Modeli brojeva

Bareta, Marija

Master's thesis / Diplomski rad

2024

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:217:726837

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2025-03-14**

Repository / Repozitorij:

Repository of the Faculty of Science - University of Zagreb

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Marija Bareta

MODELI BROJEVA

Diplomski rad

Voditelj rada:
prof. dr. sc. Zvonko Iljazović

Zagreb, rujan 2024.

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

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

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Mojim roditeljima, Anti i Jagodi. Hvala vam na strpljenju, povjerenju, podršci i savjetima tijekom mog studija.
Zahvaljujem mojim prijateljima bez kojih ne bih bila tu gdje sada jesam.
Zahvaljujem Ninu koji je svaki moj uspjeh i pad proživljavao kao vlastiti.
Posebna zahvala mom mentoru, prof. dr. sc. Zvonku Iljazoviću, na povjerenju, vodstvu i pomoći pri izradi ovoga rada.

Sadržaj

Sadržaj **iv**

Uvod **1**

1 Skupovi **3**
1.1 Uređeni par 4
1.2 Skup svih skupova 5
1.3 Unija i presjek skupova 6
1.4 Kartezijev produkt skupova 7

2 Relacije **9**
2.1 Funkcijske relacije 9
2.2 Injekcija 11
2.3 Surjekcija 12
2.4 Restrikcija funkcije 14
2.5 Razlika skupova 15

3 Peanov par **17**
3.1 Beskonačan skup 17
3.2 Postojanje Peanovog para 18

4 Skupoidi **21**
4.1 Uređeni paroid 22
4.2 Skupoid svih skupoida 23
4.3 Skup svih skupoida 23

5 Uređene algebarske strukture **25**
5.1 Monoid 26
5.2 Grupa 26
5.3 Prsten 27

5.4 Polje 28
5.5 Binarna relacija 29
5.6 Relacija uređaja 30
5.7 Uređena grupa 30
5.8 Uređeni prsten 31
5.9 Prirodni brojevi u uređenom prstenu 36
5.10 Uređeno polje 39
5.11 Uređen skup 41
5.12 Potpuno uređen skup 42
5.13 Potpuno uređeno polje 43

Bibliografija **45**

Uvod

Cilj ovog diplomskog rada jest različitim pristupima definirati pojam broja i to na precizan matematički način. Polazna točka za to će nam biti skupovi kao osnovni matematički objekt koji se ne definira. Stoga ćemo prvo dati neke činjenice iz elementarne teorije skupova. To je sadržaj prvog poglavlja u kojem govorimo o uređenim parovima, uniji i presjeku skupova, Kartezijevom produktu skupova te u kojem pokazujemo da ne postoji skup svih skupova.

U drugom poglavlju se bavimo relacijama i funkcijama te proučavamo neka svojstva tih pojmova.

Treće poglavlje posvećeno je beskonačnim skupovima, Peanovim parovima te egzistenciji Peanovog para.

U četvrtom poglavlju proučavamo pojam skupoida te, koristeći taj koncept, dokazujemo egzistenciju beskonačnog skupa.

U petom, zadnjem poglavlju, dajemo definicije nekih osnovnih algebarskih struktura te proučavamo uređene grupe, uređene prstene te potpuno uređena polja. U tom kontekstu se bavimo prirodnim brojevima u uređenom prstenu.

Poglavlje 1

Skupovi

Smatramo da su među objektima koje promatramo neki od njih skupovi te da neki objekti mogu biti elementi danog skupa.

Da je x **element skupa** S označavamo

$$x \in S.$$

Da x **nije element skupa** S označavamo

$$x \notin S.$$

Smatramo da je svaki skup u potpunosti **određen svojim elementima**, a što precizno govoreći znači sljedeće:
Ako su S i T skupovi, onda je $S = T$ ako i samo ako za svaki x vrijedi ekvivalencija

$$x \in S \Leftrightarrow x \in T.$$

Ako je a neki objekt, onda smatramo da postoji skup S čiji je **jedini element** a, to jest skup S takav da za svaki x vrijedi

$$x \in S \Leftrightarrow x = a.$$

Skup S s tim svojstvom označavamo $\{a\}$.

Nadalje, ako su a i b neki objekti, smatramo da postoji skup čiji su to jedini elementi i njega označavamo $\{a, b\}$.
Dakle, za svaki x vrijedi

$$x \in \{a, b\} \Leftrightarrow x = a \quad \text{ili} \quad x = b.$$

Analogno, za objekte a, b, c definiramo skup $\{a, b, c\}$ i tako dalje.

Prazan skup

Smatramo da postoji skup $\emptyset$ koji **nema niti jedan element**, to jest takav skup $\emptyset$ da za svaki x vrijedi

$$x \notin \emptyset.$$

Za takav $\emptyset$ kažemo da je **prazan skup**.

Podskup

Neka su S i T skupovi. Kažemo da je S **podskup** od T i pišemo $S \subseteq T$, ako za svaki x vrijedi implikacija

$$x \in S \Rightarrow x \in T.$$

Napomena 1.0.1. *Neka je S bilo koji skup. Tada je $\emptyset \subseteq S$. Naime, za svaki x implikacija $x \in \emptyset \Rightarrow x \in S$ vrijedi jer tvrdnja $x \in \emptyset$ nije istinita.*

Napomena 1.0.2. *Neka su S i T skupovi. Tada je očito*

$$S = T \text{ ako i samo ako je } S \subseteq T \text{ i } T \subseteq S.$$

Napomena 1.0.3. *Neka su A i B skupovi takvi da je $A \subseteq B$ te da je $A \neq B$. Tada postoji $x \in B$ takav da $x \notin A$.*

Naime, očito $B \nsubseteq A$ pa je jasno da takav x postoji.

1.1 Uređeni par

Za objekte a i b definiramo skup (a, b) sa $(a, b) = \{\{a\}, \{a, b\}\}$. Za (a, b) kažemo da je **uređeni par**.

Propozicija 1.1.1. *Neka su a, b, c i d objekti. Tada je*

$$(a, b) = (c, d) \text{ ako i samo ako je } a = c \text{ i } b = d.$$

Dokaz. $\boxed{\Leftarrow}$ Jasno je da $a = c$ i $b = d$ povlači $(a, b) = (c, d)$.

$\boxed{\Rightarrow}$ Obratno, pretpostavimo da je $(a, b) = (c, d)$.

Dakle,

$$\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}. \tag{1.1}$$

Stoga je $\{a\} \in \{\{c\}, \{c, d\}\}$ pa slijedi $\{a\} = \{c\}$ ili $\{a\} = \{c, d\}$.

U prvom slučaju je $a = c$, a u drugom iz $c \in \{c, d\}$ slijedi $c \in \{a\}$ pa je $a = c$. Prema tome, $a = c$.

Iz (1.1) slijedi

$$\{\{a\}, \{a, b\}\} = \{\{a\}, \{a, d\}\}. \tag{1.2}$$

Sada zaključujemo $\{a, b\} = \{a\}$ ili $\{a, b\} = \{a, d\}$.

Ako je $\{a, b\} = \{a\}$, onda je $a = b$ pa iz (1.2) slijedi da je $\{a, d\} = \{a\}$, dakle $d = a$, to jest $d = b$.

Ako je $\{a, b\} = \{a, d\}$, onda je $b = a$ ili $b = d$.

Ako je $b = a$, onda imamo $\{a\} = \{a, d\}$ pa je $d = a$, to jest $d = b$.

U svakom slučaju, $b = d$. □

1.2 Skup svih skupova

Primjer 1.2.1. *Pretpostavimo da postoji skup A čiji su elementi točno oni skupovi S takvi da $S \notin S$. Dakle,*

$$A = \{S \mid S \text{ skup i } S \notin S\}.$$

Na primjer, $\emptyset \notin \emptyset$ pa je $\emptyset \in A$.

Isto tako, $\{\emptyset\} \in A$. Naime, kada bi vrijedilo $\{\emptyset\} \in \{\emptyset\}$, onda bismo imali $\{\emptyset\} = \emptyset$, što je očito nemoguće.

Imamo da je A skup pa je $A \in A$ ili $A \notin A$.

Promotrimo prvo slučaj kada $A \in A$.
Iz definicije skupa A slijedi da $A \notin A$. Kontradikcija.

Promotrimo sada slučaj kada $A \notin A$.
Prema definiciji skupa A vrijedi da je $A \in A$, što je nemoguće.

U oba slučaja smo dobili kontradikciju pa zaključujemo da ***ne postoji*** *skup A s tim svojstvom.*

Prethodni primjer pokazuje da ne možemo uzeti neko svojstvo i definirati skup svih objekata s danim svojstvom. Naime, takav skup ne mora postojati.
Drugim riječima, **ako je P neko svojstvo, ne mora postojati skup** $\{x \mid x \text{ ima } P\}$.

No, postoji način kako možemo definirati skup svih objekata koji zadovoljavaju svojstvo P, a taj je da se **ograničimo na elemente nekog zadanog skupa**.

Naime, smatrat ćemo da ako su zadani skup S i svojstvo P, onda postoji skup koji se sastoji od svih $x \in S$ takvih da x ima svojstvo P, to jest da postoji skup

$$\{x \mid x \in S \text{ i } x \text{ ima svojstvo } P\}.$$

Ovaj skup označavamo i s $\{x \in S \mid x \text{ ima svojstvo } P\}$.

Primjer 1.2.2. *Ne postoji skup svih skupova.*

Pretpostavimo suprotno, to jest da postoji skup $\mathcal{S}$ koji se sastoji od svih skupova.
Tada, prema principu (aksiomu) kojeg smo upravo prihvatili, postoji skup $\{x \in \mathcal{S} \mid x \notin x\}$, to jest skup $\{S \in \mathcal{S} \mid S \notin S\}$. No u primjeru smo vidjeli da takav skup ne postoji.

Prema tome, ne postoji skup svih skupova.

Partitivni skup

Neka je S skup. Smatramo da postoji **skup čiji su elementi svi podskupovi** od S. Taj skup označavamo $\mathcal{P}(S)$ i nazivamo **partitivni skup** od S.
Dakle,

$$\mathcal{P}(S) = \{x \mid x \subseteq S\}.$$

Na primjer, imamo $\mathcal{P}(\emptyset) = \{\emptyset\}$, $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$.

1.3 Unija i presjek skupova

Ako su S i T skupovi, smatramo da postoji skup koji se sastoji od svih x takvih da je $x \in S$ ili $x \in T$. Taj skup nazivamo **unija skupova** S i T i označavamo $S \cup T$.
Dakle,

$$S \cup T = \{x \mid x \in S \text{ ili } x \in T\}.$$

Neka su S i T skupovi. Tada postoji skup svih x takvih da je $x \in S$ i $x \in T$, to jest skup

$$\{x \mid x \in S \text{ i } x \in T\}.$$

Naime, znamo da postoji skup $\{x \in S \mid x \in T\}$, a to je upravo skup kojeg smo tražili. Taj skup nazivamo **presjek skupova** S i T i označavamo sa $S \cap T$.

Napomena 1.3.1. *Neka su S i T skupovi te neka su $a \in S$ i $b \in T$.*
Imamo $a, b \in S \cup T$ pa je $\{a\} \subseteq S \cup T$ i $\{a, b\} \subseteq S \cup T$. To povlači da je $\{a\} \in \mathcal{P}(S \cup T)$ i $\{a, b\} \in \mathcal{P}(S \cup T)$, što znači da je $\{\{a\}, \{a, b\}\} \subseteq \mathcal{P}(S \cup T)$.

Zaključujemo da je $\{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(S \cup T))$. Dakle $(a, b) \in \mathcal{P}(\mathcal{P}(S \cup T))$.

1.4 Kartezijev produkt skupova

Propozicija 1.4.1. *Neka su S i T skupovi. Tada postoji* ***skup svih uređenih parova*** *(a, b) takvih da su $a \in S$ i $b \in T$. Drugim riječima, postoji skup*

$$\{x \mid \exists\, a \in S \text{ i } \exists\, b \in T \text{ takvi da je } x = (a, b)\}.$$

Dokaz. Znamo da postoji skup $\{x \in \mathcal{P}(\mathcal{P}(S \cup T)) \mid \exists\, a \in S \text{ i } \exists\, b \in T \text{ takvi da je } x = (a, b)\}$. Prema prethodnoj napomeni, ovo je upravo traženi skup. □

Za skup čija je egzistencija dokazana u prethodnoj propoziciji kažemo da je **Kartezijev produkt skupova** S i T te ga označavamo $S \times T$.

Dakle,

$$S \times T = \{x \in \mathcal{P}(\mathcal{P}(S \cup T)) \mid \exists\, a \in S \text{ i } \exists\, b \in T \text{ takvi da } x = (a, b)\}.$$

Kraće zapisano, $S \times T = \{(a, b) \mid a \in S, b \in T\}$.

Poglavlje 2

Relacije

Neka su S i T skupovi. Za skup čiji su elementi (neki) uređeni parovi (a, b), gdje su $a \in S$ i $b \in T$, kažemo da je **relacija** između S i T.
Drugim riječima, relacija između S i T je bilo koji podskup od $S \times T$.

Napomena 2.0.1. *Neka su S i T skupovi te neka su x i y objekti takvi da je $(x, y) \in S \times T$. Tada je*

$$x \in S \text{ i } y \in T.$$

Naime, iz $(x, y) \in S \times T$ slijedi da postoje $s \in S$ i $t \in T$ takvi da $(x, y) = (s, t)$, što povlači da je $x = s$ i $y = t$, dakle $x \in S$ i $y \in T$.

Neka su a, b i c neki objekti. Definiramo $(a, b, c) = ((a, b), c)$. Za (a, b, c) kažemo da je **uređena trojka**.
Uočimo sljedeće: Ako su a, b, c, a', b', c' objekti, onda je

$$(a, b, c) = (a', b', c') \Leftrightarrow a = a',\ b = b' \text{ i } c = c'.$$

Neka su a, b, c i d neki objekti. Definiramo $(a, b, c, d) = ((a, b, c), d)$. Za (a, b, c, d) kažemo da je **uređena četvorka**.
Ako su a, b, c, d, a', b', c' i d' objekti, onda je

$$(a, b, c, d) = (a', b'c', d') \Leftrightarrow a = a',\ b = b'\ c = c' \text{ i } d = d'.$$

2.1 Funkcijske relacije

Neka su S i T skupovi te neka je ρ relacija između S i T. Kažemo da je ρ **funkcijska relacija** između S i T ako za svaki $x \in S$ postoji jedinstveni $y \in T$ takav da je $(x, y) \in \rho$.

Primjer 2.1.1. *Neka je $S = \{u, v, w\}$ i $T = \{a, b, c\}$, pri čemu su u, v, w međusobno različiti te pri čemu su a, b, c također međusobno različiti. Neka su*

$\rho = \{(u, a), (v, a), (w, b)\}$,
$\rho' = \{(u, a), (v, b)\}$,
$\rho'' = \{(u, a), (u, b), (v, a), (w, c)\}$.

Uočimo da je ρ funkcijska relacija između S i T.

Nadalje, ρ' nije funkcijska relacija između S i T jer je $w \in S$, a ne postoji $y \in T$ takav da je $(w, y) \in \rho'$.

Također, ρ'' nije funkcijska relacija između S i T jer imamo $(u, a), (u, b) \in \rho''$ i $a \neq b$.

Uočimo da je ρ' funkcijska relacija između $\{u, v\}$ i T. Ujedno, ρ' je funkcijska relacija između $\{u, v\}$ i $\{a, b\}$.

Napomena 2.1.2. *Pretpostavimo da je ρ funkcijska relacija između S i T. Pretpostavimo da je T' skup, takav da je $T \subseteq T'$. Tada je ρ funkcijska relacija između S i T'.*

Naime, neka je $x \in S$. Znamo da postoji $y \in T$ takav da je $(x, y) \in \rho$, a zbog $T \subseteq T'$ imamo $y \in T'$.
Dakle, postoji $y \in T'$ takav da je $(x, y) \in \rho$.

Pretpostavimo da su $y, z \in T'$ takvi da je $(x, y) \in \rho$ i $(x, z) \in \rho$.
Budući da je ρ funkcijska relacija između S i T, imamo $\rho \subseteq S \times T$ pa slijedi $(x, y), (x, z) \in S \times T$. Iz napomene 2.0.1 slijedi $y, z \in T$ pa, iz činjenice da je ρ funkcijska relacija između S i T, slijedi da je $y = z$.

Definicija 2.1.3. *Neka su S i T skupovi te neka je ρ funkcijska relacija između S i T. Neka je $f = (S, T, \rho)$. Za f kažemo da je **funkcija** sa S u T i pišemo*

$$f : S \to T.$$

Ako je $x \in S$, onda sa $f(x)$ označavamo onaj (jedinstveni) $y \in T$ takav da je $(x, y) \in \rho$.

*Za S kažemo da je **domena** funkcije f, a za T kažemo da je **kodomena**. Za ρ kažemo da je **graf** od f.*

Napomena 2.1.4. *Neka je $f : S \to T$ funkcija, $f = (S, T, \rho)$. Tada je*

$$\rho = \{(x, f(x)) \mid x \in S\}. \tag{2.1}$$

Naime, neka je $(x, y) \in \rho$. *Zbog* $\rho \subseteq S \times T$ *imamo* $x \in S$ *i* $y \in T$ *pa zaključujemo da* $y = f(x)$.
Dakle, $(x, y) = (x, f(x))$ *te smo time dokazali* $\rho \subseteq \{(x, f(x)) \mid x \in S\}$.

Obratno, ako je $x \in S$, *onda je očito* $(x, f(x)) \in \rho$.

Prema tome, vrijedi jednakost (2.1).

Propozicija 2.1.5. *Neka su* $f : S \to T$ *i* $g : S' \to T'$ *funkcije. Tada je*

$$f = g \text{ ako i samo ako je } S = S',\ T = T' \text{ i } f(x) = g(x)$$

za svaki x *takav da je* $x \in S$ *i* $x \in S'$.

Dokaz. $\boxed{\Rightarrow}$ Vrijedi $f = (S, T, \rho)$ i $g = (S', T', \rho')$, gdje je ρ funkcijska relacija između S i T, a ρ' funkcijska relacija između S' i T'.

Ako je $f = g$, onda je $S = S'$, $T = T'$ i $\rho = \rho'$ pa je jasno da za svaki $x \in S$ vrijedi $f(x) = g(x)$.

$\boxed{\Leftarrow}$ Obratno, pretpostavimo da je $S = S'$, $T = T'$ i $f(x) = g(x)$ za svaki x takav da je $x \in S$ i $x \in S'$.

Prema napomeni 2.1.4 vrijedi $\rho = \{(x, f(x)) \mid x \in S\}$ i $\rho' = \{(x, g(x)) \mid x \in S'\}$ pa vidimo da je $\rho = \rho'$.

Stoga je $(S, T, \rho) = (S', T', \rho')$, to jest $f = g$. □

2.2 Injekcija

Definicija 2.2.1. *Za funkciju* $f : S \to T$ *kažemo da je* ***injekcija*** *ako za sve* $a, b \in S$ *takve da* $a \neq b$ *vrijedi* $f(a) \neq f(b)$.

Primjer 2.2.2. *Neka je* S *skup. Neka je* $\rho = \{u \in S \times S \mid u = (a, a) \text{ za neki } a \in S\}$.

Očito je $\rho \subseteq S \times S$. *Nadalje, jasno je da za svaki* $x \in S$ *postoji jedinstveni* $y \in S$ *takav da je* $(x, y) \in \rho$. *Prema tome,* ρ *je* ***funkcijska relacija*** *između* S *i* S.

Neka je $f = (S, S, \rho)$. *Tada je* f *funkcija sa* S *u* S *te za svaki* $x \in S$ *vrijedi*

$$f(x) = x.$$

Za funkciju f kažemo da je ***identiteta*** *na S. Uočimo da je f injekcija.*

Prethodni primjer pokazuje da za svaki skup S postoji funkcija sa S u S. Funkciju f iz prethodnog primjera kraće možemo definirati tako da naprosto kažemo: neka je $f\colon S \to S$ funkcija definirana s $f(x) = x$, za svaki $x \in S$.

Primjer 2.2.3. *Neka su S i T skupovi. Pretpostavimo da je T neprazan skup. Odaberimo neki $y_0 \in T$. Neka je*

$$\rho = \{u \in S \times T \mid \exists\, a \in S \text{ takav da je } u = (a, y_0)\}.$$

Očito je $\rho \subseteq S \times T$. Za svaki $x \in S$ vrijedi $(x, y_0) \in \rho$.

S druge strane, ako za $x \in S$ i $y \in T$ vrijedi $(x, y) \in \rho$, onda postoji $a \in S$ takav da je $(x, y) = (a, y_0)$, što povlači da je $y = y_0$. Prema tome, za svaki $x \in S$ postoji jedinstveni $y \in T$ takav da je $(x, y) \in \rho$.

Slijedi da je ρ funkcijska relacija između S i T.

Neka je $f = (S, T, \rho)$. Tada je f funkcija sa S u T takva da za svaki $x \in S$ vrijedi

$$f(x) = y_0.$$

Ovako definiranu funkciju f zovemo ***konstantna funkcija*** *sa S u T.*

Pretpostavimo da postoje $a, b \in S$ takvi da $a \neq b$. Tada funkcija f nije injekcija (jer je $f(a) = f(b)$, $a \neq b$).

S druge strane, ako ne postoje $a, b \in S$ takvi da $a \neq b$, onda je f očito injekcija.

2.3 Surjekcija

Neka je $f\colon S \to T$ funkcija. Kažemo da je f **surjekcija** ako za svaki $y \in T$ postoji $x \in S$ takav da je $f(x) = y$.

Slika funkcije

Neka je $f\colon S \to T$ funkcija. Definiramo

$$\operatorname{Im} f = \{y \in T \mid \exists\, x \in S \text{ takav da je } y = f(x)\}.$$

Dakle, $\operatorname{Im} f = \{f(x) \mid x \in S\}$.

Za svaki $\operatorname{Im} f$ kažemo da je **slika funkcije** f. Očito je $\operatorname{Im} f \subseteq T$.

Napomena 2.3.1. *Neka je $f\colon S \to T$ funkcija. Tada je f surjekcija ako i samo ako je* $\operatorname{Im} f = T$.

Naime, ako je f surjekcija, onda za svaki $y \in T$ postoji $x \in S$ takav da je $y = f(x)$. Dakle za svaki $y \in T$ vrijedi $y \in \operatorname{Im} f$, to jest $T \subseteq \operatorname{Im} f$. Znamo da uvijek vrijedi $\operatorname{Im} f \subseteq T$, *pa slijedi* $\operatorname{Im} f = T$.

Obratno, ako je $\operatorname{Im} f = T$, *onda je $T \subseteq \operatorname{Im} f$ pa za svaki $y \in T$ vrijedi $y \in \operatorname{Im} f$, što znači da za svaki $y \in T$ postoji $x \in S$ takav da je $y = f(x)$.*

Prema tome, f je surjekcija.

Propozicija 2.3.2. *Neka je f funkcija, $f = (S, T, \rho)$. Pretpostavimo da je T' skup takav da je* $\operatorname{Im} f \subseteq T'$. *Tada je (S, T', ρ) također funkcija.*

Dokaz. Dovoljno je dokazati da je ρ funkcijska relacija između S i T'.

Dokažimo prvo da je ρ relacija između S i T', to jest da je $\rho \subseteq S \times T'$.
Neka je $z \in \rho$. Znamo da je ρ funkcijska relacija između S i T (jer je f funkcija), dakle $\rho \subseteq S \times T$.
Slijedi $z \in S \times T$ pa postoje $x \in S$ i $y \in T$ takvi da je $z = (x, y)$. Imamo $(x, y) \in \rho$ pa vrijedi da je $y = f(x)$ (po definiciji od $f(x)$). Stoga je $y \in \operatorname{Im} f$, pa je $y \in T'$ (jer je prema pretpostavci propozicije $\operatorname{Im} f \subseteq T'$).
Stoga je $y \in \operatorname{Im} f$, pa je $y \in T'$ (jer je prema pretpostavci propozicije $\operatorname{Im} f \subseteq T'$).
Dakle $x \in S$ i $y \in T'$, pa je $(x, y) \in S \times T'$, to jest $z \in S \times T'$.

Time smo dokazali da je $\rho \subseteq S \times T'$.

Dokažimo da je ρ funkcijska relacija između S i T', odnosno da za svaki $x \in S$ postoji jedinstveni $y \in T$ takav da je $(x, y) \in \rho$.

Neka je $x \in S$. Iz činjenice da je ρ funkcijska relacija između S i T slijedi da postoji $y \in T$ takav da je $(x, y) \in \rho$. Stoga je $y = f(x)$, pa je $y \in \operatorname{Im} f$, a $\operatorname{Im} f \subseteq T'$, pa je $y \in T'$.

Time smo dokazali da postoji $y \in T'$ takav da je $(x, y) \in \rho$.

Pretpostavimo da su $y', y'' \in T'$ takvi da je $(x, y') \in \rho$ i $(x, y'') \in \rho$. Pošto je $\rho \subseteq S \times T$,

imamo da je $y' \in T$ i $y'' \in T$. Kako je ρ funkcijska relacija između S i T, vrijedi $y' = y''$.

Dakle, za svaki $x \in S$ postoji jedinstveni $y \in T'$ takav da je $(x, y) \in \rho$.

Prema tome, ρ je funkcijska relacija između S i T'. □

Napomena 2.3.3. *Uz pretpostavku i oznake iskaza prethodne propozicije, neka je* $g = (S, T', \rho)$. *Tada za svaki* $x \in S$ *vrijedi* $g(x) = f(x)$.

Naime, ako je $x \in S$, $(x, f(x)) \in \rho$, *a* $f(x) \in \operatorname{Im} f$ *povlači da je* $f(x) \in T'$. *Dakle,* $f(x) \in T'$ *i* $(x, f(x)) \in \rho$, *pa je* $g(x) = f(x)$.

Uočimo još da je $\operatorname{Im} g = \{g(x) \mid x \in S\} = \{f(x) \mid x \in S\} = \operatorname{Im} f$, *odnosno* $\operatorname{Im} g = \operatorname{Im} f$.

2.4 Restrikcija funkcije

Propozicija 2.4.1. *Neka je f funkcija,* $f = (S, T, \rho)$. *Neka je* $A \subseteq S$ *te neka je* $\rho' = \{(x, y) \in \rho \mid x \in A\}$. *Tada je* (A, T, ρ') *funkcija.*

Dokaz. Dovoljno je dokazati da je ρ' funkcijska relacija između A i T.

Dokažimo prvo da je ρ' relacija između A i T, to jest $\rho' \subseteq A \times T$.
Neka je $(x, y) \in \rho$ i $x \in A$.
Pošto je ρ funkcijska relacija između S i T slijedi da je $\rho \subseteq S \times T$ što povlači da je $x \in S$ i $y \in T$ (napomena 2.0.1). Dakle $x \in A$ i $y \in T$, pa je $(x, y) \in A \times T$.

Ovim smo pokazali da je ρ' relacija između A i T.

Neka je $x \in A$. Budući da je ρ funkcijska relacija između S i T te $x \in S$, znamo da postoji $y \in T$ takav da je $(x, y) \in \rho$. No, $x \in A$, pa je $(x, y) \in \rho'$.

Pretpostavimo da su $y', y'' \in T$ takvi da je $(x, y') \in \rho'$ i $(x, y'') \in \rho'$.
Iz definicije od ρ' vidimo da je $\rho' \subseteq \rho$ što povlači da je $(x, y') \in \rho$ i $(x, y'') \in \rho$. Iz činjenice da je ρ funkcijska relacija između S i T slijedi da je $y' = y''$.

Zaključak: Za svaki $x \in A$ postoji jedinstveni $y \in T$ takav da je $(x, y) \in \rho'$. Prema tome, ρ' je funkcijska relacija između A i T. □

Napomena 2.4.2. *Neka je f funkcija,* $f = (S, T, \rho)$. *Neka je* $A \subseteq S$ *te neka je* $\rho' = \{(x, y) \in \rho \mid x \in A\}$. *Označimo* $f|_A = (A, T, \rho')$. *Prema prethodnoj propoziciji* $f|_A$ *je funkcija.*

Imamo $f|_A : A \to T$. Neka je $x \in A$. Tada je $(x, (f|_A)(x)) \in \rho'$ pa zbog $\rho' \subseteq \rho$ vrijedi $(x, (f|_A)(x)) \in \rho$, pa slijedi da je $(f|_A)(x) = f(x)$.

Dakle, za svaki $x \in A$ vrijedi $(f|_A)(x) = f(x)$.

Za funkciju $f|_A$ kažemo da je **restrikcija** funkcije f na skup A.

2.5 Razlika skupova

Neka su S i T skupovi. Definiramo skup

$$S \setminus T = \{x \mid x \in S \text{ i } x \notin T\}.$$

Uočimo da ovako definiran skup postoji. Naime, možemo ga zapisati kao $\{x \in S \mid x \notin T\}$.

Za skup $S \setminus T$ kažemo da je **razlika skupova** S i T.

Napomena 2.5.1. *Neka su A, B i C skupovi takvi da je $A \subseteq B \cup C$. Tada je $A \setminus B \subseteq C$.*

Neka je $x \in A \setminus B$, tada imamo $x \in A$ i $x \notin B$.
Kako je $A \subseteq B \cup C$, vrijedi $x \in B \cup C$ pa, zbog $x \notin B$, slijedi da je $x \in C$.

Time smo dokazali da je $A \setminus B \subseteq C$.

Primjer 2.5.2. *Neka su S, A i B skupovi takvi da je $A \subseteq S$ i $B \subseteq S$. Pretpostavimo da je*

$$S \setminus A = S \setminus B. \tag{2.2}$$

Tada je $A = B$.

Neka je $x \in A$. Tada je očito $x \in S$. Pretpostavimo da $x \notin B$. Tada je $x \in S \setminus B$ pa iz (2.2) slijedi da je $x \in S \setminus A$, što povlači da $x \notin A$, kontradikcija.

Prema tome $x \in B$.

Time smo dokazali da $A \subseteq B$.

Analogno dobivamo $B \subseteq A$ pa slijedi da je $A = B$.

Uočimo da prethodni zaključak ne mora vrijediti ako koristimo pretpostavku da su A i B bilo kakvi skupovi.
Naime, ako su A, B bilo kakvi skupovi, onda je $\emptyset \setminus A = \emptyset$ i $\emptyset \setminus B = \emptyset$, dakle $\emptyset \setminus A = \emptyset \setminus B$, no očito A i B ne moraju biti jednaki.

Poglavlje 3

Peanov par

Definicija 3.0.1. *Neka je N skup te neka je $s\colon N \to N$ funkcija. Pretpostavimo da je s injekcija. Nadalje, pretpostavimo da postoji element od N kojeg ćemo označiti s $\mathbf{1}$ takav da vrijedi sljedeće:*

(i) $Ims = N \setminus \{\mathbf{1}\}$

(ii) Ako je $S \subseteq N$ takav da je $\mathbf{1} \in S$ te takav da za svaki $x \in S$ vrijedi $s(x) \in S$, onda je $S = N$.

*Tada za uređeni par (N, s) kažemo da je **Peanov par**.*

Uočimo da je element $\mathbf{1}$ skupa N s gornjim svojstvom jedinstven.
Naime, pretpostavimo da je $\mathbf{1}' \in N$ takav da je $\operatorname{Im} s = N \setminus \{\mathbf{1}'\}$. Tada je $N \setminus \{\mathbf{1}\} = N \setminus \{\mathbf{1}'\}$, a očito vrijedi $\{\mathbf{1}\} \subseteq N$ i $\{\mathbf{1}'\} \subseteq N$, pa iz prethodnog primjera slijedi da je $\{\mathbf{1}\} = \{\mathbf{1}'\}$, to jest $\mathbf{1} = \mathbf{1}'$.

Za $\mathbf{1}$ kažemo da je **jedinica** u Peanovom paru (N, s).

3.1 Beskonačan skup

Definicija 3.1.1. *Za skup S kažemo da je **beskonačan** ako postoji injekcija $f\colon S \to S$ takva da je* $\operatorname{Im} f \neq S$.

Primjer 3.1.2. *Prazan skup nije beskonačan.*

Naime, ako je $f\colon \emptyset \to \emptyset$ funkcija (uočimo da je $f = (\emptyset, \emptyset, \emptyset)$), onda je $\operatorname{Im} f = \emptyset$ pa je jasno, po definiciji, da $\emptyset$ nije beskonačan.

Primjer 3.1.3. *Neka je (N, s) Peanov par. Tada je N beskonačan skup.*

Naime, vrijedi da je $s\colon N \to N$ injekcija te da je $\operatorname{Im} s = N \setminus \{\mathbf{1}\}$, pri čemu je $\mathbf{1} \in N$. Jasno je da je $N \setminus \{\mathbf{1}\} \neq N$, stoga je $\operatorname{Im} s \neq N$.

Zaključujemo da je N beskonačan po definiciji.

Iz prethodnog primjera zaključujemo da vrijedi sljedeće:
Ako postoji Peanov par, onda postoji beskonačan skup.

Sada nam je cilj pokazati da vrijedi obrat prethodne tvrdnje, to jest da **ako postoji beskonačan skup, onda postoji Peanov par**.

Napomena 3.1.4. *Neka je S skup, neka je $f\colon S \to S$ funkcija te neka je $N \subseteq S$ takav da je $f(x) \in N$, za svaki $x \in N$.*

Definirajmo funkciju $g\colon N \to N$ s $g(x) = f(x)$, za svaki $x \in N$.
Uočimo da je $g(x) = (f|_N)(x)$, za svaki $x \in N$. No, funkcije $g\colon N \to N$ i $f|_N\colon N \to S$ općenito nisu jednake (jer je općenito $N \neq S$).

3.2 Postojanje Peanovog para

Teorem 3.2.1. *Neka je S beskonačan skup. Tada postoji Peanov par (N, s) takav da je $N \subseteq S$.*

Dokaz. Budući da je S beskonačan skup, postoji injekcija $f\colon S \to S$ takva da je

$$\operatorname{Im} f \neq S.$$

Očito je $\operatorname{Im} f \subseteq S$ pa iz napomene 1.0.3 slijedi da postoji $a \in S$ takav da

$$a \notin \operatorname{Im} f. \tag{3.1}$$

Neka je $T \subseteq S$. Kažemo da je T **induktivan skup** ako vrijedi sljedeće:

(i) $a \in T$,

(ii) $x \in T \Rightarrow f(x) \in T$.

Uočimo da postoji barem jedan induktivan skup. Naime, S je induktivan skup.

Definirajmo $N = \{x \in S \mid x \in T \text{ za svaki induktivan skup } T\}$. Uočimo da je $N \subseteq T$ za svaki induktivan skup T.

Tvrdimo da je N induktivan skup. Očito je $N \subseteq S$. Budući da je $a \in T$, za svaki induktivan skup T, vrijedi $a \in N$.

Neka je $x \in N$. Neka je T bilo koji induktivni skup. Tada je $x \in T$, pa je $f(x) \in T$. Stoga je prema definiciji od N, $f(x) \in N$.

Prema tome, za svaki $x \in N$ vrijedi $f(x) \in N$. Time smo dobili da je N induktivan skup.

Definirajmo funkciju $s\colon N \to N$ sa $s(x) = f(x)$, za svaki $x \in N$ (znamo da je $f(x) \in N$ za svaki $x \in N$). Tvrdimo da je (N, s) Peanov par. Budući da je f injekcija, slijedi da je i s injekcija.

Pretpostavmo da je $T \subseteq N$ takav da je $a \in T$ te takav da za svaki $x \in T$ vrijedi $s(x) \in T$. Želimo dokazati da je $T = N$.
Uočimo da je $T \subseteq S$ te da za svaki $x \in T$ vrijedi $f(x) \in T$.

Prema tome, T je induktivan skup.

Slijedi $N \subseteq T$ (prema definiciji od N). Ovo, zajedno s $T \subseteq N$, povlači da je $T = N$.

Zaključak: Za svaki podskup T od N, takav da je $a \in T$ te takav da je $s(x) \in T$, za svaki $x \in T$, vrijedi $T = N$.

Ostaje još dokazati da je $\operatorname{Im} s = N \setminus \{a\}$.

Očito je $\operatorname{Im} s \subseteq N$. Pretpostavimo da je $a \in \operatorname{Im} s$. Tada postoji $x \in N$ takav da je $s(x) = a$, dakle $f(x) = a$, što znači da je $a \in \operatorname{Im} f$, što je u kontradikciji s (3.1).
Prema tome, $a \notin \operatorname{Im} s$, pa je

$$\operatorname{Im} s \subseteq N \setminus \{a\}. \tag{3.2}$$

Da bismo dokazali obratnu inkluziju, to jest da je $N \setminus \{a\} \subseteq \operatorname{Im} f$, definiramo skup

$$T = \{a\} \cup \operatorname{Im} f.$$

Očito je $T \subseteq N$. Jasno je da je $a \in T$.

Pretpostavimo da je $x \in T$. Želimo dokazati da je $s(x) \in T$.
Iz $x \in T$ slijedi $x \in N$, stoga je $s(x) \in \operatorname{Im} s$. Po definiciji od T slijedi da je $s(x) \in T$. Prema dokazanom, vrijedi $N = T$. Dakle, $N = \{a\} \cup \operatorname{Im} s$.

Iz napomene 2.5.1 slijedi da je $N \setminus \{a\} \subseteq \operatorname{Im} s$. Iz ovoga i (3.2) slijedi $N \setminus \{a\} = \operatorname{Im} s$.

Zaključak: (N, s) je Peanov par. $\square$

Poglavlje 4

Skupoidi

Cilj nam je sada dokazati da postoji beskonačan skup i to uz pretpostavku postojanja takozvanih skupoida.

Naime, smatramo da su među objektima koje promatramo neki od njih skupoidi te da jedan skupoid može biti element drugog skupoida.

Da je x **element skupoida** S označavamo

$$x \lessdot S.$$

Da x **nije element skupoida** S označavamo

$$x \not\lessdot S.$$

Smatramo da je svaki skupoid u potpunosti **određen svojim elementima**, a što precizno govoreći znači sljedeće:
Ako su S i T skupoidi, onda je $S = T$ ako i samo ako za svaki x vrijedi ekvivalencija

$$x \lessdot S \Leftrightarrow x \lessdot T.$$

Ako je a neki skupoid, onda smatramo da postoji skupoid S čiji je **jedini element** a, to jest takav skupoid S da za svaki x vrijedi

$$x \lessdot S \Leftrightarrow x = a.$$

Skupoid s tim svojstvom označavamo $\lfloor a \rceil$.

Nadalje, ako su a i b neki skupoidi, smatramo da postoji skupoid čiji su to jedini elementi i njega označavamo $\lfloor a, b \rceil$. Dakle, za svaki x vrijedi

$$x \lessdot \lfloor a, b \rceil \Leftrightarrow x = a \text{ ili } x = b.$$

Analogno, za skupoide a, b, c definiramo skupoid $\lfloor a, b, c \rceil$ i tako dalje.

Prazan skupoid

Smatramo da postoji skupoid $\oint$ koji **nema niti jedan element**, to jest takav da za svaki x vrijedi $x \not< \oint$.

Za takav $\oint$ kažemo da je **prazan skupoid**.

Podskupoid

Neka su S i T skupoidi. Kažemo da je S **podskupoid** od T i pišemo $S \Subset T$, ako za svaki x vrijedi implikacija

$$x \lessdot S \Rightarrow x \lessdot T.$$

Da S **nije podskupoid** od T pišemo $S \not\Subset T$.

Uočimo da je $\oint \Subset S$ za svaki skupoid S.

Nadalje, kao i u slučaju skupova, imamo da za dva skupoida S i T vrijedi da je $S = T$ ako i samo ako $S \Subset T$ i $T \Subset S$.

4.1 Uređeni paroid

Za skupoide a i b definiramo skupoid $< a, b >= \lfloor \lfloor a \rceil, \lfloor a, b \rceil \rceil$. Za $< a, b >$ kažemo da je **uređeni paroid**.

Posve analogno, kao u slučaju uređenih parova (propozicija 1.1.1), dokazujemo sljedeću propoziciju:

Propozicija 4.1.1. *Neka su a, b, c i d skupoidi. Tada je*

$$< a, b >=< c, d > \text{ ako i samo ako je } a = c \text{ i } b = d.$$

4.2 Skupoid svih skupoida

Kao i kod skupova, smatramo da za zadani skupoid S i svojstvo P postoji skupoid svih $x \lessdot S$ takav da x ima svojstvo P. Taj skupoid označavamo s

$$\lfloor x \lessdot S \mid x \text{ ima svojstvo } P \rceil.$$

Primjer 4.2.1. *Kao i u slučaju skupova, sada pokazujemo da* ***ne postoji*** *skupoid svih skupoida.*

Pretpostavimo da je S skupoid svih skupoida.
Definirajmo $A = \lfloor x \lessdot S \mid x \not\lessdot x \rceil$ *(uočimo da skupoid A možemo ovako definirati prema prethodnon uvedenom pravilu). Jasno je da je* $A \lessdot S$.

Ako vrijedi $A \not\lessdot A$*, tada iz definicije od A slijedi* $A \lessdot A$*, što je nemoguće.*

S druge strane, ako vrijedi $A \lessdot A$*, onda opet imamo kontradikciju, jer prema definiciji od A dobivamo* $A \not\lessdot A$.

U svakom slučaju dolazimo do kontradikcije. Prema tome, ne postoji skupoid svih skupoida.

Partitivni skupoid

Ako je S skupoid, smatramo da postoji **skupoid svih podskupoida** od S. Taj skupoid označavamo $\Pi(S)$ i nazivamo **partitivni skupoid** od S. Dakle,

$$\Pi(S) = \lfloor x \mid x \Subset S \rceil.$$

4.3 Skup svih skupoida

Vidjeli smo da ne postoji skup svih skupova, kao ni skupoid svih skupoida. No, smatramo (i tu činjenicu uvodimo kao aksiom) da postoji **skup svih skupoida**. Taj skup označavamo sa Ⓢ.

Teorem 4.3.1. *Skup Ⓢ je beskonačan.*

Dokaz. Definirajmo funkciju $f\colon Ⓢ \to Ⓢ$ takvu da je $f(A) = \Pi(A)$, za svaki $A \in Ⓢ$.

Dokažimo da je f injekcija.
Neka su $A, B \in \textcircled{s}$ takvi da je $A \neq B$. Pretpostavimo da je $f(A) = f(B)$, to jest

$$\Pi(A) = \Pi(B). \tag{4.1}$$

Iz $A \neq B$ slijedi da je $A \notin B$ ili $B \notin A$.

Pretpostavimo da $A \notin B$. Tada postoji $x \lessdot A$ takav da

$$x \not\lessdot B. \tag{4.2}$$

Iz $x \lessdot A$ slijedi $\lfloor x \rceil \Subset A$, to jest $\lfloor x \rceil \lessdot \Pi(A)$, pa iz (4.1) slijedi $\lfloor x \rceil \lessdot \Pi(B)$, to jest $\lfloor x \rceil \Subset B$, pa je $x \lessdot B$, što je u kontradikciji s (4.2).

Dakle, $A \notin B$ vodi na kontradikciju.

Analogno vidimo da $B \notin A$ vodi na kontradikciju.

Zaključak: $f(A) \neq f(B)$. Prema tome, f je injekcija.

Dokažimo da je $\operatorname{Im} f \neq \textcircled{s}$.
Neka je $A \in \textcircled{s}$. Tada je $\oint \Subset A$, odnosno $\oint \lessdot \Pi(A)$, što povlači da je $\Pi(A) \neq \oint$. To znači da je $\oint \neq f(A)$ za svaki $A \in \textcircled{s}$.

Dakle, $\oint \in \textcircled{s}$ i $\oint \notin \operatorname{Im} f$, stoga $\operatorname{Im} f \neq \textcircled{s}$.

Time smo dokazali da je $\textcircled{s}$ beskonačan skup. $\square$

Poglavlje 5

Uređene algebarske strukture

Neka je P skup te neka je $f\colon P \times P \to P$ funkcija. Tada za f kažemo da je **binarna operacija** na skupu P.
Binarnu operaciju obično označavamo s $\bullet, +, *$ i slično.

Napomena 5.0.1. *Pretpostavimo da je $\bullet$ binarna operacija na skupu P te da je $\bullet$ ujedno binarna operacija na skupu R. Tada je $P = R$.*

Naime, vrijedi $\bullet = (P \times P, P, \sigma)$, za neki σ te ujedno $\bullet = (R \times R, R, \sigma')$, za neki σ', dakle $(P \times P, P, \sigma) = (R \times R, R, \sigma')$ pa je $P = R$.

Neka je $\bullet$ binarna operacija na skupu P. Dakle,

$$\bullet\colon P \times P \to P.$$

Za $x, y \in P$ umjesto $\bullet(x, y)$ pišemo i $x \bullet y$.

Za binarnu operaciju $\bullet$ na skupu P kažemo da je **asocijativna** ako za sve $x, y, z \in P$ vrijedi

$$x \bullet (y \bullet z) = (x \bullet y) \bullet z.$$

Napomena 5.0.2. *Da je binarna operacija $\bullet$ na skupu P asocijativna znači da za sve $x, y, z \in P$ vrijedi*

$$\bullet(x, \bullet(y, z)) = \bullet(\bullet(x, y), z).$$

Uočimo da je ovu činjenicu ipak jednostavnije izreći kao što smo to napravili u definiciji, dakle koristeći zapis $x \bullet y$ umjesto $\bullet(x, y)$.

Neka je $\bullet$ binarna operacija na skupu P. Pretpostavimo da je $e \in P$ takav da je $e \bullet x = x$ i $x \bullet e = x$ za svaki $x \in P$. Tada za e kažemo da je **neutralni element** s obzirom na $\bullet$.

Napomena 5.0.3. *Neka je $\bullet$ binarna operacija na skupu P. Tada je neutralni element s obzirom na $\bullet$, ako postoji, jedinstven.*

Naime, pretpostavimo da su e i f neutralni elementi s obzirom na $\bullet$. Tada za svaki $x \in P$ vrijedi $e \bullet x = x$ pa posebno imamo $e \bullet f = f$.

Isto tako, za svaki $x \in P$ vrijedi $x \bullet f = x$, pa je posebno $e \bullet f = e$.

Zaključujemo da je $e = f$.

5.1 Monoid

Definicija 5.1.1. *Neka je $\bullet$ binarna operacija na skupu P. Pretpostavimo da je $\bullet$ asocijativna binarna operacija te da postoji neutralni element s obzirom na $\bullet$. Tada za uređeni par $(P, \bullet)$ kažemo da je **monoid**.*
Za neutralni element s obzirom na $\bullet$ kažemo da je neutralni element u $(P, \bullet)$.

Neka je $(P, \bullet)$ monoid. Neka je e neutralni element u tom monoidu. Neka je $x \in P$. Za $y \in P$ kažemo da je **inverzni element** od x u $(P, \bullet)$ ako vrijedi

$$x \bullet y = e \quad \text{i} \quad y \bullet x = e.$$

Uočimo: ako je y inverzni element od x u $(P, \bullet)$, onda je x inverzni element od y u $(P, \bullet)$.

Napomena 5.1.2. *Neka je $(P, \bullet)$ monoid te $x \in P$. Tada je inverzni element od x, ako postoji, jedinstven.*

Naime, pretpostavimo da su y' i y'' inverzni elementi od x. Neka je e neutralni element u $(P, \bullet)$. Vrijedi: $y'' \bullet x = e$, pa je $(y'' \bullet x) \bullet y' = e \bullet y'$, to jest $y'' \bullet (x \bullet y') = y'$, odnosno $y'' \bullet e = y'$.

Slijedi $y'' = y'$.

Neka je $(P, \bullet)$ monoid. Neutralni element u $(P, \bullet)$ obično ćemo označavati s e. Za $x \in P$, inverzni element od x u $(P, \bullet)$, ako postoji, obično ćemo označavati sa x^{-1}.

5.2 Grupa

Definicija 5.2.1. *Neka je $(P, \bullet)$ monoid. Kažemo da je $(P, \bullet)$ **grupa** ako za svaki $x \in P$ postoji inverzni element od x u $(P, \bullet)$.*

Za binarnu operaciju $\bullet$ na skupu P kažemo da je **komutativna** ako za sve $x, y \in P$ vrijedi

$$x \bullet y = y \bullet x.$$

Definicija 5.2.2. *Za grupu $(P, \bullet)$ kažemo da je komutativna ili **Abelova** ako je $\bullet$ komutativna binarna operacija.*

Komutativnu binarnu operaciju obično označavamo s $+$.

Nadalje, ako je $(P, +)$ Abelova grupa, neutralni element u $(P, +)$ ćemo označavati s 0, a inverzni element od $x \in P$ ćemo označavati s $-x$. Dakle, za svaki $x \in P$ vrijedi

$$x + (-x) = 0 \quad \text{i} \quad (-x) + x = 0.$$

5.3 Prsten

Definicija 5.3.1. *Neka je $(P, +)$ Abelova grupa. Pretpostavimo da je $\bullet$ binarna operacija na P koja je asocijativna te takva da za sve $x, y, z \in P$ vrijedi*

$$x \bullet (y + z) = x \bullet y + x \bullet z \quad i \quad (y + z) \bullet x = y \bullet x + z \bullet x.$$

Pri tome, pod $x \bullet y + x \bullet z$ podrazumijevamo $(x \bullet y) + (x \bullet z)$ (to jest, koristimo standardni dogovor da "množenje" ima prioritet nad "zbrajanjem").

*Tada za uređenu trojku $(P, +, \bullet)$ kažemo da je **prsten**.*

Za prsten $(P, +, \bullet)$ kažemo da je **komutativan** ako je $\bullet$ komutativna binarna operacija.

Definicija 5.3.2. *Za prsten $(P, +, \bullet)$ kažemo da je **prsten s jedinicom** ako postoji neutralni element za $\bullet$. U tom slučaju, taj neutralni element obično označavamo s 1 i nazivamo jedinica u prstenu $(P, +, \bullet)$.*

Napomena 5.3.3. *Neka je $(P, \bullet)$ grupa te neka su $a, b, c \in P$ takvi da je*

$$a \bullet b = a \bullet c.$$

Tada je $b = c$.

Naime, iz $a \bullet b = a \bullet c$ slijedi $a^{-1} \bullet (a \bullet b) = a^{-1} \bullet (a \bullet c)$, pa je $(a^{-1} \bullet a) \bullet b = (a^{-1} \bullet a) \bullet c$, to jest $e \bullet b = e \bullet c$, dakle $b = c$.

Analogno dobivamo da $b \bullet a = c \bullet a$ povlači $b = c$.

Napomena 5.3.4. *Neka je* $(P, +, \bullet)$ *prsten. Neka je* $x \in P$. *Tada je*

$$x \bullet 0 = 0 \quad i \quad 0 \bullet x = 0.$$

Naime, imamo $x \bullet 0 = x \bullet (0 + 0) = x \bullet 0 + x \bullet 0$. *Dakle,* $x \bullet 0 = x \bullet 0 + x \bullet 0$, *to jest* $0 + x \bullet 0 = x \bullet 0 + x \bullet 0$ *pa iz prethodne napomene slijedi da je* $0 = x \bullet 0$.

Analogno dobivamo da je $0 \bullet x = 0$.

Napomena 5.3.5. *Neka je* $(P, +, \bullet)$ *prsten s jedinicom takav da je* $0 = 1$. *Tada je* $P = \{0\}$.

Da bismo ovo dokazali uzmimo $x \in P$. *Koristeći prethodnu napomenu, dobivamo*

$$x = 1 \bullet x = 0 \bullet x = 0.$$

Dakle $x = 0$. *Prema tome,* $P = \{0\}$.

Za prsten $(P, +, \bullet)$ kažemo da je **trivijalan** ako je P jednočlan skup. Inače za prsten kažemo da je netrivijalan.

Prema napomeni 5.3.5 imamo da u netrivijalnom prstenu s jedinicom vrijedi $0 \neq 1$.

Napomena 5.3.6. *Neka je* $(P, +, \bullet)$ *netrivijalan prsten. Tada* $(P, \bullet)$ *nije grupa.*

Naime, kada bi $(P, \bullet)$ *bila grupa, postojao bi neutralan element za* $\bullet$, *dakle* $(P, +, \bullet)$ *bi bio prsten s jedinicom.*

Budući da je netrivijalan, vrijedilo bi $0 \neq 1$.

Nadalje, svaki element od P *imao bi inverzni element u* $(P, \bullet)$, *posebno, element* 0 *bi imao inverzni element. Dakle postojao bi* $y \in P$ *takav da je* $0 \bullet y = 1$, *pa bi iz napomene 5.3.4 slijedilo* $0 = 1$, *što je kontradikcija.*

5.4 Polje

Definicija 5.4.1. *Neka je* $(P, +, \bullet)$ *netrivijalan komutativan prsten s jedinicom takav da za svaki* $x \in P$, *sa svojstvom da je* $x \neq 0$, *postoji* $y \in P$ *takav da je* $x \bullet y = 1$. *Tada za* $(P, +, \bullet)$ *kažemo da je* ***polje***.

Neka je $(P, +, \bullet)$ polje te neka je $x \in P$ takav da $x \neq 0$. Tada postoji $y \in P$ takav da je $x \bullet y = 1$. Budući da je prsten $(P, +, \bullet)$ komutativan, vrijedi $y \bullet x = 1$. To znači da je y

inverzni element od x u monoidu $(P, \bullet)$ (y ćemo standardno označavati s x^{-1}). Uočimo da $y \neq 0$, u suprotnom bi prema napomeni 5.3.4 vrijedilo $x \bullet y = 0$ pa bi slijedilo $0 = 1$ što je nemoguće jer u netrivijalnom prstenu s jedinicom vrijedi $0 \neq 1$.

Napomena 5.4.2. *Neka je $(P, +, \bullet)$ polje te neka su $x, y \in P$ takvi da je $x \neq 0$ i $y \neq 0$. Tada je $x \bullet y \neq 0$.*

Naime, kada bi vrijedilo $x \bullet y = 0$, imali bismo $x^{-1} \bullet (x \bullet y) = x^{-1} \bullet 0$, to jest $(x^{-1} \bullet x) \bullet y = 0$ pa bi slijedilo $1 \bullet y = 0$, dakle $y = 0$ što je u kontradikciji s $y \neq 0$.

Stoga, možemo definirati binarnu operaciju $*$ na $P \setminus \{0\}$ s $x * y = x \bullet y$ za $x, y \in P \setminus \{0\}$.

Da je $*$ asocijativna binarna operacija slijedi iz činjenice da je $\bullet$ asocijativna binarna operacija. Nadalje, budući da je prsten $(P, +, \bullet)$ netrivijalan, vrijedi $0 \neq 1$ pa je $1 \in P \setminus \{0\}$. Očito je 1 neutralni element za operaciju $*$. Prema tome, $(P \setminus \{0\}, *)$ je monoid. Za svaki $x \in P \setminus \{0\}$ vrijedi $x^{-1} \in P \setminus \{0\}$ te je $x * x^{-1} = 1 = x^{-1} * x$. Prema tome, x^{-1} je inverzni element od x u monoidu $(P \setminus \{0\}, *)$.

Zaključujemo da je $(P \setminus \{0\}, *)$ grupa.

5.5 Binarna relacija

Neka je S skup. Za relaciju između S i S kažemo da je **binarna relacija** na S. Dakle, ako je ρ binarna relacija na S, onda je $\rho \subseteq S \times S$.

Ako je ρ binarna relacija na S te ako su $x, y \in S$, onda činjenicu da je $(x, y) \in \rho$ označavamo i sa $x\rho y$.

Neka je ρ binarna relacija na skupu S. Kažemo da je ρ **refleksivna binarna relacija** na S ako za svaki $x \in S$ vrijedi

$$x\rho x.$$

Nadalje, kažemo da je ρ **simetrična binarna relacija** na S ako za sve $x, y \in S$ takve da je $x\rho y$ vrijedi

$$y\rho x.$$

Kažemo da je ρ **antisimetrična binarna relacija** na S ako za sve $x, y \in S$ takve da je $x\rho y$ i $y\rho x$ vrijedi

$$x = y.$$

Za ρ kažemo da je **tranzitivna binarna relacija** na S ako za sve $x, y, z \in S$ takve da je $x\rho y$ i $y\rho z$ vrijedi

$$x\rho z.$$

5.6 Relacija uređaja

Pretpostavimo da je ρ binarna relacija na skupu S koja je refleksivna, antisimetrična i tranzitivna. Nadalje, pretpostavimo da za sve $x, y \in S$ vrijedi $x\rho y$ ili $y\rho x$. Tada za ρ kažemo da je **relacija uređaja** na S ili, naprosto, da je ρ uređaj na S.

Uređaj na skupu S obično ćemo označavati sa $\leq$. Dakle, ako je $\leq$ uređaj na S onda za sve $x, y, z \in S$ vrijedi

(i) $x \leq x$,

(ii) $x \leq y$ i $y \leq x \Rightarrow x = y$,

(iii) $x \leq y$ i $y \leq z \Rightarrow x \leq z$,

(iv) $x \leq y$ ili $y \leq x$.

5.7 Uređena grupa

Neka je $(P, +)$ Abelova grupa te neka je $\leq$ uređaj na P. Pretpostavimo da za sve $x, y, z \in P$ vrijedi sljedeća implikacija:

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

Tada, za uređenu trojku $(P, +, \leq)$ kažemo da je **uređena grupa**.

Propozicija 5.7.1. *Neka je $(P, +, \leq)$ uređena grupa.*

(i) Neka su $x, y, z \in P$. Tada vrijedi ekvivalencija

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

(ii) Neka su $x, y, y', y' \in P$ takvi da je $x \leq y$ i $x' \leq y'$. Tada vrijedi

$$x + x' \leq y + y'.$$

Dokaz. (i) Implikacija $x \leq y \Rightarrow x + z \leq y + z$ vrijedi prema definiciji uređene grupe.

Obratno, pretpostavimo $x + z \leq y + z$. Tada je $(x + z) + (-z) \leq (y + z) + (-z)$ pa je $x \leq y$. Dakle, tvrdnja vrijedi.

(ii) Iz $x \leq y$ slijedi $x + x' \leq y + x'$. S druge strane, iz $x' \leq y'$ slijedi $y + x' \leq y + y'$. Sada tranzitivnost od $\leq$ povlači da je $x + x' \leq y + y'$.

□

Neka je $\leq$ uređaj na skupu S. Za $x, y \in S$ ćemo pisati $x < y$ ako je $x \leq y$ i $x \neq y$.

Napomena 5.7.2. *Neka je $\leq$ uređaj na skupu S. Pretpostavimo da su $x, y, z \in S$ takvi da je $x < y$ i $y \leq z$. Tada je $x < z$.*

Naime, vrijedi $x \leq y$ pa iz $y \leq z$ dobivamo $x \leq z$.

Treba još dokazati da je $x \neq z$.
Pretpostavimo suprotno, to jest $x = z$. Tada iz $y \leq z$ slijedi $y \leq x$ što, zajedno s $x \leq y$, daje $x = y$. No, ovo je u kontradikciji s $x < y$. Prema tome, $x \neq z$ pa je $x < z$.

Napomena 5.7.3. *Neka je $\leq$ uređaj na skupu S. Slično kao i u prethodnoj napomeni vidimo da vrijedi sljedeće: ako su $x, y, z \in S$ takvi da je $x \leq y$ i $y < z$, onda je $x < z$.*

Napomena 5.7.4. *Iz napomene 5.7.2, ili napomene 5.7.3, dobivamo sljedeći zaključak: ako je $\leq$ uređaj na skupu S te ako su $x, y, z \in S$ takvi da je $x < y$ i $y < z$, onda je $x < z$.*

Propozicija 5.7.5. *Neka je $(P, +, \leq)$ uređena grupa. Neka su $x, y, z \in P$ takvi da je $x < y$. Tada je $x + z < y + z$.*

Dokaz. Vrijedi $x \leq y$ pa je $x + z \leq y + z$.

Ostaje još dokazati da je $x + z \neq y + z$.
Pretpostavimo suprotno, to jest $x + z = y + z$. Iz napomene 5.3.3 slijedi $x = y$, a to je u kontradikciji s $x < y$. Prema tome, $x + z \neq y + z$ pa je $x + z < y + z$. □

Korolar 5.7.6. *Neka je $(P, +, \leq)$ uređena grupa te neka su $x, y, z \in P$ takvi da je $x+z < y+z$. Tada je $x < y$.*

Dokaz. Prethodnu propoziciju možemo primjeniti na $x + z, y + z$ i $-z$ pa iz $x + z < y + z$ slijedi $(x + z) + (-z) < (y + z) + (-z)$ pa je $x < y$. □

5.8 Uređeni prsten

Definicija 5.8.1. *Neka je $(P, +, \bullet)$ komutativan prsten s jedinicom. Pretpostavimo da je $\leq$ uređaj na P takav da je $(P, +, \leq)$ uređena grupa te takav da za sve $x, y \in P$ vrijedi sljedeća implikacija:*

$$0 \leq x \text{ i } 0 \leq y \Rightarrow 0 \leq x \bullet y.$$

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

Lema 5.8.2. *Neka je* $(P, +, \bullet)$ *prsten. Neka su* $a, b \in P$*. Tada vrijedi*

(i) $(-a) \bullet b = -(a \bullet b)$,

(ii) $a \bullet (-b) = -(a \bullet b)$.

Dokaz. (i) Uočimo da je jednakost $(-a) \bullet b = -(a \bullet b)$ ekvivalentna jednakosti

$$(-a) \bullet b + a \bullet b = 0. \tag{5.1}$$

No, $(-a) \bullet b + a \bullet b = (-a + a) \bullet b = 0 \bullet b = 0$. Dakle, vrijedi (5.1) pa je time tvrdnja dokazana.

Tvrdnju (*ii*) dokazujemo posve analogno.

□

Napomena 5.8.3. *Neka je* $(P, +)$ *Abelova grupa te neka je* $a \in P$*. Tada je*

$$-(-a) = a.$$

Naime, imamo da je $-a$ *inverzni element od* a *u* $(P, +)$*, stoga je* a *inverzni element od* $-a$ *u* $(P, +)$*, dakle* $a = -(-a)$.

Lema 5.8.4. *Neka je* $(P, +, \bullet)$ *prsten te neka su* $a, b \in P$*. Tada je*

$$(-a) \bullet (-b) = a \bullet b.$$

Dokaz. Koristeći lemu 5.8.2 i napomenu 5.8.3 dobivamo $(-a) \bullet (-b) = -(a \bullet (-b)) = -(-(a \bullet b)) = a \bullet b$. □

Propozicija 5.8.5. *Neka je* $(P, +, \bullet, \leq)$ *uređeni prsten. Tada je* $0 \leq 1$.

Dokaz. Znamo da je $0 \leq 1$ ili $1 \leq 0$.

Pretpostavimo da je $1 \leq 0$. Tada je $1 + (-1) \leq 0 + (-1)$, to jest $0 \leq -1$.

Iz definicije uređenog prstena (za $x = y = -1$) slijedi $0 \leq (-1) \bullet (-1)$. Prema lemi 5.8.4 vrijedi $(-1) \bullet (-1) = 1 \bullet 1 = 1$. Dakle, $0 \leq 1$.

U svakom slučaju smo dobili da je $0 \leq 1$. □

Neka je $(P, +)$ grupa. Za $a, b \in P$ definiramo

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

Propozicija 5.8.6. *Neka je $(P, +, \bullet)$ prsten te neka su $x, y, z \in P$. Tada je*

$$x \bullet (y - z) = x \bullet y - x \bullet z \tag{5.2}$$

i

$$(x - y) \bullet z = x \bullet z - y \bullet z. \tag{5.3}$$

Dokaz. Koristeći lemu 5.8.2 dobivamo

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

Prema tome, vrijedi (5.2).

Analogno dobivamo da vrijedi (5.3). □

Propozicija 5.8.7. *Neka je $(P, +, \bullet, \leq)$ uređeni prsten te neka su $x, y, z \in P$ takvi da je $x \leq y$ i $0 \leq z$. Tada je*

$$z \bullet x \leq z \bullet y.$$

Dokaz. Iz $x \leq y$ slijedi $0 \leq y - x$ pa iz definicije uređenog prstena dobivamo $0 \leq z \bullet (y - x)$. Sada, iz propozicije 5.8.6, slijedi $0 \leq z \bullet y - z \bullet x$, odnosno $z \bullet x \leq z \bullet y$. □

Propozicija 5.8.8. *Neka su S i T skupovi takvi da je $S \subseteq T$. Pretpostavimo da je S beskonačan skup. Tada je T beskonačan skup.*

Dokaz. Budući da je S beskonačan skup, postoji injekcija $f : S \to S$ takva da f nije surjekcija.

Definirajmo funkciju $g : T \to T$ takvu da za svaki $x \in T$ vrijedi

$$g(x) = \begin{cases} f(x), & \text{ako je } x \in S \\ x, & \text{ako } x \notin S \end{cases}$$

Dokažimo da je g injekcija.
Neka su $x, y \in T$ takvi da je $x \neq y$. Razlikujemo četiri slučaja.

1) $x, y \in S$.
   Iz definicije od g slijedi da je $g(x) = f(x)$ i $g(y) = f(y)$. No, f je injekcija pa vrijedi $f(x) \neq f(y)$, što povlači da je $g(x) \neq g(y)$.

2) $x \in S$ i $y \notin S$.
Tada je $g(x) = f(x)$ i $g(y) = y$. Očito je $f(x) \in S$, a znamo da $y \notin S$ pa je $f(x) \neq y$. Prema tome, $g(x) \neq g(y)$.

3) $x \notin S$ i $y \in S$.
Analogno, kao u prethodnom slučaju, zaključujemo da je $g(x) \neq g(y)$.

4) $x \notin S$ i $y \notin S$.
Tada je $g(x) = x$ i $g(y) = y$ pa iz $x \neq y$ slijedi $g(x) \neq g(y)$.

U svakom slučaju smo dobili da je $g(x) \neq g(y)$ pa zaključujemo da je g injekcija.

Dokažimo još da g nije surjekcija.
Budući da f nije surjekcija, postoji $y \in S$ takav da

$$y \notin \operatorname{Im} f. \tag{5.4}$$

Tvrdimo da $y \notin \operatorname{Im} g$.
Pretpostavimo suprotno. Tada postoji $x \in T$ takav da je $y = g(x)$.

1. slučaj. $x \in S$.
Tada je $g(x) = f(x)$ pa je $y = f(x)$. Stoga je $y \in \operatorname{Im} f$, što je u kontradikciji s (5.4).

2. slučaj. $x \notin S$
Tada je $g(x) = x$ pa je stoga $y = x$, što je nemoguće jer je $y \in S$, a $x \notin S$.

U oba slučaja smo dobili kontradikciju pa zaključujemo da $y \notin \operatorname{Im} g$.
Time smo dokazali da g nije surjekcija.

Rezimirajmo: $g : T \to T$ je injekcija, a nije surjekcija. Stoga je T beskonačan skup.

□

Definicija 5.8.9. *Ako je $(P, +, \bullet, \leq)$ uređeni prsten takav da skup P ima barem dva elementa, onda za $(P, +, \bullet, \leq)$ kažemo da je* ***netrivijalan uređeni prsten****.*

Analogno definiramo pojam **netrivijalne uređene grupe**.

Propozicija 5.8.10. *Neka je $(P+, \leq)$ netrivijalna uređena grupa. Tada je P beskonačan skup.*

Dokaz. Definirajmo $S = \{x \in P \mid 0 \leq x\}$. Očito je $S \subseteq P$ pa je, prema propoziciji 5.13.2, dovoljno dokazati da je S beskonačan skup.

Budući da je $(P, +, \leq)$ netrivijalna uređena grupa, postoji $x \in P$ takav da je $x \neq 0$.

Znamo, po definiciji uređaja, da vrijedi $0 \leq x$ ili $x \leq 0$ pa iz $x \neq 0$ slijedi da je $0 < x$ ili $x < 0$.
Ako $x < 0$, onda iz propozicije 5.7.6 slijedi da je $0 < -x$.
Dakle, vrijedi $0 < x$ ili $0 < -x$.

Zaključak: postoji $p \in P$ takav da $0 < p$.

Dokažimo da za svaki $x \in P$ vrijedi sljedeća implikacija:

$$x \in S \Rightarrow x + p \in S. \tag{5.5}$$

Pretpostavimo da je $x \in S$.
Tada je $0 \leq x$ pa je $0 + p \leq x + p$, to jest $p \leq x + p$.
Iz ovoga i činjenice da je $0 \leq p$ slijedi $0 \leq x + p$, dakle $x + p \in S$.

Prema tome, vrijedi implikacija (5.5) (uočimo da smo do istog zaključka mogli doći koristeći propoziciju 5.7.1).

Definirajmo funkciju $f : S \to S$ sa $f(x) = x + p$, za svaki $x \in S$.
Uočimo da je zbog implikacije (5.5) funkcija f dobro definirana.

Dokažimo da je f injekcija.
Neka su $x, y \in S$ takvi da je $x \neq y$.
Kada bi vrijedilo $f(x) = f(y)$, onda bismo imali $x + p = y + p$ pa bismo pribrajanjem $-p$ lijevoj i desnoj strani dobili $x = y$ (to je zapravo posljedica napomene 5.3.3), što je nemoguće.

Dakle $f(x) \neq f(y)$, pa je prema tome f injekcija.

Tvrdimo $0 \notin \operatorname{Im} f$.
Pretpostavimo suprotno. Tada postoji $x \in S$ takav da $0 = f(x)$, to jest $0 = x + p$. Slijedi da je $x = -p$.
Znamo da je $0 < p$ pa je $-p < 0$, to jest $x < 0$. No to je nemoguće jer je $0 \leq x$ (zbog $x \in S$).

Prema tome, $0 \notin \operatorname{Im} f$ te stoga f nije surjekcija (uočimo da je $0 \in S$).

Dakle, f je injekcija, a nije surjekcija, stoga je S beskonačan skup.
Time je tvrdnja propozicije dokazana. □

Korolar 5.8.11. *Neka je* $(P, +, \bullet, \leq)$ *netrivijalan uređeni prsten. Tada je* P *beskonačan skup.*

Dokaz. Očito je $(P, +, \leq)$ netrivijalna uređena grupa pa tvrdnja slijedi iz prethodne propozicije. □

5.9 Prirodni brojevi u uređenom prstenu

Neka je $(P, +, \bullet, \leq)$ netrivijalan uređeni prsten. Neka je $T \subseteq P$. Kažemo da je T induktivan skup u $(P, +, \bullet, \leq)$ ako vrijedi sljedeće:

(i) $1 \in T$ (pri čemu je 1 jedinica u prstenu $(P, +, \bullet, \leq)$).

(ii) Ako je $x \in T$, onda je $x + 1 \in T$.

Uočimo da je P induktivan skup u $(P, +, \bullet, \leq)$.

Neka je $N = \{x \in P \mid x \in T \text{ za svaki induktivan skup } T \text{ u } (P, +, \bullet, \leq)\}$. Za elemente od N kažemo da su **prirodni brojevi** u $(P, +, \bullet, \leq)$. Dakle, N je **skup svih prirodnih brojeva** u $(P, +, \bullet, \leq)$.

Uočimo da je N također induktivan skup u $(P, +, \bullet, \leq)$. Očito je $N \subseteq P$.

Za svaki induktivan skup T vrijedi $1 \in T$, stoga je jasno da je $1 \in N$. Nadalje, ako je $x \in N$, onda za svaki induktivan skup T vrijedi $x \in T$. Slijedi da za svaki induktivan skup T vrijedi $x + 1 \in T$. Dakle $x + 1 \in N$.

Stoga možemo definirati funkciju $s : N \to N$ sa

$$s(x) = x + 1, \text{ za svaki } x \in N.$$

Kažemo da je s **funkcija sljedbenika** u N (s obzirom na $(P, +, \bullet, \leq)$).

Teorem 5.9.1. *Neka je* $(P, +, \bullet, \leq)$ *netrivijalan uređeni prsten. Neka je* N *skup svih prirodnih brojeva u* $(P, +, \bullet, \leq)$ *te neka je* s *pripadna funkcija sljedbenika. Tada je* (N, s) *Peanov par.*

Dokaz. Da je s injekcija vidimo na isti način kao što smo vidjeli da je f injekcija u dokazu propozicije 5.8.10.
Naime, ako su $x, y \in N$ takvi da je $x \neq y$, onda bi $s(x) = s(y)$ povlačilo $x + 1 = y + 1$, to jest $x = y$, što je nemoguće, dakle $s(x) \neq s(y)$.

Dokažimo sada da je $\operatorname{Im} s = N \setminus \{1\}$.
Pretpostavimo da je $1 \in \operatorname{Im} s$. Tada postoji $x \in N$ takav da je $s(x) = 1$. Slijedi da je $x+1 = 1$, odnosno $x = 0$.
Dakle $0 \in N$.

Definirajmo $T = \{x \in P \mid 1 \leq x\}$. Očito je $1 \in T$.
Pretpostavimo da je $x \in T$. Tada je $1 \leq x$.
Znamo da je $0 \leq 1$ stoga vrijedi $x + 0 \leq x + 1$, to jest $x \leq x + 1$. Iz ovoga i $1 \leq x$ slijedi $1 \leq x + 1$. Stoga je $x + 1 \in T$.

Da rezimiramo, vrijedi sljedeće:

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

Prema tome, T je induktivan skup u $(P, +, \bullet, \leq)$.

Iz $0 \in N$ i definicije od N slijedi da je $0 \in T$, što po definiciji od T znači da je $1 \leq 0$.
Ovo, zajedno s činjenicom da je $0 \leq 1$, povlači da je $0 = 1$, no to je nemoguće jer je prsten $(P, +, \bullet)$ netrivijalan.

Zaključak: $1 \notin \operatorname{Im} s$.

Očito je $\operatorname{Im} s \subseteq N$ pa imamo da je

$$\operatorname{Im} s \subseteq N \setminus \{1\}. \tag{5.6}$$

Sada želimo dokazati obratnu inkluziju. U tu svrhu definiramo skup

$$V = \operatorname{Im} s \cup \{1\}.$$

Očito je $1 \in V$. Ako je $x \in V$, onda je $x \in N$ (jer je $V \subseteq N$) pa je $x + 1 = s(x)$ iz čega je jasno da je $x + 1 \in \operatorname{Im} s$, dakle $x + 1 \in V$.

Ovim smo pokazali da je V induktivan skup u $(P, +, \bullet, \leq)$ pa iz definicije od N slijedi $N \subseteq V$.

S druge strane, vrijedi $V \subseteq N$ stoga je $V = N$.

Dakle, $\operatorname{Im} s \cup \{1\} = N$ pa slijedi $N \setminus \{1\} \subseteq \operatorname{Im} s$ (napomena 2.5.1).
Iz ovoga i (5.6) slijedi da je $\operatorname{Im} s = N \setminus \{1\}$.

Neka je $S \subseteq N$ takav da je $1 \in S$ i da za svaki $x \in S$ vrijedi $s(x) \in S$. Ovo znači da je $1 \in S$ i da za svaki $x \in S$ vrijedi $x + 1 \in S$.

Uočimo da je S induktivan skup u $(P, +, \bullet, \leq)$.

Po definiciji od N slijedi da je $N \subseteq S$. Ovo, zajedno sa $S \subseteq N$, povlači da je $S = N$.

Time smo dokazali da je (N, s) Peanov par. □

Napomena 5.9.2. *Neka je $(P, +, \bullet, \leq)$ netrivijalan uređeni prsten te neka je N skup svih prirodnih brojeva u $(P, +, \bullet, \leq)$. Iz dokaza prethodnog teorema (ili definicije od N) vidimo da vrijedi sljedeće: ako je $S \subseteq N$ takav da je $1 \in S$ te takav da za svaki $x \in S$ vrijedi $x + 1 \in S$, onda je $S = N$.*

Napomena 5.9.3. *Neka je $(P, +, \bullet, \leq)$ netrivijalan uređeni prsten te neka je N skup svih prirodnih brojeva u $(P, +, \bullet, \leq)$. Tada za svaki $x \in N$ vrijedi da je $1 \leq x$.*

Neka je $T = \{x \in P \mid 1 \leq x\}$.
U dokazu prethodnog teorema vidjeli smo da je T induktivan skup u $(P, +, \bullet, \leq)$, stoga je $N \subseteq T$, a to znači da je $1 \leq x$, za svaki $x \in N$.

Propozicija 5.9.4. *Neka je $(P, +, \bullet, \leq)$ netrivijalan uređeni prsten te neka je N skup svih prirodnih brojeva u $(P, +, \bullet, \leq)$. Tada za sve $x, y \in N$ vrijedi*

$$x + y \in N.$$

Dokaz. Fiksirajmo $x \in N$.

Želimo dokazati da za svaki $y \in N$ vrijedi $x + y \in N$. U tu svrhu definirajmo

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

Dokazat ćemo da je $S = N$, a to će značiti upravo da za svaki $y \in N$ vrijedi $x + y \in N$.

Jasno je da je $x + 1 \in N$ (jer je $x \in N$). Stoga je $1 \in S$.

Pretpostavimo da je $y \in S$. Tada je $y \in N$ i $x + y \in N$, što povlači da je $y + 1 \in N$ i $(x + y) + 1 \in N$, to jest $x + (y + 1) \in N$. Stoga je $y + 1 \in S$.

Dakle, vrijedi sljedeće:

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

Očito je $S \subseteq N$. Iz napomene 5.9.2 slijedi $S = N$. Prema tome, za svaki $x \in N$ i za svaki $y \in N$ vrijedi $x + y \in N$. □

Propozicija 5.9.5. *Neka je $(P, +, \bullet, \leq)$ netrivijalan uređeni prsten te neka je N skup svih prirodnih brojeva u $(P, +, \bullet, \leq)$. Tada za sve $x, y \in N$ vrijedi*

$$x \bullet y \in N.$$

Dokaz. Fiksirajmo $x \in N$.

Definirajmo $S = \{y \in N \mid x \bullet y \in N\}$. Očito je $S \subseteq N$. Nadalje, jasno je da je $1 \in S$.

Neka je $y \in S$. Tada vrijedi

$$x \bullet (y + 1) = x \bullet y + x \bullet 1 = x \bullet y + x. \tag{5.7}$$

Imamo $x \bullet y \in N$ (jer je $y \in S$) pa iz $x \in N$ i prethodne propozicije slijedi da je $x \bullet y + x \in N$. Iz (5.7) slijedi da je $x \bullet (y + 1) \in N$.
Zaključujemo da je $y + 1 \in S$.

Dakle, imamo da je $1 \in S$ te da za svaki $y \in S$ vrijedi $y + 1 \in S$.

Iz napomene 5.9.2 slijedi da je $S = N$. To znači, po definiciji skupa S, da za svaki $y \in N$ vrijedi $x \bullet y \in N$. Time je tvrdnja propozicije dokazana.

□

5.10 Uređeno polje

Definicija 5.10.1. *Za uređeni prsten $(P, +, \bullet, \leq)$ takav da je $(P, +, \bullet)$ polje kažemo da je* ***uređeno polje****.*

Uočimo sljedeće: ako je $(P, +, \bullet, \leq)$ uređeno polje, onda je $(P, +, \bullet, \leq)$ netrivijalan uređeni prsten. Stoga ima smisla govoriti o prirodnim brojevima u uređenom polju $(P, +, \bullet, \leq)$.

Propozicija 5.10.2. *Neka je $(P, +, \bullet, \leq)$ uređeni prsten te neka su $x, y \in P$.*

(i) Ako je $x \leq 0$ i $0 \leq y$, onda je $x \bullet y \leq 0$.

(ii) Ako je $0 \leq x$ *i* $y \leq 0$*, onda je* $x \bullet y \leq 0$.

(iii) Ako je $x \leq 0$ *i* $y \leq 0$*, onda je* $0 \leq x \bullet y$.

Dokaz. (i) Pretpostavimo da je $x \leq 0$ i $0 \leq y$. Iz $x \leq 0$ slijedi da je $0 \leq -x$ pa iz definicije uređenog prstena dobivamo $0 \leq (-x) \bullet y$. Lema 5.8.2 povlači da je $0 \leq -(x \bullet y)$ pa je $x \bullet y \leq 0$.

(ii) Ovu tvrdnju dokazujemo analogno kao tvrdnju *(i)*.

(iii) Pretpostavimo da je $x \leq 0$ i $y \leq 0$. Tada je $0 \leq -x$ i $0 \leq -y$ pa je $0 \leq (-x) \bullet (-y)$. Iz leme 5.8.4 slijedi da je $0 \leq x \bullet y$.

□

Propozicija 5.10.3. *Neka je* $(P, +, \bullet, \leq)$ *uređeno polje te neka su* $x, y \in P$.

(i) Ako je $0 < x$ *i* $0 < y$*, onda je* $0 < x \bullet y$.

(ii) Ako je $x < 0$ *i* $0 < y$*, onda je* $x \bullet y < 0$.

(iii) Ako je $0 < x$ *i* $y < 0$*, onda je* $x \bullet y < 0$.

(iv) Ako je $x < 0$ *i* $y < 0$*, onda je* $0 < x \bullet y$.

Dokaz. (i) Pretpostavimo da je $0 < x$ i $0 < y$. Tada je posebno $0 \leq x$ i $0 \leq y$ pa iz definicije uređenog prstena slijedi $0 \leq x \bullet y$.
Nadalje, iz $0 < x$ i $0 < y$ slijedi da je $x \neq 0$ i $y \neq 0$ pa iz napomene 5.4.2 slijedi da je $x \bullet y \neq 0$. Prema tome $0 < x \bullet y$.

(ii) Pretpostavimo da je $x < 0$ i $0 < y$. Iz prethodne propozcije (tvrdnja *(i)*) slijedi da je $x \bullet y \leq 0$. Prema napomeni 5.4.2 vrijedi $x \bullet y \neq 0$, dakle $x \bullet y < 0$.

Tvrdnje *(iii)* i *(iv)* dokazujemo analogno. □

Propozicija 5.10.4. *Neka je* $(P, +, \bullet, \leq)$ *uređeno polje te neka je* $x \in P$*,* $x \neq 0$.

(i) Ako je $0 < x$*, onda je* $0 < x^{-1}$.

(ii) Ako je $x < 0$*, onda je* $x^{-1} < 0$.

Dokaz. Kada bi vrijedilo $x^{-1} = 0$, imali bismo $1 = x \bullet x^{-1} = x \bullet 0 = 0$, to jest $1 = 0$, što je nemoguće jer je polje netrivijalan prsten. Prema tome, $x^{-1} \neq 0$.

Znamo da je $x^{-1} \leq 0$ ili $0 \leq x^{-1}$, stoga je $x^{-1} < 0$ ili $0 < x^{-1}$.

(i) Pretpostavimo da je $0 < x$.
Kada bi vrijedilo $x^{-1} < 0$, onda bi iz propozicije 5.10.3 *(iii)* slijedilo da je $x \bullet x^{-1} < 0$, to jest $1 < 0$. No, to je u kontradikciji s činjenicom da je $0 \leq 1$.
Prema tome, $0 < x^{-1}$.

(ii) Ovu tvrdnju dokazujemo analogno kao tvrdnju *(i)*.

□

5.11 Uređen skup

Definicija 5.11.1. *Neka je S skup te neka je $\leq$ uređaj na skupu S. Za uređeni par $(S, \leq)$ kažemo da je* ***uređen skup****.*

Definicija 5.11.2. *Neka je $(S, \leq)$ uređen skup. Neka je $A \subseteq S$ te neka je $s_0 \in S$. Kažemo da je s_0* ***donja međa*** *skupa A u $(S, \leq)$ ako je*

$$s_0 \leq a,$$

za svaki $a \in A$.

Kažemo da je s_0 ***gornja međa*** *skupa A u $(S, \leq)$ ako je*

$$a \leq s_0,$$

za svaki $a \in A$.

Definicija 5.11.3. *Neka je $(S, \leq)$ uređen skup te neka je $A \subseteq S$. Kažemo da je A* ***odozdo omeđen skup*** *u $(S, \leq)$ ako postoji barem jedna donja međa od A u $(S, \leq)$.*

Kažemo da je A ***odozgo omeđen*** *skup u $(S, \leq)$ ako postoji barem jedna gornja međa od A u $(S, \leq)$.*

Definicija 5.11.4. *Neka je $(S, \leq)$ te neka je $A \subseteq S$. Neka je $a_0 \in A$. Kažemo da je a_0* ***minimum*** *skupa A u $(S, \leq)$ ako je*

$$a_0 \leq a,$$

za svaki $a \in A$.
Drugim riječima, minimum skupa A je donja međa tog skupa koja je element skupa A.

Za a_0 kažemo da je ***maksimum*** *skupa A u $(S, \leq)$ ako je*

$$a \leq a_0,$$

za svaki $a \in A$.
Dakle, maksimum skupa A je gornja međa tog skupa koja je element skupa A.

Definicija 5.11.5. *Neka je $(S, \leq)$ uređen skup te neka je $A \subseteq S$. Neka je $s_0 \in S$. Kažemo da je s_0* ***infimum*** *skupa A u $(S, \leq)$ ako vrijedi sljedeće:*

(i) s_0 je donja međa skupa A u $(S, \leq)$,

(ii) $s \leq s_0$, za svaku donju među s skupa A u $(S, \leq)$ (to jest, s_0 je najveća donja međa od A u $(S, \leq)$).

Napomena 5.11.6. *Neka je $(S, \leq)$ uređen skup, neka je $A \subseteq S$ te neka je a_0 minimum od A u $(S, \leq)$. Tada je a_0 infimum skupa A u $(S, \leq)$.*

Naime, očito je da vrijedi svojstvo (i) iz definicije infimuma (a_0 je donja međa jer je minimum).
Svojstvo (ii) iz definicije infimuma vrijedi jer je a_0 element skupa A, pa za svaku donju među s od A vrijedi $s \leq a_0$.

Definicija 5.11.7. *Neka je $(S, \leq)$ uređen skup te neka je $A \subseteq S$. Neka je $s_0 \in S$. Kažemo da je s_0* ***supremum*** *skupa A u $(S, \leq)$ ako vrijedi sljedeće:*

(i) s_0 je gornja međa skupa A u $(S, \leq)$,

(ii) $s_0 \leq s$, za svaku gornju među s skupa A u $(S, \leq)$ (to jest, s_0 je najmanja gornja međa od A u $(S, \leq)$).

Napomena 5.11.8. *Neka je $(S, \leq)$ uređen skup, neka je $A \subseteq S$ te neka je a_0 maksimum od A u $(S, \leq)$. Tada je a_0 supremum skupa A u $(S, \leq)$.*

To vidimo na sljedeći način: svojstvo (i) iz definicije supremuma je očito zadovoljeno.
Svojstvo (ii) vrijedi jer je a_0 element skupa A, pa za svaku gornju među vrijedi $a_0 \leq s$.

Napomena 5.11.9. *Neka je $(S, \leq)$ uređen skup te neka je $A \subseteq S$. Uočimo sljedeće: ako A ima infimum u $(S, \leq)$ (to jest, ako postoji infimum od A u $(S, \leq)$), onda je A odozdo omeđen u $(S, \leq)$.*
Slično, ako A ima supremum u $(S, \leq)$, onda je A odozgo omeđen skup u $(S, \leq)$.

5.12 Potpuno uređen skup

Definicija 5.12.1. *Neka je $(S, \leq)$ uređen skup. Pretpostavimo da za sve neprazne podskupove A i B od S takve da je $a \leq b$, za svaki $a \in A$ i svaki $b \in B$, postoji $c \in S$ takav da je*

$a \leq c$, za svaki $a \in A$ i $c \leq b$, za svaki $b \in B$. Tada za $(S, \leq)$ kažemo da je ***potpuno uređen skup****.*

Propozicija 5.12.2. *Neka je $(S, \leq)$ potpuno uređen skup. Neka je A neprazan odozdo omeđen skup u $(S, \leq)$. Tada A ima infimum u $(S, \leq)$.*

Dokaz. Definirajmo D kao skup svih $d \in S$ takvih da je d donja međa skupa A u $(S, \leq)$. Skup D je neprazan jer je A odozdo omeđen skup u $(S, \leq)$.

Ako su $d \in D$ i $a \in A$, onda je $d \leq a$ jer je d donja međa skupa A.
Iz definicije potpuno uređenog skupa, slijedi da postoji $c \in S$ takav da je $d \leq c$, za svaki $d \in D$ i $c \leq a$, za svaki $a \in A$.
Iz ovoga slijedi da je c infimum skupa A u $(S, \leq)$. Naime, prvo svojstvo iz definicije infimuma slijedi iz činjenice da je $c \leq a$, za svaki $a \in A$, a drugo svojstvo slijedi iz činjenice da je $d \leq c$, za svaki $d \in D$. □

Propozicija 5.12.3. *Neka je $(S, \leq)$ potpuno uređen skup. Neka je A neprazan odozgo omeđen skup u $(S, \leq)$. Tada A ima supremum u $(S, \leq)$.*

Dokaz. Definirajmo G kao skup svih $g \in S$ takvih da je g gornja međa skupa A u $(S, \leq)$. Pošto je A odozgo omeđen skup u $(S, \leq)$, skup G je neprazan.

Za sve $a \in A$ i $g \in G$ vrijedi $a \leq g$, pa iz definicije potpuno uređenog skupa slijedi da postoji $c \in S$ takav da je $a \leq c$, za svaki $a \in A$ i $c \leq g$, za svaki $g \in G$.
Iz ovoga zaključujemo da je c supremum skupa A u $(S, \leq)$. □

5.13 Potpuno uređeno polje

Definicija 5.13.1. *Neka je $(P, +, \bullet, \leq)$ uređeno polje takvo da je $(P, \leq)$ potpuno uređen skup. Tada za $(P, +, \bullet, \leq)$ kažemo da je* ***potpuno uređeno polje*** *ili* ***polje realnih brojeva****.*

Napomena 5.13.2. *Neka je $(S, \leq)$ uređen skup. Pretpostavimo da su $x, y \in S$ takvi da ne vrijedi $x \leq y$. Tada je $y < x$.*

Naime, po definiciji uređaja, vrijedi $x \leq y$ ili $y \leq x$, pa zaključujemo da je $y \leq x$.
Ne može vrijediti $x = y$ (jer bi vrijedilo $x \leq y$), dakle $x \neq y$, pa je $y < x$.

Napomena 5.13.3. *Neka je $(S, \leq)$ uređen skup. Pretpostavimo da su $x, y \in S$ takvi da ne vrijedi $x < y$. Tada je $y \leq x$.*

Naime, u suprotnom bi iz napomene 5.13.2 slijedilo $x < y$, što ne vrijedi.

Propozicija 5.13.4. *Neka je $(P, +, \bullet, \leq)$ potpuno uređeno polje. Neka je N skup svih prirodnih brojeva u $(P, +, \bullet, \leq)$. Tada N nije odozgo omeđen skup u $(P, \leq)$.*

Dokaz. Pretpostavimo suprotno, to jest da je N odozgo omeđen skup u $(P, \leq)$.
Očito je $N \neq \emptyset$, pa iz činjenice da je $(P, \leq)$ potpuno uređen skup i propozicije 5.12.3 slijedi da postoji element $s_0 \in P$ takav da je s_0 supremum skupa N u $(P, \leq)$.

Kada bi $s_0 - 1$ bila gornja međa skupa N, onda bi, iz činjenice da je s_0 supremum od N, slijedilo da je $s_0 \leq s_0 - 1$, što bi povlačilo da je $0 \leq -1$, to jest $1 \leq 0$. No, to je nemoguće jer je $0 \leq 1$ i $0 \neq 1$. Prema tome, $s_0 - 1$ nije gornja međa skupa N.
Iz ovoga zaključujemo da postoji barem jedan $x \in N$ takav da ne vrijedi $x \leq s_0 - 1$, to jest takav da je $s_0 - 1 < x$ (napomena 5.13.2).
Iz ovoga slijedi da je $s_0 < x + 1$. No, $x + 1 \in N$, pa je $x + 1 \leq s_0$ jer je s_0 supremum skupa N.

Dakle, $s_0 < x + 1$ i $x + 1 \leq s_0$, što je očito nemoguće.

Zaključak: N nije odozgo omeđen skup u $(P, \leq)$. □

Korolar 5.13.5. *Neka je $(P, +, \bullet, \leq)$ potpuno uređeno polje te neka je N skup svih prirodnih brojeva u $(P, +, \bullet, \leq)$. Tada za svaki $x \in P$ postoji $n \in N$ takav da je $x < n$.*

Dokaz. Neka je $x \in P$. Kada ne bi postojao $n \in N$ sa svojstvom da je $x < n$, onda bi za svaki $x \in N$ vrijedilo $n \leq x$ (napomena 5.13.3), što bi značilo da je x gornja međa skupa N, a to je nemoguće prema propoziciji 5.13.4. □

Propozicija 5.13.6. *Neka je $(P, +, \bullet, \leq)$ potpuno uređeno polje te neka je N skup svih prirodnih brojeva u $(P, +, \bullet, \leq)$. Neka su $x, y \in P$ takvi da je $0 < x$. Tada postoji $n \in N$ takav da je $y < n \bullet x$.*

Dokaz. Uočimo prije svega sljedeće: ako su $a, b, c \in P$ takvi da je $a < b$ i $0 < c$, onda je $a \bullet c < b \bullet c$.
Naime, imamo $0 < b - a$ i $0 < c$, pa iz propozicije 5.10.3 *(i)* slijedi da je $0 < (b - a) \bullet c$. Iz propozicije 5.8.6 slijedi $0 < b \bullet c - a \bullet c$, stoga je $a \bullet c < b \bullet c$.

Prema prethodnom korolaru, postoji $n \in N$ takav da je $y \bullet x^{-1} < n$. Iz ovoga i činjenice da je $0 < x$ slijedi $(y \bullet x^{-1}) \bullet x < n \bullet x$, to jest $y < n \bullet x$. □

Bibliografija

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

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

[3] K. Vidović, *Skupovi kao temeljni matematički koncept*, diplomski rad, PMF-MO, Sveučilište u Zagrebu, 2018.

Sažetak

U ovom diplomskom radu smo prvo dali neke činjenice iz elementarne teorije skupova, što je bio sadržaj prvog poglavlja. U njemu smo govorili o uređenim parovima, uniji i presjeku skupova, Kartezijevom produktu skupova te smo pokazali da ne postoji skup svih skupova.

U drugom poglavlju smo proučavali pojmove relacije i funkcije te neka svojstva tih pojmova.

Beskonačnim skupovima, Peanovim parovima te egzistencijom Peanovog para smo se bavili u trećem poglavlju.

Četvrto poglavlje je bilo posvećeno pojmu skupoida. Koristeći taj pojam, dokazali smo egzistenciju beskonačnog skupa.

U petom, zadnjem poglavlju, proučavali smo uređene grupe i uređene prstene te smo definirali prirodne brojeve u uređenom prstenu. Nadalje, proučavali smo potpuno uređene skupove i potpuno uređena polja, to jest polja realnih brojeva.

Summary

In this thesis, we first presented some facts from elementary set theory, which was the content of the first chapter. In it, we dealt with ordered pairs, the union and intersection of sets, the Cartesian product of sets, and we proved that there is no set of all sets.

In the second chapter, we studied the notions of relations and functions and some properties of these notions.

We studied infinite sets, Peano pairs and the existence of Peano pairs in the third chapter.

The fourth chapter was devoted to the concept of a setoid. Using this concept, we proved the existence of an infinite set.

In the fifth, last chapter, we studied ordered groups and ordered rings, and we defined natural numbers in an ordered ring. Furthermore, we studied completely ordered sets and completely ordered fields, that is, fields of real numbers.

Životopis

Rođena sam 28.9.1998. godine u Splitu. Školovanje započinjem 2005. godine u Osnovnoj školi Petar Berislavić u Okrugu Gornjem. Osnovnu školu završavam 2013. godine i upisujem opću gimnaziju Ivan Lucić u Trogiru. Nakon završene srednje škole 2017. godine nastavljam školovanje na preddiplomskom studiju Matematike; smjer: nastavnički, na Prirodoslovno matematičkom fakultetu u Zagrebu. Studij završavam 2022. godine te potom upisujem diplomski studij Matematika; smjer nastavnički.
Tijekom preddiplomskog i diplomskog studija radila sam u tvrtki Photomath, kreatoru istoimene aplikacije za pomoć pri učenju matematike, na mjestu *Data Annotatora*.