $A = \{1, 2, 3\}$ i $B = \{4, 5, 6\}$ vrijedi $A, B \in S$, no $A \nsim B$ i $B \nsim A$.

Neka je G skup te neka je $* : G \times G \to G$ funkcija. Tada za $*$ kažemo da je **binarna operacija** na skupu G. Ako je $*$ binarna operacija na skupu G onda ćemo za $x, y \in G$ umjesto $*(x, y)$ pisati i $x * y$. Za binarnu operaciju $*$ na skupu G kažemo da je **asocijativna** ako za sve $x, y, z \in G$ vrijedi

$$x * (y * z) = (x * y) * z.$$

Neka je $*$ binarna operacija na skupu G te neka je $e \in G$. Kažemo da je e **neutralni element** za $*$ ako za sve $x \in G$ vrijedi

$$x * e = x$$

i

$$e * x = x.$$

Uočimo sljedeće: neutralni element, ako postoji, je jedinstven. Naime, pretpostavimo da su e i f neutralni elementi za $*$. Tada za svaki $x \in G$ vrijedi $e * x = x$ pa posebno za $x = f$ dobivamo $e * f = f$. Nadalje, za svaki $x \in G$ vrijedi $x * f = x$ pa posebno za $x = e$ dobivamo $e * f = e$. Dakle

$$e * f = f$$

i

$$e * f = e$$

pa je $e = f$.

Ako je $*$ binarna operacija na skupu G takva da je $*$ asocijativna te da ima neutralni element, onda za uređeni par $(G, *)$ kažemo da je **monoid**. Ako je $(G, *)$ monoid onda ćemo sa e označavati neutralni element za $*$. Neka je $(G, *)$ monoid te $x \in G$. Za $y \in G$ kažemo da je inverzni element od x u $(G, *)$ ako vrijedi $x * y = e$ i $y * x = e$.

Propozicija 1.1.2. *Neka je $(G, *)$ monoid te neka je $x \in G$. Pretpostavimo da su $y, z \in G$ inverzni elementi od x u $(G, *)$. Tada je $y = z$.*

Dokaz. Po definiciji inverznog elementa znamo da vrijedi $x * y = e$. Iz ovoga slijedi

$$z * (x * y) = z * e.$$

Primjenom asocijativnosti i definicije neutralnog elementa dobivamo

$$(z * x) * y = z.$$

Kako je z inverzni element od x vrijedi da je $z * x = e$. Stoga je $e * y = z$, tj. $y = z$. □

1.2 Grupe i prsteni

Za monoid $(G, *)$ u kojem svaki element ima inverzni element kažemo da je **grupa**. Za binarnu operaciju $*$ na skupu G kažemo da je komutativna ako za sve $x, y \in G$ vrijedi

$$x * y = y * x.$$

Ako je $(G, *)$ grupa takva da je binarna operacija $*$ komutativna, onda za $(G, *)$ kažemo da je **komutativna (Abelova) grupa**.

Neka je P skup te neka su $+$ i $\cdot$ binarne operacije na P takve da vrijedi sljedeće:

1) $(P, +)$ je Abelova grupa;

2) $\cdot$ je asocijativna operacija na P;

3) za sve $x, y, z \in P$ vrijedi:

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

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

Tada za $(P, +, \cdot)$ kažemo da je **prsten**. (Pri tome u gornjim jednakostima koristimo standardni dogovor da $\cdot$ ima veći prioritet od $+$, tj. $x \cdot y + x \cdot z$ zapravo znači $(x \cdot y) + (x \cdot z)$.) Ako je $(P, +, \cdot)$ prsten takav da je binarna operacija $\cdot$ komutativna onda za $(P, +, \cdot)$ kažemo da je **komutativan prsten**. Ako je $(P, +, \cdot)$ prsten onda neutralni element za operaciju $+$ obično označavamo sa 0. Nadalje, za $x \in P$ inverzni element od x u $(P, +)$ označavamo s $-x$. Dakle, za svaki $x \in P$ vrijedi $x + (-x) = 0$ i $(-x) + x = 0$.

Propozicija 1.2.1. *Neka je $(P, +, \cdot)$ prsten. Tada za svaki $x \in P$ vrijedi $0 \cdot x = 0$ i $x \cdot 0 = 0$.*

Dokaz. Neka je $x \in P$. Tada je

$$0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x.$$

Uvedimo oznaku $z = 0 \cdot x$. Imamo da je $z = z + z$. Slijedi $z + (-z) = (z + z) + (-z)$ pa koristeći asocijativnost operacije $+$ dobivamo da je $0 = z$. Prema tome $0 \cdot x = 0$. Analogno dobivamo da je $x \cdot 0 = 0$. □

Ako je $(P, +, \cdot)$ prsten takav da postoji neutralni element za operaciju $\cdot$, onda kažemo da je $(P, +, \cdot)$ **prsten s jedinicom**. U tom slučaju neutralni element za operaciju $\cdot$ označavamo sa 1. Za komutativan prsten s jedinicom $(P, +, \cdot)$ kažemo da je **polje** ako je $0 \neq 1$ te ako za svaki $x \in P$ takav da je $x \neq 0$ postoji inverzni element od x u $(P, \cdot)$(tj. postoji $y \in P$ takav da je $x \cdot y = 1$). U tom slučaju za $x \in P$, $x \neq 0$, inverzni element od x u $(P, \cdot)$ označavamo s x^{-1}. Za prsten $(P, +, \cdot)$ kažemo da je **integralna domena** ako za sve $x, y \in P$ takve da je $x \neq 0$ i $y \neq 0$ vrijedi $x \cdot y \neq 0$.

Propozicija 1.2.2. *Neka je $(P, +, \cdot)$ polje. Tada je $(P, +, \cdot)$ integralna domena.*

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

$$x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0$$

pa koristeći asocijativnost operacije $\cdot$ i propoziciju 1.2.1 dobivamo

$$(x^{-1} \cdot x) \cdot y = 0.$$

No, $x^{-1} \cdot x = 1$ pa je $1 \cdot y = 0$, tj $y = 0$, što je u kontradikciji s pretpostavkom da je $y \neq 0$. Prema tome, $x \cdot y \neq 0$. Time je tvrdnja propozicije dokazana. □

Neka je $(P, +, \cdot)$ prsten te neka je $\leq$ uređaj na P takav da vrijedi sljedeće:

1) ako su $x, y \in P$ takvi da je $x \leq y$ onda za svaki $z \in P$ vrijedi $x + z \leq y + z$;

2) ako su $x, y \in P$ takvi da je $0 \leq x$ i $0 \leq y$ onda je $0 \leq x \cdot y$.

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

Propozicija 1.2.3. *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) $(-x) \cdot (-y) = x \cdot y$ *(pri tome $-x \cdot y$ znači $-(x \cdot y)$).*

Dokaz. Imamo, koristeći propoziciju 1.2.1

$$x \cdot (-y) + x \cdot y = x \cdot (-y + y) = x \cdot 0 = 0,$$

tj.

$$x \cdot (-y) + x \cdot y = 0$$

pa kada lijevoj i desnoj strani jednakosti "dodamo" $-x \cdot y$ dobivamo

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

Analogno dobivamo $(-x) \cdot y = -x \cdot y$. Koristeći upravo dokazane tvrdnje dobivamo

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

dakle

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

Ovdje smo koristili da za svaki $z \in P$ vrijedi $-(-z) = z$. Naime, to je posljedica sljedećeg: ako je y inverzni element od x u nekom monoidu onda je x inverzni element od y (u istom monoidu). □

Ako je $(P, +, \cdot)$ prsten onda ćemo za $x, y \in P$ umjesto $x + (-y)$ pisati i $x - y$.

Napomena 1.2.4. *Neka je $(P, +, \cdot)$ prsten te neka su $x, y, z \in P$. Tada je*

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

Naime, koristeći propoziciju 1.2.3 , dobivamo

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

Analogno dobivamo,

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

Propozicija 1.2.5. *Neka je $(P, +, \cdot, \leq)$ uređeni prsten. Neka su $x, y, z \in P$ takvi da je $x \leq y$ te $0 \leq z$. Tada je*

$$zx \leq zy$$

i

$$xz \leq yz.$$

Dokaz. Iz $x \leq y$ i definicije uređenog prstena slijedi

$$x + (-x) \leq y + (-x),$$

tj. $0 \leq y - x$. Iz ovoga te $0 \leq z$ i definicije uređenog prstena slijedi $0 \leq (y - x) \cdot z$. Iz ovoga i napomene, slijedi

$$0 \leq y \cdot z - x \cdot z.$$

Zbrajajući lijevoj i desnoj strani ove nejednakosti xz, dobivamo $xz \leq yz$. Analogno dobivamo $zx \leq zy$. □

Neka je $(P, +, \cdot, \leq)$ uređeni prsten. Kažemo da je $(P, +, \cdot, \leq)$ **uređeno polje** ako je $(P, +, \cdot)$ polje.

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

Neka je $(S, \leq)$ uređen skup sa sljedećim svojstvom: Ako su A i B neprazni podskupovi od S takvi da za svaki $x \in A$ i za svaki $y \in B$ vrijedi $x \leq y$, onda postoji $z \in S$ takav da je $x \leq z$ i $z \leq y$, za svaki $x \in A$ i za svaki $y \in B$. Tada za $(S, \leq)$ kažemo da je **potpuno uređen skup**.

Za uređeno polje $(P, +, \cdot, \leq)$ kažemo da je potpuno uređeno polje ako je $(P, \leq)$ potpuno uređen skup. Za potpuno uređeno polje kažemo još i da je **polje realnih brojeva**.

Propozicija 1.2.6. *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 ne vrijedi $0 \leq 1$. Tada je $1 \leq 0$. Slijedi $1 + (-1) \leq 0 + (-1)$, tj $0 \leq -1$. Prema svojstvu (2) iz definicije uređenog prstena vrijedi

$$0 \leq (-1) \cdot (-1),$$

no

$$(-1) \cdot (-1) = 1 \cdot 1 = 1$$

prema propoziciji 1.2.3, pa je $0 \leq 1$, kontradikcija. Prema tome,

$$0 \leq 1.$$

□

Neka je $(S, \leq)$ uređen skup. Za $x, y \in S$ pišemo $x < y$ ako je $x \leq y$ i $x \neq y$. Nadalje, pišemo $x \not\leq y$ ako ne vrijedi $x \leq y$. Pišemo $x \not< y$, ako ne vrijedi $x < y$.

Propozicija 1.2.7. *Neka je $(S, \leq)$ uređen skup. Neka su $x, y, z \in S$.*

1) Ako je $x < y$ i $y \leq z$, onda je $x < z$.

2) Ako je $x \leq y$ i $y < z$, onda je $x < z$.

3) Ako je $x < y$ i $y < z$, onda je $x < z$.

4) $x \not< y \Leftrightarrow y \leq x$

5) $x \not\leq y \Leftrightarrow y < x$

6) Ako je $x \neq y$*, onda je* $x < y$ *ili je* $y < x$*.*

7) $x \not< x$

Dokaz. 1) Iz $x < y$ slijedi $x \leq y$. Ovo zajedno sa $y \leq z$ daje $x \leq z$. Pretpostavimo da je $x = z$. Stoga je $y \leq x$ (jer je $y \leq z$) pa zbog $x \leq y$ imamo $x = y$. Ovo je u kontradikciji s $x < y$. Prema tome $x \neq z$. Zaključak: $x < z$.

2) Iz $y < z$ slijedi $y \leq z$, što zajedno sa $x \leq y$ povlači $x \leq z$. Pretpostavimo da je $x = z$. Tada je $x \leq y$ i $y < x$ pa iz antisimetričnosti relacije $\leq$ slijedi $x = y$ što je u kontradikciji s $y < x$. Prema tome $x \neq z$ pa zaključujemo da je $x < z$.

3) Iz $y < z$ slijedi $y \leq z$. Dakle, $x < y$ i $y \leq z$, pa prema 1) vrijedi $x < z$.

4) Pretpostavimo da $x \not< y$. Želimo dokazati da je $y \leq x$. Pretpostavimo suprotno. Znamo da je $x \leq y$ ili $y \leq x$ pa zaključujemo da je $x \leq y$. Iz $x \not< y$ slijedi $x = y$ pa posebno vrijedi $y \leq x$, a to je u kontradikciji s pretpostavkom da $y \not\leq x$. Prema tome $y \leq x$.

   Uzmimo sada da je $y \leq x$. Želimo dokazati da $x \not< y$. Pretpostavimo suprotno, tj da je $x < y$. Iz $x < y$ i $y \leq x$ i antisimetričnosti relacije $\leq$ slijedi $x = y$ što je u kontradikciji s $x < y$. Prema tome $x \not< y$.

5) Pretpostavimo da $x \not\leq y$. Znamo da je $x \leq y$ ili $y \leq x$ pa zaključujemo da je $y \leq x$. Kada bi vrijedilo $y = x$ onda bismo imali $x \leq y$ što je u kontradikciji s pretpostavkom. Prema tome $y \neq x$ pa je $y < x$.

   Uzmimo sada da je $y < x$. Želimo dokazati da $x \not\leq y$. Pretpostavimo suprotno, tj da je $x \leq y$. Iz ovoga i $y < x$ kao i maloprije dolazimo do kontradikcije. Prema tome $x \not\leq y$.

6) Pretpostavimo da je $x \neq y$. Znamo da je $x \leq y$ ili $y \leq x$. U prvom slučaju $(x \leq y)$ vrijedi $x < y$ a u drugom $y < x$.

7) Ovo je očito.

□

Napomena 1.2.8. *Neka je* $(P, +, \cdot, \leq)$ *uređeno polje. Znamo da je tada* $0 \neq 1$*, a prema propoziciji 1.2.6 vrijedi* $0 \leq 1$*. Stoga je* $0 < 1$*.*

Propozicija 1.2.9. *Neka je* $(P, +, \cdot, \leq)$ *uređeni prsten.*

1) Neka su $x, y, z \in P$ *takvi da je* $x < y$*. Tada je* $x + z < y + z$*.*

2) Pretpostavimo da je $(P, +, \cdot)$ integralna domena te da su $x, y \in P$ takvi da $0 < x$ i $0 < y$. Tada je $0 < x \cdot y$.

Dokaz. 1) Iz $x < y$ slijedi $x \leq y$ pa je

$$x + z \leq y + z.$$

Pretpostavimo da je $x + z = y + z$. Tada je

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

pa je $x = y$. Ovo je u kontradikciji s pretpostavkom da je $x < y$. Prema tome

$$x + z \neq y + z$$

pa zaključujemo da je $x + z < y + z$.

2) Iz $0 < x$ slijedi $0 \leq x$ i $0 \neq x$. Iz $0 < y$ slijedi $0 \leq y$ i $0 \neq y$. Iz definicije uređenog prstena slijedi $0 \leq x \cdot y$. Iz definicije integralne domene slijedi $0 \neq x \cdot y$. Prema tome, $0 < x \cdot y$.

□

Napomena 1.2.10. *Neka je $(P, +, \cdot)$ polje te neka su $x, y \in P$, $x \neq 0, y \neq 0$. Tada je $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$. Naime, vrijedi,*

$$(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = ((x \cdot y) \cdot y^{-1}) \cdot x^{-1} = (x \cdot (y \cdot y^{-1})) \cdot x^{-1} = (x \cdot 1) \cdot x^{-1} = x \cdot x^{-1} = 1.$$

Dakle, $(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = 1$ pa množenjem ove jednakosti sa $(x \cdot y)^{-1}$ dobivamo

$$y^{-1} \cdot x^{-1} = (x \cdot y)^{-1}.$$

Nadalje ako su $x, y \in P$ onda na analogan način dobivamo $-(x + y) = -x + (-y)$.

Propozicija 1.2.11. *Neka je $(P, +, \cdot, \leq)$ uređeni prsten takav da je $(P, +, \cdot)$ integralna domena. Neka su $x, y, z \in P$ takvi da je $x < y$ i $0 < z$. Tada je*

$$x \cdot z < y \cdot z$$

i

$$z \cdot x < z \cdot y.$$

Dokaz. Iz propozicije 2.4.2 slijedi

$$x \cdot z \leq y \cdot z.$$

Pretpostavimo da je $x \cdot z = y \cdot z$. Tada je $0 = yz - xz$ pa iz napomene 1.2.4 slijedi $0 = (y - x) \cdot z$. Iz $0 < z$ slijedi $z \neq 0$, a iz $x < y$ slijedi $0 < y - x$ pa je $y - x \neq 0$. Ovo je u kontradikciji s činjenicom da je $0 = (y - x) \cdot z$ te da je $(P, +, \cdot)$ integralna domena. Zaključujemo da je

$$xz < yz.$$

Analogno dobivamo da je

$$zx < zy.$$

□

Propozicija 1.2.12. *Neka je $(P, +, \cdot, \leq)$ uređeni prsten. Neka su $x, y \in P$.*

1) ako je $0 \leq x$ i $y \leq 0$ onda $xy \leq 0$

2) ako je $x \leq 0$ i $0 \leq y$ onda je $xy \leq 0$

3) ako je $x \leq 0$ i $y \leq 0$ onda je $0 \leq xy$

Dokaz. 1. Pretpostavimo da je $0 \leq x$ i $y \leq 0$. Iz definicije uređenog prstena i $y \leq 0$ slijedi

$$y + (-y) \leq 0 + (-y),$$

tj. $0 \leq -y$. Iz definicije uređenog prstena sada zaključujemo da je $0 \leq x \cdot (-y)$. Iz propozicije 1.2.1 (1) slijedi $0 \leq -(x \cdot y)$ pa zaključujemo da je

$$x \cdot y \leq 0.$$

2. Ovu tvrdnju dokazujemo posve analogno kao tvrdnju (1.)

3. Pretpostavimo da je $x \leq 0$ i $y \leq 0$. Tada je

$$0 \leq -x$$

i

$$0 \leq -y$$

pa je

$$0 \leq (-x) \cdot (-y),$$

a ovo zajedno s propozicijom 1.2.1 daje

$$0 \leq x \cdot y.$$

□

Propozicija 1.2.13. *Neka je $(P, +, \cdot, \leq)$ uređeni prsten pri čemu je $(P, +, \cdot)$ integralna domena. Neka su $x, y \in P$.*

1) ako je $0 < x$ i $y < 0$ onda je $xy < 0$

2) ako je $x < 0$ i $0 < y$ onda je $xy < 0$

3) ako je $x < 0$ i $y < 0$ onda je $0 < xy$

Dokaz. 1) Pretpostavimo da je $0 < x$ i $y < 0$. Tada je $x \cdot y \leq 0$ prema propoziciji 1.2.12 te je $x \cdot y \neq 0$ prema definiciji integralne domene. Dakle, $x \cdot y < 0$. Tvrdnje 2) i 3) se dokazuju posve analogno.

□

Propozicija 1.2.14. *Neka je $(P, +, \cdot, \leq)$ uređeno polje. Neka je $x \in P$.*

1.) ako je $0 < x$ onda je $0 < x^{-1}$

2.) ako je $x < 0$ onda je $x^{-1} < 0$

Dokaz. Uočimo sljedeće: ako je $x \neq 0$, onda je $x^{-1} \neq 0$. Naime, u slučaju da je $x^{-1} = 0$, imamo

$$1 = x \cdot x^{-1} = x \cdot 0 = 0,$$

dakle $1 = 0$ što je nemoguće.

1.) Pretpostavimo da je $0 < x$. Tada je $x^{-1} \neq 0$. Stoga je $0 < x^{-1}$ ili $x^{-1} < 0$. Pretpostavimo da je $x^{-1} < 0$. Prema propoziciji 1.2.13 (1) imamo

$$x^{-1} \cdot x < 0, \text{ tj. } 1 < 0,$$

što je u kontradikciji s napomenom 1.2.9. Prema tome, $0 < x^{-1}$.

2.) Ovu tvrdnju dokazujemo analogno.

□

Poglavlje 2

Potpuno uređena polja

Neka je $(\mathbb{R}, +, \cdot, \leq)$ jedno fiksirano polje realnih brojeva.

2.1 Skup prirodnih brojeva

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. Definirajmo

$$\mathbb{N} = \{x \in \mathbb{R} \mid x \in S, \text{ za svaki induktivan skup } S\}.$$

Imamo $1 \in \mathbb{N}$ (jer je $1 \in S$ za svaki induktivan skup S). Ako je $x \in \mathbb{N}$, onda je $x \in S$, za svaki induktivan skup S pa je $x + 1 \in S$, za svaki induktivan skup S, prema tome $x + 1 \in \mathbb{N}$. Zaključak: $\mathbb{N}$ je induktivan skup.

Napomena 2.1.1. *Ako je S induktivan skup, onda za svaki $x \in \mathbb{N}$, prema definiciji od $\mathbb{N}$, vrijedi $x \in S$. Prema tome, $\mathbb{N} \subseteq S$, za svaki induktivan skup S.*

Propozicija 2.1.2 (**princip indukcije**)**.** *Neka je $S \subseteq \mathbb{N}$ takav da vrijedi sljedeće:*

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 prema napomeni $\mathbb{N} \subseteq S$. No, prema pretpostavci propozicije vrijedi $S \subseteq \mathbb{N}$ pa slijedi $S = \mathbb{N}$. □

Propozicija 2.1.3. *Za svaki $x \in \mathbb{N}$ vrijedi $1 \leq x$.*

Dokaz. Neka je

$$S = \{x \in \mathbb{N} \mid 1 \leq x\}.$$

Očito je $S \subseteq \mathbb{N}$. Nadalje, očito je $1 \in S$. Pretpostavimo da je $x \in S$. Iz $0 \leq 1$ slijedi $x + 0 \leq x + 1$, tj $x \leq x + 1$. Iz $x \in S$ slijedi $x \in \mathbb{N}$ i $1 \leq x$. Stoga je

$$1 \leq x + 1$$

i

$$x + 1 \in \mathbb{N}.$$

Prema tome $x + 1 \in S$. Dakle, za svaki $x \in S$ vrijedi $x + 1 \in S$. Prema propoziciji 2.1.2 slijedi $S = \mathbb{N}$. To znači da za svaki $x \in \mathbb{N}$ vrijedi $1 \leq x$. □

Napomena 2.1.4. *Vrijedi $0 < 1$ pa iz propozicije 2.1.3 i propozicije 1.2.7 slijedi $0 < x$, za svaki $x \in \mathbb{N}$. Posebno, $0 \notin \mathbb{N}$.*

Propozicija 2.1.5. *1) Za svaki $x \in \mathbb{R}, x \neq 0$ vrijedi $\frac{x}{x} = 1$*

1') Za svaki $x \in \mathbb{R}$ vrijedi $\frac{x}{1} = x$

2) Neka su $x, y, k \in \mathbb{R}, y \neq 0, k \neq 0$. Tada je $\frac{x}{y} = \frac{k \cdot x}{k \cdot y}$

3) Neka su $a, b, c, d \in \mathbb{R}, b \neq 0, d \neq 0$. Tada je $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$.

4) Neka su $x, y, z \in \mathbb{R}, z \neq 0$. Tada je $\frac{x}{z} + \frac{y}{z} = \frac{x+y}{z}$.

5) Neka su $a, b, c, d \in \mathbb{R}, b \neq 0, d \neq 0$. Tada je $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$.

6) Neka su $x, y \in \mathbb{R}, x \neq 0, y \neq 0$. Tada je $(\frac{x}{y})^{-1} = \frac{y}{x}$.

Dokaz. 1) Neka je $x \in \mathbb{R}, x \neq 0$. Vrijedi $\frac{x}{x} = x \cdot x^{-1} = 1$.

1') Očito vrijedi.

3) Koristeći napomenu 1.2.10 dobivamo:

$$\frac{a \cdot c}{b \cdot d} = (a \cdot c) \cdot (b \cdot d)^{-1} = (a \cdot c) \cdot (b^{-1} \cdot d^{-1}) = (a \cdot b^{-1}) \cdot (c \cdot d^{-1}) = \frac{a}{b} \cdot \frac{c}{d}.$$

2) Koristeći 3) i 1) dobivamo:

$$\frac{k \cdot x}{k \cdot y} = \frac{k}{k} \cdot \frac{x}{y} = 1 \cdot \frac{x}{y} = \frac{x}{y}.$$

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

5) Koristeći 2) i 4) dobivamo:

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d}{b \cdot d} + \frac{c \cdot b}{b \cdot d} = \frac{ad + bc}{bd}.$$

6) Ovo slijedi iz napomene 1.2.10.

□

Propozicija 2.1.6. *Za sve $x, y \in \mathbb{N}$ vrijedi $x + y \in \mathbb{N}$.*

Dokaz. Neka je $x \in \mathbb{N}$ fiksan. Definirajmo skup

$$S = \{y \in \mathbb{N} \mid x + y \in \mathbb{N}\}.$$

Imamo $1 \in \mathbb{N}$ i $x + 1 \in \mathbb{N}$ pa je $1 \in S$. Pretpostavimo da je $y \in S$. Tada je

$$y \in \mathbb{N}$$

i

$$x + y \in \mathbb{N}.$$

Slijedi $y + 1 \in \mathbb{N}$ te

$$x + (y + 1) = (x + y) + 1 \in \mathbb{N}.$$

Stoga je $y + 1 \in S$. Očito je $S \subseteq \mathbb{N}$ pa prema principu indukcije vrijedi

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

To znači da za svaki $y \in \mathbb{N}$ vrijedi

$$x + y \in \mathbb{N}.$$

Time je tvrdnja propozicije dokazana. □

Propozicija 2.1.7. *Za sve $x, y \in \mathbb{N}$ vrijedi $x \cdot y \in \mathbb{N}$.*

Dokaz. Neka je $x \in \mathbb{N}$ fiksan. Definirajmo skup

$$S = \{y \in \mathbb{N} \mid x \cdot y \in \mathbb{N}\}.$$

Imamo $1 \in \mathbb{N}$ i $x \cdot 1 = x \in \mathbb{N}$ pa je $1 \in S$. Pretpostavimo da je $y \in S$. Tada je $y \in \mathbb{N}$ i $x \cdot y \in \mathbb{N}$. Imamo

$$y + 1 \in \mathbb{N}$$

i

$$x \cdot (y + 1) = x \cdot y + x \cdot 1 = x \cdot y + x \in \mathbb{N}.$$

(ovdje smo koristili prethodnu propoziciju). Dakle,

$$x \cdot (y + 1) \in \mathbb{N}$$

pa slijedi da je $y + 1 \in S$. Prema principu indukcije vrijedi $S = \mathbb{N}$. To znači da za svaki $y \in \mathbb{N}$ vrijedi

$$x \cdot y \in \mathbb{N}.$$

□

Propozicija 2.1.8. *Vrijedi* $\mathbb{N} = \{1\} \cup \{x + 1 \mid x \in \mathbb{N}\}$.

Dokaz. Označimo

$$S = \{1\} \cup \{x + 1 \mid x \in \mathbb{N}\}.$$

Očito je $S \subseteq \mathbb{N}$ i $1 \in S$. Neka je $x \in S$. Tada je $x \in \mathbb{N}$ pa je $x + 1 \in S$. Prema principu indukcije vrijedi $S = \mathbb{N}$. Time je tvrdnja propozicije dokazana. □

Definirajmo $2 = 1 + 1$.

Korolar 2.1.9. *Neka je* $y \in \mathbb{N}$ *takav da je* $1 \neq y$. *Tada je* $2 \leq y$.

Dokaz. Prema prethodnoj propoziciji imamo $y = x + 1$ za neki $x \in \mathbb{N}$. Prema propoziciji 1.2.9 vrijedi $1 \leq x$. Slijedi

$$1 + 1 \leq x + 1,$$

tj. $2 \leq y$. □

Lema 2.1.10. *Ako je* $x \in \mathbb{N}$ *onda ne postoji* $y \in \mathbb{N}$ *takav da je* $x < y < x + 1$.

Dokaz. Neka je

$$S = \{x \in \mathbb{N} \mid \nexists y \in \mathbb{N} \text{ takav da } x < y < x + 1\}.$$

Pretpostavimo da postoji $y \in \mathbb{N}$ takav da $1 < y < 2$. Iz $1 < y$ slijedi $1 \neq y$ pa iz korolara slijedi $2 \leq y$, što je u kontradikciji s $y < 2$. Prema tome ne postoji $y \in \mathbb{N}$ takav da $1 < y < 2$ pa zaključujemo da je $1 \in S$. Pretpostavimo da je $x \in S$. Želimo dokazati da je

$$x + 1 \in S.$$

Očito je

$$x + 1 \in \mathbb{N}.$$

Pretpostavimo da postoji $y \in \mathbb{N}$ takav da je

$$x + 1 < y < (x + 1) + 1.$$

Kad bi vrijedilo $y = 1$, tada bismo imali $x + 1 < 1$ pa bi iz propozicije 1.2.9 slijedilo

$$x + 1 + (-1) < 1 + (-1),$$

tj $x < 0$, a ovo bi zajedno sa $0 < 1$ povlačilo da je $x < 1$ a to je u kontradikciji s propozicijom 2.1.3. Dakle, $y \neq 1$ pa iz propozicije 2.1.7 slijedi $y = z + 1$, za neki $z \in \mathbb{N}$. Stoga je

$$x + 1 < z + 1 < (x + 1) + 1$$

pa iz propozicije 1.2.9 dodavanjem (-1) slijedi

$$x < z < x + 1.$$

Ovo je u kontradikciji s činjenicom da je $x \in S$. Prema tome ne postoji $y \in \mathbb{N}$ takav da

$$x + 1 < y < (x + 1) + 1.$$

To znači da je $x + 1 \in S$. Prema principu indukcije

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

Time je tvrdnja leme dokazana. □

Lema 2.1.11. *Neka su $x, y \in \mathbb{N}$ takvi da je $x < y$. Tada je $x + 1 \leq y$.*

Dokaz. Pretpostavimo suprotno. Prema propoziciji 1.2.7 vrijedi $y < x + 1$. Ovo je zajedno s $x < y$ u kontradikciji s lemom 2.1.10. Prema tome vrijedi $x + 1 \leq y$. □

Lema 2.1.12. *Neka je $y \in \mathbb{N}$. Tada je*

$$\{x \in \mathbb{N} \mid x \leq y\} \cup \{y + k \mid k \in \mathbb{N}\} = \mathbb{N}.$$

Dokaz. Označimo

$$S = \{x \in \mathbb{N} \mid x \leq y\} \cup \{y + k \mid k \in \mathbb{N}\}.$$

Očito je $S \subseteq \mathbb{N}$. Iz $1 \leq y$ (propozicija 2.1.3) slijedi $1 \in S$. Pretpostavimo da je $x \in S$. Želimo pokazati da je

$$x + 1 \in S.$$

Imamo dva slučaja:

1) $x \in \mathbb{N}$ i $x \leq y$. Vrijedi $x = y$ ili $x < y$. Ako je

$$x = y$$

onda je

$$x + 1 = y + 1$$

pa je $x + 1 \in S$. Ako je

$$x < y,$$

tada iz leme slijedi

$$x + 1 \leq y,$$

tj $x + 1 \in S$.

2) $x = y + k$, za neki $k \in \mathbb{N}$. Sada je

$$x + 1 = (y + k) + 1 = y + (k + 1)$$

pa je $x + 1 \in S$.

U oba slučaja vrijedi $x + 1 \in S$. Prema principu indukcije imamo

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

Time je tvrdnja leme dokazana. □

Teorem 2.1.13. *Neka su $x, y \in \mathbb{N}$ takvi da $y < x$. Tada je*

$$x - y \in \mathbb{N}.$$

Dokaz. Iz prethodne leme slijedi da je $x = y + k$, za neki $k \in \mathbb{N}$. Slijedi $x - y = k$ pa je time tvrdnja teorema dokazana. □

2.2 Skup cijelih brojeva

Definirajmo

$$\mathbb{Z} = \{-n \mid n \in \mathbb{N}\} \cup \{0\} \cup \mathbb{N}.$$

Za elemente od $\mathbb{Z}$ kažemo da su cijeli brojevi. Za $x, y \in \mathbb{R}$, $y \neq 0$ definiramo $\frac{x}{y} = x \cdot y^{-1}$.

Propozicija 2.2.1. *Neka su $x, y \in \mathbb{Z}$. Tada je $x + y \in \mathbb{Z}$.*

Dokaz. Ako je $x = 0$ ili $y = 0$, tvrdnja je očita. Pretpostavimo stoga da je $x \neq 0$ i $y \neq 0$. Imamo nekoliko slučajeva:

1) $x, y \in \mathbb{N}$. Prema propoziciji 2.1.6 vrijedi

$$x + y \in \mathbb{N}.$$

Stoga je

$$x + y \in \mathbb{Z}.$$

2) $x, y \in \{-n \mid n \in \mathbb{N}\}$. Tada postoje $n, m \in \mathbb{N}$ takvi da je $x = -n$ i $y = -m$. Koristeći napomenu 1.2.10 dobivamo

$$x + y = (-n) + (-m) = -(n + m).$$

Vrijedi

$$n + m \in \mathbb{N}$$

(propozicija 2.1.6) pa je

$$x + y \in \mathbb{Z}.$$

3) $x \in \mathbb{N}$ i $y \in \{-n \mid n \in \mathbb{N}\}$. Tada postoji $n \in \mathbb{N}$ takav da je $y = -n$. Imamo

$$x + y = x - n.$$

Znamo da vrijedi $n \leq x$ ili $x \leq n$ pa zaključujemo da je $n = x$ ili $n < x$ ili $x < n$. Ako je $n = x$ onda je $x - n = 0$ pa je

$$x + y \in \mathbb{Z}.$$

Ako je $n < x$ onda je prema teoremu 2.1.13

$$x - n \in \mathbb{N}$$

pa je

$$x + y \in \mathbb{Z}.$$

Pretpostavimo da je $x < n$. Prema teoremu 2.1.13 vrijedi $n - x \in \mathbb{N}$. Koristeći napomenu 1.2.10 dobivamo

$$-(n - x) = -(n + (-x)) = -n - (-x) = -n + (-(-x)) = -n + x = x - n.$$

Dakle, $x - n = -(n - x)$ pa je očito

$$x - n \in \mathbb{Z}.$$

Dakle,

$$x + y \in \mathbb{Z}.$$

4) $x \in \{-n \mid n \in \mathbb{N}\}$ i $y \in \mathbb{N}$. Analogno kao u slučaju 3) dobivamo da je $x+y \in \mathbb{Z}$.

□

Propozicija 2.2.2. *Neka su $x, y \in \mathbb{Z}$. Tada je $x \cdot y \in \mathbb{Z}$.*

Dokaz. Ako je $x = 0$ ili $y = 0$ tada prema propoziciji 1.2.1 vrijedi $x \cdot y = 0$ te je stoga očito

$$x \cdot y \in \mathbb{Z}.$$

Pretpostavimo da je $x \neq 0$ i $y \neq 0$. Imamo nekoliko slučajeva:

1) $x, y \in \mathbb{N}$. Prema propoziciji 2.1.7 vrijedi $x \cdot y \in \mathbb{N}$. Stoga je

$$x \cdot y \in \mathbb{Z}.$$

2) $x, y \in \{-n \mid n \in \mathbb{N}\}$. Tada postoje $n, m \in \mathbb{N}$ takvi da je $x = -n$ i $y = -m$. Koristeći propoziciju 1.2.1 (3) dobivamo

$$x \cdot y = (-n) \cdot (-m) = n \cdot m,$$

a

$$n \cdot m \in \mathbb{N}$$

prema propoziciji 2.1.7 pa je

$$x \cdot y \in \mathbb{Z}.$$

3) $x \in \mathbb{N}$ i $y \in \{-n \mid n \in \mathbb{N}\}$. Tada postoji $n \in \mathbb{N}$ takav da je $y = -n$. Koristeći propoziciju 1.2.1 (1) dobivamo

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

pa je

$$x \cdot y \in \mathbb{Z}$$

jer je $x \cdot n \in \mathbb{N}$.

4) $x \in \{-n \mid n \in \mathbb{N}\}$ i $y \in \mathbb{N}$. Analogno kao u slučaju 3) dobivamo da je $x \cdot y \in \mathbb{Z}$.

□

Propozicija 2.2.3. *Neka je $x \in \mathbb{Z}$. Tada je $-x \in \mathbb{Z}$.*

Dokaz. Imamo tri slučaja:

1) $x \in \mathbb{N}$. Tada je očito $-x \in \mathbb{Z}$.

2) $x = 0$. Iz $0 + 0 = 0$ je očito da je $-0 = 0$. Stoga je $-x = 0$ pa je $-x \in \mathbb{Z}$.

3) $x \in \{-n \mid n \in \mathbb{N}\}$. Tada postoji $n \in \mathbb{N}$ takav da je $x = -n$. Iz

$$n + (-n) = 0$$

odmah slijedi da je $-(-n) = n$. Stoga je $-x = -(-n) = n$ pa je očito

$$-x \in \mathbb{Z}.$$

□

2.3 Skup racionalnih brojeva

Definirajmo

$$\mathbb{Q} = \{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\}.$$

Neka je $m \in \mathbb{Z}$. Imamo $1 \in \mathbb{N}$ pa je $\frac{m}{1} \in \mathbb{Q}$, tj $m \in \mathbb{Q}$. Prema tome $\mathbb{Z} \subseteq \mathbb{Q}$.

Propozicija 2.3.1. *Neka su $x, y \in \mathbb{Q}$. Tada je $x + y \in \mathbb{Q}$ i $x \cdot y \in \mathbb{Q}$.*

Dokaz. Imamo $x = \frac{m}{n}$ i $y = \frac{p}{q}$ gdje su $m, p \in \mathbb{Z}$ i $n, q \in \mathbb{N}$. Koristeći propoziciju 2.1.5 slijedi

$$x + y = \frac{m}{n} + \frac{p}{q} = \frac{mq + np}{nq}.$$

Iz $\mathbb{N} \subseteq \mathbb{Z}$ i prethodne dvije propozicije slijedi

$$mq + np \in \mathbb{Z}.$$

Iz propozicije 2.1.7 slijedi $nq \in \mathbb{N}$. Stoga je

$$x + y \in \mathbb{Q}.$$

Nadalje, prema propoziciji 2.1.5 vrijedi

$$x \cdot y = \frac{m}{n} \cdot \frac{p}{q} = \frac{mp}{nq}$$

pa zaključujemo da je

$$x \cdot y \in \mathbb{Q}.$$

□

Propozicija 2.3.2. *Neka su $x, y \in \mathbb{R}$, $y \neq 0$. Tada je*

$$-\frac{x}{y} = \frac{-x}{y}.$$

Nadalje vrijedi $(-y)^{-1} = -y^{-1}$ te $-\frac{x}{y} = \frac{x}{-y}$. Također vrijedi

$$\frac{x}{y} = \frac{-x}{-y}.$$

Dokaz. Koristeći propoziciju 1.2.1 (1) dobivamo

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

Dakle, $\frac{x}{y} = \frac{-x}{y}$. Koristeći propoziciju 1.2.1 (1) i (3) dobivamo

$$(-y) \cdot (-y^{-1}) = y \cdot y^{-1} = 1,$$

dakle

$$(-y) \cdot (-y^{-1}) = 1$$

pa množenje ove jednakosti s $(-y)^{-1}$ slijedi

$$-y^{-1} = (-y)^{-1}.$$

Slijedi

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

dakle $\frac{x}{y} = \frac{x}{-y}$. Koristeći dobivene jednakosti dobivamo

$$\frac{-x}{-y} = -\frac{x}{-y} = -(-\frac{x}{y}) = \frac{x}{y}.$$

Time je tvrdnja propozicije dokazana. □

Propozicija 2.3.3. *Neka je $x \in \mathbb{Q}$. Tada je $-x \in \mathbb{Q}$. Ako je $x \neq 0$ onda je $x^{-1} \in \mathbb{Q}$.*

Dokaz. Znamo da postoje $m \in \mathbb{Z}$ i $n \in \mathbb{N}$ takvi da je $x = \frac{m}{n}$. Tada, prema propoziciji 2.3.2 vrijedi

$$-x = -\frac{m}{n} = \frac{-m}{n},$$

a prema propoziciji 2.2.3, $-m \in \mathbb{Z}$. Stoga je $-x \in \mathbb{Q}$. Pretpostavimo da je $x \neq 0$. Tada je $m \neq 0$. Imamo

$$x^{-1} = (\frac{m}{n})^{-1} = \frac{n}{m},$$

pri čemu smo koristili propoziciju 2.1.5. Ako je $m \in \mathbb{N}$, onda je očito

$$\frac{n}{m} \in \mathbb{Q},$$

dakle $x^{-1} \in \mathbb{Q}$. Pretpostavimo da $m \notin \mathbb{N}$. Tada iz $m \in \mathbb{Z}$ i $m \neq 0$ slijedi

$$m \in \{-p \mid p \in \mathbb{N}\}$$

pa je $-m \in \mathbb{N}$. Iz propozicije 2.3.2 slijedi

$$\frac{n}{m} = \frac{-n}{-m}$$

pa je $\frac{n}{m} \in \mathbb{Q}$, tj

$$x^{-1} \in \mathbb{Q}.$$

Time je tvrdnja propozicije dokazana. □

2.4 Potpolja

Neka su $(P', +', \cdot')$ i $(P, +, \cdot)$ dva polja. Kažemo da je $(P', +', \cdot')$ potpolje od $(P, +, \cdot)$ ako je $P' \subseteq P$ te ako za sve $x, y \in P'$ vrijedi $x +' y = x + y$ i $x \cdot' y = x \cdot y$.

Propozicija 2.4.1. *Neka je $(P', +', \cdot')$ potpolje od $(P, +, \cdot)$. Neka je $0'$ neutralni element za $+'$, neka je 0 neutralni element za $+$, neka je $1'$ neutralni element za $\cdot'$ te neka je 1 neutralni element za $\cdot$. Tada je:*

1) $0' = 0$ i $1' = 1$.

2) Nadalje neka je $x \in P'$, $x \neq 0$. Neka je y' inverzni element od x u $(P', \cdot')$ te neka je y inverzni element od x u $(P, \cdot)$. Tada je

$$y' = y.$$

3) Neka je $a \in P'$. Neka je b' inverzni element od a u $(P', +')$ te neka je b inverzni element od a u $(P, +)$. Tada je

$$b' = b.$$

Dokaz. 1) Uzmimo bilo koji $z \in P'$, $z \neq 0'$. Vrijedi $z +' 0' = z$, tj $z + 0' = z$. Dodavanjem $(-z)$ lijevoj i desnoj strani ove jednakosti (pri čemu je $-z$ inverzni element od z u $(P, +)$) dobivamo

$$0' = 0.$$

Imamo $z \cdot' 1' = z$, tj $z \cdot 1' = z$. Iz $z \neq 0'$ slijedi $z \neq 0$ pa z ima inverzni element u $(P, \cdot)$; označavamo ga sa z^{-1}. Kada jednakost $z \cdot 1' = z$ pomnožimo sa z^{-1} dobijemo

$$1' = 1.$$

3) Imamo $a +' b' = 0'$, tj $a + b' = 0$. S druge strane vrijedi $a + b = 0$ pa je $a + b' = a + b$ iz čega slijedi

$$b' = b.$$

2) Imamo $x \cdot' y' = 1'$, tj $x \cdot y' = 1$. S druge strane vrijedi $x \cdot y = 1$ pa je $x \cdot y' = x \cdot y$ što povlači

$$y' = y.$$

□

Neka je $(P, +\cdot)$ polje te neka je $P' \subseteq P$. Kažemo da je P' potpolje od $(P, +, \cdot)$ ako postoje binarne operacije $+'$ i $\cdot'$ takve da je $(P', +', \cdot')$ potpolje od $(P, +, \cdot)$. Uočimo sljedeće: ako je P' potpolje od $(P, +, \cdot)$ onda postoje jedinstvene binarne operacije $+'$ i $\cdot'$ na P' takve da je $(P', +', \cdot')$ potpolje od $(P, +, \cdot)$. Naime, ako su $+', +'', \cdot', \cdot''$ binarne operacije na P' takve da su $(P', +', \cdot')$ i $(P', +'', \cdot'')$ potpolja od $(P, +, \cdot)$ onda za sve $x, y \in P'$ vrijedi

$$x +' y = x +'' y,$$

tj

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

što znači da su funkcije $+', +'' : P' \times P' \to P'$ jednake. Analogno zaključujemo da je $\cdot' = \cdot''$.

Propozicija 2.4.2. *Neka je $(P, +, \cdot)$ polje te neka je $P' \subseteq P$. Pretpostavimo da P' ima bar 2 elementa. Tada je P' potpolje od $(P, +, \cdot)$ ako i samo ako za sve $x, y \in P'$ vrijedi:*

$$x - y \in P', x \cdot y \in P'$$

te za svaki $x \in P'$ takav da je $x \neq 0$ vrijedi $x^{-1} \in P'$.

Dokaz. Pretpostavimo da je P' potpolje od $(P, +, \cdot)$. Tada postoje binarne operacije $+'$ i $\cdot'$ takve da je $(P', +', \cdot')$ potpolje od $(P, +, \cdot)$. Neka su $x, y \in P'$. Iz propozicije 2.4.1 slijedi

$$-y \in P'.$$

Stoga je

$$x - y = x + (-y) = x +' (-y) \in P',$$

dakle

$$x - y \in P'.$$

Nadalje, $x \cdot y = x \cdot' y \in P'$. Iz propozicije 2.4.1 (3) slijedi da je

$$x^{-1} \in P',$$

za svaki $x \in P'$ takav da je $x \neq 0$.

Pretpostavimo da za sve $x, y \in P'$ vrijedi $x - y \in P'$, $x \cdot y \in P'$ te da za svaki $x \in P'$ takav da je $x \neq 0$ vrijedi $x^{-1} \in P'$. Odaberimo neki $x \in P'$. Tada je

$$x - x \in P',$$

tj $0 \in P'$. Stoga za svaki $y \in P'$ vrijedi $0 - y \in P'$, tj $-y \in P'$. Sada, ako su $x, y \in P'$, imamo $x, -y \in P'$ pa je $x - (-y) \in P'$ tj $x + y \in P'$. Dakle,

$$x + y \in P',$$

za sve $x, y \in P'$. Definiramo binarne operacije $+'$ i $\cdot'$ na P' na sljedeći način:

$$x +' y = x + y$$

i

$$x \cdot' y = x \cdot y,$$

za sve $x, y \in P'$. Tvrdimo da je $(P', +', \cdot')$ potpolje od $(P, +, \cdot)$. Dovoljno je provjeriti da je $(P', +', \cdot')$ polje. Dokažimo da je $(P', +')$ Abelova grupa.

Neka su $x, y, z \in P'$. Koristeći činjenicu da je binarna operacija $+$ asocijativna na P dobivamo

$$x +' (y +' z) = x + (y + z) = (x + y) + z = (x +' y) +' z.$$

Prema tome, binarna operacija $+'$ je asocijativna na P'. Znamo da je $0 \in P'$ te za svaki $x \in P'$ vrijedi

$$x +' 0 = x + 0 = x.$$

Isto tako

$$0 +' x = 0 + x = x$$

za svaki $x \in P'$. Prema tome 0 je neutralni element za binarnu operaciju $+'$ na P'. Neka je $x \in P'$. Znamo da je $-x \in P'$ te imamo

$$x +' (-x) = x + (-x) = 0$$

te je analogno $(-x) +' x = 0$. Prema tome, $(P', +')$ je grupa. Komutativnost binarne operacije $+'$ slijedi iz komutativnosti binarne operacije $+$. Stoga je $(P', +')$ Abelova grupa. Asocijativnost binarne operacije $\cdot'$ slijedi iz asocijativnosti binarne operacije $\cdot$. Distributivnost operacije $\cdot'$ u odnosu na $+'$ slijedi iz distributivnosti operacije $\cdot$ u odnosu na $+$. Prema tome, $(P', +', \cdot')$ je prsten. Komutativnost operacije $\cdot'$ slijedi iz komutativnosti operacije $\cdot$. Prema tome, $(P', +', \cdot')$ je komutativan prsten. Odaberimo $x \in P'$ takav da je $x \neq 0$ (a to možemo jer P' sadrži bar dva elementa). Prema pretpostavci vrijedi $x^{-1} \in P'$. Dakle, $x, x^{-1} \in P'$ pa iz pretpostavke slijedi

$$x \cdot x^{-1} \in P'.$$

Dakle, $1 \in P'$. Sada je jasno da je 1 neutralni element u $(P', \cdot')$. Prema tome, $(P', +', \cdot')$ je komutativan prsten s jedinicom. Ako je $x \in P', x \neq 0$ tada je $x^{-1} \in P'$ te je

$$x \cdot' x^{-1} = x \cdot x^{-1} = 1$$

pa zaključujemo da je $(P', +', \cdot')$ polje. □

Primjer 2.4.3. *1. $\mathbb{Q}$ je potpolje od $(\mathbb{R}, +, \cdot)$. To slijedi iz propozicije 2.3.3.*

2. $\mathbb{Z}$ nije potpolje od $(\mathbb{R}, +, \cdot)$.

Naime to slijedi iz propozicije 2.4.2 jer je $2 \in \mathbb{Z}$, a $2^{-1} \notin \mathbb{Z}$. Dokažimo da $2^{-1} \notin \mathbb{Z}$.

Iz $0 < 1$ slijedi $1 < 1 + 1$, tj $1 < 2$ pa slijedi $0 < 2$. Prema propoziciji 1.2.14 vrijedi $0 < 2^{-1}$. Podsjetimo se da je $\mathbb{Z} = \{-n \mid n \in \mathbb{N}\} \cup \{0\} \cup \mathbb{N}$. Za svaki $n \in \mathbb{N}$ vrijedi $0 < n$ pa je $-n < 0$. Stoga $2^{-1} \notin \{-n \mid n \in \mathbb{N}\}$. Također, $2^{-1} \neq 0$. Iz $1 < 2$ i $0 < 2^{-1}$ te propozicije 1.2.11 slijedi $2^{-1} < 1$. S druge strane za svaki $n \in \mathbb{N}$ vrijedi $1 \leq n$. Stoga $2^{-1} \notin \mathbb{N}$. Prema tome $2^{-1} \notin \mathbb{Z}$.

Uočimo da iz istog razloga ni $\mathbb{N}$ nije potpolje od $(\mathbb{R}, +, \cdot)$.

Ako je $(P, +, \cdot)$ prsten i $x \in P$ onda umjesto $x \cdot x$ pišemo x^2.

Korolar 2.4.4. *Neka je $(P, +, \cdot, \leq)$ uređeni prsten. Tada za svaki $x \in P$ vrijedi $0 \leq x^2$.*

Dokaz. Neka je $x \in P$. Tada je $0 \leq x$ ili $x \leq 0$. Ako je $0 \leq x$ onda je $0 \leq x \cdot x$ prema definiciji uređenog prstena (2), tj $0 \leq x^2$. Ako je $x \leq 0$ tada iz propozicije 1.2.12 slijedi $0 \leq x \cdot x$. Dakle,

$$0 \leq x^2.$$

□

Poglavlje 3

Polje kompleksnih brojeva

Napomena 3.0.1. *Od sada više ne smatramo da je* $(\mathbb{R}, +, \cdot, \leq)$ *jedno fiksirano polje realnih brojeva.*

3.1 Polje kompleksnih brojeva

Neka je $(\mathbb{C}, +, \cdot)$ polje. Kažemo da je $(\mathbb{C}, +, \cdot)$ **polje kompleksnih brojeva** ako vrijedi sljedeće:

1) Postoji polje realnih brojeva $(\mathbb{R}, +', \cdot', \leq)$ takvo da je $(\mathbb{R}, +', \cdot')$ potpolje od $(\mathbb{C}, +, \cdot)$.

2) Postoji $i \in \mathbb{C}$ takav da je
$$i^2 = -1$$
te takav da za svaki $z \in \mathbb{C}$ postoje $x, y \in \mathbb{R}$ takvi da je
$$z = x + iy.$$

U tom slučaju kažemo da je $(\mathbb{R}, +', \cdot')$ realno potpolje od $(\mathbb{C}, +, \cdot)$.

Propozicija 3.1.1. *Neka je* $(P, +, \cdot)$ *polje te neka je* R *potpolje od* $(P, +, \cdot)$. *Pretpostavimo da je* $i \in P$ *takav da* $i \notin R$ *te da su* $x, y, x', y' \in R$ *takvi da je*
$$x + iy = x' + iy'.$$
Tada je $x = x'$ *i* $y = y'$.

Dokaz. Iz $x + iy = x' + iy'$ slijedi

$$x - x' = (y' - y)i.$$

Pretpostavimo da je $y' \neq y$. Tada je $y' - y \neq 0$ pa množenjem prethodne jednakosti s $(y' - y)^{-1}$ dobivamo

$$(x - x') \cdot (y' - y)^{-1} = i.$$

Iz $x, x' \in R$ i propozicije 2.4.2 slijedi $x - x' \in R$. Analogno $y' - y \in R$ pa prema istoj propoziciji vrijedi $(y' - y)^{-1} \in R$. Stoga je

$$(x - x') \cdot (y' - y) \in R$$

što je u kontradikciji s tim da $i \notin R$. Zaključujemo da je $y' = y$ pa iz $(x - x') = (y' - y)i$ slijedi $x = x'$ što smo i htjeli dokazati. □

3.2 Izomorfizam polja

Neka su $(P, +, \cdot)$ i $(R, +', \cdot')$ polja. Za bijekciju $f : P \to R$ kažemo da je **izomorfizam** ovih polja ako za svaki $x, y \in P$ vrijedi sljedeće:

1) $f(x + y) = f(x) +' f(y)$

2) $f(x \cdot y) = f(x) \cdot' f(y)$.

Za dva polja kažemo da su **izomorfna** ako postoji izomorfizam između njih.

Lema 3.2.1. *Neka su $(P, +, \cdot)$ i $(R, +', \cdot')$ izmorfna polja. Pretpostavimo da postoji uređaj $\leq$ na P takav da je $(P, +, \cdot, \leq)$ potpuno uređeno polje. Tada postoji uređaj $\leq'$ na R takav da je $(R, +', \cdot', \leq')$ potpuno uređeno polje.*

Dokaz. Neka je $f : P \to R$ izomorfizam. Definirajmo binarnu relaciju $\leq'$ na R sa: $a \leq' b$ ako je $f^{-1}(a) \leq f^{-1}(b)$. Dakle,

$$\leq' = \{(a, b) \in R \times R \mid f^{-1}(a) \leq f^{-1}(b)\}.$$

Dokažimo da je $\leq'$ uređaj na R. Uzmimo $a \in R$. Vrijedi $a \leq' a$ zato što je $f^{-1}(a) \leq f^{-1}(a)$, što je posljedica toga da je relacija $\leq$ refleksivna na P. Prema tome $\leq'$ je refleksivna na R.

Neka su $a, b \in R$ takvi da je $a \leq' b$ i $b \leq' a$. Tada je $f^{-1}(a) \leq f^{-1}(b)$ i $f^{-1}(b) \leq f^{-1}(a)$ pa je $f^{-1}(a) = f^{-1}(b)$ jer je $\leq$ antisimetrična relacija na P. Stoga je $a = b$. Time smo dokazali da je $\leq'$ je antisimetrična relacija na R.

Neka su $a, b, c \in R$ takvi da je $a \leq' b$ i $b \leq' c$. Tada je $f^{-1}(a) \leq f^{-1}(b)$ i $f^{-1}(b) \leq f^{-1}(c)$ pa je $f^{-1}(a) \leq f^{-1}(c)$ zbog tranzitivnosti relacije $\leq$. Stoga je $a \leq' c$. Prema tome $\leq'$ je tranzitivna relacija na R.

Neka su $a, b \in R$. Budući da je $\leq$ uređaj na P vrijedi $f^{-1}(a) \leq f^{-1}(b)$ ili $f^{-1}(b) \leq f^{-1}(a)$ pa slijedi $a \leq' b$ ili $b \leq' a$. Prema tome $\leq'$ je uređaj na R.

Neka su $a, b, c \in R$ takvi da $a \leq' b$. Dokažimo da je $a +' c \leq' b +' c$. Imamo $f^{-1}(a) \leq f^{-1}(b)$. Iz činjenice da je $(P, +, \cdot)$ uređeni prsten slijedi

$$f^{-1}(a) + f^{-1}(c) \leq f^{-1}(b) + f^{-1}(c).$$

Prema lemi 3.2.3 $f^{-1} : R \to P$ je izmorofizam polja pa je $f^{-1}(a +' c) \leq f^{-1}(b +' c)$. Stoga je $a +' c \leq' b +' c$.

Neka su $a, b \in R$ takvi da je $0 \leq' a$ i $0 \leq' b$. Dokažimo da je $0 \leq' a \cdot b$. Imamo $f^{-1}(0) \leq f^{-1}(a)$ i $f^{-1}(0) \leq f^{-1}(b)$. Iz leme 3.2.4 slijedi $0 \leq f^{-1}(a)$ i $0 \leq f^{-1}(b)$. Koristeći činjenicu da je $(P, +, \cdot)$ uređeni prsten dobivamo $0 \leq f^{-1}(a) \cdot f^{-1}(b)$. Kako je f izomorfizam polja slijedi $0 \leq f^{-1}(a \cdot b)$, tj $f^{-1}(0) \leq f^{-1}(a \cdot b)$. Stoga je $0 \leq' a \cdot b$. Dakle, $(R, +', \cdot', \leq')$ je uređeno polje.

Neka su $A, B \subseteq R$, $A \neq 0$,$B \neq 0$ takvi da za svaki $a \in A$ i za svaki $b \in B$ vrijedi $a \leq' b$. Tvrdimo da onda postoji $c \in R$ takav da je $a \leq' c$ i $c \leq' b$ za svaki $a \in A$ i za svaki $b \in B$.

Definirajmo skupove $C = \{f^{-1}(a) \mid a \in A\}$ i $D = \{f^{-1}(b) \mid b \in B\}$. Očito su C i D neprazni podskupovi od P. Neka su $x \in C$ i $y \in D$. Tada postoje $a \in A$ i $b \in B$ takvi da je $f^{-1}(a) = x$ i $f^{-1}(b) = y$. Prema pretpostavci vrijedi $a \leq' b$ pa iz definicije od $\leq'$ slijedi $f^{-1}(a) \leq f^{-1}(b)$, tj $x \leq y$. Budući da je $(P, \leq)$ potpuno uređen skup postoji $z \in P$ takav da je

$$x \leq z \text{ i } z \leq y \tag{3.1}$$

za svaki $x \in C$ i za svaki $y \in D$. Definiramo $c = f(z)$. Očito je $c \in R$. Neka je $a \in A$. Tvrdimo da je $a \leq' c$. To je ekvivalentno sa $f^{-1}(a) \leq f^{-1}(c)$, tj sa $f^{-1}(a) \leq z$. Zadnja nejednakost vrijedi prema 3.1 jer je $f^{-1}(a) \in C$. Dakle, $a \leq' c$ za svaki $a \in A$. Analogno dokazujemo da je $c \leq' b$ za svaki $b \in B$. Time smo dokazali da je $(R, \leq')$ potpuno uređen skup. Dakle, $(R, +', \cdot', \leq')$ je potpuno uređeno polje,tj. polje realnih brojeva. □

Teorem 3.2.2. *Neka je $(\mathbb{R}, +, \cdot, \leq)$ neko polje realnih brojeva. Tada postoje polja $(\mathbb{C}, +', \cdot')$ i $(R, +'', \cdot'')$ takva da vrijedi sljedeće:*

1) $(\mathbb{C}, +', \cdot')$ je polje kompleksnih brojeva.

2) $(R, +'', \cdot'')$ je realno potpolje od $(\mathbb{C}, +', \cdot')$.

3) Polja $(\mathbb{R}, +, \cdot)$ i $(R, +'', \cdot'')$ su izomorfna.

Dokaz. 1) Definirajmo $\mathbb{C} = \mathbb{R} \times \mathbb{R}$. Definiramo na $\mathbb{C}$ binarne operacije $+'$ i $\cdot'$ na sljedeći način:

$$(x_1, y_1) +' (x_2, y_2) = (x_1 + x_2, y_1 + y_2),$$
$$(x_1, y_1) \cdot' (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$$

za $x_1, x_2, y_1, y_2 \in \mathbb{R}$. Dokažimo da je $(\mathbb{C}, +, \cdot)$ polje. Neka su $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{C}$. Koristeći činjenicu da je binarna operacija $+$ asocijativna na $\mathbb{R}$ dobivamo

$$(x_1, y_1) +' [(x_2, y_2) +' (x_3, y_3)] = (x_1, y_1) +' [(x_2 + x_3, y_2 + y_3)] =$$
$$= (x_1 + (x_2 + x_3), y_1 + (y_2 + y_3)) = ((x_1 + x_2) + x_3, (y_1 + y_2) + y_3) =$$
$$= (x_1 + x_2, y_1 + y_2) +' (x_3, y_3) = [(x_1, y_1) +' (x_2, y_2)] +' (x_3, y_3).$$

Prema tome, binarna operacija $+'$ je asocijativna na $\mathbb{C}$.

Znamo da je $0 \in \mathbb{R}$ te za svaki $(x, y) \in \mathbb{C}$ vrijedi

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

Isto tako,

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

za svaki $(x, y) \in \mathbb{C}$. Prema tome $(0, 0)$ je neutralni element za binarnu operaciju $+'$ na $\mathbb{C}$.

Neka je $(x, y) \in \mathbb{C}$. Znamo da je $(-x, -y) \in \mathbb{C}$ te imamo

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

te je analogno $(-x, -y) +' (x, y) = (0, 0)$. Prema tome, $(\mathbb{C}, +')$ je grupa.

Komutativnost binarne operacije $+'$ slijedi iz komutativnosti binarne operacije $+$ na $\mathbb{R}$. Stoga je $(\mathbb{C}, +')$ Abelova grupa.

Neka su $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{C}$. Imamo

$$(x_1, y_1) \cdot' [(x_2, y_2) \cdot' (x_3, y_3)] = (x_1, y_1) \cdot' (x_2x_3 - y_2y_3, x_2y_3 + y_2x_3) =$$
$$= (x_1(x_2x_3 - y_2y_3) - y_1(x_2y_3 + y_2x_3), x_1(x_2y_3 + y_2x_3) + y_1(x_2x_3 - y_2y_3)) =$$
$$= (x_1x_2x_3 - x_1y_2y_3 - y_1x_2y_3 - y_1y_2x_3, x_1x_2y_3 + x_1y_2x_3 + y_1x_2x_3 - y_1y_2y_3).$$

S druge strane,

$$[(x_1, y_1) \cdot' (x_2, y_2)] \cdot' (x_3, y_3) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2) \cdot' (x_3, y_3) =$$
$$= [(x_1x_2 - y_1y_2) \cdot x_3 - (x_1y_2 + y_1x_2) \cdot y_3, (x_1x_2 - y_1y_2) \cdot y_3 + (x_1y_2 + y_1x_2) \cdot x_3] =$$

$$= (x_1x_2x_3 - x_1y_2y_3 - y_1x_2y_3 - y_1y_2x_3, x_1x_2y_3 + x_1y_2x_3 + y_1x_2x_3 - y_1y_2y_3).$$

Prema tome,

$$(x_1, y_1) \cdot' [(x_2, y_2) \cdot' (x_3, y_3)] = [(x_1, y_1) \cdot' (x_2, y_2)] \cdot' (x_3, y_3).$$

pa je binarna operacija $\cdot'$ asocijativna na $\mathbb{C}$. Komutativnost operacije $\cdot'$ slijedi iz komutativnosti operacije $\cdot$ na $\mathbb{R}$.

Imamo

$$(x_1, y_1) \cdot' [(x_2, y_2) +' (x_3, y_3)] = (x_1, y_1) \cdot' (x_2 + x_3, y_2 + y_3) =$$

$$= (x_1 \cdot (x_2 + x_3) - y_1 \cdot (y_2 + y_3), x_1 \cdot (y_2 + y_3) + y_1(x_2 + x_3)) =$$

$$= (x_1x_2 + x_1x_3 - y_1y_2 - y_1y_3, x_1y_2 + x_1y_3 + y_1x_2 + y_1x_3).$$

S druge strane,

$$[(x_1, y_1) \cdot' (x_2, y_2)] +' [(x_1, y_1) \cdot' (x_3, y_3)] =$$

$$= (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2) +' (x_1x_3 - y_1y_3, x_1y_3 + y_1x_3) =$$

$$= x_1x_2 + x_1x_3 - y_1y_2 - y_1y_3, x_1y_2 + x_1y_3 + y_1x_2 + y_1x_3).$$

Prema tome,

$$(x_1, y_1) \cdot' [(x_2, y_2) +' (x_3, y_3)] = [(x_1, y_1) \cdot' (x_2, y_2)] +' [(x_1, y_1) \cdot' (x_3, y_3)].$$

pa vrijedi distributivnost operacije $\cdot'$ u odnosu na $+'$ na $\mathbb{C}$. Dokazali smo da je $(\mathbb{C}, +', \cdot')$ komutativan prsten.

Neutralan element za množenje je par $(1, 0)$, tj za svaki (x, y) imamo

$$(x, y) \cdot' (1, 0) = (x \cdot 1 - y \cdot 0, x \cdot 0 + y \cdot 1) = (x, y)$$

i

$$(1, 0) \cdot' (x, y) = (1 \cdot x - 0 \cdot y, 1 \cdot y + 0 \cdot x) = (x, y).$$

Dakle, $(\mathbb{C}, +', \cdot')$ je komutativan prsten s jedinicom. Za svaki $(x, y) \neq (0, 0)$, tj $x^2 + y^2 \neq 0$ definiramo $a = (\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2})$. Vrijedi

$$(x, y) \cdot a = (x, y) \cdot (\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2} = (\frac{x \cdot x - y \cdot (-y)}{x^2 + y^2}, \frac{x \cdot (-y) + y \cdot x}{x^2 + y^2}) = (1, 0).$$

Dakle, $(\mathbb{C}, +', \cdot')$ je polje. Uočimo da za sve $x, y \in \mathbb{R}$ vrijedi:

1) $-(x,y) = (-x,-y)$
2) ako je $(x,y) \neq (0,0)$ onda je $(x,y)^{-1} = (\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2})$.

2) Definirajmo $R = \{(x,0) \mid x \in \mathbb{R}\}$. Tvrdimo da je R potpolje od $(\mathbb{C}, +', \cdot')$. Neka su $u, v \in R$. Tada je $u = (x,0)$ i $v = (y,0)$ gdje su $x, y \in \mathbb{R}$. Imamo

$$u - v = u +' (-v) = (x,0) +' (-y,0) = (x-y,0).$$

Dakle, $u - v \in R$. Vrijedi

$$u \cdot v = (x,0) \cdot' (y,0) = (x \cdot y - 0, x \cdot 0 + 0 \cdot y) = (x \cdot y, 0).$$

Dakle, $u \cdot v \in R$. Pretpostavimo da je $u \neq (0,0)$. Tada je $x \neq 0$ pa je

$$u^1 = (x,0)^{-1} = (\frac{x}{x^2}, \frac{0}{x^2}) = (x^{-1}, 0)$$

jer je $\frac{x}{x^2} = x \cdot (x^2)^{-1} = x \cdot (x \cdot x)^{-1} = x \cdot x^{-1} \cdot x^{-1} = x^{-1}$. Prema propoziciji 2.4.2 zaključujemo da je R potpolje od $(\mathbb{C}, +', \cdot')$. Stoga postoje binarne operacije $+''$ i $\cdot''$ na R takve da je $(R, +'', \cdot'')$ potpolje od $(\mathbb{C}, +', \cdot')$. Tvrdimo da su polja $(\mathbb{R}, +, \cdot)$ i $(R, +'', \cdot'')$ izomorfna. Definirajmo funkciju $f : \mathbb{R} \to R$ sa $f(x) = (x,0)$. Ako su $x_1, x_2 \in \mathbb{R}$ takvi da je $x_1 \neq x_2$, onda je $(x_1,0) \neq (x_2,0)$, tj $f(x_1) \neq f(x_2)$. Dakle, f je injekcija. Neka je $y \in R$. Tada postoji $x \in \mathbb{R}$ takav da je $y = (x,0)$. Stoga je $y = f(x)$. Prema tome, f je surjekcija. Dakle, f je bijekcija. Neka su $x, y \in \mathbb{R}$. Imamo

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

Dakle,

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

za sve $x, y \in \mathbb{R}$. Neka su $x, y \in \mathbb{R}$. Imamo

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

Dakle,

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

za sve $x, y \in \mathbb{R}$. Prema tome, f je izomorfizam polja $(\mathbb{R}, +, \cdot)$ i $(R, +'', \cdot'')$. Prema lemi 3.2.1 postoji uređaj $\leq'$ na R takav da je $(R, +'', \cdot'', \leq'')$ potpuno uređeno polje, tj polje realnih brojeva. Definiramo $i = (0,1)$. Vrijedi $i^2 = (0,1) \cdot' (0,1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1,0) = -(1,0)$. Dakle, $i^2 = -(1,0)$, a $(1,0)$ je jedinica u polju $(\mathbb{C}, +', \cdot')$ (tj neutralni element za operaciju $\cdot'$).

Neka je $z \in \mathbb{C}$. Imamo $z = (x, y)$, gdje su $x, y \in \mathbb{R}$. Definiramo $u = (x, 0)$ i $v = (y, 0)$. Očito su $u, v \in R$. Vrijedi

$$u +' i \cdot' v = (x,0) +' (0,1) \cdot' (y,0) = (x,0) +' (0 \cdot y - 1 \cdot 0, 0 \cdot 0 + 1 \cdot y) = (x,0) +' (0,y) = (x,y) = z.$$

Dakle, za svaki $z \in \mathbb{C}$ postoje $u, v \in R$ takvi da je $z = u +' i \cdot' v$. Zaključujemo da je $(\mathbb{C}, +', \cdot')$ polje kompleksnih brojeva te da je $(R, +'', \cdot'')$ njegovo realno potpolje koje je izomorfno sa $(\mathbb{R}, +, \cdot)$. □

Lema 3.2.3. *Neka su $(P, +, \cdot)$ i $(R, +', \cdot')$ polja te neka je $f : P \to R$ izomorfizam tih polja. Tada je $f^{-1} : R \to P$ izomorfizam polja $(R, +', \cdot')$ i $(P, +, \cdot)$.*

Dokaz. Jasno je da je f^{-1} bijekcija. Treba još dokazati da je

$$f^{-1}(a +' b) = f^{-1}(a) + f^{-1}(b) \tag{3.2}$$

i

$$f^{-1}(a \cdot' b) = f^{-1}(a) \cdot f^{-1}(b) \tag{3.3}$$

za sve $a, b \in R$.

Neka su $a, b \in R$. Definiramo $u = f^{-1}(a +' b)$, $v = f^{-1}(a) + f^{-1}(b)$. Želimo dokazati da je $u = v$ (dakle da vrijedi (3.2).) U tu svrhu dovoljno je dokazati da je $f(u) = f(v)$. (jer je f injekcija) Imamo

$$f(u) = a +' b,$$

a koristeći činjenicu da je f izomorfizam dobivamo

$$f(v) = f(f^{-1}(a) + f^{-1}(b)) = f(f^{-1}(a)) + f(f^{-1}(b)) = a +' b.$$

Prema tome $f(u) = f(v)$, tj $u = v$. Analogno dokazujemo da vrijedi i jednakost (3.3). □

Lema 3.2.4. *Neka su $(P, +, \cdot)$ i $(R, +', \cdot')$ polja te neka je $f : R \to P$ izomorfizam tih polja. Neka je 0_P neutralni element za operaciju $+$ te neka je 0_R neutralni element za operaciju $+'$. Tada je $f(0_P) = 0_R$.*

Dokaz. Uočimo prvo sljedeće: ako je $x \in R$ takav da je $x = x +' x$ tada je $x = 0_R$. Naime, iz $x = x +' x$ slijedi

$$(-x) +' x = (-x) +' (x +' x)$$

što povlači $0_R = x$. Iz činjenice da je f izomorfizam slijedi $f(0_P + 0_P) = f(0_P) +' f(0_P)$, tj $f(0_P) = f(0_P) +' f(0_P)$ pa prema dokazanom imamo da je $f(0_P) = 0_R$. □

Lema 3.2.5. *Neka su $(P,+,\cdot)$ i $(R,+',\cdot')$ polja te neka je $f : P \to R$ izomorfizam ovih polja. Neka je 1_P neutralni element s obzirom na operaciju $\cdot$ te neka je 1_R neutralni element s obzirom na operaciju $\cdot'$. Tada je $f(1_P) = 1_R$. Nadalje neka je $x \in P$. Tada je $f(-x) = -f(x)$.*

Dokaz. Budući da je f bijekcija postoji $x \in P$ takav da je $1_R = f(x)$. Imamo

$$f(1_P) = f(1_P) \cdot' 1_R = f(1_P) \cdot' f(x) = f(1_P \cdot x) = f(x) = 1_R.$$

Dakle, $f(1_P) = 1_R$.

Imamo $0_P = x + (-x)$ pa je $f(0_P) = f(x + (-x))$. Iz leme 3.2.4 slijedi $f(0_P) = 0_R$ pa je $0_R = f(x) +' f(-x)$. Kad ovoj jednakosti dodamo $-f(x)$ s lijeve i desne strane dobivamo $-f(x) = f(-x)$. □

3.3 Proširenje polja realnih brojeva do polja kompleksnih brojeva

Propozicija 3.3.1. *Neka su $(A,+,\cdot)$, $(B,+',\cdot')$, $(D,+'',\cdot'')$ polja. Neka je C skup takav da je $A \subseteq C$ te neka je $f : C \to D$ bijekcija takva da je $f(A) \subseteq B$. Pretpostavimo da za sve $x, y \in A$ vrijedi $f(x + y) = f(x) +' f(y)$ i $f(x \cdot' y) = f(x) \cdot' f(y)$. Nadalje pretpostavimo da je $(B,+',\cdot')$ potpolje od $(D,+'',\cdot'')$. Tada postoje binarne operacije $\oplus$ i $*$ na C takve da je $(C,\oplus,*)$ polje te da je $(A,+,\cdot)$ potpolje od $(C,\oplus,*)$ i da je f izomorfizam polja $(C,\oplus,*)$ i $(D,+'',\cdot'')$.*

Dokaz. Za $x, y \in C$ definiramo

$$x \oplus y = f^{-1}(f(x) +'' f(y)) \tag{3.4}$$

i

$$x * y = f^{-1}(f(x) \cdot'' f(y)). \tag{3.5}$$

Tvrdimo da je $(C,\oplus,*)$ polje te da je f izomorfizam polja $(C,\oplus,*)$ i $(D,+'',\cdot'')$. Iz (3.4) i (3.5) slijedi da je

$$f(x \oplus y) = f(x) +'' f(y) \tag{3.6}$$

i

$$f(x * y) = f(x) \cdot'' f(y) \tag{3.7}$$

za sve $x, y \in C$. Stoga je dovoljno dokazati da je $(C,\oplus,*)$ polje. Neka su $x, y, z \in C$. Definirajmo $u = (x \oplus y) \oplus z$ i $v = x \oplus (y \oplus z)$. Tvrdimo da je $u = v$. Dovoljno je u tu svrhu dokazati da je $f(u) = f(v)$ (jer je f injekcija). Koristeći (3.6) dobivamo

$$f(u) = f((x \oplus y) \oplus z) = f(x \oplus y) +'' f(z) = ((f(x) +'' f(y)) +'' f(z).$$

S druge strane

$$f(v) = f(x \oplus (y \oplus z)) = f(x) +'' f(y \oplus z) = f(x) +'' ((f(y) +'' f(z)).$$

Iz činjenice da je $+''$ asocijativna binarna operacija na D slijedi $f(u) = f(v)$. Stoga je $u = v$. Dakle, $\oplus$ je asocijativna binarna operacija na C. Analogno dobivamo da je binarna operacija $\oplus$ komutativna te da je binarna operacija $*$ asocijativna i komutativna na C. Neka je 0 neutralni element za operaciju $\cdot''$. Tvrdimo da je $f^{-1}(0)$ neutralni element za $\oplus$.

Neka je $x \in C$. Imamo

$$x \oplus f^{-1}(0) = f^{-1}(f(x) +'' f(f^{-1}(0)) = f^{-1}(f(x) +'' 0) = f^{-1}(f(x)) = x.$$

Dakle, $x \oplus f^{-1}(0) = x$, a zbog komutativnosti operacije $\oplus$ vrijedi $f^{-1}(0) \oplus x = x$. Prema tome, $f^{-1}(0)$ je neutralni element za operaciju $\oplus$. Analogno dobivamo da je $f^{-1}(1)$ neutralni element za binarnu operaciju $*$ pri čemu je 1 neutralni element za binarnu operaciju $\cdot''$. Neka je $x \in C$. Definirajmo $y = f^{-1}(-f(x))$. Vrijedi

$$x \oplus y = f^{-1}(f(x) +'' f(y)) = f^{-1}(f(x)) +'' f(f^{-1}(-f(x))) = f^{-1}(f(x) +'' (-f(x)) = f^{-1}(0).$$

Dakle, $x \oplus y = f^{-1}(0)$. Zaključujemo da je $(C, \oplus)$ Abelova grupa.

Neka su $x, y, z \in C$. Neka je $u = (x \oplus y) * z$ i $v = x * z \oplus y * z$. Tvrdimo da je $u = v$. Koristeći 3.6 i 3.7 dobivamo

$$f(u) = f((x \oplus y) * z) = f(x \oplus y) \cdot'' f(z) = (f(x) +'' f(y)) \cdot'' f(z) =$$

$$= f(x) \cdot'' f(z) +'' f(y) \cdot'' f(z) = f(x * z) +'' f(y * z) = f((x * z) \oplus (y * z)) = f(v).$$

Dakle, $f(u) = f(v)$ pa je $u = v$. Zaključujemo da je operacija $*$ distributivna u odnosu na operaciju $\oplus$.

Neka je $x \in C$ takav da je $x \neq f^{-1}(0)$. Tada je $f(x) \neq 0$. Derfiniramo $y = f^{-1}(f(x)^{-1})$. Imamo

$$x * y = f^{-1}(f(x) \cdot'' f(y)) = f^{-1}(f(x) \cdot'' f(f^{-1}(f(x)^{-1}))) = f^{-1}(f(x) \cdot'' (f(x)^{-1}) = f^{-1}(1).$$

Dakle, $x * y = f^{-1}(1)$. Prema tome, za svaki $x \in C$ takav da je $x \neq f^{-1}(0)$ postoji $y \in C$ takav da je $x * y = f^{-1}(1)$. Zaključujemo da je $(C, \oplus, *)$ polje. Preostaje još dokazati da je $(A, +, \cdot)$ potpolje od $(C, \oplus, *)$. Neka su $x, y \in A$. Označimo $u = x + y$ i $v = x \oplus y$. Tada je $f(u) = f(x + y) = f(x) +' f(y)$ i $f(v) = f(x \oplus y) = f(x) +'' f(y)$. Zbog $f(A) \subseteq B$ vrijedi $f(x), f(y) \in B$ pa iz činjenice da je $(B, +', \cdot')$ potpolje od $(D, +'', \cdot'')$ slijedi da je $f(x) +' f(y) = f(x) +'' f(y)$. Stoga je $f(u) = f(v)$ pa je $u = v$. Dakle, $x + y = x \oplus y$. Analogno se dokaže da je $x \cdot y = x * y$. Zaključujemo da je $(A, +, \cdot)$ potpolje od $(C, \oplus, *)$. □

Lema 3.3.2. *Neka su A i B skupovi te neka je $f : A \to B$ bijekcija. Pretpostavimo da je D skup takav da je $B \subseteq D$. Tada postoji skup C takav da je $A \subseteq C$ i bijekcija $g : C \to D$ takva da je $g(x) = f(x)$, za svaki $x \in A$.*

Dokaz. Definirajmo $A' = \{y \mid \exists x \text{ takav da je } (x, y) \in A\}$. Odaberimo z takav da $z \notin A'$. Tvrdimo da su skupovi $(D \setminus B) \times \{z\}$ i A disjunktni. Pretpostavimo suprotno, tj. da ovi skupovi nisu disjunktni. Dakle, postoji $a \in ((D \setminus B) \times \{z\}) \cap A$. Slijedi da je $a \in (D \setminus B) \times \{z\}$ i $a \in A$. Slijedi $a = (x, z)$, gdje je $x \in D \setminus B$. Stoga je $(x, z) \in A$ pa slijedi $z \in A'$. To je u kontradikciji s činjenicom da $z \notin A'$. Dakle, skupovi $(D \setminus B) \times \{z\}$ i A su disjunktni.

Definirajmo $C = ((D \setminus B) \times \{z\}) \cup A$. Definiramo funkciju $h : (D \setminus B) \times \{z\} \to D \setminus B$ na sljedeći način: $h(d, z) = d$. Ako su $x_1, x_2 \in (D \setminus B) \times \{z\}$ takvi da je $x_1 \neq x_2$, onda imamo $x_1 = (d_1, z)$ i $x_2 = (d_2, z)$ gdje su $d_1, d_2 \in D \setminus B$. Iz $x_1 \neq x_2$ slijedi $d_1 \neq d_2$, tj. $h(x_1) \neq h(x_2)$. Stoga je h injekcija. Ako je $d \in D \setminus B$, tada je $h(d, z) = d$ pa je očito h surjekcija. Dakle, h je bijekcija.

Definirajmo funkciju $g : C \to D$ na sljedeći način:

$$g(x) = \begin{cases} f(x), & x \in A \\ h(x), & x \in (D \setminus B) \times \{z\} \end{cases}$$

Očito je $g(x) = f(x)$ za svaki $x \in A$. Tvrdimo da je g bijekcija. Neka su $x_1, x_2 \in C$ takvi da je $x_1 \neq x_2$. Imamo nekoliko slučajeva:

1) $x_1 \in (D \setminus B) \times \{z\}$ i $x_2 \in A$. Tada je $g(x_1) = h(x_1) \in D \setminus B$ i $g(x_2) = f(x_2) \in B$ pa je očito $g(x_1) \neq g(x_2)$

2) $x_1 \in A$ i $x_2 \in (D \setminus B) \times \{z\}$. Analogno dobivamo $g(x_1) \neq g(x_2)$.

3) $x_1 \in A$ i $x_2 \in A$. Imamo $g(x_1) = f(x_1)$ i $g(x_2) = f(x_2)$, a $f(x_1) \neq f(x_2)$ jer je f injekcija. Stoga je $g(x_1) \neq g(x_2)$.

4) $x_1 \in (D \setminus B) \times \{z\}$ i $x_2 \in (D \setminus B) \times \{z\}$. Iz činjenice da je h injekcija slijedi da je $g(x_1) \neq g(x_2)$.

Zaključujemo: g je injekcija. Neka je $y \in D$. Promotrimo 2 slučaja:

1) $y \in D \setminus B$. Budući da je h surjekcija postoji $x \in (D \setminus B) \times \{z\}$ takav da je $y = h(x)$. Slijedi $y = g(x)$.

2) $y \in B$. Budući da je f surjekcija postoji $x \in A$ takav da je $y = f(x)$. Slijedi $y = g(x)$.

U oba slučaja postoji $x \in C$ takav da je $g(x) = y$. Prema tome g je surjekcija. Zaključujemo: g je bijekcija. □

Teorem 3.3.3. *Neka je* $(\mathbb{R}, +, \cdot, \leq)$ *polje realnih brojeva. Tada postoji polje kompleksnih brojeva* $(\mathbb{C}, +', \cdot')$ *takvo da je* $(\mathbb{R}, +, \cdot)$ *realno potpolje od* $(\mathbb{C}, +', \cdot')$.

Dokaz. Prema teoremu 3.2.2 postoje polja $(C, +', \cdot')$ i $(R, +'', \cdot'')$ takva da je $(C, +', \cdot')$ polje kompleksnih brojeva, $(R, +'', \cdot'')$ njegovo realno potpolje te postoji funkcija $f : \mathbb{R} \to R$ takva da je f izomorfizam polja $(\mathbb{R}, +, \cdot)$ i $(R, +'', \cdot'')$. Posebno, f je bijekcija i vrijedi $R \subseteq C$. Prema lemi 3.3.2 postoji skup $\mathbb{C}$ takav da je $\mathbb{R} \subseteq \mathbb{C}$ te postoji bijekcija $g : \mathbb{C} \to C$ takva da je $g(x) = f(x)$, za svaki $x \in \mathbb{R}$. Uočimo da je $g(\mathbb{R}) \subseteq R$(naime ako je $x \in \mathbb{R}$, onda je $g(x) = f(x) \in R$).

Nadalje, ako su $x, y \in \mathbb{R}$ onda je

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

dakle, $g(x+y) = g(x)+''g(y)$. Analogno dobivamo da je $g(x \cdot y) = g(x) \cdot'' g(y)$. Prema propoziciji 3.3.1 postoje binarne operacije $\oplus$ i $*$ na $\mathbb{C}$ takve da vrijedi sljedeće:

1) $(\mathbb{C}, \oplus, *)$ je polje

2) g je izomorfizam polja $(\mathbb{C}, \oplus, *)$ i $(C, +', \cdot')$

3) $(\mathbb{R}, +, \cdot)$ je potpolje od $(\mathbb{C}, \oplus, *)$

Tvrdimo da je $(\mathbb{C}, \oplus, *)$ polje kompleksnih brojeva te da je $(\mathbb{R}, +, \cdot)$ njegovo realno potpolje. Znamo da je $(C, +', \cdot')$ polje kompleksnih brojeva te da je $(R, +'', \cdot'')$ njegovo realno potpolje. Stoga postoji $i \in C$ takav da je $i^2 = -1_C$ te da za svaki $w \in C$ postoje $u, v \in R$ takvi da je $w = u +' i \cdot' v$. Imamo $i \cdot' i = -1_C$ pa je $g^{-1}(i \cdot' i) = g^{-1}(-1_C)$. Koristeći lemu 3.2.3 i lemu 3.2.5 dobivamo $g^{-1}(i) * g^{-1}(i) = -1_{\mathbb{C}}$. Označimo $i_{\mathbb{C}} = g^{-1}(i)$. Dakle, $i_{\mathbb{C}} * i_{\mathbb{C}} = -1_C$. Neka je $z \in \mathbb{C}$. Želimo dokazati da postoje $x, y \in \mathbb{R}$ takvi da je $z = x \oplus i_{\mathbb{C}} * y$. Imamo $g(z) \in C$ pa postoje $u, v \in \mathbb{R}$ takvi da je $g(z) = u +' i \cdot' v$. Budući da je $f : \mathbb{R} \to R$ bijekcija postoje $x, y \in \mathbb{R}$ takvi da je $u = f(x)$ i $v = f(y)$. Koristeći činjenicu da je g^{-1} izomorfizam dobivamo:

$$z = g^{-1}(u +' i \cdot' v) = g^{-1}(f(x) +' i \cdot' f(y)) = g^{-1}(f(x)) \oplus g^{-1}(i) * g^{-1}(f(y)) = x \oplus i_{\mathbb{C}} * y.$$

Dakle, $z = x \oplus i_{\mathbb{C}} * y$.

Zaključak: $(\mathbb{C}, \oplus, *)$ je polje kompleksnih brojeva i $(\mathbb{R}, +, \cdot)$ je njegovo realno potpolje. □

Bibliografija

[1] S.Kurepa, *Matematička analiza 1*, Školska knjiga, Zagreb, 1997.

[2] B.Pavković, D.Veljan, *Elementarna matematika 1*, Tehnička knjiga, Zagreb, 1992.

Sažetak

Ovaj diplomski rad podijelili smo na tri poglavlja. U prvom poglavlju definiraju se osnovni pojmovi kao što su binarne relacije i operacije te grupe i prsteni. U drugom poglavlju smo se bavili skupovima brojeva; skupom prirodnih, cijelih i racionalnih brojeva te smo uveli pojam potpolja. U trećem smo poglavlju definirali polje kompleksnih brojeva te prikazali jedno proširenje polja realnih brojeva do polja kompleksnih brojeva.

Summary

This diploma thesis is divided into three chapters. In first chapter we define basic notions; binary relations and operations and also some basic algebraic structures; groups and rings. In second chapter we examine sets of numbers; natural numbers, integers and rational numbers and we define subfield. In third chapter we define field of complex numbers and we represent one extension of real numbers field to the field of complex numbers.

Životopis

Rođena sam 29. listopada 1990. godine u Zagrebu. Osnovnu školu Trnsko upisala sam 1997. godine. Nakon završetka osnovne škole 2005. godine, upisala sam XI.gimnaziju koju sam pohađala do 2009. godine kada sam upisala Prirodoslovno-matematički fakultet u Zagrebu preddiplomski sveučilišni studij Matematika; smjer: nastavnički. Nakon završetka preddiplomskog sveučilišnog studija stekla sam titulu sveučilišne prvostupnice edukacije matematike te 2016. godine upisujem diplomski sveučilišni studij Matematika; smjer:nastavnički.