25. svibnja 2016.

# UVOD U TEORIJU SKUPOVA I MATEMATIČKU LOGIKU

Šime Ungar
http://www.mathos.unios.hr/~sime/

Literatura:

P. Papić. *Uvod u teoriju skupova*, HMD, Zagreb 2000.

M. Vuković. *Teorija skupova*, predavanja, PMF–Matematički odjel, Zagreb 2010.

M. Vuković. *Matematička logika 1*, skripta, PMF–Matematički odjel, Zagreb 2000.

M. Vuković. *Matematička logika*, Element, Zagreb 2009.

F. R. Drake, D. Singh. *Intermediate Set Theory*, John Wiley & Sons, 1996.

S. Lipschutz. *Schaum's Outline of Set Theory and Related Topics*, McGraw-Hill, New York 1998.

S. Mardešić. *Matematička analiza*, 1. dio, Školska knjiga, Zagreb, 1974.

## Što predavati prije: Teoriju skupova ili Matematičku logiku?

To je isto kao pitanje: Što je bilo prije — kokoš ili jaje?

Teorija skupova treba Matematičku logiku, kao što i Matematička logika treba Teoriju skupova.

Odgovor je dao Darwin: evolucija — niti je kokoš nastala prije jajeta niti je jaje nastalo prije kokoši — razvijali su se istovremeno.

Tako su se *Teorija skupova* i *Matematička logika* razvijale istovremeno. (Za razliku od *Logike* koja se razvijala već od Aristotela, a i ranije.)

Ako se ML i TS predaju u isto vrijeme, onda će svako malo nastavnik iz ML reći „A kao što znate iz teorije skupova, ...”, a isto će tako nastavnik iz TS svako malo reći „A kao što ste učili u matematičkoj logici, ...”

U početku može se raditi i ne-aksiomatski, ali uz izvjestan oprez:
— *NAIVNA TEORIJA SKUPOVA*.

# Ključni momenti razvoja teorije skupova

- G. Cantor (1845–1918): radovi o teoriji skupova (1871–1883);
- D. Hilbert: *Nitko nas neće istjerati iz raja u koji nas je uveo Cantor.*
- B. Russell (1903): zamah otkrićem paradoksa;
- E. Zermelo:
  - 1908. prvi prijedlog aksiomatizacije;
  - pokazao da se svaki skup može dobro urediti, što je izazvalo mnoge kritike zbog neočekivanosti rezultata;
- A. Fraenkel: 1922. precizirao shemu aksioma zamjene;
- A. Fraenkel i T. Skolem predložili shemu aksioma zamjene kao novi aksiom;
- J. von Neumann eksplicirao aksiom dobre utemeljenosti i definirao ordinalne brojeve;
- K. Gödel: 1918. dokazao relativnu konzistentnost ZF teorije skupova s aksiomom izbora i hipotezom kontinuuma;
- P. Cohen: 1963. dokazao nezavisnost hipoteze kontinuuma od ZF teorije skupova.

## 1 POJAM SKUPA

- Počeci i paradoksi
- Općenito o skupovima i osnovnim operacijama
- Prirodni brojevi

# Što je skup?

U ***naivnoj teoriji skupova***, a to ćemo raditi, odgovor je jednostavan:

- skup je primitivan pojam, i kao takav se ne definira;
- smatramo da već imamo razvijen intuitivan pojam skupa;
- skup je kolekcija objekata koji zajedno čine cjelinu.

Velik dio teorije skupova Cantor je izgradio na tako klimavim nogama.

# Osnovno u Cantorovoj teoriji

Cantor se nije eksplicite pozivao na aksiome, ali se manje-više sve svodi na sljedeća tri aksioma:

1. AKSIOM EKSTENZIONALNOSTI: Dva su skupa jednaka ako imaju iste elemente.
2. PRINCIP KOMPREHENZIJE: Za unaprijed zadano svojstvo[1] $\sigma$ postoji skup čiji su elementi točno oni elementi koji imaju to svojstvo, tj. $\{x : \underbrace{\sigma(x)}_{\text{tj. } \sigma(x) \text{ je ispunjeno}}\}$ je skup.
3. AKSIOM IZBORA Za svaki neprazan skup postoji (barem jedna) funkcija čiji su argumenti neprazni podskupovi toga skupa, a vrijednosti funkcije su elementi argumenta.

[1] Svojstvo (izjavna funkcija) $\sigma$ je funkcija jedne ili više varijabli, t.d. je za svaku vrijednost varijabli, dobivena izjava ili istinita ili lažna.

# Paradoksi

## Russellov paradoks

$\{x : x \text{ je skup i } x \notin x\}$ nije skup.

Tako se nešto u matematici dotada još nije dogodilo!

Uoči: PARADOKS $\neq$ KONTRADIKCIJA

Kasnije su uočeni i drugi paradoksi:

- Cantorov paradoks skupa svih skupova;
- Buralli-Fortijev paradoks;
- i drugi.

Problem je u principu komprehenzije: Nije sve što se može opisati nekim svojstvom, skup.

## Primjeri 1.1

*$\{A :$ postoji bijekcije skupa $A$ na skup $\mathbb{N}\}$ – nije skup*

*$\{f : f$ je neprekidna realna funkcija na segmentu $[0, 1]\}$ – je skup;*

*$\{G :$ postoji binarna operacija $*$ t.d. je $(G, *)$ grupa$\}$ – nije skup.*

# OPREZ !

ZAKLJUČAK: U teoriji skupova ne smijemo graditi nove skupove pomoću skupova koji još nisu izgrađeni.

TREBA BITI OPREZAN !

TERMINOLOGIJA: Ako je $\sigma$ neko svojstvo (izjavna funkcija) onda ćemo kolekciju $\{x : \sigma(x)\}$ zvati ***klasa***.

Neke klase *jesu* skupovi a neke *nisu*.

Klase koje nisu skupovi zvat ćemo *prave klase.*

## Općenito o skupovima i osnovnim operacijama

O oznakama: U „pravoj” teoriji skupova elementi skupova su uvijek skupovi, i svi se skupovi označavaju malim slovima. Naime, drugačije oznake dovode do problema jer se promatraju skupovi skupova, pa onda skupovi skupôva skupova, itd. Kod nas će se rijetko pojaviti više od 3–4 nivoa, pa ćemo rabiti oznake $a$, $A$, $\mathcal{A}$, $\mathscr{A}$, $\mathfrak{A}$.

Navedimo najprije nekoliko osnovnih aksioma, bez kojih ne možemo ništa:

# Aksiom ekstenzionalnosti

**AKSIOM EKSTENZIONALNOSTI**

Dva su skupa jednaka ako imaju iste elemente. Pišemo: $A = B$.

*Dakle:* $A \neq B$ znači da $\exists\, a \in A$ t.d. $a \notin B$, ili $\exists\, b \in B$ t.d. $b \notin A$ (ili oboje).

Ako se radi o konačno mnogo elemenata pišemo npr. $A = \{a_1, a_2, \ldots, a_n\}$.

Jednočlan skup: $\{a\}$.

Elementi skupa mogu biti skupovi: $\big\{\{0\}, \{0, 1\}, \{1, 2, 3\}, \{5\}\big\}$.

Ali: $S \neq \{S\}$. Uvijek! Ali: $S \in \{S\}$.

Oznake za neke standardne skupove: $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$

# Aksiom praznog skupa

**AKSIOM PRAZNOG SKUPA**

Postoji skup koji ne sadrži niti jedan element.

$$\exists\, S \text{ t.d. } \forall\, x,\ x \notin S.$$

● Iz AX ekstenzionalnosti slijedi da je takav skup jedinstven. Zovemo ga ***prazan skup*** i označavamo $\emptyset$.

Naprimjer:

$$\{x : x \in \mathbb{R} \text{ i } x = 2 \text{ i } x = 3\} = \emptyset$$

ili

$$\{x : x \in \mathbb{Q} \text{ i } x^2 = 2\} = \emptyset.$$

Crvenim kružićem ● u margini označivat ćemo tvrdnje čiji dokaz ostavljamo za vježbu.

# Aksiom partitivnog skupa

Inkluzija: $A \subseteq B$ znači: $a \in A \Rightarrow a \in B$. Čita se: $A$ je ***podskup*** od $B$.

Kako iz postojećih skupova izgraditi (tvoriti) nove skupove?
Postoji više načina.

**AKSIOM PARTITIVNOG SKUPA**

Ako je $A$ skup onda je klasa svih njegovih podskupova također skup.

$$\forall A \, \exists \mathscr{P} \text{ t.d. } \forall B \, (B \in \mathscr{P} \Leftrightarrow B \subseteq A)$$

- Iz AX ekstenzionalnosti slijedi da je za svaki skup $A$ takav skup jedinstven.
  Naziva se ***partitivni skup*** skupa $A$ i označava s $\mathscr{P}(A)$ ili $2^A$.

# Aksiom para

## AKSIOM PARA

Za svaka dva skupa $A$ i $B$ postoji skup čiji su $A$ i $B$ jedini elementi.

$$\forall A\ \forall B\ \exists C \text{ t.d. za } \forall X\ \big(X \in C \Rightarrow (X = A \text{ ili } X = B)\big)$$

- Iz AX ekstenzionalnosti opet slijedi da je za zadane $A$ i $B$ takav skup $C$ jedinstven, i naziva se ***(neuređen) par***.
  Oznaka: $\{A, B\}$ ili $\{B, A\}$, svejedno.

Posljedica: Za svaki skup $A$ postoji par $\{A, A\}$, i njega ćemo dogovorno označivati jednostavno $\{A\}$. Dakle, $\{A\} :\equiv \{A, A\}$

# Aksiom unije

## AKSIOM UNIJE

Za svaki skup je klasa elemenata svih njegovih elemenata opet skup.

ili, običnim jezikom:

Za svaki skup skupova $\mathscr{S}$ postoji skup $S$ koji se sastoji od onih, i samo onih elemenata, koji su elementi barem jednog skupa iz $\mathscr{S}$.

$$\forall \mathscr{S}\ \exists S \text{ t.d. } \forall x\ \big(x \in S \Leftrightarrow \exists A \text{ t.d. je } (A \in \mathscr{S}\ \&\ x \in A)\big)$$

- Iz AX ekstenzionalnosti slijedi da je takav $S$ jedinstven.
  Naziva se ***unija*** skupa $\mathscr{S}$ (govori se i o uniji familije $\mathscr{S}$).
  Oznaka: $\bigcup \mathscr{S}$, ili $\bigcup\{A : A \in \mathscr{S}\}$, ili $\bigcup\limits_{A \in \mathscr{S}} A$.

  Kada se radi o uniji od dva skupa uobičajena je oznaka $\bigcup\{A, B\} \equiv A \cup B$.

# Postojanje tročlanog skupa

## Primjer 2.1

Neka je $\mathscr{S} = \big\{\emptyset, \{b\}, \{b, c\}, \{b, d\}\big\}$. Prema AX unije je klasa $\{b, c, d\}$ svih elemenata članova od $\mathscr{S}$ također skup, tj. $\bigcup \mathscr{S} = \{b, c, d\}$ je skup. Dakle, postoji tročlan skup.

Ali, kako znamo da je $\mathscr{S}$ skup? Prazan skup $\emptyset$ i jednočlan skup $\{b\}$, npr. $\{b\} = \big\{\{\emptyset\}\big\} = \big\{\{\emptyset\}, \{\emptyset\}\big\}$, postoje. Trebamo još vidjeti da postoje skupovi oblika $\{b, c\}$ i $\{b, d\}$, gdje su $b$, $c$ i $d$ međusobno različiti. U tu svrhu stavimo npr. $c = \{\emptyset, \{\emptyset\}\}$ i $d = \Big\{\emptyset, \big\{\emptyset, \{\emptyset\}\big\}\Big\}$. Tada je

$$\bigcup \mathscr{S} = \bigcup \left\{\emptyset, \{\{\emptyset\}\}, \Big\{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}\Big\}, \left\{\{\emptyset\}, \Big\{\emptyset, \big\{\emptyset, \{\emptyset\}\big\}\Big\}\right\}\right\}$$
$$= \Big\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\Big\}$$

zaista tročlan skup.

# Postojanje *n*-članih skupova

**Teorem 2.2**

*Ako su $A_1, \ldots, A_n$ skupovi onda postoji skup $\{A_1, \ldots, A_n\}$.*

Dokaz: Neka su $A_1, \ldots, A_n$ skupovi. Prema AX para postoje skupovi $\{A_1, A_2\}$ i $\{A_3\}$ $\big(=\{A_3, A_3\}\big)$, pa, ponovno zbog AX para, postoji skup $\big\{\{A_1, A_2\}, \{A_3\}\big\}$.
Sada, zbog AX unije, postoji skup $\bigcup \big\{\{A_1, A_2\}, \{A_3\}\big\} = \{A_1, A_2, A_3\}$.
AX para $\Rightarrow \exists$ skup $\big\{\{A_1, A_2, A_3\}, \{A_4\}\big\}$; AX unije $\Rightarrow \exists$ skup $\{A_1, A_2, A_3, A_4\}$;
itd. indukcijom. $\square$

**Korolar 2.3**

*Za svaki prirodan broj n postoji n-člani skup.*

Dokaz: Iz prethodnog teorema i činjenice da postoji beskonačno mnogo *različitih* skupova. Npr. $\emptyset, \{\emptyset\}, \big\{\{\emptyset\}\big\}, \Big\{\big\{\{\emptyset\}\big\}\Big\}, \bigg\{\Big\{\big\{\{\emptyset\}\big\}\Big\}\bigg\}, \ldots$. $\square$

# Postoje li beskonačni skupovi?

Dakle, sada ***znamo*** *da postoji beskonačno mnogo skupova*, ali ***ne znamo*** postoji li ijedan beskonačan skup.
Naime, *kada bismo znali* da je beskonačna klasa $\mathscr{S}$ skupova iz dokaza prethodnog korolara 2.3, za koje znamo da postoje, *skup*, onda bi po AX unije znali da postoji i njihova unija, koja bi tada bila beskonačan skup jer su svi skupovi iz $\mathscr{S}$ međusobno različiti.

Ali to ne znamo! Ne znamo je li klasa $\mathscr{S}$ skup.

# Shema aksioma separacije

Sljedeći aksiom omogućuje definiciju (*ne* aksiomatizaciju!) presjeka, Kartezijevog produkta, i drugih stvari, a zamjenjuje Princip Komprehenzije, koji je u osnovi većine paradoksa.

## SHEMA AKSIOMA SEPARACIJE[2]

Ako je $A$ skup a $\sigma$ neko zadano svojstvo[3] na $A$, tada je klasa svih $a \in A$ koji imaju svojstvo $\sigma$ također skup.

$$\forall A\ \exists B \text{ t.d. } \forall a\ \big(a \in B \Leftrightarrow (a \in A\ \&\ \sigma(a))\big)$$

Zašto „shema aksioma” a ne „aksiom”?

Zato jer se tu radi o, u principu, beskonačno mnogo aksioma: za svako svojstvo $\sigma$ — jedan aksiom.

Ako je $\sigma$ neko zadano svojstvo, onda se govori o *aksiomu separacije za svojstvo* $\sigma$.

[2] Vuković str. 10; Papić: Aksiom izbora podskupova (specifikacije), str. 10

[3] vidi fusnotu na str. 5

# Presjek skupova

### Definicija 2.4

Za proizvoljan skup $\mathscr{S}$ se s $\bigcap \mathscr{S}$ označava klasa

$$\{x : \text{za svaki } A \in \mathscr{S} \text{ je } x \in A\}$$

i naziva se *presjek* skupa (familije) $\mathscr{S}$.

Ako su $A$ i $B$ skupovi onda se $\bigcap\{A, B\}$ označava $A \cap B$,

i analogno za $n$ skupova, $A_1 \cap \cdots \cap A_n \equiv \bigcap\{A_1, \ldots, A_n\} \equiv \bigcap\limits_{j=1}^{n} A_j$.

Uoči da je ovo *definicija* a ne *aksiom* presjeka (za razliku od uvođenja unije skupova).

Potrebno je, dakle, dokazati da je klasa kojom je gornjom definicijom definiran presjek, zaista skup.

# Presjek skupa skupova je zaista skup

**Teorem 2.5**

*Za svaki skup $\mathscr{S}$ je presjek $\bigcap \mathscr{S}$ također skup.*

Dokaz: Prema AX unije postoji skup $S = \bigcup \mathscr{S}$.

Neka je $\sigma$ svojstvo na $S$ definirano ovako:

$$\sigma(x) = \text{za svaki } A \in \mathscr{S} \text{ vrijedi } x \in A.$$

Prema AX separacije za svojstvo $\sigma$, klasa svih $x \in S = \bigcup \mathscr{S}$ koji imaju svojstvo $\sigma$, tj. klasa svih $x$-eva t. d. za svaki $A \in \mathscr{S}$ vrijedi $x \in A$, je skup, a to je upravo bila definicija presjeka. $\square$

# Razlika skupova

**Definicija 2.6**

Za proizvoljne skupove $A$ i $B$ s $A \setminus B$ označavamo klasu $\{x : x \in A \;\&\; x \notin B\}$, i to se naziva *razlika* skupova $A$ i $B$.

Ako je $U$ neki fiksni skup i $A \subseteq U$, onda se razlika $U \setminus A$ naziva *komplement* skupa $A$ (u odnosu na skup $U$), i često se označava $A^{\complement}$.

**Teorem 2.7**

*Za proizvoljne skupove $A$ i $B$, razlika $A \setminus B$ također je skup.*

Dokaz: Razlika $A \setminus B$ definirana je svojstvom $\sigma$ na $A$ ovako: $\sigma(x) = x \notin B$ pa je prema AX separacije za svojstvo $\sigma$, $A \setminus B$ skup. $\square$

**Korolar 2.8**

*Ako je $U$ neki fiksni skup i $A \subseteq U$ podskup, onda je komplement $A^{\complement} = U \setminus A$ također skup.* $\square$

# Algebra skupova

## Osnovna svojstva unije, presjeka i komplementa

| | | | |
|---|---|---|---|
| $(i)$ | komutativnost | $A \cup B = B \cup A$ | $A \cap B = B \cap A$ |
| $(ii)$ | asocijativnost | $A \cup (B \cup C) = (A \cup B) \cup C$ | $A \cap (B \cap C) = (A \cap B) \cap C$ |
| $(iii)$ | distributivnost | $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ | $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ |
| $(iv)$ | idempotentnost | $A \cup A = A$ | $A \cap A = A$ |
| $(v)$ | De Morganovi zakoni | $(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}$ | $(A \cap B)^{\complement} = A^{\complement} \cup B^{\complement}$ |
| $(vi)$ | | $A \cup \emptyset = A$ | $A \cap \emptyset = \emptyset$ |
| $(vii)$ | | $A \cup U = U$ | $A \cap U = A$ |
| $(viii)$ | | $A \cup A^{\complement} = U$ | $A \cap A^{\complement} = \emptyset$ |
| $(ix)$ | | $\emptyset^{\complement} = U$ | $U^{\complement} = \emptyset$ |

# Indeksirana familija (indeksirani skup)

**Definicija 2.9**

Neka je $\mathscr{A}$ neka neprazna familija skupova (tj. neprazan skup), i neka je $J$ neki skup. Svaka surjekcija $J \twoheadrightarrow \mathscr{A}$ naziva se *indeksna funkcija*. $J$ je *indeksni skup* ili *skup indeksa*, a familija $\mathscr{A}$ zajedno s indeksnom funkcijom $f$ je *indeksirana familija* (skupova).

Za $j \in J$ vrijednost $f(j) \in \mathscr{A}$ označujemo $A_j$ pa indeksiranu familiju označujemo $\{A_j\}_{j \in J}$ ili $\{A_j\}_j$ ako je jasno, ili nevažno, o kojem se skupu indeksa $J$ radi.

Napomena: Indeksna funkcija *ne mora* biti injektivna, tj. može biti $A_i = A_j$ iako je $i \neq j$.

Drugim riječima, isti skup familije $\mathscr{A}$ može se pojaviti više puta kao element indeksirane familije $\{A_j\}_j$.

# Dvije napomene

1. Na svaki skup možemo gledati kao na skup indeksa tako da identitetu $\mathbb{1}_S\colon S \to S$ interpretiramo kao indeksnu funkciju. Za $s \in S$ je $\mathbb{1}_S(s) = s \in S$, tako da dobivamo *indeksiran skup*
$$\{s_s\}_{s\in S} = \{s\}_{s\in S} = \{s : s \in S\} = S.$$

2. Na svaku familiju skupova možemo gledati kao na indeksiranu familiju $\mathscr{A} = \{A_j\}_{j\in\mathscr{A}} = \{A_j : j \in \mathscr{A}\} = \{A : A \in \mathscr{A}\}$, ali se obično ipak indeksni skup označuje različitim slovom, npr. $\mathscr{A} = \{A_j : j \in J\}$.

   Uz takvu oznaku, unije i presjeci familija skupova označuju se ovako:

$$\bigcup \mathscr{A} = \bigcup\{A : A \in \mathscr{A}\} = \bigcup\{A_j : j \in J\} = \bigcup_{j\in J} A_j = \bigcup_j A_j$$

$$\bigcap \mathscr{A} = \bigcap\{A : A \in \mathscr{A}\} = \bigcap\{A_j : j \in J\} = \bigcap_{j\in J} A_j = \bigcap_j A_j$$

# Asocijativnost, distributivnost, komplement

Kao i za dvočlane unije i presjeke, vrijede ove formule:

$$A \cup \bigcup_{j \in J} A_j = \bigcup_{j \in J} (A \cup A_j) \qquad A \cap \bigcap_{j \in J} A_j = \bigcap_{j \in J} (A \cap A_j)$$

$$A \cap \bigcup_{j \in J} A_j = \bigcup_{j \in J} (A \cap A_j) \qquad A \cup \bigcap_{j \in J} A_j = \bigcap_{j \in J} (A \cup A_j)$$

Ako su $A_j \subseteq U$ za sve $j$ onda vrijede De Morganove formule

$$\Big(\bigcup_{j \in J} A_j\Big)^{\mathsf{C}} = \bigcap_{j \in J} A_j^{\mathsf{C}} \qquad \Big(\bigcap_{j \in J} A_j\Big)^{\mathsf{C}} = \bigcup_{j \in J} A_j^{\mathsf{C}}$$

tj.

$$U \setminus \bigcup_{j \in J} A_j = \bigcap_{j \in J} (U \setminus A_j) \qquad U \setminus \bigcap_{j \in J} A_j = \bigcup_{j \in J} (U \setminus A_j)$$

- Korisna je i ova, manje „prozirna" jednakost:

$$\bigcup(\mathscr{A} \cup \mathscr{B}) = \bigcup \mathscr{A} \cup \bigcup \mathscr{B} \qquad (*)$$

- OPREZ: Analogna jednakost za presjek ne *vrijedi*! Objasni!

# Induktivni skupovi

Intuitivno znamo što je beskonačan skup. Takvi su npr. skupovi $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$,... ali iz dosadašnjih aksioma ne možemo zaključiti da beskonačni skupovi postoje. No, najprije jedna definicija:

**Definicija 3.1**

Neka je $S$ neki skup. Skup $S^+ := S \cup \{S\}$ (koji postoji prema aksiomima para i unije), naziva se *sljedbenik skupa* $S$.

**Primjer 3.2**

$$\begin{aligned}
\emptyset^+ &= \emptyset \cup \{\emptyset\} = \{\emptyset\} \\
\emptyset^{++} &= \emptyset^+ \cup \{\emptyset^+\} = \{\emptyset\} \cup \big\{\{\emptyset\}\big\} = \big\{\emptyset, \{\emptyset\}\big\} \\
&\vdots
\end{aligned}$$

**Definicija 3.3**

Za skup $A$ kažemo da je *induktivan* ako mu pripadaju prazan skup i sljedbenik svakog elementa skupa $A$.

# Aksiom beskonačnosti

**AKSIOM BESKONAČNOSTI**

Postoji induktivan skup.

**Teorem 3.4**

*Presjek bilo koje neprazne familije $\mathscr{S}$ induktivnih skupova je induktivan skup.*

Dokaz: Za $\forall A \in \mathscr{S}$ je $\emptyset \in A$ pa je $\emptyset \in \bigcap \mathscr{S}$.

Ako je $x \in \bigcap \mathscr{S}$ onda je $x \in A$ za svaki $A \in \mathscr{S}$,

$\Rightarrow \quad x^+ \in A$ za sve $A \in \mathscr{S}$ jer su skupovi $A$ induktivni

$\Rightarrow \quad x^+ \in \bigcap \mathscr{S}$

$\Rightarrow \quad$ presjek $\bigcap \mathscr{S}$ je induktivan skup. $\square$

# Najmanji induktivan skup

**Teorem 3.5**

*Postoji najmanji (u smislu inkluzije) induktivan skup.*

Dokaz: Neka je $A$ bilo koji induktivan skup i neka je $\omega$ presjek svih induktivnih podskupova od $A$. Prema teoremu 3.4, $\omega$ je induktivan skup.

Tvrdnja: $\omega$ je najmanji induktivan skup, tj. svaki induktivan skup $B$ sadrži $\omega$. Zaista, $A \cap B$ je induktivan skup, i podskup je od $A$, pa sadrži $\omega$ koji je sadržan u svim induktivnim podskupovima od $A$, tj. $\omega \subseteq A \cap B$; specijalno je $\omega \subseteq B$. $\square$

# $\omega$ — prošireni skup prirodnih brojeva

Navedimo nekoliko elemenata skupa $\omega$ i njihove uobičajene nazive i oznake:

$$
\begin{aligned}
\emptyset &=: 0 \\
0^+ &= 0 \cup \{0\} = \emptyset \cup \{\emptyset\} = \{\emptyset\} =: 1 \\
1^+ &= 1 \cup \{1\} = \{\emptyset\} \cup \big\{\{\emptyset\}\big\} = \big\{\emptyset, \{\emptyset\}\big\} = \{0, 1\} =: 2 \\
2^+ &= 2 \cup \{2\} = \{0, 1\} \cup \{2\} = \{0, 1, 2\} =: 3 \\
&\vdots \\
n^+ &= n \cup \{n\} = \{0, 1, 2, \ldots, n-1\} \cup \{n\} = \{0, 1, 2, \ldots, n-1, n\} =: n+1 \\
&\vdots
\end{aligned}
$$

**Definicija 3.6**

Skup $\omega$ naziva se *prošireni skup prirodnih brojeva*.
Koristi se i oznaka $\mathbb{N}_0$. Dakle, $\omega = \mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

# Princip matematičke indukcije

Jedno od najvažnijih svojstava skupa $\omega$ je sljedeće:

**Teorem 3.7 (Princip matematičke indukcije)**

*Neka je $S \subseteq \omega$ podskup sa svojstvom da je $0 \in S$ i da ako je $n \in S$ onda je i $n^+ \in S$. Tada je $S = \omega$.*

Dokaz: Iz pretpostavki teorema slijedi da je skup $S$ induktivan, a kako je $\omega$ najmanji induktivan skup, to je $\omega \subseteq S \subseteq \omega$, pa je $S = \omega$. □

Iz definicije prirodnih brojeva, tj. skupa $\omega$, vidimo da je, npr.,
$3 = \{0, 1, 2\} \subseteq \{0, 1, 2, 3\} = 4$, tj. $3 \subseteq 4$. Ali i $3 \in 4$.
Slično je $2 \in 3 \in 5$, ali i $2 \in 5$.

Zato nije neobična sljedeća definicija:

**Definicija 3.8**

Za skup $A$ kažemo da je *tranzitivan* ako je svaki element nekog elementa skupa $A$ i sâm element skupa $A$.

# Tranzitivni skupovi

**Teorem 3.9**

(a) *Skup $A$ je tranzitivan ako i samo ako je svaki element skupa $A$ ujedno i podskup skupa $A$.*

(b) *Skup $A$ je tranzitivan ako i samo ako je $\bigcup A \subseteq A$.*

Dokaz: (a) $\Rightarrow$ Ako je $a \in A$ i $x \in a$ onda je $x \in A$, pa je $a \subseteq A$.

$\Leftarrow$ $(\forall a \in A \Rightarrow a \subseteq A) \implies \forall x \in a$ je $x \in a \subseteq A$, pa je $x \in A$. $\triangle$

(b) $\Rightarrow$ Neka je skup $A$ tranzitivan i $x \in \bigcup A$. Tada $\exists a \in A$ t.d. je $x \in a$, pa je, zbog tranzitivnosti, i $x \in A$, tj. $\bigcup A \subseteq A$.

$\Leftarrow$ Neka je $\bigcup A \subseteq A$. Za $a \in A$ i $x \in a$ je $x \in a \subseteq \bigcup_{a' \in A} a' = \bigcup A \subseteq A$, t.j. $x \in A$, pa je skup $A$ tranzitivan. $\square$

# Tranzitivni skupovi

**Teorem 3.10**

*Ako je $A$ tranzitivan skup onda je $\bigcup A^+ = A$.*

Dokaz: $A^+ = A \cup \{A\}$ pa je

$$\begin{aligned}
\bigcup A^+ &= \bigcup \left(A \cup \{A\}\right) \\
&= \left(\bigcup A\right) \cup \Big(\underbrace{\bigcup \{A\}}_{\text{unija jednočlane familije}}\Big) \qquad \text{(prema jednakosti } (*) \text{ na str. 24)} \\
&= \Big(\underbrace{\bigcup A}_{\subseteq A \text{ jer je } A \text{ tranzitivan, tm. 3.9}(b)}\Big) \cup A = A
\end{aligned}$$

$\square$

# Prirodni brojevi su tranzitivni skupovi

**Teorem 3.11**

*Svaki element skupa $\omega$, t.j. svaki prirodan broj uključujući i 0, je tranzitivan skup.*

Dokaz: Indukcijom: Neka je $S \subseteq \omega$ podskup onih prirodnih brojeva koji su tranzitivni. Očito je $0 \in S$, po definiciji tranzitivnosti.

$n \rightsquigarrow n^+$: Neka je $n \in S$ i neka je $x \in n^+ = n \cup \{n\}$. Tada je $x \in n$ ili $x = n$.

1. Ako je $x \in n$ onda je $\underbrace{x \subseteq n}_{\text{jer je } n \text{ tranzitivan, tm. 3.9}(a)} \subseteq n^+$, t.j. $x \subseteq n^+$.
2. Ako je pak $x = n$ onda je $x \subseteq n \cup \{n\} = n^+$.

Dakle, svaki element skupa $n^+$ je ujedno i njegov podskup, pa je, prema teoremu 3.9($a$), skup $n^+$ tranzitivan, t. j. $n^+ \in S$.

Prema principu matematičke indukcije zaključujemo da je $S = \omega$, tj. svaki prirodan broj je tranzitivan skup. □

# Prirodni brojevi kao skupovi nekih prirodnih brojeva

**Korolar 3.12**

*Svaki je prirodan broj skup nekih prirodnih brojeva.*

Dokaz: Neka je $n \in \omega$. Za svaki element $x \in n$ je $x \in n \in \omega$, pa kako je skup $\omega$ tranzitivan, to je $x \in \omega$, tj. svaki element skupa $n$ je prirodan broj. $\square$

NAPOMENA: Na skupu $\omega$ može se definirati uređaj ovako:

$$m < n \text{ ako je } m \in n$$

pa se dokaže da je svaki prirodan broj jednak skupu svih od njega manjih prirodnih brojeva.

Također, definiraju se i računske operacije i dokazuju njihova svojstva, ali se mi time nećemo baviti.

# Peanovi aksiomi

Osnovna svojstva skupa $\omega$ opisana su ovim teoremom:

**Teorem 3.13 (Peanovi aksiomi[4])**

(*i*) $0 \in \omega$

(*ii*) $n \in \omega \Rightarrow n^+ \in \omega$

(*iii*) *Ne postoji* $x \in \omega$ *t.d. je* $x^+ = 0$, *tj. za* $\forall x \in \omega$ *je* $x^+ \neq 0$.

(*iv*) *Ako* $S \subseteq \omega$ *ima svojstvo da je* $0 \in S$ *i da* $(n \in S \Rightarrow n^+ \in S)$, *onda je* $S = \omega$.

(*v*) *Ako za* $m, n \in \omega$ *vrijedi* $m^+ = n^+$ *onda je* $m = n$.

Dokaz: (*i*) i (*ii*) slijede neposredno iz definicije induktivnog skupa.

(*iii*) Za svaki $x \in \omega$ je $x^+ = x \cup \{x\} \neq \emptyset = 0$.

(*iv*) To je princip matematičke indukcije koji smo dokazali.

(*v*) $m^+ = n^+ \Rightarrow \bigcup m^+ = \bigcup n^+$. Kako su $m$ i $n$ tranzitivni skupovi, to je prema teoremu 3.10, $\bigcup m^+ = m$ i $\bigcup n^+ = n$, pa je $m = n$. $\square$

[4] Ovim je aksiomima 1889. J. Peano definirao prirodne brojeve i iz njih izveo sva uobičajena svojstva.

# Dokaz matematičkom indukcijom

Što je to *dokaz matematičkom indukcijom*?

Želimo dokazati da je neka tvrdnja T, koja ovisi o prirodnom broju $n$, istinita za sve prirodne brojeve.

*Dokaz matematičkom indukcijom* sastoji se od dvije faze:

($i$) *baza indukcije:* dokaže se da vrijedi $\mathrm{T}(0)$ ili $\mathrm{T}(1)$;

($ii$) *korak indukcije:* za svaki $n \in \omega$, uz pretpostavku istinitosti tvrdnje $\mathrm{T}(n)$, dokaže se istinitost tvrdnje $\mathrm{T}(n+1)$.[5]

Time je dokazano da je tvrdnja $\mathrm{T}(n)$ istinita za sve $n \in \omega$ odnosno $n \in \mathbb{N}$.

Dokaz da *dokaz matematičkom indukcijom* zaista dokazuje istinitost tvrdnje $\mathrm{T}(n)$ za sve $n$:

Neka je $S \subseteq \omega$ skup onih $n$-ova za koje je tvrdnja $\mathrm{T}(n)$ istinita.

Zbog ($i$) je $0 \in S$, a iz ($ii$) slijedi da $(n \in S \Rightarrow n+1 = n^+ \in S)$,

pa je $S = \omega$ prema principu matematičke indukcije.

[5] Korak indukcije može izgledati i ovako:

($ii$)* za svaki $n \in \omega$, uz pretpostavku istinitosti tvrdnji $\mathrm{T}(k)$ za $k = 0, \ldots, n$, dokaže se istinitost tvrdnje $\mathrm{T}(n+1)$.

## 2 RELACIJE I FUNKCIJE

- Funkcije – neformalno
- Kartezijev produkt
- Binarne relacije

# Oznake i terminologija koju znamo od ranije

Podsjetimo se nekih oznaka i terminologije koju ćemo rabiti:

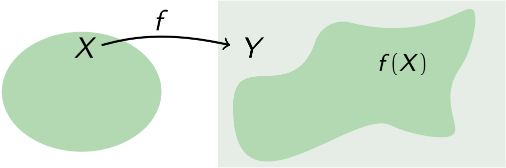
$f : X \to Y$ domena / kodomena Čitaj: „f sa X u Y".

$f(x)$ je *vrijednost* funkcije $f$ u točki $x$, $f(x) \in Y$.

sin $x$ **nije** funkcija! To je *vrijednost* funkcije $\sin : \mathbb{R} \to \mathbb{R}$ u točki $x \in \mathbb{R}$.

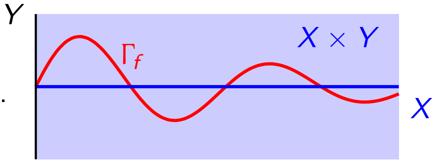
$f(A) := \{f(x) : x \in A\}$ gdje je $A$ podskup od $X$,

dakle $f(A) \subseteq Y$ i naziva se *slika* skupa $A$.




*Slika funkcije f* je skup $f(X) \subseteq Y$.

*Graf funkcije f* je skup $\Gamma_f := \{(x, f(x)) : x \in X\} \subseteq X \times Y$.



# Kompozicija; injekcija–surjekcija–bijekcija; praslika

*Kompozicija funkcija* $f\colon X \to Y$ i $g\colon Y \to Z$ je funkcija $g\circ f\colon X \to Z$
definirana s $(g \circ f)(x) := g(f(x))$ i piše se $g\,f(x)$ ili $(g\,f)(x)$.

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[rr, bend right, "g\circ f"'] & Y \arrow[r, "g"] & Z \end{tikzcd}$$

Za $A \subseteq X$ *inkluzija* $\iota\colon A \to X$ je dana s $\iota(x) = x$, $x \in A$.
Za $f\colon X \to Y$ i $A \subseteq X$ *restrikcija* $f|_A\colon A \to Y$ je definirana s
$(f|_A)(x) := f(x)$, $x \in A$.

*injekcija (1–1 preslikavanje)* / *surjekcija (preslikavanje na)* / *bijekcija*
*identiteta* $id\colon X \to X$, ili $\mathbb{1}\colon X \to X$, ili $\mathbb{1}_X\colon X \to X$: $id(x) = x, \forall x \in X$
*konstantna funkcija* $c\colon X \to Y$ za koju je $c(x) = c(x')$ za sve $x, x' \in X$
*Praslika* skupa $B \subseteq Y$ je skup $f^{-1}(B) := \{x \in X : f(x) \in B\} \subseteq X$
bez obzira postoji li funkcija $f^{-1}$ ili ne!
[rabi se i oznaka $f^{\leftarrow}(B)$ posebno $f^{\leftarrow}(y)$ za $f^{-1}(y) \equiv f^{-1}(\{y\})$
kada $f^{-1}$, kao funkcija s $Y$ u $X$, ne postoji.]

# Inverzna funkcija

Nekoliko činjenica o kompoziciji funkcija:

- Kompozicija funkcija je asocijativna, tj. $h \circ (g \circ f) = (h \circ g) \circ f$.
- Ako je $g \circ f$ injekcija onda je $f$ injekcija.
- Ako je $g \circ f$ surjekcija onda je $g$ surjekcija.
- Ako su $f$ i $g$ bijekcije onda je i kompozicija $g \circ f$ bijekcija.
- Ako je $g \circ f$ bijekcija, može li se išta reći o funkcijama $f$ i/ili $g$?

Inverzna funkcija: Neka je $f\colon X \to Y$. Ako postoji funkcija $g\colon Y \to X$ t.d. je $g \circ f = \mathbb{1}_X$ i $f \circ g = \mathbb{1}_Y$ onda je $g$ *inverzna funkcija* funkcije $f$.
Nema svaka funkcija inverznu funkciju. Ali ako inverzna funkcija postoji onda je ona jedinstvena i označuje se $f^{-1}\colon Y \to X$.

Još nekoliko činjenica:

- $\forall A \subseteq X$ je $A \subseteq f^{-1}\big(f(A)\big)$. Jednakost vrijedi akko je $f$ injekcija.
- $\forall B \subseteq Y$ je $f\big(f^{-1}(B)\big) \subseteq B$. Jednakost vrijedi akko je $f$ surjekcija.
- $f(\bigcup_\alpha A_\alpha) = \bigcup_\alpha f(A_\alpha)$, $\qquad f(\bigcap_\alpha A_\alpha) \subseteq \bigcap_\alpha f(A_\alpha)$
- $f^{-1}(\bigcup_\beta B_\beta) = \bigcup_\beta f^{-1}(B_\beta) \qquad f^{-1}(\bigcap_\beta B_\beta) = \bigcap_\beta f^{-1}(B_\beta)$

# Uređen par

Za definiciju Kartezijevog produkta dvaju skupova treba nam pojam uređenog para:

## Definicija 5.1

Neka su $x$ i $y$ dva objekta (tj. skupa u „pravoj" teoriji skupova). Skup $\{\underbrace{\{x\}}, \underbrace{\{x,y\}}\}$ naziva se *uređen par* i označuje se $(x,y)$.

ova dva (neuređena) para postoje prema aksiomima para i unije

$x$ se naziva *prva* a $y$ *druga koordinata* uređenog para $(x,y)$, a od ranije „poznatu" činjenicu da su dva uređena para jednaka ako i samo ako su im jednake odgovarajuće koordinate, treba dokazati — ona nije dio definicije.

## Teorem 5.2

$$(x,y)=(x',y') \;\Leftrightarrow\; x=x' \;\&\; y=y'$$

# Dokaz teorema 5.2 o jednakosti uređenih parova

Dokaz: $\Leftarrow$ Ovaj smjer je očit.

$\Rightarrow$ Neka je $\underbrace{\big\{\{x\},\{x,y\}\big\} = (x,y)}_{\Rightarrow \{x\} \in (x,y) = (x',y') = \{\{x'\},\{x',y'\}\}} = (x',y') = \big\{\{x'\},\{x',y'\}\big\}$.

Stoga je $\{x\} = \{x'\}$ ili $\{x\} = \{x',y'\}$.

$(a)$ Ako je $\{x\} = \{x'\}$ onda je prema AX ekstenzionalnosti $x = x'$.

Tada je $\{x,y\} \in \big\{\{x'\},\{x',y'\}\big\} = \big\{\{x\},\{x,y'\}\big\}$, pa je

ili $(a_1)$ $\{x,y\} = \{x\} \;\Rightarrow\; y \in \{x\} \;\Rightarrow\; y = x$, te je

$$\left.\begin{aligned} (x,y) &= \big\{\{x\},\{x,x\}\big\} = \big\{\{x\},\{x\}\big\} = \big\{\{x\}\big\} \\ &= (x',y') = (x,y') = \big\{\{x\},\{x,y'\}\big\} \end{aligned}\right] =$$

$\Rightarrow \{x,y'\} \in \{\{x\}\} \;\Rightarrow\; \{x,y'\} = \{x\} \;\Rightarrow\; y' = x$, dakle $x = x' = y = y'$, $\triangle$

ili $(a_2)$ $\{x,y\} = \{x,y'\}$ pa je ili $y = y'$ te smo gotovi,

ili je $y = x$ pa kao u $(a_1)$ dobivamo $x = x' = y = y'$. $\triangle$

$(b)$ Ako je $\{x\} = \{x',y'\}$ onda su $x', y' \in \{x\}$ pa je $x' = y' = x$. Kao u $(a)$ zaključujemo da je i $y = x$ pa je opet $x = x' = y = y'$. $\square$

# Kartezijev produkt

**Teorem 5.3**

*Neka su $A$ i $B$ skupovi. Tada je klasa $\{(a, b) : a \in A,\ b \in B\}$ također skup.*
*Nazivamo ga Kartezijev ili direktan produkt skupova $A$ i $B$ i označujemo $A \times B$.*

Dokaz: Prema aksiomima para i unije postoji skup $A \cup B$,
pa prema AX partitivnog skupa postoji skup $\mathscr{P}(\mathscr{P}(A \cup B))$.
Prema AX separacije, klasa

$$\{z : \underbrace{z \in \mathscr{P}(\mathscr{P}(A \cup B)) \text{ i } \big(\exists u \in A,\ \exists v \in B \text{ t.d. je } z = (u, v)\big)}_{\sigma(z)}\}$$

je skup, i to je upravo Kartezijev produkt $A \times B$. Naime,

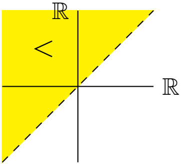
$$z = (u, v) = \underbrace{\{\underbrace{\{u\}}_{\in \mathscr{P}(A) \subseteq \mathscr{P}(A \cup B)}, \underbrace{\{u, v\}}_{\in \mathscr{P}(A \cup B)}\}}_{\in \mathscr{P}(\mathscr{P}(A \cup B))}.$$

□

# Primjeri

- $a < b$, („$a$ je manji od $b$"), je jedna relacija među realnim brojevima. Za neke uređene parove $(a, b)$ realnih brojeva ona vrijedi, a za neke ne. Za par $(2, 5)$ ona vrijedi jer je $2 < 5$, ali za par $(7, 1)$ ne vrijedi jer $7 \not< 1$. Kaže se i da neki parovi $(a, b) \in \mathbb{R} \times \mathbb{R}$ jesu u relaciji $<$, a neki nisu.

  Dakle, relacija $<$ je podskup skupa $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$.




- Djeljivost prirodnih brojeva, $m \mid n$, $(m, n) \in \mathbb{N} \times \mathbb{N}$.
- Sličnost trokutova u ravnini.

  Ali u relaciji mogu biti i elementi različitih skupova, naprimjer:

- Neka je $\mathcal{K}$ skup svih kružnica ravnine $\mathbb{R}^2$, i neka su $P \in \mathbb{R}^2$ i $k \in \mathcal{K}$ u relaciji „je središte od" ako je točka $P$ središte kružnice $k$. Dakle, „je središte od" je neki podskup skupa $\mathbb{R}^2 \times \mathcal{K}$.

# Binarna relacija

**Definicija 6.1**

Neka su $X$ i $Y$ dva skupa. Svaki podskup $R \subseteq X \times Y$ naziva se *binarna relacija* iz $X$ u $Y$.
Umjesto $(x, y) \in R$ najčešće se piše $x\,R\,y$, i čita se „$x$ je u relaciji s $y$”.
Ako je $X = Y$ kaže se da „$R$ je relacija na $X$”.

Neka svojstva koja relacija $R$ na $X$ može imati:

- $(a)$ *refleksivnost*: za svaki $x$ je $x\,R\,x$; $\Delta := \{(x, x) : x \in X\} \subseteq R$
- $(b)$ *antirefleksivnost*: za svaki $x$ je $\neg(x\,R\,x)$; $R \cap \Delta = \emptyset$
- $(c)$ *simetričnost*: $x\,R\,y \Rightarrow y\,R\,x$;
- $(d)$ *antisimetričnost*: $(x\,R\,y \;\&\; y\,R\,x) \;\Rightarrow\; x = y$;
- $(e)$ *asimetričnost*: $x\,R\,y \;\Rightarrow\; \neg(y\,R\,x)$;
- $(f)$ *tranzitivnost*: $(x\,R\,y \;\&\; y\,R\,z) \;\Rightarrow\; x\,R\,z$;
- $(g)$ *povezanost* ili *usporedivost*: $x \neq y \;\Rightarrow\; (x\,R\,y$ ili $y\,R\,x)$.

# Relacija ekvivalencije

Nas će u ovom kolegiju zanimati prvenstveno relacije uređaja, $<$ ili $\leqslant$ (jer relacije ekvivalencije „znamo”). Ipak, ponovimo:

**Definicija 6.2**

Relacija koja je refleksivna, simetrična i tranzitivna naziva se *relacija ekvivalencije*.

**Primjeri 6.3**

- *jednakost (brojeva, podskupova, funkcija, ...);*
- *sličnost i kongruencija trokutova u ravnini;*
- *paralelnost pravaca u ravnini;*
- *sličnost matrica;*

  $\vdots$

# Particija skupa i relacija ekvivalencije

DEFINICIJA: Svaki rastav skupa $X$ na međusobno disjunktne podskupove naziva se *particijom skupa* $X$.

**Teorem**

*Svaka relacija ekvivalencije na skupu $X$ definira jednu particiju toga skupa, i obratno, svaka particija skupa $X$ definira jednu relaciju ekvivalencije na tom skupu.*

Za relaciju ekvivalencije $R$ na skupu $X$, članove pripadne particije toga skupa nazivamo *klase ekvivalencije* (s obzirom na relaciju $R$), i te klase zaista jesu skupovi.

Klasu ekvivalencije koja sadrži element $x \in X$ označujemo $[x]$. Dakle, $[x] = \{x' \in X : x' R\, x\}$. Svaki element klase $[x]$ naziva se *reprezentantom* ili *predstavnikom* te klase.

DEFINICIJA: Skup $\{[x] : x \in X\}$ svih klasa ekvivalencije skupa $X$ s obzirom na relaciju ekvivalencije $R$ naziva se *kvocijentni skup* i označuje $X/R$.

# Primjer: racionalni brojevi

U skupu $\mathbb{N} \times \mathbb{N}$ definiramo relaciju $\sim \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ ovako:

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

Refleksivnost i simetrija su očite, pa provjerimo tranzitivnost:

$$\left.\begin{array}{l} (a,b) \sim (c,d) \;\Rightarrow\; ad = bc \;\overset{\cdot f}{\Rightarrow}\; adf = bcf \\ (c,d) \sim (e,f) \;\Rightarrow\; cf = de \;\overset{\cdot b}{\Rightarrow}\; bcf = bde \end{array}\right] \Rightarrow adf = bde \;\overset{:d}{\Rightarrow}\; af = be,$$

te je $(a, b) \sim (e, f)$. □

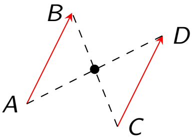
A što je kvocijentni skup $(\mathbb{N}\times\mathbb{N})/\sim$? Što su klase ekvivalencije $[(a, b)]$? To su pozitivni *racionalni brojevi*. (Da smo gledali istu relaciju $\sim$ na $\mathbb{Z} \times \mathbb{N}$ dobili bismo sve racionalne brojeve, tj. skup $\mathbb{Q}$.)

Dakle, *racionalni brojevi su klase ekvivalencije razlomaka*.

Umjesto npr. $[(2, 3)]$ piše se i $\left[\frac{2}{3}\right]$, ali najčešće samo $\frac{2}{3}$, t. j. identificira se klasa ekvivalencije s nekim reprezentantom te klase. Tako $\frac{2}{3} = \frac{4}{6}$ (kako nas uče u osnovnoj školi), zapravo znači $\left[\frac{2}{3}\right] = \left[\frac{4}{6}\right]$, tj. $(2, 3) \sim (4, 6)$, ili drukčije pisano, $\frac{2}{3} \sim \frac{4}{6}$.

# Primjer: orijentirane dužine i vektori

Slična je situacija s definicijom vektora u ravnini ili prostoru. *Vektori* u ravnini su *klase ekvivalencije* orijentiranih dužina, pri čemu su dvije orijentirane dužine $\overrightarrow{AB}$ i $\overrightarrow{CD}$ ekvivalentne ako se dužine $\overline{AD}$ i $\overline{CB}$ raspolavljaju.




(Ima posla da se dokaže tranzitivnost.)

U prostoru treba još zahtijevati da su orijentirane dužine $\overrightarrow{AB}$ i $\overrightarrow{CD}$ komplanarne.

OBJASNITI frazu „definicija je dobra” na primjeru zbrajanja racionalnih brojeva i zbrajanja vektora.

# Funkcije kao relacije

U §4 govorili smo o funkcijama ali ih zapravo nismo bili definirali.

## Definicija 6.4

*Funkcija* $f$ sa skupa $X$ u skup $Y$ je svaka relacija $f \subseteq X \times Y$ za koju vrijedi:

$(i)$ za $\forall x \in X, \exists y \in Y$ t.d. je $(x, y) \in f$, i

$(ii)$ ako su $(x, y) \in f$ i $(x, y') \in f$ onda je $y' = y$.

$(i)$ i $(ii)$ se zajednički mogu zapisati ovako:

za $\forall x \in X, \exists! y \in Y$ t.d. je $(x, y) \in f$.

Umjesto $(x, y) \in f$ piše se $y = f(x)$, a umjesto $f \subseteq X \times Y$ piše se $f\colon X \to Y$.

Dakle, funkcija $f$ se ***definira*** kao njezin graf $\Gamma_f \subseteq X \times Y$.

# Slika funkcije je skup

**Teorem 6.5**

*Neka su $X$ i $Y$ skupovi a $f : X \to Y$ funkcija. Za svaki podskup $A \subseteq X$ je klasa*

$$f(A) := \{y : \underbrace{y \in Y \text{ i } \exists x \in A \text{ t.d. je } (x,y) \in f}_{\sigma(y)}\}$$

*također skup.*
*Specijalno, $f(X) := \{y \in Y : \exists x \in X \text{ t.d. je } y = f(x)\}$ je skup, $f(X) \subseteq Y$, i naziva se slika funkcije $f$.*

Dokaz: Tvrdnja slijedi iz AX separacije za svojstvo $\sigma(y)$. $\square$

**Teorem 6.6**

*Neka su $X$ i $Y$ skupovi, $B \subseteq Y$, i $f : X \to Y$ funkcija. Tada je klasa $f^{-1}(B) := \{x \in X : \exists y \in B \text{ t.d. je } y = f(x)\} \subseteq X$ također skup, i naziva se praslika ili original skupa $B$.*

## 3 POTENTNOST SKUPOVA

- Ekvipotentni skupovi
- Konačni skupovi
- Prebrojivi i neprebrojivi skupovi
- Princip rekurzivne definicije
- Beskonačni skupovi i aksiom izbora
- Kardinalnost

# Ekvipotentnost

Želimo nekako razlikovati skupove „po veličini”.
Za konačne skupove to je lako — „prebrojimo” ih.
Ali što to znači: prebrojiti? I što znači da je npr. $3 < 7$?

- Priča o putnicima i sjedalima u autobusu.

## Definicija 7.1

Za skupove $A$ i $B$ kažemo da su *ekvipotentni* ako postoji bijekcija $f\colon A \to B$. (Dakle, injektivna surjekcija ***s*** $A$ ***na*** $B$.)
U tom slučaju pisat ćemo $A \sim B$.

## Primjeri 7.2

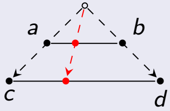
- $\{7, 15, -6\} \sim \{2, \pi, \sqrt{-1}\}$
- $\{0, 1\} \sim \{\Box, \triangle\}$
- $\{1, 2, 3, \dots\} \sim \{2, 4, 6, \dots\}$
- $\mathbb{N} \sim \mathbb{Z}$

# Primjeri

## Primjeri 7.3

- $[a, b] \sim [c, d]$ geometrijski:

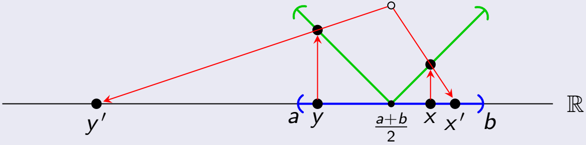
  $x \mapsto c + \frac{d-c}{b-a}(x-a)$




- $\langle a, b\rangle \sim \mathbb{R}$

  $x \mapsto x'$

  $y \mapsto y'$




ili:

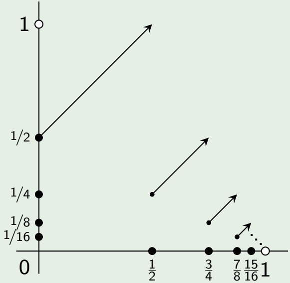
$$\begin{tikzcd}
\langle a, b\rangle \arrow[r, bend left, "x \mapsto \frac{\pi}{2} + \frac{\pi}{b-a}(x-b)"] \arrow[rr, bend right, "x \mapsto \mathrm{tg}\left(\frac{\pi}{2} + \frac{\pi}{b-a}(x-b)\right)"'] & \left\langle -\frac{\pi}{2}, \frac{\pi}{2}\right\rangle \arrow[r, bend left, "\mathrm{tg}"] & \mathbb{R}
\end{tikzcd}$$

# Primjeri

## Primjer 7.4

$[0,1\rangle \sim \langle 0,1\rangle$

$$f(x) = \begin{cases} x + \frac{1}{2} & , 0 \leqslant x < \frac{1}{2} \\ x - \frac{1}{4} & , \frac{1}{2} \leqslant x < \frac{3}{4} \\ x - \frac{5}{8} & , \frac{3}{4} \leqslant x < \frac{7}{8} \\ x - \frac{13}{16} & , \frac{7}{8} \leqslant x < \frac{15}{16} \\ & \vdots \end{cases}$$




Za vježbu dokažite

## Primjer 7.5

$[0,1] \sim \langle 0,1\rangle$

# Primjeri

## Primjer 7.6

$$\langle 0,1] \sim \langle 0,1] \times \langle 0,1]$$

Svaki broj $x \in \langle 0,1]$ ima jedinstven zapis bez beskonačno mnogo nula. Kao primjer, neka je $x = 0.02300100054309500041\ldots$

Znamenke svrstamo u grupe koje završavaju znamenkom različitom od nule: $x = 0.02\ 3\ 001\ 0005\ 4\ 3\ 09\ 5\ 004\ 1\ \ \ldots$

i takav $x \in \langle 0,1]$ preslikamo u par $(x_1, x_2) \in \langle 0,1] \times \langle 0,1]$ ovako:

$$x \mapsto (x_1, x_2) := (0.02\ 001\ 4\,09\ 004\ \ \ldots,\ 0.3\ 0005\ 3\ 5\ 1\ \ \ldots)$$

Jasno je kako se definira inverzno preslikavanje: $x_1$ i $x_2$ se zapišu u grupama kao gore, pa se paru $(x_1, x_2)$ pridruži $x$ definiran tako da se za decimale uzimaju naizmjence grupe od $x_1$ odnosno $x_2$.

# O injekcijama početnog komada skupa $\mathbb{N}$

OZNAKA: Za svaki $k \in \mathbb{N}$ skup $\{1, 2, \ldots, k\}$ nazivamo *početnim komadom* ili *početnim segmentom* skupa $\mathbb{N}$, i označujemo ga $[1\,..\,k]$.[6]

**Teorem 8.1**

*Za svaki $k \in \mathbb{N}$ je svaka injekcija $f\colon [1\,..\,k] \to [1\,..\,k]$ ujedno i surjekcija, dakle, bijekcija.*

Dokaz: Indukcijom po $k$. Za $k = 1$ je $[1\,..\,1] = \{1\}$, pa je tvrdnja očigledna.

$k \rightsquigarrow k+1$: Neka je $f\colon [1\,..\,k+1] \to [1\,..\,k+1]$ injekcija.
Tada je i restrikcija $f|_{[1\,..\,k]}\colon [1\,..\,k] \to [1\,..\,k+1]$ injekcija.
Imamo dva slučaja:

1. slučaj: $f(k+1) = k+1$. Tada je $f\big([1\,..\,k]\big) \subseteq [1\,..\,k]$, pa je restrikcija $f|_{[1\,..\,k]}\colon [1\,..\,k] \to [1\,..\,k]$ injekcija, dakle, PPI,[7] i surjekcija. Stoga je i $f\colon [1\,..\,k+1] \to [1\,..\,k+1]$ surjekcija. $\triangle$

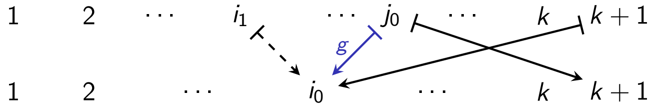
---

[6] Vuković, *Teorija skupova*, koristi oznaku $\mathbb{N}_k$.

[7] Koristit ćemo skraćenicu PPI umjesto „po pretpostavci indukcije”.

# Završetak dokaza teorema 8.1

2. slučaj: $f(k+1) =: i_0 \in [1\,..\,k]$. Zbog injektivnosti $\exists!\, j_0 \in [1\,..\,k]$ t.d. je $f(j_0) = k+1$. Inače bi bilo $f\big([1\,..\,k]\big) \subseteq [1\,..\,k]$ pa bi restrikcija $f|_{[1\,..\,k]} \colon [1\,..\,k] \to [1\,..\,k]$ bila injekcija, pa onda PPI, i surjekcija, te bi postojao $i_1 \in [1\,..\,k]$ t.d. je $f(i_1) = i_0 = f(k+1)$.




Ali kako je $i_1 \neq k+1$ dobili bismo kontradikciju s injektivnošću od $f$. Postoji, dakle, jedinstven $j_0 \in [1\,..\,k]$ t.d. je $f(j_0) = k+1$. △

Definirajmo $g \colon [1\,..\,k] \to [1\,..\,k]$ ovako: $g(j) = \begin{cases} f(j)\,, & \text{za } j \neq j_0 \\ i_0\,, & \text{za } j = j_0 \end{cases}$.

$g$ je očito injekcija, pa je PPI i surjekcija. Stoga je i $f$ surjekcija. Naime, neka je $\ell \in [1\,..\,k+1]$ proizvoljan.

a) Ako je $\ell \neq i_0, k+1$ onda zbog surjektivnosti od $g$, $\exists j \in [1\,..\,k]$ t.d. je $f(j) = \ell$.

b) Ako je $\ell = i_0$ onda je $f(k+1) = i_0 = \ell$.

c) Ako je $\ell = k+1$ onda je $f(j_0) = k+1 = \ell$. □

# Konačni skupovi

## Definicija 8.2

Za skup $A$ kažemo da je *konačan* ako je prazan ili ako postoji $n \in \mathbb{N}$ t.d. je $A$ ekvipotentan skupu $[1 \,..\, n]$.

Teorem 8.1 pokazuje da je $n$ iz definicije jedinstven. Pišemo $\mathrm{k}(A) = n$, i kažemo da je *kardinalnost* od $A$ jednaka $n$.

Iz definicije neposredno slijedi:

## Korolar 8.3

*Ako su skupovi $A$ i $B$ ekvipotentni i skup $A$ je konačan, onda je i skup $B$ konačan.* □

Jednostavna posljedica teorema 8.1 je:

## Korolar 8.4

*Svaka injekcija $A \rightarrowtail A$ konačnog skupa $A$ u sâma sebe je ujedno i surjekcija, dakle i bijekcija.* □

# Podskupovi konačnih skupova su konačni skupovi

**Teorem 8.5**

*Za svaki podskup $A \subseteq [1\,..\,m]$ postoji $\ell \in \mathbb{N}$, $\ell \leqslant m$, takav da je $A$ ekvipotentan skupu $[1\,..\,\ell]$, pa je $\mathrm{k}(A) = \ell$.*

Dokaz: Indukcijom po $m$. Za $m = 1$ tvrdnja je očigledna.

$m \rightsquigarrow m+1$ : Neka je $m \in \mathbb{N}$ t. d. za $\forall B \subseteq [1\,..\,m]$, $\exists \ell \leqslant m$ t.d. je $\mathrm{k}(B) = \ell$.
Neka je $A \subseteq [1\,..\,m{+}1]$. Ako je $A \subseteq [1\,..\,m]$ onda tvrdnja slijedi iz PI.
Ostaje slučaj $m+1 \in A$. Tada je $A \setminus \{m+1\} \subseteq [1\,..\,m]$ pa PPI
$\exists \ell$ t.d. je $\mathrm{k}(A \setminus \{m+1\}) = \ell$, tj. $A \setminus \{m+1\} \sim [1\,..\,\ell]$.
Tada je $A \sim [1\,..\,\ell+1]$, tj. $\mathrm{k}(A) = \ell + 1$. $\square$

**Korolar 8.6**

*Svaki podskup konačnog skupa je konačan skup.*

Dokaz: Neka je $A \subseteq B$ gdje je $B$ neki konačan skup. Prema definiciji, postoji $m \in \mathbb{N}$ t.d. je $B \sim [1\,..\,m]$, pa je $A \sim A'$ za neki $A' \subseteq [1\,..\,m]$.
Prema teoremu 8.5 postoji $\ell \leqslant m$ t.d. je $A \sim [1\,..\,\ell]$. $\square$

# Podsjetnik: induktivni skupovi

Vratimo se načas prirodnim brojevima. Jedna varijanta definicije induktivnog podskupa od $\mathbb{R}$, je sljedeća:

**Definicija 8.7**

Podskup $A \subseteq \mathbb{R}$ je *induktivan* ako sadrži broj 1 i za svaki $x \in A$ je i $x + 1 \in A$.

Očito je presjek svih induktivnih podskupova od $\mathbb{R}$ jednak skupu $\mathbb{N}$.

Dakle,

- $\mathbb{N}$ je induktivan skup, i
- vrijedi ***princip indukcije***:

  Ako je $A \subseteq \mathbb{N}$ induktivan podskup od $\mathbb{N}$ onda je $A = \mathbb{N}$.

# Dobro uređenje skupa prirodnih brojeva

**Teorem 8.8 (o dobrom uređenju skupa $\mathbb{N}$)**

(a) *Za svaki $n \in \mathbb{N}$, svaki neprazan podskup skupa $[1 \,..\, n]$ ima najmanji element.*

(b) *Svaki neprazan podskup skupa $\mathbb{N}$ ima najmanji element.*

Dokaz: (a): Neka je $A \subseteq \mathbb{N}$ skup onih $n$-ova za koje (a) vrijedi.

Očito je $1 \in A$ jer je jedini neprazan podskup od $[1 \,..\, 1] = \{1\}$ on sâm.

$n \rightsquigarrow n+1$ : Pretpostavimo da je $n \in A$ i neka je $C \subseteq [1 \,..\, n+1]$.

Ako je $C = \{n+1\}$ onda je $n+1$ najmanji element od $C$.

U protivnom promotrimo $C \cap [1 \,..\, n]$ koji je neprazan podskup od $[1 \,..\, n]$.

PPI je $n \in A$ pa $C \cap [1 \,..\, n]$ ima najmanji element, te je taj ujedno i najmanji element skupa $C$. Dakle, $C$ ima najmanji element, tj. $n+1 \in A$.

Kako je $A$ induktivan skup, zaključujemo da je $A = \mathbb{N}$. $\Rightarrow$ (a)

(b) Neka je $\emptyset \neq D \subseteq \mathbb{N}$, i odaberimo neki $n \in D$. Skup $D \cap [1 \,..\, n]$ je neprazan, pa prema (a) ima najmanji element. To će automatski biti i najmanji element skupa $D$. $\square$

# Karakterizacija konačnih skupova

## Teorem 8.9

*Neka je $A$ neprazan skup. Sljedeće su tvrdnje ekvivalentne:*

(i) *skup $A$ je konačan;*

(ii) *postoji $k \in \mathbb{N}$ i surjekcija $[1\,..\,k] \twoheadrightarrow A$;*

(iii) *postoji $m \in \mathbb{N}$ i injekcija $A \rightarrowtail [1\,..\,m]$.*

Dokaz: $(i) \Rightarrow (ii)$: $A \neq \emptyset$ je konačan pa postoji bijekcija $g\colon A \to [1\,..\,k]$ za neki $k$. Inverzna funkcija $g^{-1}\colon [1\,..\,k] \to A$ je tražena surjekcija. $\triangle$

$(ii) \Rightarrow (iii)$: Neka je $f\colon [1\,..\,k] \twoheadrightarrow A$ surjekcija. Za $a \in A$ neka je $b_a$ najmanji element skupa $f^{-1}(a) \subseteq [1\,..\,k]$.
Za $a \neq a'$ su skupovi $f^{-1}(a)$ i $f^{-1}(a')$ disjunktni, pa je $b_a \neq b_{a'}$.
Stoga je funkcije $g\colon A \to [1\,..\,k]$ definirana s $f(a) = b_a$ injekcija. $\triangle$

$(iii) \Rightarrow (i)$: Neka je $g\colon A \to [1\,..\,m]$ injekcija. Tada je korestrikcija $g\colon A \to g(A)$ bijekcija, pa je $A \sim g(A) \subseteq [1\,..\,m]$. Prema teoremu 8.5 je $g(A)$, a onda i $A$, konačan skup. $\square$

# Konačne unije i produkti konačnih skupova

**Korolar 8.10**

*Konačne unije i konačni Kartezijevi produkti konačnih skupova su konačni skupovi.*

Dokaz: Neka su $A$ i $B$ neprazni konačni skupovi, i neka su $f\colon [1\,..\,m] \to A$ i $g\colon [1\,..\,n] \to B$ bijekcije. Funkcija $h\colon [1\,..\,m+n] \to A \cup B$ definirana s $h(j) = \begin{cases} f(j) & , 1 \leqslant j \leqslant m \\ g(j-m) & , m+1 \leqslant j \leqslant m+n \end{cases}$
je očito surjekcija (možde ne i bijekcija!), pa je $A \cup B$ konačan skup. Sada se tvrdnja za proizvoljne konačne unije, dokaže indukcijom.

Dokažimo da je i produkt $A \times B$ konačan skup.
Za svaki $a \in A$ je skup $\{a\} \times B$ konačan jer je ekvipotentan skupu $B$, pa je produkt $A \times B = \bigcup\limits_{a \in A} \{a\} \times B$ konačan kao konačna unija konačnih skupova.

Tvrdnja za konačne produkte dokazuje se sada indukcijom. $\square$

# Beskonačni skupovi

Evo još jedne jednostavne posljedice teorema 8.1, točnije korolara 8.4:

**Korolar 8.11**

*Ako je A konačan skup onda ne postoji bijekcija skupa A na neki njegov pravi podskup, tj. konačan skup ne može biti ekvipotentan nekom svom pravom podskupu.* $\square$

i njegove posljedice

**Korolar 8.12**

*Skup $\mathbb{N}$ nije konačan.*

Dokaz: Funkcija $f\colon \mathbb{N} \to \mathbb{N}$ definirana s $f(n) = n + 1$ je bijekcija skupa $\mathbb{N}$ na njegov pravi podskup $\mathbb{N} \setminus \{1\}$. $\square$

**Definicija 8.13** (Ovo je definicija, ne tautologija !)

Skup koji nije konačan je *beskonačan skup* .

# Prebrojivi i neprebrojivi skupovi

Odsada ćemo se gotovo isključivo baviti takvim, beskonačnim skupovima. Pa pogledajmo najprije „najmanje" beskonačne skupove.

## Definicija 9.1

Skup $A$ je *prebrojivo beskonačan* ako postoji bijekcija $f\colon A \to \mathbb{N}$.
Skup je *prebrojiv* ako je konačan ili prebrojivo beskonačan.
Skup koji nije prebrojiv je *neprebrojiv.*

Evo nekoliko jednostavnih primjera prebrojivo beskonačnih skupova:

## Primjeri 9.2

- $\mathbb{N}$; $2\,\mathbb{N} = \{2, 4, 6, \ldots\}$; $2\,\mathbb{N} - 1 = \{1, 3, 5, \ldots\}$
- $\mathbb{Z}$: funkcija $f\colon \mathbb{Z} \to \mathbb{N}$ definirana s $f(n) = \begin{cases} 2n & , n > 0 \\ -2n+1 & , n \leqslant 0 \end{cases}$ je bijekcija.

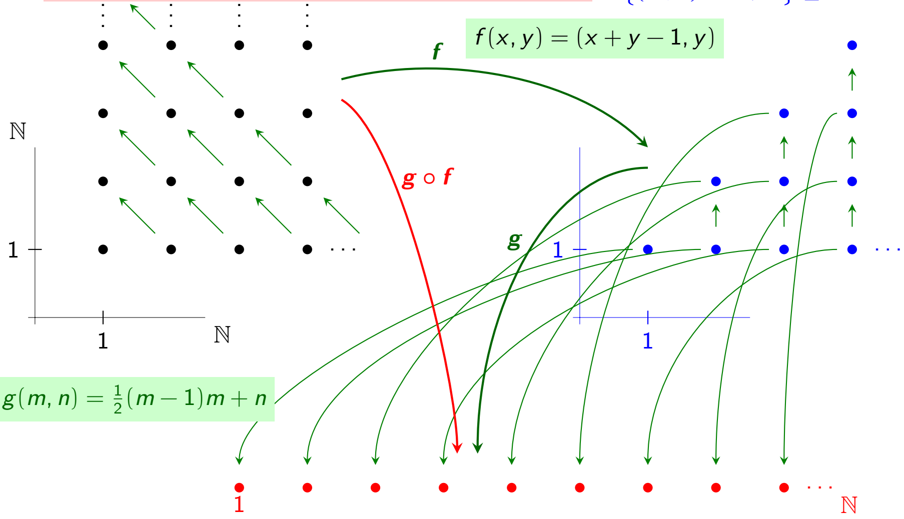
# Primjer 9.3: Skup $\mathbb{N} \times \mathbb{N}$ je prebrojivo beskonačan

$$(g \circ f)(x, y) = \tfrac{1}{2}(x + y - 2)(x + y - 1) + y$$

$$\{(m, n) : n \leqslant m\} \subseteq \mathbb{N} \times \mathbb{N}$$

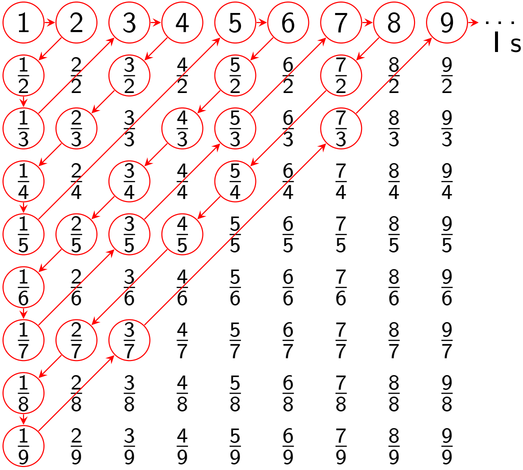
$$f(x, y) = (x + y - 1, y)$$

$$g(m, n) = \tfrac{1}{2}(m - 1)m + n$$



# Primjer 9.4: Skup $\mathbb{Q}$ racionalnih brojeva je prebrojiv

Dovoljno je dokazati da postoji bijekcija $\mathbb{N} \to \mathbb{Q}_+$, tj. da je $\mathbb{Q}_+$ prebrojiv.
Tada lako konstruiramo bijekciju $\mathbb{Q} = \mathbb{Q}_- \cup \{0\} \cup \mathbb{Q}_+ \to -\mathbb{N} \cup \{0\} \cup \mathbb{N} = \mathbb{Z} \to \mathbb{N}$.



I sljedeći su skupovi prebrojivi:

- $\mathbb{Q} \times \mathbb{Q}$;
- skup intervala realnih brojeva s racionalnim krajevima;
- skup točaka ravnine s racionalnim koordinatama.

# Karakterizacija prebrojivih skupova

Za prepoznavanje prebrojivih skupova, koristan je sljedeći teorem:

**Teorem 9.5**

*Za neprazan skup $B$ sljedeće su tvrdnje ekvivalentne:*

(a) *$B$ je prebrojiv;*
(b) *postoji surjekcija $f\colon \mathbb{N} \twoheadrightarrow B$;*
(c) *postoji injekcija $g\colon B \rightarrowtail \mathbb{N}$.*

Dokaz: (a) $\Rightarrow$ (b) Ako je $B$ prebrojivo beskonačan onda, po definiciji postoji bijekcija, dakle i surjekcija $\mathbb{N} \to B$.
Ako je $B \neq \emptyset$ konačan, onda postoji bijekcija $h\colon [1\,..\,n] \to B$ za neki $n$.
Proširimo $h$ do surjekcije $f\colon \mathbb{N} \to B$ ovako: $f(j) = \begin{cases} h(j)\,, & 1 \leqslant j \leqslant n \\ h(1)\,, & j > n \end{cases}$. $\triangle$

# Završetak dokaza teorema 9.5

$(b) \Rightarrow (c)$ Neka je $f\colon \mathbb{N} \twoheadrightarrow B$ surjekcija. Definirajmo $g\colon B \to \mathbb{N}$ s

$$g(b) := \text{ najmanji element skupa } f^{-1}(b)$$

(takav postoji prema teoremu 8.8 o dobrom uređenju skupa $\mathbb{N}$).

Kako je $f$ surjekcija, to je $f^{-1}(b) \neq \emptyset$ za svaki $b \in B$, a jer je najmanji element jedinstven, funkcija $g$ je dobro definirana. Za $b \neq b'$ skupovi $f^{-1}(b)$ i $f^{-1}(b')$ su disjunktni, pa su i njihovi najmanji elementi različiti. Stoga je funkcija $g$ injektivna. $\triangle$

$(c) \Rightarrow (a)$ Neka je $g\colon B \rightarrowtail \mathbb{N}$ injekcija. Tada je $g$ bijekcija s $B$ na $g(B)$, pa bi dovoljno bilo pokazati da je svaki podskup od $\mathbb{N}$ prebrojiv. Ako je $C \subseteq \mathbb{N}$ konačan onda je prebrojiv po definiciji. Ostaje, dakle, pokazati da je svaki beskonačan podskup od $\mathbb{N}$ prebrojivo beskonačan. Ta je tvrdnja razumna (plauzibilna): treba samo „nanizati” elemente od $C$. Jednostavno: uzmemo $\mathbb{N}$ u uobičajenom uređaju i „izbrišemo” članove koji ne pripadaju skupu $C$. $\square$

Ipak, plauzibilnost nije dovoljan argument za dokaz — možda smo nešto previdjeli. Pedantnom dokazu posvetimo zato sljedeću lemu:

# Beskonačni podskupovi od $\mathbb{N}$

**Lema 9.6**

*Svaki beskonačan podskup $C \subseteq \mathbb{N}$ je prebrojivo beskonačan.*

Dokaz: Definirajmo induktivno bijekciju $h\colon \mathbb{N} \to C$ ovako: Neka je $h(1)$ najmanji element od $C$ (postoji, i jedinstven je prema teoremu 8.8).

$n-1 \rightsquigarrow n$: Skup $C \setminus h\big([1\,..\,n-1]\big)$ je neprazan, inače bi $C$ bio konačan, pa definiramo $h(n) :=$ najmanji element od $C \setminus h\big([1\,..\,n-1]\big)$ $(*)$.
Dakle, **induktivno smo definirali** $h(n)$ za sve $n \in \mathbb{N}$.

$h$ je injekcija: Za $m < n$ je $h(m) \in h\big([1\,..\,n-1]\big)$, dok $h(n) \notin h\big([1\,..\,n-1]\big)$.

$h$ je surjekcija: Neka je $c \in C$. Pokažimo da je $c \in h(\mathbb{N})$.
$h(\mathbb{N}) \not\subseteq [1\,..\,c]$ jer je $h$ injekcija. Stoga $\exists n \in \mathbb{N}$ t.d. je $h(n) > c$.
Neka je $m \in \mathbb{N}$ najmanji broj t.d. je $h(m) \geqslant c$. Tada za sve $j < m$ vrijedi $h(j) < c$, pa $c \notin h\big([1\,..\,m-1]\big)$, tj. $c \in C \setminus h\big([1\,..\,m-1]\big)$.

Kako je $h(m) \overset{(*)}{=} \min\big(C \setminus h([1\,..\,m-1])\big)$, mora biti $h(m) \leqslant c$.
Dakle, $h(m) = c$, tj. $c \in h(\mathbb{N})$ pa je $h$ i surjekcija. $\square$

# Analiza prethodnog dokaza: u čemu je problem? Zašto smo taj dokaza morali istaknuti u zasebnu lemu?

Zasigurno smo slične dokaze već ranije vidjeli i u drugim kolegijima, ali bez posebne pompe i naglaska. Ipak, u prethodnom smo dokazu malo „rastegnuli" logičke principe. To smo učinili kada smo induktivno *definirali* $h(n)$ za sve $n \in \mathbb{N}$. Što kaže PRINCIP INDUKCIJE?

Ako je $A \subseteq \mathbb{N}$ induktivan skup onda je $A = \mathbb{N}$.

I taj se princip koristi za dokazivanje tvrdnji indukcijom, a tipičan dokaz teče ovako: Neka je $A \subseteq \mathbb{N}$ skup brojeva za koje tvrdnja vrijedi. Pokažimo da je $1 \in A$ i da iz $n \in A$ slijedi $n + 1 \in A$.

Međutim, mi u prethodnom dokazu tvrdnju *nismo dokazivali indukcijom*, mi smo nešto, $h$, *definirali indukcijom*. Kako je onda trebao teći dokaz? Neka je $A$ skup brojeva za koje je funkcija $h$ definirana. ...

Ali to je besmislica: *$h$ nema smisla na početku dokaza*, $h$ dobiva smisao istom *tijekom dokaza*. Treba nam, dakle, nešto novo.

Treba nam PRINCIP REKURZIVNE DEFINICIJE.

# Rekurzivna definicija

U dokazu leme 9.6 htjeli smo, zapravo, ustvrditi sljedeće:
Ako je $C \subseteq \mathbb{N}$ beskonačan podskup onda postoji jedinstvena funkcija $h\colon \mathbb{N} \to C$ koja zadovoljava sljedeću formulu:

$$(*) \quad \begin{cases} h(1) = \text{najmanji element skupa } C \\ h(j) = \text{najmanji element skupa } C \setminus h\big([1\,..\,j-1]\big), \quad \text{za sve } j > 1. \end{cases}$$

$(*)$ se naziva *rekurzivna formula* za $h$ — definira $h$ pomoću nje same, a definicija dâna takvom formulom naziva se *rekurzivna definicija*.

Ali, rekurzivne definicije mogu dovesti do logičkih poteškoća.
Nema svaka rekurzivna formula smisla. Npr., rekurzivna formula

$$h(j) = \text{najmanji element skupa } C \setminus h\big([1\,..\,j+1]\big)$$

je sama sebi kontradiktorna: svakako je $h(j) \in h\big([1\,..\,j+1]\big)$ a formula upravo tvrdi da $h(j)$ *nije* element od $h\big([1\,..\,j+1]\big)$.

Slična situacija je s Russellovim paradoksom (brico koji brije sve one koji se ne briju sâmi).

# Princip rekurzivne definicije

Na sreću, neke rekurzivne formule imaju smisla. Točnije, vrijedi ovaj

PRINCIP REKURZIVNE DEFINICIJE (Dedekind)

Neka je $A$ skup. Ako je dâna formula koja definira $h(1)$ kao *jedinstven* element skupa $A$, i za sve $j > 1$ definira $h(j)$ kao *jedinstven* element skupa $A$ pomoću vrijednosti od $h$ za prirodne brojeve manje od $j$, onda ta formula definira *jedinstvenu* funkciju $h\colon \mathbb{N} \to A$.

Formula $(*)$ u našem dokazu leme 9.6 zadovoljavala je princip rekurzivne definicije, pa je naš dokaz, a time i dokaz teorema 9.5 koji karakterizira prebrojive skupove, bio korektan.

A dokaz principa rekurzivne definicije dat ćemo u sljedećem § 10.

# Podskupovi prebrojivog skupova su prebrojivi

Dokažimo nekoliko posljedica teorema 9.5:

**Korolar 9.7**

*Svaki podskup prebrojivog skupa je prebrojiv.*

Dokaz: Neka je skup $B$ prebrojiv i $A \subseteq B$. Prema teoremu 9.5 postoji injekcija $f\colon B \rightarrowtail \mathbb{N}$, pa je restrikcija $f|_A$ injekcija skupa $A$ u $\mathbb{N}$, te je skup $A$ prebrojiv prema teoremu 9.5. $\square$

# $\mathbb{N} \times \mathbb{N}$ je prebrojivo beskonačan

Iako smo sljedeću činjenicu već dokazali direktno, primjer 9.3, evo je opet:

**Korolar 9.8**

*Skup $\mathbb{N} \times \mathbb{N}$ je prebrojivo beskonačan.*

Dokaz: Prema teoremu 9.5 treba samo konstruirati injekciju $f\colon \mathbb{N}\times\mathbb{N} \rightarrowtail \mathbb{N}$.
Definirajmo $f(m,n) := 2^m 3^n$. Dokažimo da je $f$ injekcija:

Neka je $(m,n) \neq (p,q)$, i neka je $m < p$. Ako je $f(m,n) = f(p,q)$, onda je

$$2^m 3^n = 2^p 3^q \qquad : 2^m$$

$$\underbrace{3^n}_{\text{neparan}} = \underbrace{2^{p-m}}_{\Rightarrow\, m=p} 3^q$$

Dakle, $3^n = 3^q$, pa je i $n = q$, tj. $f$ je injekcija. $\square$

Komponiranjem surjekcije $\mathbb{N} \twoheadrightarrow \mathbb{N} \times \mathbb{N}$ s funkcijom $g\colon \mathbb{N} \times \mathbb{N} \to \mathbb{Q}_+$ definiranom s $g(m,n) = \left[\frac{m}{n}\right]$, koja je očito surjekcija, dobiva se surjekcija $\mathbb{N} \twoheadrightarrow \mathbb{Q}_+$, koja ponovno (v. primjer 9.4) pokazuje da je skup $\mathbb{Q}_+$ prebrojiv. A da je beskonačan — jasno je.

# Prebrojiva unija prebrojivih skupova

**Teorem 9.9**

*Prebrojiva unija prebrojivih skupova je prebrojiv skup.*

Dokaz: Neka je $\{A_j\}_{j\in J}$ familija prebrojivih skupova, gdje je $J = \mathbb{N}$ ili $J = [1\,..\,n]$, i neka su svi $A_j$ neprazni. Kako su skupovi $J$ i $A_j$, $j \in J$, prebrojivi, postoje surjekcije $g\colon \mathbb{N} \twoheadrightarrow J$ i $f_j\colon \mathbb{N} \twoheadrightarrow A_j$, $j \in J$.

Definiramo $h\colon \mathbb{N} \times \mathbb{N} \to \bigcup\limits_{j\in\mathbb{N}} A_j$ formulom $h(k,\ell) := f_{g(k)}(\ell)$.

Lako se vidi da je $h$ surjekcija. Komponiramo li $h$ s bijekcijom $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$, dobivamo surjekciju $\mathbb{N} \twoheadrightarrow \bigcup\limits_{j\in J} A_j$. $\square$

# Konačan produkt prebrojivih skupova

**Teorem 9.10**

*Konačan produkt prebrojivih skupova je prebrojiv skup.*

Dokaz: Indukcijom.

Neka su $A$ i $B$ prebrojivi skupovi. Ako je $A = \emptyset$ ili $B = \emptyset$ onda je $A \times B = \emptyset$. Za $A \neq \emptyset$ i $B \neq \emptyset$ odaberimo surjekcije $f \colon \mathbb{N} \twoheadrightarrow A$ i $g \colon \mathbb{N} \twoheadrightarrow B$. Tada je funkcija $h \colon \mathbb{N} \times \mathbb{N} \to A \times B$ definirana s $h(m, n) := \big(f(m), g(n)\big)$ surjekcija, pa je $A \times B$ prebrojiv.

$n - 1 \rightsquigarrow n$: Postoji bijekcija $A_1 \times \cdots \times A_n \to \big((A_1 \times \cdots \times A_{n-1}) \times A_n\big)$ definirana s $(x_1, \ldots, x_n) \mapsto \big((x_1, \ldots, x_{n-1}), x_n\big)$.

PPI skup $A_1 \times \cdots \times A_{n-1}$ je prebrojiv, pa tvrdnja slijedi iz prvog dijela dokaza. $\square$

# Potencije skupova

Specijalne vrste produkata su potencije.
Za neprazan skup $A$ i prirodan broj $n$ definira se $A^n := \underbrace{A \times \cdots \times A}_{n \text{ faktora}}$,
naziva se *$n$-ta potencija* skupa $A$,
i sastoji se od uređenih $n$-torki $(a_1, \ldots, a_n)$, $a_j \in A$, $j \in [1 \,..\, n]$.

Dakle, $A^n$ je skup svih funkcija $f\colon [1 \,..\, n] \to A$, uz oznaku $f(j) =: a_j$.

**Teorem 9.11**

*Neka su $A$ i $B$ neprazni skupovi. Klasa svih funkcija s $B$ u $A$ je skup.* $\square$

Uobičajena oznaka za skup svih funkcija s $B$ u $A$ je $A^B$ (Vuković: ${}^B A$).
Dakle, $A^n = A^{[1 \,..\, n]}$.

Svaka funkcija $\mathbb{N} \to A$ naziva se *niz* u skupu $A$, pa je $A^{\mathbb{N}}$, ili $A^{\omega}$, skup svih nizova u $A$, a njegovi se elementi, dakle nizovi u $A$, obično označuju $(a_1, a_2, a_3, \ldots)$, ili $(a_0, a_1, a_2, \ldots)$.

# Skup svih nizova nula i jedinica nije prebrojiv

Na osnovi teorema 9.9 i 9.10 lako je pomisliti da je i prebrojiv produkt prebrojivih skupova prebrojiv skup.
Međutim, čak niti prebrojiv produkt dvočlanih skupova nije prebrojiv.

**Teorem 9.12**

*Skup nizova nula i jedinica, tj. skup $\{0,1\}^\omega$, nije prebrojiv.*

Dokaz: Pokazat ćemo da niti jedna funkcija $g\colon \mathbb{N} \to \{0,1\}^\omega$ nije surjekcija.
Označimo $g(n) = (x_{n_1}, x_{n_2}, \ldots, x_{n_n}, \ldots)$, gdje je svaki $x_{n_j}$ jednak 0 ili 1, i neka je $y = (y_1, y_2, \ldots, y_n, \ldots) \in \{0,1\}^\omega$ definiran ovako:

$$y_n := \begin{cases} 0\,, \text{ ako je } x_{n_n} = 1 \\ 1\,, \text{ ako je } x_{n_n} = 0 \end{cases}.$$

Očito je $y \neq g(n)$ za svaki $n$, tj. $g$ nije surjekcija. □

Provedeni se dokaz, kao i dokaz sljedećeg poopćenja, naziva *Cantorov dijagonalni postupak*.

# Poopćenje

**Teorem 9.13 (Cantor)**

*Neka je $A$ bilo kakav neprazan skup. Ne postoji injekcija $\mathscr{P}(A) \rightarrowtail A$ niti surjekcija $A \twoheadrightarrow \mathscr{P}(A)$. Specijalno, $A$ i $\mathscr{P}(A)$ nisu ekvipotentni.*

Dokaz: Općenito, ako je $B$ neprazan skup i $f\colon B \to C$ injekcija, onda uvijek postoji surjekcija $g\colon C \to B$: definira se s

$$g(c) = \begin{cases} f^{-1}(c) & \text{, za } c \in f(B) \\ \text{bilo kako} & \text{, za } c \in C \setminus f(B) \end{cases}.$$

Treba, dakle, pokazati da niti jedna funkcija $g\colon A \to \mathscr{P}(A)$ nije surjekcija.

Za $\forall a \in A$ je $g(a) \subseteq A$. Neka je $B = \{a \in A : a \notin g(a)\} \subseteq A$.

Tvrdnja: $B \not\subseteq g(A)$, pa $g$ nije surjekcija.

Pretpostavimo da $g$ je surjekcija. Tada $\exists a_0 \in A$ t.d. je $g(a_0) = B$.

Je li $a_0 \in B$ ili $a_0 \notin B$?

$$a_0 \in B \Leftrightarrow a_0 \in A \setminus g(a_0) \Leftrightarrow a_0 \in A \setminus B$$

Dobivena kontradikcija dokazuje teorem. $\square$

# Neprebrojivost skupa realnih brojeva.

„Najvažniji" neprebrojiv skup je svakako $\mathbb{R}$, skup realnih brojeva. U primjerima 7.3 i 7.4 pokazali smo ekvipotentnosti $\mathbb{R} \sim \langle 0, 1\rangle \sim \langle 0, 1]$, pa je dovoljno pokazati da je skup $\langle 0, 1]$ neprebrojiv. Evo dokaza:

Svaki broj iz $\langle 0, 1]$ ima beskonačan decimalan prikaz $0.x_1\, x_2\, x_3 \ldots$, gdje su $x_j \in \{0, 1, \ldots, 9\}$, i ako ne dozvolimo konačne decimalne zapise, tj. decimalne zapise koji završavaju beskonačnim brojem nula, onda je taj zapis jedinstven.

Pretpostavimo da je $\langle 0, 1]$ prebrojiv. Tada njegove elemente možemo svrstati u niz:

$$\begin{aligned} x_1 &= 0.x_{11}\, x_{12}\, x_{13} \ldots \\ x_2 &= 0.x_{21}\, x_{22}\, x_{23} \ldots \\ x_3 &= 0.x_{31}\, x_{32}\, x_{33} \ldots \\ &\;\;\vdots \end{aligned}$$

Definirajmo broj $y = 0.y_1\, y_2\, y_3 \ldots$ t.d. je $y_n = \begin{cases} 3\,, & \text{ako je } x_{nn} \neq 3 \\ 2\,, & \text{ako je } x_{nn} = 3 \end{cases}$.

Očito je $y \in \langle 0, 1]$ i $y \neq x_n$ za sve $n$. $\square$

# Kritika prethodnog „dokaza”

Činjenica kako svaki realan broj ima beskonačan decimalan prikaz, je vrlo netrivijalna posljedica definicije realnih brojeva, bilo da se počne s prirodnim brojevima $\mathbb{N}$ pa se preko $\mathbb{Z}$ i $\mathbb{Q}$ dođe do $\mathbb{R}$, bilo da se $\mathbb{R}$ definira aksiomatski kao potpuno uređeno polje.

S druge strane, neprebrojivost od $\mathbb{R}$ nije posljedica beskonačnog decimalnog zapisa ili nekog drugog algebarskog ili analitičkog svojstva skupa $\mathbb{R}$, već isključivo uređajnih svojstava od $\mathbb{R}$:

- postojanje supremuma svakog nepraznog odozgo omeđenog podskupa
- gustoća.

Takav se uređen skup naziva *linearni kontinuum*.

# Analiza dokaza leme 9.6

Vratimo se principu rekurzivne definicije, i u tu svrhu analizirajmo dokaz leme 9.6 kako je svaki beskonačan podskup $C \subseteq \mathbb{N}$ prebrojivo beskonačan.

U dokazu smo bili rekurzivno definirali funkciju $h\colon \mathbb{N} \to C$ formulom

$$(*)\quad \begin{cases} h(1) = \text{ najmanji element skupa } C \\ h(j) = \text{ najmanji element skupa } C \setminus h\big([1\,..\,j-1]\big), \quad \text{za sve } j > 1. \end{cases}$$

Dokažimo zaista postojanje jedinstvene, ovako definirane funkcije, tj. dokažimo Princip rekurzivne definicije u ovom specijalnom slučaju.

**Lema 10.1**

*Za svaki zadani prirodan broj $n$ postoji funkcija $f_n\colon [1\,..\,n] \to C$ koja zadovoljava $(*)$ za $1 \leqslant j \leqslant n$.*

Dokaz: Tvrdnja ovisi o $n$ pa ima smisla dokaz indukcijom.
Neka je $A$ skup brojeva $n \in \mathbb{N}$ za koje lema vrijedi.
Dokazat ćemo da je skup $A$ induktivan, dakle $A = \mathbb{N}$.

# Završetak dokaza leme 10.1

Za $n = 1$ lema je istinita jer je $f_1 \colon \{1\} \to C$ jednoznačno definirana s $f_1(1) =$ najmanji element od $C$ (skup $\mathbb{N}$ je dobro uređen, teorem 8.8), i tako definirana funkcija $f_1$ zadovoljava $(*)$.

$n-1 \rightsquigarrow n$: PPI postoji funkcija $f_{n-1} \colon [1\,.\,.\,n-1] \to C$ koja zadovoljava $(*)$ za sve $1 \leqslant j \leqslant n-1$. Definirajmo $f_n \colon [1\,.\,.\,n] \to C$ formulom

$$f_n(j) = \begin{cases} f_{n-1}(j) & , j \in [1\,.\,.\,n-1] \\ \text{najmanji element skupa } C \setminus f_{n-1}([1\,.\,.\,n-1]) & , j = n \end{cases}.$$

Kako je skup $C$ beskonačan, $f_{n-1}$ nije surjekcija, pa je skup $C \setminus f_{n-1}([1\,.\,.\,n-1])$ neprazan, te je $f_n(n)$ definirano.

POANTA: ova je definicija korektna jer $f_n$ *nije* definirana pomoću nje sâme, nego pomoću već legitimne funkcije $f_{n-1}$.

Sada se lako provjeri da $f_n$ zadovoljava $(*)$ za sve $1 \leqslant j \leqslant n$.

Naime, za $1 \leqslant j \leqslant n-1$ je $f_n(j) = f_{n-1}(j)$, pa $(*)$ vrijedi PPI.

Za $j = n$ je $f_n(n) =$ najmanji element skupa $C \setminus \underbrace{f_{n-1}([1\,.\,.\,n-1])}_{=f_n([1\,.\,.\,n-1])}$ pa $f_n$ zadovoljava $(*)$ za sve $1 \leqslant j \leqslant n$. $\square$

# Jedinstvenost rekurzivno definirane funkcije

Osim postojanja, treba nam i *jedinstvenost* rekurzivno definirane funkcije.

**Lema 10.2**

*Neka funkcije* $f\colon [1\,..\,m] \to C$ *i* $g\colon [1\,..\,n] \to C$ *zadovoljavaju* $(*)$, *svaka na svojoj domeni. Tada je* $f(j) = g(j)$ *za sve* $1 \leqslant j \leqslant \min\{m, n\}$.

Dokaz: Pretpostavimo suprotno, pa neka je $k$ najmanji broj za koji je $f(k) \neq g(k)$. Tada je $k \neq 1$ jer je $f(1) =$ najmanji element od $C = g(1)$. Kako je $k$ najmanji broj za koji se $f$ i $g$ razlikuju, za sve $j < k$ vrijedi $f(j) = g(j)$, a kako $f$ i $g$ zadovoljavaju $(*)$, to je

$$\begin{aligned} f(k) &= \text{najmanji element od } C \setminus \underbrace{f\big([1\,..\,k-1]\big)} \\ & \qquad\qquad\qquad\qquad\qquad\qquad \| \\ g(k) &= \text{najmanji element od } C \setminus \overbrace{g\big([1\,..\,k-1]\big)} \end{aligned}$$

pa je $f(k) = g(k)$ $\quad \Rightarrow\!\Leftarrow \quad$ $f(k) \neq g(k)$. $\square$

# Specijalan slučaj principa rekurzivne definicije

Dokažimo zaista ranije najavljeni specijalni slučaj principa rekurzivne definicije, koji je potreban u dokazu leme 9.6.

**Teorem 10.3**

*Postoji jedinstvena funkcija $h\colon \mathbb{N} \to C$ koja zadovoljava $(*)$ za sve $n \in \mathbb{N}$.*

Dokaz: Prema lemi 10.1, za $\forall n \in \mathbb{N}$ postoji funkcija $[1\,..\,n] \to C$ koja zadovoljava $(*)$ za sve $1 \leqslant j \leqslant n$, a lema 10.2 pokazuje da je takva funkcija jedinstvena. Označimo ju s $f_n\colon [1\,..\,n] \to C$.

KLJUČNI KORAK: Dakle, za $\forall n \in \mathbb{N}$ imamo jedinstvenu funkciju $f_n$, tj. jedinstven podskup $f_n \subseteq [1\,..\,n] \times C \subseteq \mathbb{N} \times C$.

$$\text{Definirajmo } h := \bigcup f_n.$$

Očito je $h \subseteq \mathbb{N} \times C$, i treba samo pokazati da je to funkcija, tj. da se svaki $j \in \mathbb{N}$ pojavljuje kao prva koordinata točno jednog elementa od $h$, i da $h$ zadovoljava $(*)$.

# Završetak dokaza teorema 10.3

$h$ je funkcija: Neka je $j \in \mathbb{N}$. Tada $j$ pripada domeni funkcije $f_n$ ako i samo ako je $n \geqslant j$. Stoga je skup točaka iz $h$ kojima je $j$ prva koordinata, točno skup parova $\big(j, f_n(j)\big)$, $n \geqslant j$.
Ali, prema lemi 10.2, za $m, n \geqslant j$ je $f_m(j) = f_n(j)$, pa je za dâni $j \in \mathbb{N}$ skup $\big\{\big(j, f_n(j)\big) : n \geqslant j\big\} = \big\{\big(j, f_j(j)\big)\big\}$ jednočlan.
Dakle, za svaki $j \in \mathbb{N}$ postoji i jedinstven je element od $h$ kojemu je prva koordinata jednaka $j$, tj. $h$ je funkcija. $\triangle$

$h$ zadovoljava $(*)$: To je posljedica činjenice da je $h(j) = f_n(j)$ za sve $n \geqslant j$, i činjenice da $f_n$ zadovoljava $(*)$ za sve $1 \leqslant j \leqslant n$.

Jedinstvenost funkcije $h$ dokazuje se posve analogno dokazu leme 10.2. $\square$

Ovime je u potpunosti opravdan dokaz leme 9.6,
a time i karakterizacije prebrojivih skupova, teorem 9.5.

# Princip rekurzivne definicije

Dokaz sljedećeg, općeg teorema o principu rekurzivne definicije, zapravo je isti kao i upravo proveden dokaz leme 9.6 i teorema 10.3, pa ga ostavljamo studentima za vježbu.

**Teorem 10.4 (Princip rekurzivne definicije)**

*Neka je $A$ neprazan skup i $a_0 \in A$ neki element. Neka je $\varphi$ funkcija koja svakoj funkciji s nekog $[1\,..\,n]$ u $A$ pridružuje neki element skupa $A$. Tada postoji jedinstvena funkcija $h\colon \mathbb{N} \to A$ t.d. je*

$$(\mathrm{RF})\ \begin{cases} h(1) = a_0 \\ h(j) = \varphi\left(h|_{[1\,..\,j-1]}\right) \text{ za } j > 1. \end{cases} \qquad \square$$

$(\mathrm{RF})$ se naziva *rekurzivna formula* za funkciju $h$.
Ona specificira $h(1)$ i izražava $h(j)$ koristeći vrijednosti od $h$ u brojevima $1, 2, \ldots, j-1$, a pomoću funkcije $\varphi$.

# Primjer

**Primjer 10.5 (Teorem 10.3 je zaista specijalan slučaj teorema 10.4)**

Za beskonačan podskup $C \subseteq \mathbb{N}$ neka je $a_0 = \min C$, a funkcija $\varphi$ neka je definirana kao

$$\varphi(f) = \text{ najmanji element skupa } C \setminus \underbrace{(\text{slika od } f)}_{\operatorname{Im} f},$$

gdje je $f$ bilo koja funkcija $f\colon [1 \,..\, n] \to C$ za bilo koji $n$.
Budući su domene funkcije $f$ (argumenata od $\varphi$) konačni skupovi, a $C$ je beskonačan, to su skupovi $C \setminus \operatorname{Im} f$ uvijek neprazni, pa je $\varphi$ dobro definirana funkcija. Prema teoremu 10.4, postoji jedinstvena funkcija $h\colon \mathbb{N} \to C$ t.d. je $h(1) = a_0$, i da za $j > 1$ vrijedi

$$\begin{aligned} h(j) &= \varphi\big(h|_{[1\,..\,j-1]}\big) \\ &= \text{ najmanji element skupa } C \setminus \operatorname{Im}\big(h|_{[1\,..\,j-1]}\big) \\ &= \text{ najmanji element skupa } C \setminus h\big([1\,..\,j-1]\big). \end{aligned}$$

□

# Primjer: definicija potencije

## Primjer 10.6

Neka je $a \in \mathbb{R}$. Potencija se rekurzivno definira ovako:

$$\begin{cases} a^1 = a \\ a^n = a^{n-1} \cdot a \end{cases}$$

Pokažimo „strogu" definiciju funkcije $h\colon \mathbb{N} \to \mathbb{R}$ za koju je $h(n) = a^n$.
Stavimo $a_0 = a$ i definiramo funkciju $\varphi$ ovako:
$\varphi(f) = f(m) \cdot a$, gdje je za $\forall m$, $f\colon [1 \mathinner{..} m] \to \mathbb{R}$ proizvoljna funkcija.
Prema teoremu 10.4 postoji jedinstvena funkcija $h\colon \mathbb{N} \to \mathbb{R}$ t.d. je

$$h(1) = a$$

$$h(j) = \varphi\left(h|_{[1 \mathinner{..} j-1]}\right) \text{ za } j > 1.$$

To znači da je $h(1) = a$ i $h(j) = h(j-1) \cdot a$ za $j > 1$.
Označimo li $h(j) =: a^j$, dobili smo $a^1 = a$ i $a^j = a^{j-1} \cdot a$ za $j > 1$.

- Slično se definiraju faktorijeli.

# Prepoznavanje beskonačnih skupova

Znamo već nekoliko *dovoljnih* uvjeta za prepoznavanje beskonačnih skupova. Naprimjer:

- Ako skup $A$ sadrži prebrojivo beskonačan podskup onda je skup $A$ beskonačan (jer korolar 8.6 kaže da je svaki podskup konačnog skupa konačan).
- Ako postoji bijekcija skupa $A$ na neki njegov pravi podskup, onda je skup $A$ beskonačan (jer korolar 8.11 kaže da *ne postoji* bijekcija konačnog skupa na njegov pravi podskup).

Sljedeći teorem pokazuje da su ovi uvjeti i nužni.

# Karakterizacija beskonačnih skupova

**Teorem 11.1**

*Neka je $A$ skup. Sljedeće su tvrdnje ekvivalentne:*

(a) *Postoji injekcija $f\colon \mathbb{N} \to A$.*

(b) *Postoji bijekcija skupa $A$ na neki pravi podskup od $A$.*

(c) *Skup $A$ je beskonačan.*

Dokaz: (a) $\Rightarrow$ (b) Neka je $f\colon \mathbb{N} \to A$ injekcija. Označimo $f(n) =: a_n$, $n \in \mathbb{N}$, i $B := \{a_n : n \in \mathbb{N}\} = f(\mathbb{N}) \subseteq A$. Kako je $f$ injekcija, to $m \neq n \Rightarrow a_m \neq a_n$.

Definirajmo $g\colon A \to A \setminus \{a_1\}$ ovako: $g(x) = \begin{cases} a_{n+1}, & \text{za } x = a_n \in B \\ x, & \text{za } x \notin B \end{cases}$.

$g$ je očito bijekcija. $\triangle$

(b) $\Rightarrow$ (c) To je upravo kontrapozicija korolara 8.11 (ne postoji bijekcija konačnog skupa na njegov pravi podskup). $\triangle$

# „Završetak" dokaza teorema 11.1

(c) $\Rightarrow$ (a) Pretpostavljamo da je skup $A$ beskonačan i želimo *induktivno konstruirati* injekciju $f\colon \mathbb{N} \to A$.
Prvo, jer je $A \neq \emptyset$, odaberimo neki $a_1 \in A$ i definiramo $f(1) := a_1$.
Zatim, pretpostavimo da već imamo definirano $f(1), \ldots, f(n-1)$, i želimo definirati $f(n)$. Skup $A \setminus f\big([1\mathinner{..}n-1]\big)$ je neprazan, jer bismo inače imali surjekciju $[1\mathinner{..}n] \to A$ pa bi $A$ bio konačan.
Stoga možemo odabrati neki element skupa $A \setminus f\big([1\mathinner{..}n-1]\big)$ i njega definirati kao $f(n)$.

Koristeći „princip rekurzivne definicije" definirali smo $f$ za sve $n \in \mathbb{N}$.

$f$ je očito injekcija jer za $m < n$, $f(m)$ pripada skupu $f\big([1\mathinner{..}n-1]\big)$, a $f(n)$ mu ne pripada, pa je $f(m) \neq f(n)$. ?

Je li provedeni dokaz korektan? KAKO SE UZME !

# Analiza „dokaza” implikacije $(c) \Rightarrow (a)$

Pogledajmo kako smo to točno koristili princip rekurzivne definicije. Za beskonačan skup $A$ pokušali smo rekurzivno definirati funkciju $f\colon \mathbb{N} \to A$ formulom:

$$(**)\quad \begin{cases} f(1) = \textit{bilo koji} \text{ element } a_1 \text{ skupa } A \\ f(j) = \textit{bilo koji} \text{ element skupa } A \setminus f\big([1\,..\,j-1]\big), \text{ za } j > 1. \end{cases}$$

Ali *to nije prihvatljiva rekurzivna formula*, njome nije definiran $f(j)$ pomoću *jedinstvenih* $f(1)$ i $f|_{[1\,..\,j-1]}$.

Za razliku, u dokazu leme 9.6 smo za beskonačan podskup $C \subseteq \mathbb{N}$ funkciju $h\colon \mathbb{N} \to C$ rekurzivno definirali formulom

$$(*)\quad \begin{cases} h(1) = \underbrace{\text{najmanji element od } C}_{\text{ovime je } h(1) \text{ jedinstveno definiran}} \\ h(j) = \underbrace{\text{najmanji element skupa } C \setminus h\big([1\,..\,j-1]\big)}_{\text{ovime je } h(j) \text{ jedinstveno definiran}}, \text{ za } j > 1, \end{cases}$$

a to je *bitna razlika.*

# Još malo o primjeni principa rekurzivne definicije

Primijetimo da kada bi $(**)$ bila prihvatljiva rekurzivna formula, onda bi prema teoremu 10.4 o principu rekurzivne definicije, slijedilo da postoji *jedinstvena* funkcija $f \colon \mathbb{N} \to A$ koja zadovoljava $(**)$, što je očito nemoguće očekivati, jer postoji beskonačno mnogo različitih izbora za $f(1)$ i za $f(j)$, $j > 1$.

Dakle, „dokaz" implikacije $(c) \Rightarrow (a)$ nije dobar, tj. na osnovu aksioma i teorema teorije skupova *koje smo dosada razmatrali, nije moguće* dokazati implikaciju $(c) \Rightarrow (a)$. Trebamo još nešto!

Kako smijemo definirati skupove?

- popisom elemenata;
- specifikacijom nekog svojstva elemenata nekog, već definiranog skupa;
- unijom, presjekom, razlikom, već definiranih skupova;
- uzimanjem svih podskupova nekog skupa;
- konačnim Kartezijevim produktom već definiranih skupova.

# Aksiom izbora

Funkcija sa skupa $\mathbb{N}$ u skup $A$ je izvjestan podskup Kartezijevog produkta $\mathbb{N} \times A$. Stoga za dokazati postojanje funkcije $f : \mathbb{N} \to A$ trebamo konstruirati (definirati) odgovarajući podskup skupa $\mathbb{N} \times A$, i to koristeći dozvoljene metode.

Međutim, za naše potrebe, dosadašnje metode definiranja skupova nisu dovoljne. Trebamo novi aksiom — *aksiom izbora*.

## AKSIOM IZBORA

Za svaku nepraznu familiju $\mathscr{A}$ međusobno disjunktnih nepraznih skupova, postoji skup $C$ koji se sastoji od po *točno jednog* elementa iz svakog skupa familije $\mathscr{A}$.

Dakle, $C \subseteq \bigcup \mathscr{A}$ i za svaki $A \in \mathscr{A}$ je skup $C \cap A$ jednočlan.

Napomena Općenito, skup $C$ nije jedinstven.

Skupovi familije $\mathscr{A}$ *moraju* biti disjunktni:

KONTRAPRIMJER: $\mathscr{A} = \big\{\{1\}, \{2\}, \{1, 2\}\big\}$.

# Izborna funkcija

Aksiom izbora izgleda *nevino* ali je izazvao dosta bure zbog vrlo neočekivanih posljedica (npr. da se svaki skup može dobro urediti).

K. Gödel je 1938–40. pokazao da uporaba aksioma izbora ne može dovesti do kontradikcije ako već nije postojala kontradikcija i bez njega.

Najprije definicija koja omogućuje jedan ekvivalentan iskaz aksioma izbora:

**Definicija 11.2**

Neka je $\{A_\alpha : \alpha \in J\}$ neprazna indeksirana familija nepraznih skupova, i neka je $A = \bigcup\{A_\alpha : \alpha \in J\}$. Funkcija $i \colon J \to A$ t.d. je $i(\alpha) \in A_\alpha$ za svaki $\alpha$, naziva se *funkcija izbora* ili *izborna funkcija*.

# Aksiom izbora može se iskazati i ovako:

**Teorem 11.3 (AI[8])**

*Za svaku nepraznu indeksiranu familiju $\mathscr{A} = \{A_\alpha : \alpha \in J\}$ nepraznih skupova postoji funkcija izbora.*

Dokaz: Za svaki $\alpha$ neka je $A'_\alpha = A_\alpha \times \{\alpha\} = \{(x, \alpha) : x \in A_\alpha\}$.
Skupovi $A'_\alpha$ indeksirane familije $\{A'_\alpha : \alpha \in J\}$ su međusobno disjunktni, pa prema aksiomu izbora, postoji skup $C'$ t.d. je za svaki $\alpha \in J$, $C' \cap A'_\alpha = \{(a_\alpha, \alpha)\}$ za neki $a_\alpha \in A_\alpha$.
Definiramo funkciju $i\colon J \to A = \bigcup A_\alpha$ s $i(\alpha) = a_\alpha$.
Funkcija $i$ je očito izborna funkcija za polaznu familiju $\mathscr{A}$. $\square$

Jedna preformulacija prethodnog teorema koja ne koristi indekse, je ova:

**Teorem 11.3' (AI)**

*Neka je $\mathscr{A}$ neprazna familija nepraznih skupova. Tada postoji funkcija $i\colon \mathscr{A} \to \bigcup_{A \in \mathscr{A}} A$ t.d. je $i(A) \in A$ za sve $A \in \mathscr{A}$.* $\square$

[8] U iskazu teorema čiji dokaz zahtijeva aksiom izbora, pisat ćemo (AI).

# Ekvivalentnost aksioma izbora i teorema 11.3

NAPOMENA: Razlika između aksioma izbora i prethodnog teorema 11.3 je u tome da u teoremu članovi familije ne moraju biti međusobno disjunktni (ali zato ne izabiremo točno jedan element iz svakog $A_\alpha$).

Teorem 11.3 je zapravo ekvivalentan aksiomu izbora. Naime, ako su skupovi familije $\{A_\alpha : \alpha \in J\}$ međusobno disjunktni, onda je $i(\alpha) \in A_\alpha$, $i(\beta) \in A_\beta$, pa je za $\alpha \neq \beta$, $a_\alpha \neq a_\beta$ jer je $A_\alpha \cap A_\beta = \emptyset$. Stoga je $C = \{a_\alpha : \alpha \in J\}$ upravo skup kakav se traži u aksiomu izbora.

# Još o dokazu implikacija $(c) \Rightarrow (a)$ u teoremu 11.1

Vratimo se dokazu implikacije $(c) \Rightarrow (a)$ u dokazu teorema 11.1. $A$ je beskonačan skup i trebamo konstruirati injekciju $f\colon \mathbb{N} \to A$. Označimo s $\mathscr{B}$ familiju svih nepraznih podskupova od $A$, dakle, $\mathscr{B} = \mathscr{P}(A) \setminus \{\emptyset\}$. Prema teoremu 11.3' postoji izborna funkcija $i\colon \mathscr{B} \to \bigcup_{B \in \mathscr{B}} B = A$ t.d. je $i(B) \in B$ za sve $B \in \mathscr{B}$.

Definirajmo $f\colon \mathbb{N} \to A$ rekurzivnom formulom

$$(***)\quad \begin{cases} f(1) = i(A) \\ f(j) = i\big(A \setminus f([1\,..\,j-1])\big), \text{ za } j > 1. \end{cases}$$

Kako je $A$ beskonačan, skup $A \setminus f([1\,..\,j-1])$ je neprazan, pa desna strana u $(***)$ ima smisla. Budući su sada $f(1)$ i $f(j)$ *jedinstveno* definirani, $f(j)$ pomoću $f|_{[1\,..\,j-1]}$, princip rekurzivne definicije je primjenjiv, pa postoji *jedinstvena* funkcija $f$ definirana s $(***)$. Injektivnost se dokazuje kao i ranije.

Time je teorem 11.1, konačno, u potpunosti korektno dokazan. $\square$

# A u praksi . . .

KOMENTAR: Kako bismo dali korektan, logički ispravan dokaz teorema 11.1, trebali smo specificirati uporabu izborne funkcije. Ali, budimo iskreni, i priznajmo da većina matematičara to neće napraviti. Napravit će, bez grižnje savjesti, dokaz poput našeg prvog „dokaza” teorema 11.1, dakle dokaz koji koristi beskonačno mnogo izbora.

Ipak, oni jesu svjesni da koriste aksiom izbora, i da, ako je potrebno, znaju i mogu napraviti logički korektan dokaz specificiranjem izborne funkcije. Ali, najčešće to ne rade.

Kao primjer vidi sljedeću napomenu.

# Cipele i čarape

NAPOMENA: U dokazu teorema 9.9, da je prebrojiva unija prebrojivih skupova prebrojiv skup, također je, zapravo, korišten aksiom (prebrojivog) izbora, i to za numeraciju (nizanje) elemenata skupova $A_j$, $j \in \mathbb{N}$, tj. pri odabiru funkcija $f_j$ i $g$.

Međutim, pri dokazu da su skupovi $\mathbb{N}\times\mathbb{N}$, $\mathbb{Q}$, $\mathbb{Q}\times\mathbb{Q}$ i slično, prebrojivi, nije trebao aksiom izbora, jer smo za nizanje (indeksiranje) koristili prirodan uređaj na $\mathbb{N}$ i jasno definiran uređaj na $\mathbb{Q}$.

Pojasnimo to jednim primjerom:

**Primjer 11.4 (Russell)**

Zamislimo dvije hrpe — prva je beskonačna gomila parova cipela, a druga je beskonačna gomila parova čarapa.
Za izbor po jedne cipele iz svakog para ne trebamo aksiom izbora, ali za izbor po jedne čarape iz svakog para — trebamo.

# Kartezijev produkt proizvoljne familije skupova

Svojedobno smo, u § 5, definirali Kartezijev produkt od dva, pa onda induktivno, i produkt od konačno mnogo skupova. Sada, kada imamo aksiom izbora, možemo se pozabaviti i proizvoljnim produktima.

**Definicija 11.5 (AI)**

Neka je $\{A_\alpha : \alpha \in J\}$ neprazna indeksirana familija nepraznih skupova. *Kartezijev* ili *direktan produkt* $\prod\limits_{\alpha \in J} A_\alpha$ te familije, definira se kao skup svih funkcija $f\colon J \to \bigcup\limits_{\alpha \in J} A_\alpha$ za koje je $f(\alpha) \in A_\alpha$ za sve $\alpha \in J$.

NAPOMENA: Mogli smo ovo definirati i ranije, ali bez aksioma izbora, tj. teorema 11.3, nemamo garancije da funkcije $f$ uopće postoje.

Dakle, $\prod\limits_{\alpha \in J} A_\alpha$ je *skup svih izbornih funkcija* za familiju $\{A_\alpha : \alpha \in J\}$.

# Konačni Kartezijevi produkti

Kada je skup indeksa $J$ konačan, dakle kada se radi o konačnoj familiji $\{A_1, \dots, A_n\}$, tj. $\{A_j : j \in [1\,..\,n]\}$, onda se produkt $\prod\limits_{j\in[1\,..\,n]} A_j$ obično označuje $\prod\limits_{j=1}^{n} A_j$ ili $A_1 \times \cdots \times A_n$, i to je skup svih funkcija $f\colon [1\,..\,n] \to \bigcup\limits_{j=1}^{n} A_j$ t.d. je $f(j) \in A_j$ za sve $j = 1, \dots, n$.

Običaj je označiti $f(j) =: a_j \in A_j$, pa je

$$\prod_{j=1}^{n} A_j = \big\{(a_1, \dots, a_n) : a_j \in A_j,\ j = 1, \dots, n\big\},$$

dakle, radi se o skupu *uređenih n-torki*.

NAPOMENA: za ekvivalenciju ove definicije Kartezijevog produkta konačno mnogo skupova s onom korištenom u dokazu teorema 9.10, potrebne su bijekcije

$$\begin{array}{ccccc} A \times (B \times C) & \sim & (A \times B) \times C & \sim & A \times B \times C \\ \big(a, (b, c)\big) & \leftrightarrow & \big((a, b), c\big) & \leftrightarrow & (a, b, c) \end{array}$$

i slične za više faktora.

# Skup funkcija sa skupa u skup

Promotrimo specijalan slučaj Kartezijevog produkta familije skupova $\{A_\alpha : \alpha \in J\}$ kada su svi skupovi te familije međusobno jednaki, i jednaki nekom skupu $A$, tj. $A_\alpha = A$ za sve $\alpha \in J$. Tada je $\bigcup\limits_{\alpha \in J} A_\alpha = A$, pa je $\prod\limits_{\alpha \in J} A_\alpha = A^J$ — skup svih funkcija $J \to A$, kao što je bilo definirano i u § 9 (i za to nam ne treba aksiom izbora !).

Zapravo, $A^J \subseteq \mathscr{P}(J \times A)$ je skup onih podskupova od $J \times A$ koji su funkcije, dakle onih $f \subseteq J \times A$ takvih da

$$\forall \alpha \in J \ \ \exists! a \in A \text{ t. d. je } (\alpha, a) \in f\,.$$

# Kardinalnost

Skupovi $A$ i $B$ su „jednako veliki" ako su ekvipotentni, tj. ako postoji bijekcija s $A$ na $B$ (i obratno). Dva konačna skupa su ekvipotentna ako i samo ako su ekvipotentna istom skupu $[1\,..\,n]$, tj. ako „imaju isti broj elemenata", $n$, i pišemo $\mathrm{k}(A) = \mathrm{k}(B) = n$, i kažemo da $A$ i $B$ imaju „isti kardinalni broj".
Nešto takvo htjeli bismo i za proizvoljne, dakle i beskonačne, skupove.

**Definicija 12.1**

Za ekvipotentne skupove $A$ i $B$ kažemo da imaju *istu kardinalnost*, i pišemo $\mathrm{k}(A) = \mathrm{k}(B)$ (ili $\mathrm{k}A = \mathrm{k}B$).

Dakle, $\mathrm{k}(A) = \mathrm{k}(B)$ ne znači ništa drugo nego da postoji bijekcija s $A$ na $B$, tj. da su $A$ i $B$ ekvipotentni

$$\boxed{\mathrm{k}(A) = \mathrm{k}(B) \text{ je isto što i } A \sim B}\,.$$

Ali, željeli bismo ipak na $\mathrm{k}(A)$ gledati kao na „nekakav broj" i „računati" s takvim objektima.

# Jedan pokušaj definicije kardinalnog broja

Ekvipotentnost, $\sim$, je relacija ekvivalencije — ali na čemu?
Ne na *skupu svih skupova*, jer to nije skup (Cantorov paradoks).
Onda na *klasi* svih skupova?

„Kardinalnim brojem" mogli bismo zvati klase ekvivalencije s obzirom na relaciju $\sim$ (ekvipotentnost), tj.

$$\mathrm{k}(A) = \{B : B \text{ je skup t.d. je } B \sim A\}.$$

Problem je u tome što je jedino za $A = \emptyset$ ovako definiran $\mathrm{k}(A)$ skup. Za $A \neq \emptyset$, $\mathrm{k}(A)$ *nije* skup — to je *prava klasa* (vidi § 2), a onda s time ne znamo što bi — s pravim klasama ne znamo raditi.

Dokaz da za $A \neq \emptyset$ ovako definiran $\mathrm{k}(A)$ nije skup: Neka je $A \neq \emptyset$, i pretpostavimo da je $\mathscr{C} := \{B : B \text{ je skup t.d. je } B \sim A\}$ skup. Tada je prema AX partitivnog skupa, i $\mathscr{P}(\mathscr{C})$ skup. Za svaki $x \in \mathscr{P}(\mathscr{C})$ neka je $A_x := A \times \{x\}$. $A_x$ je skup, i očito je $A_x \sim A$, pa je $A_x \in \mathscr{C}$.
Pridruživanje $x \mapsto A_x$ je funkcija $\mathscr{P}(\mathscr{C}) \to \mathscr{C}$, i ona je očito injektivna, jer $x' \neq x \Rightarrow A_{x'} = A \times \{x'\} \neq A \times \{x\} = A_x$.
Ali, to je u suprotnosti s Cantorovim teoremom 9.13. $\square$

# Izlaz

„Obični" brojevi $1, 2, 3, \ldots$ imaju dvostruku ulogu: govore o tome ***koliko*** nečega ima i ***koji je po redu***. Dakle svaki „običan broj" je *glavni* (kardinalni) i *redni* (ordinalni).

Najprije ćemo, u idućem poglavlju, definirati beskonačne ordinalne brojeve, a onda, pomoću njih, beskonačne kardinalne brojeve.

Zato zasada nećemo govoriti o *kardinalnom broju* nekog skupa, nego o *kardinalnosti* toga skupa.

Ali, uvedimo najprije standardne oznake:

$$\mathrm{k}(\emptyset) = 0$$
$$\mathrm{k}([1\,..\,n]) = n$$
$$\mathrm{k}(\mathbb{N}) = \aleph_0 \qquad \text{(čitaj: kardinalnost skupa } \mathbb{N} \text{ je alef nula)}$$
$$\mathrm{k}(\mathbb{R}) = \mathfrak{c}$$

Dakle, kada piše $\mathrm{k}(A) = \aleph_0$, to je isto što i $A \sim \mathbb{N}$, tj. $A$ i $\mathbb{N}$ su ekvipotentni; postoji bijekcija s $A$ na $\mathbb{N}$.

# Činjenice o kardinalnostima koje već znamo

$\mathrm{k}(\mathbb{N}) = \aleph_0$

$\mathrm{k}(\mathbb{Z}) = \aleph_0$

$\mathrm{k}(\mathbb{N} \times \mathbb{N}) = \aleph_0$

$\mathrm{k}(\mathbb{Q}) = \aleph_0$

$\mathrm{k}(\mathbb{Q} \times \mathbb{Q}) = \aleph_0$

$\mathrm{k}(\mathbb{N}^k) = \mathrm{k}(\mathbb{Q}^k) = \aleph_0$ (indukcijom iz prethodnog)

$\mathrm{k}(\langle a, b\rangle) = \mathrm{k}([a, b]) = \mathrm{k}(\langle a, b]) = \mathrm{k}([a, b\rangle) = \mathrm{k}(\mathbb{R}) = \mathfrak{c}$

$\mathrm{k}(\mathbb{R}^n) = \mathfrak{c}$

$\mathrm{k}\big(\{0, 1\}^{\mathbb{N}}\big) = \mathrm{k}\big(\mathscr{P}(\mathbb{N})\big) \neq \aleph_0$

$\mathrm{k}\big(\{0, 1\}^{\mathbb{N}}\big) = \mathfrak{c}$ ako prihvatimo dokaz koji koristi beskonačne decimalne, ili beskonačne binarne brojeve, vidi § 9.

$\mathrm{k}\big(\{0, 1\}^{\mathbb{R}}\big) = \mathrm{k}\big(\mathscr{P}(\mathbb{R})\big) \neq \mathfrak{c}$

- $\mathrm{k}(\mathbb{R} \setminus \mathbb{N}) = \mathrm{k}(\mathbb{R} \setminus \mathbb{Z}) = \mathrm{k}(\mathbb{R} \setminus \mathbb{Q}) = \mathfrak{c}$

# Uspoređivanje kardinalnosti

**Definicija 12.2**

Kažemo da je kardinalnost skupa $A$ *manja* od kardinalnosti skupa $B$ ako postoji injekcija $A \rightarrowtail B$, i pišemo $\mathrm{k}(A) \leqslant \mathrm{k}(B)$.

Dakle, $\mathrm{k}(A) \leqslant \mathrm{k}(B)$ ako je $A$ ekvipotentan nekom podskupu od $B$.

Ako je $\mathrm{k}(A) \leqslant \mathrm{k}(B)$ a $A$ i $B$ nisu ekvipotentni, pišemo $\mathrm{k}(A) < \mathrm{k}(B)$.
Naprimjer,
- $\mathrm{k}(\mathbb{N}) < \mathrm{k}(\mathbb{R})$: tj. $\aleph_0 < \mathfrak{c}$;
- za svaki $A$ je $\mathrm{k}(A) < \mathrm{k}\big(\mathscr{P}(A)\big)$ (teorem 9.13).

Uvijek vrijedi: $A \subseteq B \Rightarrow \mathrm{k}(A) \leqslant \mathrm{k}(B)$.

Jedan od najvažnijih teorema u teoriji skupova, pogotovo „početnoj", je sljedeći teorem:

**Teorem 12.3 (Cantor-Schröder-Bernstein)**

*Ako postoje injekcije $f\colon A \rightarrowtail B$ i $g\colon B \rightarrowtail A$ onda postoji i bijekcija između $A$ i $B$, tj. skupovi $A$ i $B$ su ekvipotentni.*

# Malo povijesti

Prethodni se teorem često naziva i Cantor-Bernsteinovim ili Schröder-Bernsteinovim teoremom, i to stoga što su se različite verzije i dokazi, objavljeni ili ne, pojavili u približno isto vrijeme.

1887 Richard Dedekind dokazao, ali nije objavio;

1895 Georg Cantor, kao posljedicu jednog teorema koji će objaviti kasnije;

1896 Ernst Schröder najavio dokaz;

1897 Felix Bernstein (Cantorov student) prikazao svoj dokaz u Cantorovom seminaru;

1897 Dedekind — drugi dokaz;

1898 Bernsteinov je dokaz objavljen u jednoj Borelovoj knjizi.

Cantor je, zapravo, bio svjestan tog teorema već 1882/83, ali se to implicite oslanjalo na aksiom izbora. A važna je činjenica da taj teorem *ne ovisi* o aksiomu izbora, iako su svi njegovi dokazi ne-konstruktivni i ovise o logičkom principu *tertium non datur*, (treća mogućnost ne postoji) pa ga intuicionisti ne prihvaćaju.

# Dokaz Cantor-Schröder-Bernsteinova teorema

Dokaz: BSO[9] možemo pretpostaviti da su skupovi $A$ i $B$ disjunktni.
Napravit ćemo jednu particiju unije $A \cup B$ u „lance" elemenata, ovako:
Odaberimo proizvoljan $a_0 \in A$, i primijenimo $f$, pa $g$, pa $f$, pa $g, \ldots$ itd.
Moguća su dva slučaja:

1. slučaj: ciklus se zatvara

$$\begin{tikzcd}
a_0 \arrow[r, mapsto, "f"] & b_0 \arrow[r, mapsto, "g"] & a_1 \arrow[r, mapsto, "f"] & b_1 \arrow[r, mapsto, "g"] & \cdots \arrow[r, mapsto, "g"] & a_k \arrow[r, mapsto, "f"] & b_k \arrow[llllll, mapsto, bend left, "g"]
\end{tikzcd}$$

pa dobivamo ciklus od $2k+2$ različitih elemenata. Naime, $g$ vraća $b_k$ na neki raniji $a_j$, ali zbog injektivnosti, to može biti jedino $a_0$.

2. slučaj: lanac se ne zatvara, tj. uvijek dobivamo nove i nove elemente od $A \cup B$. U tom slučaju pokušamo lanac proširiti ulijevo, ići natraške.
Ako je $a_0$ u slici od $g$, dodamo s lijeve strane $\mathrm{g}^{-1}(a_0)$, pa onda, ako je $g^{-1}(a_0)$ u slici od $f$, dodamo $f^{-1}\big(g^{-1}(a_0)\big)$, itd.
Mogu nastupiti tri slučaja:

---

[9] BSO — bez smanjenja općenitosti

# Završetak dokaza Cantor-Schröder-Bernsteinova teorema

$(2a)$ lanac se ulijevo ne završava, tj. proteže se beskonačno ulijevo:

$$\cdots \xmapsto{g} a_0 \xmapsto{f} b_0 \xmapsto{g} a_1 \xmapsto{f} b_1 \xmapsto{g} a_2 \xmapsto{f} b_2 \xmapsto{g} \cdots$$

$(2b)$ lanac staje ulijevo na nekom elementu iz $A$ koji nije u slici od $g$. Prenumeriramo:

$$a_0 \xmapsto{f} b_0 \xmapsto{g} a_1 \xmapsto{f} b_1 \xmapsto{g} a_2 \xmapsto{f} b_2 \xmapsto{g} \cdots$$

$(2c)$ lanac staje ulijevo na nekom elementu iz $B$ koji nije u slici od $f$. Prenumeriramo:

$$b_0 \xmapsto{g} a_0 \xmapsto{f} b_1 \xmapsto{g} a_1 \xmapsto{f} b_2 \xmapsto{g} a_2 \xmapsto{f} \cdots$$

Dobivamo četiri vrste lanaca. Definiramo $F\colon A \to B$ s $F(a_j) = b_j$ unutar svakog lanca. $F$ je očito bijekcija. $\square$

Prikazani dokaz Cantor-Schröder-Bernsteinova teorema pripisuje se Gyula (Julius) Königu (1849–1913).

## Zašto trebamo još jedan novi aksiom

Znamo da postoje beskonačni skupovi — barem jedan: $\omega$ (i $\mathbb{N}$).
Prema AX o partitivnom skupu, postoje skupovi

$$A_1 = \mathscr{P}(\mathbb{N}), A_2 = \mathscr{P}(A_1) = \mathscr{P}\big(\mathscr{P}(\mathbb{N})\big), \ldots, A_n = \mathscr{P}(A_{n-1}), \ldots$$

Kako je partitivni skup uvijek veći od samoga skupa, ovdje se radi o nizu sve većih i većih skupova. Među njima nema najvećeg.
Ali, kada bismo uzeli njihovu uniju, ona bi bila veća od svakog od njih.

A možemo li uzeti njihovu uniju? Zasada ne!
Naime, kada bismo znali da je klasa $\mathscr{S} = \{A_1, A_2, \ldots, A_n, \ldots\}$ skup, onda bi prema aksiomu unije, i unija $S = \bigcup \mathscr{S} = \bigcup\limits_{j \in \mathbb{N}} A_j$ bila skup, i on bi bio veći od svakog $A_n$.

Ali to ne znamo, i zato nam treba novi aksiom:

# Aksiom supstitucije

## AKSIOM SUPSTITUCIJE (ZAMJENE)

Ako je na skupu $A$ definirana funkcija $f$ takva da je za svaki $a \in A$ vrijednost $f(a)$ skup, onda je klasa $B = \{f(a) : a \in A\}$ također skup.

U našem primjeru: $A = \mathbb{N}$, $f : n \mapsto A_n$, $B = \mathscr{S}$.

Formalan zapis aksioma supstitucije izgleda ovako:

## AKSIOM SUPSTITUCIJE — formalan zapis

Neka je $A$ skup, $\sigma(x, y)$ svojstvo (izjavna funkcija[10]) dviju varijabli tako da za svaki $a \in A$ postoji jedinstven skup $b$ za koji je $\sigma(a, b)$ istinito. Tada postoji jedinstven skup $B$ kojemu su elementi svi skupovi $y$ za koje postoji element $x \in A$ t.d. je $\sigma(x, y)$ istinito.

---

[10] vidi fusnotu na str. 5.

# Aritmetika kardinalnosti

Kardinalnosti *nisu* brojevi, ali uz sljedeću definiciju, možemo s njima „računati".

**Definicija 12.4**

(a) $\mathrm{k}A + \mathrm{k}B := \mathrm{k}(A' \cup B')$
gdje su $A' \sim A$ i $B' \sim B$ takvi da je $A' \cap B' = \emptyset$

(b) $\mathrm{k}A \cdot \mathrm{k}B := \mathrm{k}(A \times B)$

(c) $\mathrm{k}A^{\mathrm{k}B} := \mathrm{k}(A^B)$.

U dokazu sljedećeg teorema, koji popisuje osnovna svojstva upravo definiranih operacija s kardinalnostima, pretpostavljat ćemo da su već skupovi $A$, $B$ i $C$ međusobno disjunktni.

# Svojstva operacija s kardinalnostima

**Teorem 12.5**

(1) $(\mathrm{k}A + \mathrm{k}B) + \mathrm{k}C = \mathrm{k}A + (\mathrm{k}B + \mathrm{k}C)$

(2) $\mathrm{k}A + \mathrm{k}B = \mathrm{k}B + \mathrm{k}A$

(3) $(\mathrm{k}A \cdot \mathrm{k}B) \cdot \mathrm{k}C = \mathrm{k}A \cdot (\mathrm{k}B \cdot \mathrm{k}C)$

(4) $\mathrm{k}A \cdot \mathrm{k}B = \mathrm{k}B \cdot \mathrm{k}A$

(5) $\mathrm{k}A \cdot (\mathrm{k}B + \mathrm{k}C) = \mathrm{k}A \cdot \mathrm{k}B + \mathrm{k}A \cdot \mathrm{k}C$

(6) $\mathrm{k}A^{\mathrm{k}B} \cdot \mathrm{k}A^{\mathrm{k}C} = \mathrm{k}A^{\mathrm{k}B + \mathrm{k}C}$

(7) $\mathrm{k}A^{\mathrm{k}C} \cdot \mathrm{k}B^{\mathrm{k}C} = (\mathrm{k}A \cdot \mathrm{k}B)^{\mathrm{k}C}$

(8) $\left(\mathrm{k}A^{\mathrm{k}B}\right)^{\mathrm{k}C} = \mathrm{k}A^{\mathrm{k}B \cdot \mathrm{k}C}$ (eksponencijalni zakon)

(9) $1 \cdot \mathrm{k}A = \mathrm{k}A$

(10) $0 \cdot \mathrm{k}A = 0$

Dokazat ćemo svojstva (6), (7) i (8). Ostala su svojstva jednostavne posljedice asocijativnosti, komutativnosti i distributivnosti unije i produkta.

# Dokaz svojstava (6), (7) i (8)

Dokaz: (6) $\mathrm{k}A^{\mathrm{k}B} \cdot \mathrm{k}A^{\mathrm{k}C} = \mathrm{k}A^{\mathrm{k}B+\mathrm{k}C}$ znači $A^B \times A^C \sim A^{B\cup C}$.

$$\text{Pridruživanje } \big(f\colon B\cup C \to A\big) \longmapsto \big(f|_B, f|_C\big)$$

$$\text{je bijekcija } A^{B\cup C} \longrightarrow A^B \times A^C.$$

(7) $\mathrm{k}A^{\mathrm{k}C} \cdot \mathrm{k}B^{\mathrm{k}C} = (\mathrm{k}A\cdot \mathrm{k}B)^{\mathrm{k}C}$ znači $A^C \times B^C \sim (A\times B)^C$.

$$\text{Pridruživanje } \big(f = (f_1, f_2)\colon C \to A\times B\big) \longmapsto (f_1, f_2)$$

$$\text{je bijekcija } (A\times B)^C \longrightarrow A^C \times B^C.$$

(8) $\big(\mathrm{k}A^{\mathrm{k}B}\big)^{\mathrm{k}C} = \mathrm{k}A^{\mathrm{k}B\cdot \mathrm{k}C}$ znači $\big(A^B\big)^C \sim A^{B\times C}$.
Za $f\colon B\times C \to A$ definiramo $F\colon C \to A^B$ s $\big(F(c)\big)(b) := f(b,c)$,
a za $G\colon C \to A^B$ definiramo $g\colon B\times C \to A$ s $g(b,c) := \big(G(c)\big)(b)$.
Tada su preslikavanja

$$\varphi\colon A^{B\times C} \to A^B \times A^C \text{ definirano s } \varphi(f) := F$$

$$\psi\colon A^B \times A^C \to A^{B\times C} \text{ definirano s } \psi(G) := g$$

međusobno inverzne bijekcije. $\square$

# Još nekoliko (ne)jednakosti

Kao i za nenegativne brojeve, vrijedi sljedeće:

## Teorem 12.6

*Neka su A, B i C neprazni skupovi, i neka je* $\mathrm{k}A \leqslant \mathrm{k}B$. *Tada je:*

- $\mathrm{k}A \cdot \mathrm{k}C \leqslant \mathrm{k}B \cdot \mathrm{k}C$
- $\mathrm{k}A^{\mathrm{k}C} \leqslant \mathrm{k}B^{\mathrm{k}C}$
- $\mathrm{k}C^{\mathrm{k}A} \leqslant \mathrm{k}C^{\mathrm{k}B}$

## Primjeri 12.7

- $\aleph_0 + \aleph_0 = \aleph_0 \qquad \aleph_0 \cdot \aleph_0 = \aleph_0$
- $\mathfrak{c} + \aleph_0 = \mathfrak{c}$
- $\mathfrak{c} + \mathfrak{c} = \mathfrak{c} \qquad \mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}$
- $2^{\aleph_0} = \mathfrak{c}$
- $\mathfrak{c}^{\aleph_0} = \left(2^{\aleph_0}\right)^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} = \mathfrak{c}$
- $\mathfrak{c} = 2^{\aleph_0} \leqslant \aleph_0^{\aleph_0} \leqslant \mathfrak{c}^{\aleph_0} = \mathfrak{c}$ Specijalno je $\aleph_0^{\aleph_0} = \mathfrak{c}$.
- Ali zapamtimo da *uvijek je* $\mathrm{k}A < 2^{\mathrm{k}A}$.

# Cantorova hipoteza kontinuuma

Postoji li kardinalnost *između* $\aleph_0$ i $\mathfrak{c}$, tj. ako je $S \subseteq \mathbb{R}$ beskonačan podskup, mora li nužno $S$ biti ekvipotentan ili s $\mathbb{N}$ ili s $\mathbb{R}$?
Dakle, postoji li podskup $S \subseteq \mathbb{R}$ t. d. ne postoji surjekcija $\mathbb{N} \twoheadrightarrow S$ niti surjekcija $S \twoheadrightarrow \mathbb{R}$?

Drugačije rečeno, je li $\mathfrak{c}$ prva veća kardinalnost od $\aleph_0$ tj. je li $\mathfrak{c} = \aleph_1$?
(O tome kako se definiraju viši kardinalni brojevi bit će govora kasnije.)

Hipoteza kontinuuma: Ne postoji kardinalnost između $\aleph_0$ i $\mathfrak{c}$.

Kurt Gödel je 1940. pokazao da je hipoteza kontinuuma konzistentna sa ZFC teorijom skupova (Zermelo-Fraenkelovi aksiomi + aksiom izbora), a Paul Cohen je 1963. dokazao da je i negacija hipoteze kontinuuma konzistentna sa ZFC teorijom skupova, i time je dokazana neovisnost hipoteze kontinuuma o ZFC teoriji skupova.

Poopćena hipoteza kontinuuma: Za nijedan beskonačan skup $A$ ne postoji kardinalnost između $\mathrm{k}A$ i $2^{\mathrm{k}A}$?

## Jedan, gotovo elementaran primjer

U različitim se dijelovima matematike prirodno pojavljuju tvrdnje čija istinitost ili ne-istinitost, ovisi o hipotezi kontinuuma.

1962. je Wetzel u *Ann Arbor Problem Book*, postavio sljedeće pitanje: Neka je $\{f_\alpha\}_\alpha$ familija međusobno različitih holomorfnih (analitičkih) funkcija t.d. je za svaki $z \in \mathbb{C}$ skup vrijednosti $\{f_\alpha(z)\}_\alpha$ prebrojiv. Znači li to da je i sâma familija $\{f_\alpha\}_\alpha$ prebrojiva ?

Ubrzo je Paul Erdös dao sljedeći odgovor:

**Teorem (P. Erdös, 1964)**

*Ako je $\mathfrak{c} > \aleph_1$ onda je svaka familija $\{f_\alpha\}_\alpha$ s opisanim svojstvom prebrojiva.*
*Ako je $\mathfrak{c} = \aleph_1$ onda postoji familija $\{f_\alpha\}_\alpha$ s opisanim svojstvom, koja je kardinaliteta $\mathfrak{c}$, dakle neprebrojiva.*

Za dokaz vidi `http://www.renyi.hu/~p_erdos/1964-04.pdf`; treba samo nešto malo kompleksne analize i nešto materijala iz sljedećeg poglavlja.

## 4 UREĐENI SKUPOVI

- Parcijalno uređeni skupovi
- Kategorija parcijalno uređenih skupova
- Redni tipovi linearno uređenih skupova
- Zornova lema
- Dobro uređeni skupovi
- Segmentni skupovi

# Parcijalno uređeni skupovi, PUS

## Definicija 13.1

*Parcijalni uređaj* na skupu $X$ je svaka antirefleksivna i tranzitivna relacija na $X$; oznaka $<$. Pâr $(X, <)$ naziva se *parcijalno uređen skup*.

## Primjeri 13.2

- $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sa „standardnim uređajem"
- $(\mathscr{P}(A), \subsetneqq)$ (umjesto $\subsetneqq$ rabit ćemo simbol $\subset$)
- $(\mathbb{N}, \mid)$: $m \mid n$ znači „$m$ dijeli $n$ i $m \neq n$"
- skup funkcija $[0,1] \to \mathbb{R}$ uz $f < g \Leftrightarrow f(x) < g(x)$ za sve $x \in [0,1]$
- *leksikografski uređaj* na $\mathbb{N} \times \mathbb{N}$:

$$(m, n) < (m', n') \;\Leftrightarrow\; (m < m') \text{ ili } (m = m' \text{ i } n < n')$$

Ako je $x < y$ ili $y < x$ kažemo da su $x$ i $y$ *usporedivi*.
Definira se i relacija $\leqslant$ kao $<$ ili $=$, pa se onda za $<$ često kaže „strogi parcijalni uređaj".
Jasno je kako se definiraju relacije $>$ i $\geqslant$.

# Najmanji (najveći) i minimalni (maksimalni) element

Ako je $(X, <)$ PUS (parcijalno uređen skup), a $A \subseteq X$, onda ćemo uvijek smatrati da $A$ nasljeđuje uređaj od $X$, i pisat ćemo $(A, <)$.

**Definicija 13.3 (Uoči problem s terminologijom !)**

Neka je $(X, <)$ parcijalno uređen skup, i $A \subseteq X$.

- *Najmanji element (minimum)* skupa $A$
  je element $a_0 \in A$ t.d. je $a_0 \leqslant a$ za sve $a \in A$.
- *Minimalni element* skupa $A$
  je element $a' \in A$ t. d. ne postoji $a \in A$ za koji vrijedi $a < a'$.

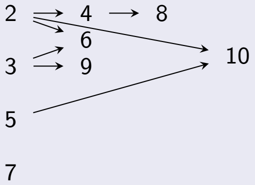
Analogno se definiraju *najveći element* i *maksimalni element*.

Lako se vidi da najmanji element, ako postoji, onda je jedinstven, i on je ujedno jedini minimalni element. Minimalnih elemenata može biti više, i u tom slučaju najmanji element ne postoji. Niti najmanji niti minimalni elementi ne moraju postojati.
Analogne činjenice vrijede za najveći i za maksimalni element.

# Primjeri

## Primjeri 13.4

- $(\mathbb{N}, <)$ 1 je i najmanji, dakle i jedini minimalni element.
- $\mathbb{Z}$, $\mathbb{R}$, $\langle 0, 1 \rangle$ nemaju niti najmanjeg niti minimalnog elementa
- $(\mathbb{N}, \mid)$ 1 je najmanji element
- $(\mathbb{N} \setminus \{1\}, \mid)$ nema najmanjeg elementa, a svi prosti brojevi su minimalni elementi




*Hasseov dijagram*

- $\mathbb{Z} \cup \{\sqrt{2}\}$ uz standardni uređaj na $\mathbb{Z}$, a $\sqrt{2}$ nije usporediv s nikim, ima jedan minimalni element, ali nema najmanjeg elementa

$$\cdots \longrightarrow -1 \longrightarrow 0 \longrightarrow 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow \cdots$$

$$\sqrt{2}$$

# Konačni parcijalno uređeni skupovi

**Teorem 13.5**

*Svaki konačan neprazan parcijalno uređen skup ima barem jedan minimalan i barem jedan maksimalan element.*

Dokaz: Indukcijom po $\mathrm{k}(X)$: ako je $X$ jednočlan, tvrdnja je očita.

$n \rightsquigarrow n+1$: Fiksirajmo neki $x_0 \in X$ i neka je $A = X \setminus \{x_0\}$. Neka je $B \subseteq A$ skup svih maksimalnih elemenata skupa $A$. $B$ je neprazan PPI.

1. slučaj Ako je $x_0$ neusporediv sa svim elementima od $B$, onda su svi elementi skupa $B$ maksimalni elementi skupa $X$, a može i $x_0$ biti maksimalan element skipa $X$. Svakako $X$ ima barem jedan maksimalan element.
2. slučaj Pretpostavimo da postoji element $b \in B$ koji je usporediv s $x_0$. Ako je $b < x_0$ onda je $x_0$ jedan maksimalan element skupa $X$. Ako je $b > x_0$ onda je $B$ skup svih maksimalnih elemenata skupa $X$.

Analogno se dokazuje postojanje minimalnog elementa. $\square$

# Nekoliko napomena

**Napomena 13.6**

(a) Ako je $a_0 \in A$ najmanji element onda je on i minimalan element.

(a′) Ako $A$ nema niti jedan minimalan element, onda $A$ nema niti najmanji element. [kontrapozicija od (a).]

(b) Ako $A$ ima više minimalnih elemenata, onda $A$ nema najmanjeg elementa.

(c) Ako je $a_0 \in A$ jedinstven minimalan element, to još ne znači da je $a_0$ najmanji element (vidi primjer $\mathbb{Z} \cup \{\sqrt{2}\}$ u 13.4).

Analogna napomena vrijedi za najveći i maksimalni element.

# Donja/gornja međa. Infimum/supremum.

## Definicija 13.7

Neka je $(X, <)$ PUS, $A \subseteq X$.
Element $x_0 \in X$ je *donja međa* skupa $A$ ako je $x_0 \leqslant a$ za sve $a \in A$.
Skup $A$ je *odozdo omeđen* ako postoji donja međa za $A$.
Najveća donja međa skupa $A$ (ako postoji), naziva se *infimum*.

Analogno se definira *gornja međa*, *odozgo omeđen* i *supremum*.

Skup $A$ je *omeđen* ako je omeđen odozdo i odozgo.

## Primjeri 13.8

- $\mathbb{N}$; $\mathbb{Z}$; $\langle 0, 1\rangle$ kao podskup od $\mathbb{R}$; $\langle 0, 1\rangle$ apstraktno;
- $\mathbb{Q}_+ = \{q \in \mathbb{Q} : q > 0\}$, $A = \{x \in \mathbb{Q}_+ : x^2 > 2\}$
- $\mathscr{F} \subseteq \mathscr{P}(A)$ proizvoljna familija podskupova skupa $A$;
- $\big(\{1, 2, 3, 5, 6, 10, 15\}, \mid\big) \subseteq (\mathbb{N}, \mid)$ *pravi* divizori broja 30;

NAPOMENA: Min/Max *vs.* Inf/Sup

# Linearno uređeni skupovi, LUS

U parcijalno uređenom skupu ne moraju svaka dva elementa biti usporediva. Naprimjer, brojevi 6 i 8 nisu usporedivi u $(\mathbb{N}, |)$.

## Definicija 13.9

Za parcijalno uređen skup $(X, <)$ kažemo da je *linearno uređen* ili *totalno uređen* ili *potpuno uređen* ili da je *lanac*, ako su svaka dva *različita elementa usporediva.*
*Drugim riječima, PUS* $(X, <)$ *je LUS, ukoliko je relacija* $<$ *na* $X$ *antisimetrična, tranzitivna i povezana.*

## Primjeri 13.10

- $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\langle 0, 1\rangle$ uz uobičajeni uređaj
- $(\mathbb{N} \times \mathbb{N}, \text{leksikografski uređaj})$
- $(\{2^k : k \in \mathbb{N}\}, |) \subseteq (\mathbb{N}, |)$

# Min/Max realnih funkcija i konačnih LU skupova

NAPOMENA: U linearno uređenom skupu je *najmanji element* (*minimum*) isto što i *minimalan element*, i *najveći element (maksimum)* je isto što i *maksimalan element*.

Zato, kada govorimo o minimumu ili o maksimumu *realne* funkcije, tj. o minimumu ili o maksimumu *skupa vrijednosti* realne funkcije, dakle podskupa od $\mathbb{R}$, onda nema problema s terminologijom.

**Korolar 13.11 (posljedica teorema 13.5)**

*Svaki konačan neprazan LUS ima minimum i maksimum.* $\square$

# Uzlazne funkcije

U *linearnoj algebri* promatraju se *vektorski prostori* i *linearni operatori*, i to zajedno čini ***kategoriju vektorskih prostora***.
U *metričkim prostorima* promatraju se *metrički prostori* i *neprekidna preslikavanja*, i to zajedno čini ***kategoriju metričkih prostora***.
U *teoriji grupa* promatraju se *grupe*, kao ***objekti*** i *homomorfizmi grupa* kao ***morfizmi***, i to zajednički čini ***kategoriju grupa***.

Iako to nismo posebno isticali, ***kategoriju skupova*** čine *skupovi* (bez ikakve dodatne strukture), kao objekti i *funkcije* kao morfizmi.

## Definicija 14.1

Neka su $(X, <)$ i $(Y, \prec)$ parcijalno uređeni skupovi.
Za funkciju $f\colon X \to Y$ kažemo da *čuva uređaj* ili da je *uzlazna*, ako

$$x \leqslant x' \;\Rightarrow\; f(x) \preccurlyeq f(x').$$

Parcijalno uređeni skupovi kao objekti, i uzlazne funkcije kao morfizmi, čine ***kategoriju parcijalno uređenih skupova***.

# Fiksne točke

**Definicija 14.2**

Neka je $f\colon X \to X$. Svaki element $x \in X$ za koji je $f(x) = x$ naziva se *fiksna točka* funkcije $f$.

Neke funkcije imaju fiksnu točku (jednu ili više), a neke nemaju.

**Teorem 14.3 (o fiksnim točkama uzlaznih funkcija PU skupova)**

(a) *Neka je $(X, <)$ PUS koji **ima minimum** i takav je da svaki neprazan $A \subseteq X$ **ima supremum**. Tada svaka uzlazna funkcija $f\colon X \to X$ **ima najveću** fiksnu točku.*

(b) *(dualno) Neka je $(X, <)$ PUS koji ima maksimum i takav je da svaki neprazan $A \subseteq X$ ima infimum. Tada svaka uzlazna funkcija $f\colon X \to X$ ima najmanju fiksnu točku.*

# Fiksne točke uzlaznih funkcija — dokaz teorema 14.3

Dakle, tvrdnja $(a)$ teorema govori da ako

- parcijalno uređen skup $X$ ***ima minimum***, i
- svaki neprazan podskup $A \subseteq X$ ***je omeđen odozgo*** i ***ima supremum***,

onda svaka uzlazna funkcija $f\colon X \to X$ ***ima fiksnu točku***, i ***skup svih fiksnih točaka ima maksimum***. I slično za tvrdnju $(b)$.

Dokaz: $(a)$: Neka je $x_0 = \min X$ i neka je $A := \{x \in X : x \leqslant f(x)\}$.
Očito je $x_0 \leqslant f(x_0)$, pa je $x_0 \in A$, te je $A \neq \emptyset$. Neka je $a := \sup A$.
Za $\forall x \in A$ je $x \leqslant a$, pa je $f(x) \leqslant f(a)$, te je i $\underbrace{x \leqslant f(x)}_{\text{jer je } x \in A} \leqslant f(a)$.

Dakle, $f(a)$ je gornja međa skupa $A$, pa je $a = \sup A \leqslant f(a) \quad (*)$.
Nadalje, $(*) \Rightarrow f(a) \leqslant f\big(f(a)\big)$, pa je $f(a) \in A$, te je $f(a) \leqslant \sup A = a$.
Dakle, $f(a) = a$, tj. $a$ je fiksna točka funkcije $f$, i $a \in A$ (zbog $(*)$).
Konačno, neka je $x \in X$ t.d. je $f(x) = x$. Tada je, specijalno, $x \leqslant f(x)$ pa je $x \in A$, te je $x \leqslant \sup A = a = \max A$ (zbog $a \in A$).
Dokaz tvrdnje $(b)$ je analogan uz $A := \{x : f(x) \leqslant x\}$. $\square$

# Knaster-Tarskijev teorem

Kao jednostavnu posljedicu prethodnog teorema, dobivamo

**Teorem 14.4 (Knaster-Tarski)**

*Neka je $X$ neprazan skup a $f : \mathscr{P}(X) \to \mathscr{P}(X)$ uzlazna funkcija, tj. takva da $A \subseteq B \Rightarrow f(A) \subseteq f(B)$. Tada postoji podskup $A \subseteq X$ takav da je $f(A) = A$.*

Dokaz: Parcijalno uređen skup $(\mathscr{P}(X), \subset)$ ima maksimum — skup $X$, i svaka familija $\mathscr{F} \subseteq \mathscr{P}(X)$ ima infimum — presjek $\bigcap\limits_{A \in \mathscr{F}} A$, pa tvrdnja slijedi iz teorema 14.3 $(b)$ o fiksnoj točki. $\square$

# Sličnost

Izomorfizam u kategoriji parcijalno uređenih skupova i uzlaznih funkcija, naziva se *sličnost* i definira se ovako:

## Definicija 14.5

Za PU skupove $(X, <)$ i $(Y, \prec)$ kažemo da su *slični* ako postoje uzlazne funkcije $f\colon (X, <) \to (Y, \prec)$ i $g\colon (Y, \prec) \to (X, <)$ t.d. je $g \circ f = \mathbb{1}_X$ i $f \circ g = \mathbb{1}_Y$; oznaka $(X, <) \simeq (Y, \prec)$, ili jednostavno $X \simeq Y$ ako je jasno, ili nevažno, o kojim se uređajima radi.

Svaka takva funkcija naziva se *sličnost* ili *preslikavanje sličnosti*.

Dakle, sličnost je uzlazna bijekcija $f$ čiji je inverz $f^{-1}$ također uzlazan.

## Primjeri 14.6

- $\langle 0, 1\rangle \simeq \langle -\frac{\pi}{2}, \frac{\pi}{2}\rangle \simeq \mathbb{R}$ uz uobičajeni uređaj;
- $\mathbb{N} \simeq 2\,\mathbb{N} = \{2\,n : n \in \mathbb{N}\}$ uz uobičajeni uređaj.

NAPOMENA: Slični skupovi su uvijek ekvipotentni, tj. $X \simeq Y \Rightarrow X \sim Y$.

# Nije svaka uzlazna bijekcija sličnost

U nekim kategorijama je svaki morfizam koji je bijekcija, automatski izomorfizam.

Naprimjer, svaki je linearni operator među **konačnodimenzionalnim** vektorskim prostorima, koji je bijekcija, izomorfizam vektorskih prostora.

Ili, svaka je neprekidna bijekcija kompaktnog metričkog prostora na neki metrički prostor, homeomorfizam.

Ali, nije svaka neprekidna bijekcija metričkih prostora homeomorfizam.

Isto tako, nije svaka uzlazna bijekcija PU skupova sličnost.

## Primjer 14.7

$(X, <)$ $\qquad\qquad$ $(Y, \prec)$

$$\begin{tikzcd}
a \arrow[r] \arrow[rrr, mapsto, bend right] & b \arrow[rrr, mapsto, bend left] & & 1 \arrow[r] & 2 \arrow[r] & 3 \\
c \arrow[urrrrr, mapsto] & & & & &
\end{tikzcd}$$

# Reprezentabilnost PU skupa u partitivnom skupu

**Teorem 14.8**

*Neka je $(X, <)$ PUS. Tada postoji podskup $\mathscr{X} \subseteq \mathscr{P}(X)$ takav da su $(X, <)$ i $(\mathscr{X}, \subset)$ slični.*

Dakle, svaki se PUS $X$ može realizirati (reprezentirati) kao neki podskup partitivnog skupa $\mathscr{P}(X)$ uređenog inkluzijom.

Dokaz: Za $\forall a \in X$ neka je $X_a = \{x \in X : x \leqslant a\} \subseteq X$, i neka je $\mathscr{X} = \{X_a : a \in X\}$.
Definirajmo $f : X \to \mathscr{X}$ s $f(a) := X_a$, $a \in X$. Surjektivnost je očita.
$f$ je injekcija: Zaista, $X_a = X_b \Rightarrow (a \leqslant b \ \& \ b \leqslant a) \Rightarrow a = b$.
$f$ je uzlazna: $a \leqslant b \Rightarrow \forall c \in X_a$ je $c \leqslant a \Rightarrow c \leqslant b \Rightarrow c \in X_b$, pa je $X_a \subseteq X_b$.
$f^{-1}$ je uzlazna: $X_a \subseteq X_b \Rightarrow \forall c \in X_a$, tj. $c \leqslant a$, je $c \in X_b$, tj. $c \leqslant b$.
Specijalno za $a \in X_a$ je $a \leqslant b$. $\square$

**Primjer 14.9**

$X = \{a, b, c, d, e\}$ uz uređaj dân Hasseovim dijagramom:
a realizacija u $\mathscr{P}(X)$ je familija
$\mathscr{X} = \{\{a\}, \{b\}, \{a, c\}, \{a, c, d\}, \{a, c, e\}\}$

$$\begin{tikzcd}
 & & d \\
a \arrow[r] & c \arrow[ur] \arrow[dr] & \\
 & & e \\
b & &
\end{tikzcd}$$

# Sličnost konačnih LU skupova

Za svaki prirodan broj $n$ postoji, do na sličnost, samo jedan $n$-član linearno uređen skup:

**Teorem 14.10**

*Neka su $(X,<)$ i $(Y,\prec)$ konačni LU skupovi s jednakim brojem elemenata. Tada su $(X,<)$ i $(Y,\prec)$ slični.*

Dokaz: Indukcijom: Tvrdnja je očita kada su $X$ i $Y$ jednočlani.

$n \rightsquigarrow n+1$: Prema korolaru 13.11 $X$ ima prvi element (minimum); označimo ga $a$. Isto tako $Y$ ima prvi element, $b$.

Neka je $A = X \setminus \{a\}$, $B = Y \setminus \{b\}$. PPI postoji sličnost $f\colon A \to B$.

Tada je funkcija $g\colon X \to Y$ definirana s $g(x) = \begin{cases} f(x)\,, & \text{za } x \in A \\ b\,, & \text{za } x = a \end{cases}$

sličnost s $X$ na $Y$. $\square$

# Svaka uzlazna bijekcija LU skupova je sličnost

Primjer 14.7 pokazuje da nije svaka uzlazna bijekcija PU skupova sličnost. Ali, kada se radi o LU skupovima, onda je.

**Teorem 14.11**

*Neka su $(X, <)$ i $(Y, \prec)$ LU skupovi, a $f\colon X \to Y$ uzlazna bijekcija. Tada je $f$ sličnost.*

Dokaz: Treba samo dokazati da je i funkcija $f^{-1}$ uzlazna, tj. da

$$f(x) \preccurlyeq f(x') \Rightarrow x \leqslant x'.$$

Kako je $X$ LUS, $x$ i $x'$ su usporedivi, pa kada ne bi bilo $x \leqslant x'$, bilo bi $x' < x$. Ali tada bi, zbog uzlaznosti funkcije $f$, bilo $f(x') \preccurlyeq f(x)$, te bi zbog injektivnosti, bilo $f(x') \prec f(x)$, u kontradikciji s $f(x) \preccurlyeq f(x')$. $\square$

# Nekoliko jednostavnih svojstava za vježbu

## Teorem 14.12

*Neka su $(X,<)$ i $(Y,\prec)$ PU skupovi i $f\colon X \to Y$ sličnost.*

(a) *$(X,<)$ je LUS ako i samo ako je $(Y,\prec)$ LUS.*

(b) *Ako je $A \subseteq X$ lanac u $X$, onda je $f(A)$ lanac u $Y$.*

(c) *Ako je $a$ minimalan element u $X$, onda je $f(a)$ minimalan element u $Y$.*
*Analogno za maksimalan element.*

(d) *Ako je $x_0$ minimum od $X$, onda je $f(x_0)$ minimum od $Y$.*
*Analogno za maksimum.*

(e) *Ako je podskup $A \subseteq X$ omeđen odozdo, onda je i $f(A) \subseteq Y$ omeđen odozdo.*
*Analogno za skupove omeđene odozgo.*

(f) *Ako je za $A \subseteq X$, $x_0 = \inf A$, onda je $f(x_0) = \inf f(A)$.*
*Analogno za supremum.*

# Redni tip linearno uređenih skupova

Odsada bavit ćemo se isključivo linearno uređenim skupovima, LU skupovima.

**Definicija 15.1**

Za dva LU skupa kažemo da *imaju isti redni tip* ako su slični, tj. ako postoji uzlazna bijekcija jednoga na drugi (inverzna bijekcija je tada također uzlazna prema teoremu 14.11); oznaka: $\mathrm{t}A = \mathrm{t}B$.

Prema teoremu 14.10, svaka dva konačna LU skupa s jednakim brojem elemenata, su slična, tj. njihov je redni tip jednoznačno određen brojem elemenata. Stoga se i njihov redni tip označuje istim prirodnim brojem kao i njihova kardinalnost, tj. $\mathrm{t}A = \mathrm{k}A$ (vidi definiciju 8.2).

**Definicija 15.2 (Standardne oznake za neke redne tipove)**

$$\mathrm{t}\mathbb{N} = \mathrm{t}\omega =: \omega, \text{ ili } \omega_0$$
$$\mathrm{t}(-\mathbb{N}) =: \omega^*$$
$$\mathrm{t}\mathbb{Q} =: \eta$$
$$\mathrm{t}\mathbb{R} =: \lambda$$

# Aritmetika rednih tipova

Neka su $(A, <)$ i $(B, \prec)$ LU skupovi. Htjeli bismo definirati $\mathrm{t}A + \mathrm{t}B$, i to kao redni tip skupa $(C, \propto)$ koji se sastoji od elemenata skupova $A$ i $B$, ali uređenih tako da svaki $a \in A$ bude ispred, $\propto$, svakog $b \in B$, a da unutar $A$ i $B$ budu sačuvani originalni uređaji $<$ odnosno $\prec$.

Očito, to je moguće jedino u slučaju da je $A \cap B = \emptyset$. Ako $A$ i $B$ nisu disjunktni, zamijenimo ih disjunktnim kopijama, npr. $A' = A \times \{1\}$ i $B' = B \times \{2\}$.[11]

Možemo, dakle, odmah pretpostaviti da su $A$ i $B$ disjunktni.

**Definicija 15.3**

Neka su $A$ i $B$ disjunktni LU skupovi. Njihova *redna unija*, $A \sqcup B$, je unija $A \cup B$ s uređajem t. d. $A$ i $B$ zadržavaju svaki svoj uređaj, i svaki je $a \in A$ ispred svakog $b \in B$.

Uoči da je $A \sqcup B \neq B \sqcup A$! Općenito je čak $A \sqcup B \not\simeq B \sqcup A$!

[11] Kako treba definirati uređaje na $A'$ i $B'$ da bude $\mathrm{t}A' = \mathrm{t}A$ i $\mathrm{t}B' = \mathrm{t}B$?

# Zbroj dvaju rednih tipova

Za sljedeću definiciju trebat će nam ova jednostavna lema:

**Lema 15.4**

*Neka su $A$, $B$, $A'$ i $B'$ LU skupovi t.d. je $A \cap B = \emptyset$, $A' \cap B' = \emptyset$, $A' \simeq A$ i $B' \simeq B$. Tada je $A \sqcup B \simeq A' \sqcup B'$.* □

**Definicija 15.5**

Neka su $\alpha$ i $\beta$ redni tipovi. *Suma*, $\alpha + \beta$, definira se kao redni tip redne unije $A \sqcup B$, gdje su $A$ i $B$ LU skupovi t.d. je $\mathrm{t}A = \alpha$ i $\mathrm{t}B = \beta$.

Prethodna lema pokazuje ***da je definicija dobra***, tj. da ne ovisi o odabranim reprezentantima $A$ i $B$ za redne tipove $\alpha$ odnosno $\beta$.

# Zbroj proizvoljne familije rednih tipova

Može se definirati i redna unije proizvoljne LU familije LU skupova. Točnije, neka je $J$ LUS, a $\{A_\alpha : \alpha \in J\}$ familija međusobno disjunktnih LU skupova. *Redna unija*, $\bigsqcup_{\alpha \in J} A_\alpha$, je skup $\bigcup_{\alpha \in J} A_\alpha$ s uređajem u kojem svaki $A_\alpha$ zadržava svoj uređaj, a za različite $\alpha, \beta \in J$, npr. $\alpha < \beta$, je svaki element iz $A_\alpha$ ispred svakog elementa iz $A_\beta$.

- Jasno je sada kako se definira *suma bilo kojeg LU skupa rednih tipova*.

**Teorem 15.6**

*Zbrajanje rednih tipova je asocijativno, tj.* $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$.

Dokaz: Slijedi iz sličnosti $(A \sqcup B) \sqcup C \simeq A \sqcup (B \sqcup C)$. □

Komutativnost ne vrijedi: Npr., $1 + \omega = t(\{0\} \sqcup \mathbb{N}) = t\omega = \omega$,
dok je $\omega + 1 = t(\mathbb{N} \sqcup \{0\}) \neq \omega$, jer $\mathbb{N} \sqcup \{0\}$ *nije sličan* skupu $\mathbb{N}$.

# Produkt rednih tipova

U primjeru 13.2 vidjeli smo kao se u $\mathbb{N}\times\mathbb{N}$ definira leksikografski uređaj. Tako se može i za svaka dva (parcijalno) uređena skupa, na njihovom produktu definirati (parcijalni) uređaj. Ali, ako su oba skupa LU skupovi, onda je i njihov produkt LU skup. To omogućuje

**Definicija 15.7**

*Produkt* $\alpha\cdot\beta$ rednih tipova $\alpha$ i $\beta$ definira se kao redni tip produkta $B\times A$, $\alpha\cdot\beta := \mathrm{t}(B\times A)$, gdje su $A$ i $B$ LU skupovi t.d. je $\mathrm{t}A=\alpha$ i $\mathrm{t}B=\beta$, a $B\times A$ je uređen leksikografski.

Uoči redoslijed u produktu![12]

- Pokazuje se da je definicija produkta rednih tipova dobra.
- Produkt od konačno mnogo rednih tipova definira se induktivno,
- i pokazuje se da je produkt asocijativan, ali nije komutativan:

$$\left.\begin{array}{l} 2\cdot\omega=\mathrm{t}(\mathbb{N}\times\{0,1\})=\mathrm{t}(:\,:\,:\,:\,:\,\cdots)=\mathrm{t}(\mathbb{N})=\omega \\ \omega\cdot 2=\mathrm{t}(\{0,1\}\times\mathbb{N})=\mathrm{t}(\mathbb{N}\sqcup\mathbb{N})=\omega+\omega \end{array}\right]\neq$$

[12] Može se definirati i $\alpha\cdot\beta=\mathrm{t}(A\times B)$, ali s antileksikografskim uređajem na $A\times B$.

# Aksiom izbora i ekvivalenti

Vidjeli smo kako je za uporabu principa rekurzivne definicije u dokazu karakterizacije beskonačnih skupova, kao i za definiciju Kartezijevog produkta proizvoljne familije skupova, potreban Aksiom izbora.

I mnoge su druge tvrdnje i dokazi u matematici nemogući bez njega:

- u analizi: ekvivalentnost $\varepsilon$-$\delta$ i Heineove definicije neprekidnosti;
- u linearnoj algebri: postojanje algebarske (Hamelove) baze vektorskog prostora;
- u algebri: svako polje ima algebarski zatvoreno proširenje.

Postoji, međutim, nekoliko tvrdnji koje su ekvivalentne aksiomu izbora, i koje se često koriste. Neke od njih su:

- Zornova lema
- Hausdorffov princip maksimalnosti
- Zermelov teorem o dobrom uređenju
- Trihotomija za kardinalne brojeve (Hartogsov teorem)
- Tarskijev teorem o kvadratima beskonačnih kardinalnih brojeva

# Zornova lema

Zornova lema će nam poslužiti u dokazu Zermelovog teorema o dobrom uređenju, koji će nam pak, u § 20, trebati pri definiciji kardinalnih brojeva.

U ovom ćemo paragrafu, zbog kratkoće, linearno uređene skupove, najčešće podskupove nekog PU skupa, nazivati *lancima*.

**Teorem 16.1 (Zornova lema)**

*Neka je $(X, <)$ PUS u kojem svaki lanac ima gornju među. Tada u $X$ postoji barem jedan maksimalan element.*

Iako je dokaz podugačak, zbog potpunosti ćemo ga prikazati.

Dokaz: Prema teoremu 14.8, $(X,<)$ je sličan podskupu $(\mathscr{X},\subset) \subseteq (\mathscr{P}(X),\subset)$, pa je postojanje gornje međe nekog lanca u $X$ ekvivalentno postojanju gornje međe odgovarajućeg lanca u $\mathscr{X}$, a maksimalan element u $\mathscr{X}$ odgovara maksimalnom elementu u $X$.

Podsjetimo da su elementi od $\mathscr{X}$ skupovi $X_a = \{x \in X : x \leqslant a\}$ i da je sličnost $(X, <) \to (\mathscr{X}, \subset)$ dâna s $a \mapsto X_a$ (vidi dokaz teorema 14.8).

# Dokaz Zornove leme

Kako je $\mathscr{X}$ uređen inkluzijom, gornja međa lanca $\mathscr{L} \subseteq \mathscr{X}$ je svaki element od $\mathscr{X}$ koji sadrži uniju svih članova od $\mathscr{L}$.

Treba, dakle, dokazati sljedeće: *Ako svaki lanac u $(\mathscr{X}, \subset)$ ima svojstvo da je unija njegovih elemenata sadržana u nekom elementu od $\mathscr{X}$, onda $\mathscr{X}$ ima barem jedan maksimalan element.*

Primijetimo da elementi od $\mathscr{X}$ nisu samo lanci u $X$, niti je svaki lanac u $X$ element od $\mathscr{X}$, jer $X$ nije LUS. Zato ćemo umjesto $\mathscr{X}$ promatrati jedan drugi skup.

Nazovimo sa $\mathfrak{X}$ skup svih lanaca u $X$, i uredimo ga inkluzijom (elementi od $\mathfrak{X}$ su lanci u $X$, dakle podskupovi od $X$).

$(\mathfrak{X}, \subset)$ je PUS i ima ova svojstva:

(*a*) Ako je $A \in \mathfrak{X}$ onda je i svaki podskup od $A$, uključivši i $\emptyset$, element od $\mathfrak{X}$.

(*b*) Ako je $\mathfrak{L} = \{A_\lambda : \lambda \in \Lambda\}$ lanac u $\mathfrak{X}$, onda je i unija $L = \bigcup\{A_\lambda : \lambda \in \Lambda\}$ element od $\mathfrak{X}$, tj. lanac u $X$.

(*c*) Svaki lanac u $\mathfrak{X}$ ima supremum (u $\mathfrak{X}$).

# Nastavak dokaza Zornove leme – 1

Tvrdnja $(a)$ je očita jer je svaki podskup lanca opet lanac.

Za tvrdnju $(b)$, neka su $a, b \in L$, $a \neq b$, i $\lambda, \mu \in \Lambda$ t.d. je $a \in A_\lambda$ i $b \in A_\mu$. Kako je $\mathfrak{L}$ lanac, to je $A_\lambda \subseteq A_\mu$ ili je $A_\mu \subseteq A_\lambda$. Neka je npr. $A_\lambda \subseteq A_\mu$. Tada su $a, b \in A_\mu$, a kako je $A_\mu \in \mathfrak{X}$, dakle lanac u $X$, to je ili $a < b$ ili $b < a$, tj. $L$ je lanac u $X$, dakle, element od $\mathfrak{X}$.

Lanac $L$ iz $(b)$ je očito najmanji element u $\mathfrak{X}$ koji sadrži sve članove od $\mathfrak{L}$, pa je $L = \sup \mathfrak{L}$, te vrijedi $(c)$.

Tvrdnja 1: *Svaki element iz $\mathfrak{X}$ sadržan je u nekom elementu iz $\mathscr{X}$.*
Zaista, element $L \in \mathfrak{X}$ je lanac u $X$, pa prema pretpostavci, ima u $X$ gornju među, nazovimo ju $\ell$. Tada je $L \subseteq \{x \in X : x \leqslant \ell\} = X_\ell \in \mathscr{X}$.

Tvrdnja 2: *Ako je $L$ maksimalan element u $\mathfrak{X}$ i $\ell$ je gornja međa od $L$, onda je $X_\ell$ maksimalan element u $\mathscr{X}$.*
Naime, kada bi postojao $C \in \mathscr{X}$ koji striktno sadrži $X_\ell$, bio bi $C = X_c$ za neki $c \in X$, pa bi redna unija $L \sqcup \{c\}$ bio lanac u $X$ koji striktno sadrži $L$ $\quad\Rightarrow\!\Leftarrow\quad$ $L$ je maksimalan element u $\mathfrak{X}$.

# Nastavak dokaza Zornove leme – 2

Prethodne tvrdnje pokazuju da razmatranjem skupa $\mathfrak{X}$ umjesto skupa $\mathscr{X}$ nećemo dobiti nove maksimalne elemente — za svaki maksimalan element u $\mathfrak{X}$ postoji odgovarajući maksimalni element u $\mathscr{X}$.

Treba, dakle, dokazati da $(\mathfrak{X}, \subset)$ ima barem jedan maksimalan element.

Prema aksiomu izbora, točnije teoremu 11.3', postoji funkcija $f$ koja svakom nepraznom podskupu $S \subseteq X$ pridružuje element $f(S) \in S$.

Za svaki $A \in \mathfrak{X}$, dakle lanac u $X$, označimo s $\overline{A}$ skup svih $x \in X$ t.d. je $A \cup \{x\}$ opet lanac u $X$, tj. $\overline{A} = \{x \in X : A \cup \{x\} \in \mathfrak{X}\}$.

Definirajmo funkciju $g\colon \mathfrak{X} \to \mathfrak{X}$ s $g(A) = \begin{cases} A \cup \{f(\overline{A} \setminus A)\}, & \text{za } \overline{A} \setminus A \neq \emptyset \\ A & \text{, za } \overline{A} \setminus A = \emptyset \end{cases}$.

Dakle, funkcija $g$ dodaje lancu $A$ u $X$ jedan, funkcijom $f$ izabran $x$, t.d. je $A \cup \{x\}$ opet lanac u $X$, i $g(A) = A$ ako i samo ako je $A$ maksimalan lanac u $X$, tj. maksimalan element u $\mathfrak{X}$.

Primijetimo da je uvijek $A \subseteq g(A)$, a ako je $g(A) \neq A$ onda je skup $g(A) \setminus A$ jednočlan (podskup od $X$).

# Nastavak dokaza Zornove leme – 3

Dakle, Zornova lema će biti dokazana ako dokažemo

Tvrdnja 3: Postoji $A \in \mathfrak{X}$ t.d. je $g(A) = A$.

Neka je $\mathfrak{J} \subseteq \mathfrak{X}$ proizvoljan podskup od $\mathfrak{X}$ t. d.

(*i*) $\emptyset \in \mathfrak{J}$

(*ii*) ako je $A \in \mathfrak{J}$ onda je $g(A) \in \mathfrak{J}$;

(*iii*) ako je $\mathfrak{L} \subseteq \mathfrak{J}$ lanac u $\mathfrak{J}$, onda je unija $\bigcup \mathfrak{L}$ element u $\mathfrak{J}$ (tj. unija lanca lanaca u $X$ koji su elementi od $\mathfrak{J}$, je lanac u $X$ koji je opet element od $\mathfrak{J}$).

Primijetimo najprije, kako neprazni podskupovi $\mathfrak{J} \subseteq \mathfrak{X}$ s ova tri svojstva, postoje — naprimjer $\mathfrak{X}$ je takav.

Neka je $\mathfrak{J}_0$ presjek svih podskupova $\mathfrak{J} \subseteq \mathfrak{X}$ koji zadovoljavaju gornja tri svojstva. $\mathfrak{J}_0$ je očito najmanji podskup od $\mathfrak{X}$ koji zadovoljava (*i*)–(*iii*).

Dokažimo da je $\mathfrak{J}_0$ lanac u $\mathfrak{X}$.

# Nastavak dokaza Zornove leme – 4

Za $C \in \mathfrak{J}_0$ kažemo da je *usporediv u* $\mathfrak{J}_0$ ako je usporediv sa svakim elementom iz $\mathfrak{J}_0$, tj. za svaki $A \in \mathfrak{J}_0$ je $A \subseteq C$ ili $C \subseteq A$.
Usporedivi elementi u $\mathfrak{J}_0$ postoje, npr. $\emptyset$ je usporediv, $\emptyset \subseteq A$, $\forall A \in \mathfrak{J}_0$.

Očito je $\mathfrak{J}_0$ lanac ako i samo ako je svaki njegov element usporediv u $\mathfrak{J}_0$.

Neka je $C \in \mathfrak{J}_0$ usporediv u $\mathfrak{J}_0$, i $A \in \mathfrak{J}_0$ pravi podskup od $C$, $A \subset C$.

Tvrdnja 4: $g(A) \subseteq C$. Zaista, zbog $(ii)$ je $g(A) \in \mathfrak{J}_0$ pa, kako je $C$ usporediv u $\mathfrak{J}_0$, to je ili $g(A) \subseteq C$ ili je $C \subset g(A)$. Međutim $C \subset g(A)$ nije moguće, jer bi tada bilo $A \subset C \subset g(A)$, pa bi $g(A)$ imao barem dva elementa više nego $A$, a to, prema definicije funkcije $g$, nije moguće. Dakle, za svaki $A \subset C$ je $g(A) \subseteq C$.

Za $C \in \mathfrak{J}_0$ neka je $\mathrm{I}(C) := \{A \in \mathfrak{J}_0 : A \subseteq C \text{ ili } g(C) \subseteq A\}$.

Zbog $(ii)$, za svaki $C \in \mathfrak{J}_0$, je $g(C) \in \mathfrak{J}_0$, pa skupovi $\emptyset$, $C$ i $g(C)$ pripadaju skupu $\mathrm{I}(C)$. Osim toga, ta su tri skupa i usporediva u $\mathrm{I}(C)$, jer za $\forall A \in \mathrm{I}(C)$ vrijedi $\emptyset \subseteq A$ i $A \subseteq C \subseteq g(C)$ ili $C \subseteq g(C) \subseteq A$.

# Nastavak dokaza Zornove leme – 5

Za završetak dokaza Zornove leme trebat će nam dvije leme:

**Lema 16.2**

*Za svaki* $C \in \mathfrak{J}_0$ *je* $\mathrm{I}(C) = \mathfrak{J}_0$.

Dokaz: Prema definiciji skupa $\mathrm{I}(C)$ je $\mathrm{I}(C) \subseteq \mathfrak{J}_0$, pa treba dokazati samo obratnu inkluziju, a za to je dovoljno pokazati da $\mathrm{I}(C)$ zadovoljava $(i)$–$(iii)$ jer je $\mathfrak{J}_0$ najmanji podskup od $\mathfrak{X}$ koji ih zadovoljava.
$\emptyset \in \mathrm{I}(C)$ pa $(i)$ vrijedi. Dokažimo $(ii)$, tj. $A \in \mathrm{I}(C) \Rightarrow g(A) \in \mathrm{I}(C)$.
Za $A \in \mathrm{I}(C)$ je $A \in \mathfrak{J}_0$ jer $\mathfrak{J}_0$ zadovoljava $(ii)$, pa
ako je $A \subset C$ onda je $g(A) \subseteq C$, te je $g(A) \in \mathrm{I}(C)$;
ako je $A = C$ onda je $g(A) = g(C)$, te je $g(A) = g(C) \in \mathrm{I}(C)$;
a ako je $g(C) \subseteq A$ onda je $g(C) \subseteq g(A)$, te je $g(A) \in \mathrm{I}(C)$.

Ostaje pokazati da $\mathrm{I}(C)$ zadovoljava i $(iii)$, tj. da

ako je $\mathfrak{L} \subseteq \mathrm{I}(C)$ lanac u $\mathrm{I}(C)$, onda je $\bigcup \mathfrak{L} \in \mathrm{I}(C)$.

# Nastavak dokaza Zornove leme – 6

Mogu nastupiti dva slučaja:

1. Za svaki $A \in \mathfrak{L}$ je $A \subseteq C$.
   Tada je i $\bigcup \mathfrak{L} \subseteq C$, pa, kako je $\mathfrak{L}$ lanac u $\mathfrak{J}_0$ i $\mathfrak{J}_0$ zadovoljava $(iii)$, to je $\bigcup \mathfrak{L} \in \mathrm{I}(C)$.
2. Postoji $A_0 \in \mathfrak{L}$ t. d. $A_0 \not\subseteq C$, pa je $g(C) \subseteq A_0$.
   No, tada je pogotovo $g(C) \subseteq \bigcup \mathfrak{L}$, pa je opet $\bigcup \mathfrak{L} \in \mathrm{I}(C)$.

Dakle, $\mathrm{I}(C)$ zadovoljava i $(iii)$, pa je zaista $\mathrm{I}(C) = \mathfrak{J}_0$. Q.E.D. leme 16.2.

**Lema 16.3**

*Svaki element iz $\mathfrak{J}_0$ usporediv je u $\mathfrak{J}_0$, tj. $\mathfrak{J}_0$ je lanac u $\mathfrak{X}$.*

Dokaz: Neke je $C \in \mathfrak{J}_0$ proizvoljan. Prema prethodnoj lemi je $\mathrm{I}(C) = \mathfrak{J}_0$, pa iz definicije skupa $\mathrm{I}(C)$ slijedi da za svaki $A \in \mathfrak{J}_0$ vrijedi $A \subseteq C$ ili $C \subseteq g(C) \subseteq A$. Dakle, $C$ je usporediv sa svakim $A \in \mathfrak{J}_0$, tj. svaka dva elementa iz $\mathfrak{J}_0$ su usporediva, pa je $\mathfrak{J}_0$ lanac. Q.E.D. leme 16.3.

# Završetak dokaza Zornove leme

Sada konačno možemo završiti dokaz Zornove leme.

Neka je $J_0 := \bigcup \mathfrak{J}_0$. Prema lemi 16.2 je $J_0 \in \mathfrak{J}_0$,
pa kako $\mathfrak{J}_0$ zadovoljava $(iii)$, to je i $g(J_0) \in \mathfrak{J}_0$.

Ali, $J_0$ je unija svih skupova lanca $\mathfrak{J}_0$, pa ih sve i sadrži. Specijalno je i $g(J_0) \subseteq J_0$, a kako je $J_0 \subseteq g(J_0)$, zaključujemo da je $g(J_0) = J_0$.
Time smo, jer je $J_0 \in \mathfrak{J}_0 \subseteq \mathfrak{X}$, dokazali tvrdnju 3,
a time i Zornovu lemu. $\square$

# Dobro uređeni skupovi, DUS

U teoremu 8.8 dokazali smo da je skup $\mathbb{N}$ dobro uređen.
Općenita definicija je sljedeća:

**Definicija 17.1**

*Dobro uređen skup*, DUS, je linearno uređen skup sa svojstvom da svaki njegov neprazan podskup ima minimum.

Očito je svaki podskup DU skupa (s naslijeđenim uređajem), i sâm DUS.

**Primjeri 17.2**

- $\mathbb{N}$
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, [0,1], \ldots$ *nisu* dobro uređeni skupovi
- $\mathbb{N} \sqcup \mathbb{N} = 1 \to 3 \to 5 \to \cdots \to 2 \to 4 \to 6 \to \cdots$ je DUS

# Skoro svatko ima neposrednog sljedbenika

Uočimo da svaki element $a$ DU skupa $X$, osim maksimuma ako postoji, ima neposrednog sljedbenika: $\min\{x \in X : x > a\}$, $a \neq \max X$.
Ali, ne mora svaki element, iako različit od minimuma, imati neposrednog prethodnika !

**Teorem 17.3**

*Ako su $(X, <)$ i $(Y, \prec)$ slični LU skupovi i $X$ je dobro uređen skup, onda je i $Y$ dobro uređen skup.*

Dokaz: Neka je $f : X \to Y$ sličnost. Kada bi postojao neprazan podskup $B \subseteq Y$ koji nema minimum, onda niti skup $f^{-1}(B) \subseteq X$ ne bi imao minimum (teorem14.12 ($c$)). $\square$

# Segmenti (početni komadi) DU skupova

## Definicija 17.4

Neka je $(X, <)$ DUS i $a \in X$. *Segment* ili *početni komad* definiran elementom $a$ je skup $X[a] := \{x \in X : x < a\}$ svih prethodnika od $a$ (***ne uključujući a***).[13] Za $a = \min X$ je $X[a] := \emptyset$.

Primjer: $1 \to 3 \to 5 \to 7 \to \cdots \to 2 \to 4 \to 6 \to 8 \to \cdots$

## Teorem 17.5

*Neka je $(X, <)$ DUS a $f : X \to X$ strogo uzlazna funkcija (tj. $x < y \Rightarrow f(x) < f(y)$). Tada za svaki $x \in X$ vrijedi $x \leqslant f(x)$.*

Dokaz: Pretpostavimo suprotno, tj. da postoji $x \in X$ t.d. je $f(x) < x$.
Neka je $S = \{x : f(x) < x\}$ i $x_0 = \min S$.
Tada je $f(x_0) < x_0$, a jer je $f$ strogo uzlazna, vrijedi $f\big(f(x_0)\big) < f(x_0)$,
pa je $f(x_0) \in S \quad \Rightarrow\!\Leftarrow \quad x_0 = \min S$. $\square$

[13] $X[a] \neq X_a = \{x \in X : x \leqslant a\}$ iz dokaza teorema 14.8 i Zornove leme.

# Jedinstvenost sličnosti

Dokažimo nekoliko jednostavnih posljedica:

**Korolar 17.6**

*Neka su $(X,<)$ i $(Y,\prec)$ slični DU skupovi, a $f, g\colon X \to Y$ preslikavanja sličnosti. Tada je $f = g$, tj. sličnost DU skupova je jedinstvena.*

Dokaz: Kompozicija $f^{-1} \circ g\colon X \to X$ je sličnost, pa prema teoremu 17.5, za $\forall x \in X$ vrijedi $x \leqslant f^{-1}\big(g(x)\big)$, te je i $f(x) \leqslant f\Big(f^{-1}\big(g(x)\big)\Big) = g(x)$. Analogno dobivamo $g(x) \leqslant f(x)$, pa je $f(x) = g(x)$, $\forall x \in X$. □

**Korolar 17.7**

*Za DUS $(X,<)$ jedina sličnost $X \to X$ je identiteta.* □

**Korolar 17.8**

*DUS nije sličan niti jednom svom segmentu (početnom komadu).*

Dokaz: Kada bi postojala sličnost $f\colon X \to X[a]$ za neki $a \in X$, bilo bi $f(a) < a$, što je u kontradikciji s teoremom 17.5. □

# Sličnosti dobro uređenih skupova

**Korolar 17.9**

*Različiti segmenti $X[a]$ i $X[b]$ DU skupa $X$ ne mogu biti slični.*

Dokaz: Ako je $a < b$ onda je $X[a]$ ujedno i segment skupa $X[b]$, pa, prema korolaru 17.8, ne mogu biti slični. □

**Teorem 17.10**

*Sličnost $f\colon (X,<) \to (Y,\prec)$ DU skupova preslikava svaki segment skupa $X$ na neki segment skupa $Y$.*

Dokaz: Neka je $a \in X$. Dokazat ćemo da je $f\big(X[a]\big) = Y\big[f(a)\big]$.

$\subseteq$ Za $y \in f\big(X[a]\big)$, $\exists x \in X[a]$ t.d. je $y = f(x)$, pa $x < a \Rightarrow y = f(x) \prec f(a) \Rightarrow y \in Y\big[f(a)\big]$. △

$\supseteq$ Neka je $y \in Y\big[f(a)\big]$, tj. $y \prec f(a)$. $f$ je bijekcija, pa neka je $x \in X$ t.d. je $y = f(x)$. Dakle, $f(x) = y \prec f(a)$, pa je $x = f^{-1}\big(f(x)\big) < f^{-1}\big(f(a)\big) = a$, tj. $x \in X[a] \;\Rightarrow\; y = f(x) \in f\big(X[a]\big)$. □

# Segmenti uređeni inkluzijom

DU skupovi su reprezentirani skupom svojih početnih komada. Točnije,

**Teorem 17.11**

*Svaki je DUS sličan skupu svih svojih segmenata uređenih inkluzijom.*

Dokaz: Neka je $(X, <)$ DUS i $(Y, \prec) = \big(\{X[a] : a \in X\}, \subset\big)$ skup svih segmenata od $X$, uključujući i $\emptyset$. Definirajmo $f\colon X \to Y$ s $f(a) := X[a]$. Kako je $(X, <)$ LUS, dovoljno je pokazati da je $f$ uzlazna bijekcija.

$f$ čuva uređaj: $a \leqslant b \;\Rightarrow\; f(a) = X[a] \subseteq X[b] = f(b)$.

$f$ je surjekcija: Za $\forall y \in Y$ je $y = X[a]$ za neki $a \in X$, pa je $y = f(a)$.

$f$ je injekcija: Zbog korolara 17.9, $a \neq b \;\Rightarrow\; X[a] \neq X[b]$. $\square$

# Princip transfinitne indukcije

Sljedeći teorem govori o jednom od najmoćnijih oruđa za dokazivanje, ne samo u teoriji skupova, nego i u analizi, topologiji, algebri, i drugdje.

**Teorem 17.12 (Princip transfinitne indukcije)**

*Neka je* $(X, <)$ *DUS i* $A \subseteq X$ *takav podskup da za svaki* $a \in X$, *iz* $X[a] \subseteq A$ *slijedi* $a \in A$. *Tada je* $A = X$.

Dokaz: Pretpostavimo da je $A \neq X$, tj. $X \backslash A \neq \emptyset$, i neka je $m = \min X \backslash A$.

Tvrdnja: $X[m] \subseteq A$. Zaista, za svaki $x \in X[m]$ je $x < m = \min X \setminus A$, pa $x \notin X \setminus A$, tj. $x \in X \setminus (X \setminus A) = A$. Dakle, $X[m] \subseteq A$. $\triangle$

Prema pretpostavci o skupu $A$, slijedi $m \in A$, $\Rightarrow\!\Leftarrow$ $m \in X \setminus A$. $\square$

Napomena 1. Vrijedi i obratno: ako je $(X, <)$ LUS koji ima minimum i u kojem vrijedi princip transfinitne indukcije, onda je $(X, <)$ DUS (za dokaz vidi Vuković, *Teorija skupova*, teorem 1.87).

Napomena 2. Općenito, u LU skupu princip transfinitne indukcije ne vrijedi: $X = \mathbb{Z}$, $A = 2\,\mathbb{Z} \subseteq \mathbb{Z}$. Očito $\forall a \in X$, $(X[a] \subseteq A \Rightarrow a \in A)$, iako $A \neq X$.

# Produljenje

Kako su DU skupovi reprezentirani skupom svojih segmenata, koristan je sljedeći termin.

**Definicija 17.13**

Za dobro uređen skup $Y$ kaže se da je *produljenje* DU skupa $X$ ako je $X$ neki segment (početni komad) skupa $Y$.

Relacija produljenja je očito tranzitivna, a zbog korolara 17.8 je i antirefleksivna, pa je ona relacija (strogog) uređaja.

**Primjer 17.14**

Neka je $X$ DUS, $a, b \in X$, $a < b$. Tada je $X[b]$ produljenje od $X[a]$.

Uoči da je $X[a] = \big(X[b]\big)[a]$.

# Segmentni skupovi

Neformalno se *ordinalni brojevi* mogu definirati kao redni tipovi DU skupova. Mi ćemo ih, prema von Neumannu ($\sim$1925.), definirati kao specijalne DU skupove. Ali najprije jedna definicija:

**Definicija 18.1**

DUS $(X, <)$ naziva se *segmentni skup* ako za $\forall a \in X$ vrijedi $a = X[a]$.

OPREZ ! NE $a \in X[a]$, to ne može biti !

POJAŠNJENJE: Prema teoremu 17.11, DUS $(X, <)$ sličan je skupu $\{X[a] : a \in X\}$ svih svojih segmenata, uređenom inkluzijom, a prema dokazu tog teorema, preslikavanje $a \mapsto X[a]$ je sličnost. Ali, prema korolaru 17.6, sličnost DU skupova je jedinstvena, pa je $a \mapsto X[a]$ *jedina* sličnost $X \to \{X[a] : a \in X\}$. Dakle, ako je $(X, <)$ segmentni skup, tj. $X[a] = a$ za $\forall a$, onda je $X = \{X[a] : a \in X\}$, i $< \equiv \subset$, tj.

uređaj u segmentnom skupu uvijek je inkluzija, tj. produljenje.

# Kako izgledaju segmentni skupovi ?

Zapravo, svi segmentni skupovi u početku izgledaju jednako.
Naime, neka je $(X,<)$ neki segmentni skup. Kako je $(X,<)$ DUS, postoji minimum, $m = \min X$.
Međutim, $m = X[m] = \emptyset$ (vidi definiciju 17.4).

Nadalje, segment određen sljedbenikom od $m$ jednak je $\{m\} = \{\emptyset\}$, a segment određen njegovim sljedbenikom je $\big\{m,\{m\}\big\} = \big\{\emptyset,\{\emptyset\}\big\}$, itd. Dakle,

**Korolar 18.2**

*Svaki segmentni skup s* $\geqslant 3$ *člana počinje ovako:* $\{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\},\dots\}$.

**Primjer 18.3**

- Skup $\omega = \{\emptyset, \emptyset^+, \emptyset^{++}, \dots\} = \big\{\emptyset, \{\emptyset\}, \big\{\emptyset, \{\emptyset\}\big\}, \dots\big\}$ je segmentni skup (vidi primjer 3.2 i definiciju 3.6).
- Skup $\{\emptyset, \emptyset^+, \emptyset^{++}, \dots, \omega, \omega^+, \omega^{++}, \dots\}$ je segmentni skup *različit* od $\omega$.

# Segmenti segmentnih skupova su segmentni skupovi

**Teorem 18.4**

(a) *Svaki je segment segmentnog skupa $(X,<)$ segmentni skup.*

(b) *Ako je pravi podskup $Y \subset X$ segmentni skup, onda je $Y$ segment, tj. početni komad skupa $X$ (dakle ne može $Y$ biti „u sredini”).*

Dokaz: (a) Neka je $Y = X[a]$ za neki $a \in X$. Za $\forall b \in Y = X[a]$ je $b < a$, pa je $Y[b] = \big(X[a]\big)[b] = X[b] = b$, tj. $Y$ je segmentni skup. $\triangle$

(b) Neka je $Y \subsetneqq X$ segmentni skup. Tada za $\forall a \in Y$ je $Y[a] = a$, ali je i $X[a] = a$, pa je $X[a] = Y[a]$. Kako je $Y \neq X$ to je $X \setminus Y \neq \emptyset$.

Tvrdnja: $Y = X[m]$, gdje je $m = \min X \setminus Y$.

$\subseteq$ $Y$ je segmentni skup, pa za $\forall a \in Y$ i za $\forall b \in X \setminus Y$ vrijedi $a < b$ (inače bi bilo $b \leqslant a$, te bi bilo $b \in Y$), pa je $a < m$, tj. $a \in X[m]$. $\triangle$

$\supseteq$ Za $\forall a \in X[m]$ je $a < m$, pa $a \notin X \setminus Y$ jer je $m = \min X \setminus Y$. Dakle, $a \in X \setminus (X \setminus Y) = Y$. $\square$

Napomena: Odavde slijedi i da je uređaj, tj. relacija sadržavanja kojom je uređen segmentni skup, zapravo relacija produljenja (definicija 17.13).

# Slični segmentni skupovi su jednaki

**Teorem 18.5**

*Ako su segmentni skupovi $X$ i $Y$ slični, onda su jednaki.*

Drugim riječima, različiti segmentni skupovi ne mogu biti slični, ili, drugačije rečeno, klase ekvivalencije segmentnih skupova, s obzirom na relaciju sličnosti, su jednočlane.

Dokaz: Neka je $f\colon X \to Y$ sličnost.

Transfinitnom indukcijom dokazat ćemo da je $f(x) = x$, $\forall x \in X$.

Neka je $A = \{x \in X : f(x) = x\}$. Tvrdimo da je $A = X$.

U protivnom, postojao bi najmanji $x_0 \in X$ t.d. je $f(x_0) \neq x_0$, pa bi $f(x_0)$ bio najmanji element u $Y$ koji ne pripada skupu $f(A)$ (jer sličnost LU skupova čuva minimum, teorem 14.12 $(c)$).

Ali, $\underbrace{Y[f(x_0)]}_{=f(x_0)} = \underbrace{X[x_0]}_{=x_0}$, jer je za sve $x < x_0$, $f(x) = x$, pa je $f(x_0) = x_0$, u kontradikciji s $f(x_0) \neq x_0$. $\square$

# Je li svaki DUS sličan nekom segmentnom skupu ?

Cilj ovog poglavlja je dokazati teorem 18.14, kako je svaki DUS sličan, i to jedinstvenom, segmentnom skupu. Zasada, kao posljedicu prethodnog teorema 18.5, dobivamo samo

**Korolar 18.6**

*DUS može biti sličan najviše jednom segmentnom skupu.* $\square$

Trebat će nam i sljedeća činjenica:

**Teorem 18.7**

*Presjek dvaju segmentnih skupova je segmentni skup.*

Dokaz: Segmentni skupovi $X$ i $Y$ uređeni su inkluzijom $\subset$, pa je i $X \cap Y$ uređen inkluzijom. Neka je $a \in X \cap Y$. Kako je $X[a] = a = Y[a]$, to je i $(X \cap Y)[a] = X[a] = Y[a] = a$, jer su prethodnici od $a$ u $X$ i u $Y$ jednaki, pa je $X \cap Y$ segmentni skup. $\square$

# Usporedivost segmentnih skupova

**Teorem 18.8 (o usporedivosti segmentnih skupova)**

*Neka su $X$ i $Y$ segmentni skupovi. Tada vrijedi jedna i samo jedna od sljedećih mogućnosti:*

(a) *ili je $X = Y$;*

(b) *ili je $X$ segment (početni komad) od $Y$;*

(c) *ili je $Y$ segment (početni komad) od $X$.*

Dokaz: Neka je $X \neq Y$. Dovoljno je pokazati da je ili $X$ pravi podskup od $Y$, ili je $Y$ pravi podskup od $X$, jer je onda, prema teoremu 18.4 (b), $X$ segment od $Y$ ili je $Y$ segment od $X$. Treba, dakle, pokazati da nije moguće $X \not\subseteq Y$ i $Y \not\subseteq X$. Pretpostavimo suprotno, pa neka je $a = \min X \setminus Y$ i $b = \min Y \setminus X$. $X \cap Y$ je segmentni skup pa, kao u dokazu teorema 18.4 (b), zaključujemo da je $X \cap Y = X[a]$ i $X \cap Y = Y[b]$. Stoga je $a = X[a] = X \cap Y = Y[b] = b \in Y$, pa je $a \in X \cap Y = X[a]$, što je u kontradikciji s $a = X[a] = \{x : x < a\}$. $\square$

# Segmentni skupovi su tranzitivni

Iz prethodnog teorema 18.8, neposredno slijedi

**Korolar 18.9**

*Svaka je familija segmentnih skupova linearno uređena inkluzijom.* □

Iz definicije 18.1 neposredno slijedi da je svaki segmentni skup tranzitivan (vidi definiciju 3.8 i teorem 3.9).

Sljedeću, nešto slabiju tvrdnju, upotrijebit ćemo u dokazu teorema 18.12.

**Korolar 18.10**

*Neka su $X$ i $Y$ segmentni skupovi i $X \subset Y$ je pravi podskup od $Y$. Onda je $X \in Y$.* □

# Aksiom regularnosti (dobre utemeljenosti)

Prema korolaru 18.9, svaki je skup segmentnih skupova LUS. Kako bismo dokazali više, tj. da je svaki skup segmentnih skupova DUS, treba nam još jedan aksiom teorije skupova (von Neumann, 1925):

**AKSIOM REGULARNOSTI (DOBRE UTEMELJENOSTI)**

Svaki neprazan skup $S$ ima barem jedan element $s$ t.d. je $s \cap S = \emptyset$.

**Korolar 18.11**

*Ne postoji skup $A = \{a_n : n \in \mathbb{N}\}$ t.d. je $a_{n+1} \in a_n$ za sve $n \in \mathbb{N}$.*

Dokaz: Pretpostavimo da takav skup $A$ postoji. Dakle, za $\forall n \in \mathbb{N}$ je $a_{n+1} \in a_n$.

Tvrdnja: Za $\forall n$ je $a_n \cap A \neq \emptyset$:

Zaista, zbog $a_{n+1} \in a_n$ i $a_{n+1} \in A$, je $a_{n+1} \in a_n \cap A$, pa je $a_n \cap A \neq \emptyset$. $\triangle$

No, dokazana tvrdnja je u suprotnosti s AX regularnosti. $\square$

# Dobro uređenje familijâ segmentnih skupova

Sada možemo dokazati najavljenu činjenicu o dobrom uređenju svakog skupa segmentnih skupova.

**Teorem 18.12**

*Svaki je skup segmentnih skupova dobro uređen relacijom produljenja.*

Dokaz: Neka je $\mathscr{A}$ neki skup segmentnih skupova. Prema korolaru 18.9, $\mathscr{A}$ je LUS. Treba pokazati da svaki neprazan podskup od $\mathscr{A}$ ima minimum. Pretpostavimo da $\exists \mathscr{B} \subseteq \mathscr{A}$ koji nema minimum. Neka je $X_0 \in \mathscr{B}$. Kako $\mathscr{B}$ nema minimum, $\exists X_1 \in \mathscr{B}$ t.d. je $X_1 < X_0$, tj. $X_1 \subsetneq X_0$. Indukcijom dobivamo niz segmentnih skupova $X_n \in \mathscr{B}$ t.d. je $X_{n+1} \subsetneq X_n$ za sve $n \in \mathbb{N}$.
Kako su $X_{n+1}$ i $X_n$ segmentni skupovi, i $X_{n+1} \subset X_n$, to je, prema korolaru 18.10, $X_{n+1} \in X_n$, za $\forall n$, što se protivi aksiomu regularnosti.
Dakle, $\mathscr{B}$ ima minimum, pa je $\mathscr{A}$ dobro uređen skup. $\square$

# Supremum LU familije segmentnih skupova

Za dokaz glavne tvrdnje ovog poglavlja, teorema 18.14, kao i Zermelova teorema 19.10 o dobrom uređenju, potreban nam je još i

**Teorem 18.13**

*Neka je $\mathscr{A}$ LU skup segmentnih skupova uređen relacijom produljenja, i neka je $A = \bigcup \mathscr{A}$. Tada postoji jedinstveno uređenje skupa $A$ t.d. je $A$ segmentni skup koji je produljenje svakog elementa iz $\mathscr{A}$ (različitog od $A$). Skup $A$ je ujedno i supremum familije $\mathscr{A}$.*

Dokaz: Prema prethodnom teoremu 18.12, $\mathscr{A}$ je DUS.

Ako je $A = \bigcup \mathscr{A} \in \mathscr{A}$, onda je tvrdnja teorema očita.

Ako $A \notin \mathscr{A}$, neka su $x, y \in A$ i $X, Y \in \mathscr{A}$ t.d. je $x \in X$ i $y \in Y$.

Kako je $\mathscr{A}$ LUS, segmentni skupovi $X$ i $Y$ su usporedivi, pa neka je $Y$ produljenje od $X$, $X \subseteq Y$. Definirajmo uređaj u $A$ ovako:

$$x < y \text{ u } A \;\Leftrightarrow\; x < y \text{ u } Y.$$

Tada je $x < y$ i u svakom $Z \in \mathscr{A}$ koji sadrži $x$ i $y$ (jer $Y \subseteq Z$ ili $Z \subseteq Y$).

# Završetak dokaza teorema 18.13

Tvrdnja 1: $A$ je DUS. Neka je $\emptyset \neq C \subseteq A$. Tada $\exists Z \in \mathscr{A}$ t.d. je $C \cap Z \neq \emptyset$.
$C \cap Z$ je DUS, kao podskup segmentnog skupa $Z$, pa neka je $c = \min C \cap Z$.

Tvrdnjica: $c = \min C$.
Zaista, jer je $Z$ segmentni skup, i $Z \subseteq A$, zbog $c \in Z$ bit će $x \in Z$ za $\forall x \in \{a \in A : a < c\}$; a kada bi u $C$ postojao element manji od $c$, on bi bio i u $Z$, pa bi bio i u $C \cap Z$ $\Rightarrow\!\Leftarrow$ $c = \min C \cap Z$.
Dakle, $C$ ima minimum, što dokazuje tvrdnju 1. △

Tvrdnja 2: $A$ je segmentni skup. Neka je $a \in A$. Tada je $a \in X$ za neki $X \in \mathscr{A}$, pa je $X[a] = a$. Ali $X[a] = A[a]$, jer je skup svih prethodnika od $a$ u $X$ i u $A$ isti, pa je $A[a] = X[a] = a$, tj. $A$ je segmentni skup. △
Kako je $A = \bigcup \mathscr{A}$, to je $A$ gornja međa familije $\mathscr{A}$.
S druge strane, za svaki $a \in A$, postoji $X \in \mathscr{A}$ t.d. je $a \in X$, pa $A \setminus \{a\}$ ne sadrži $X$, tj. $A \setminus \{a\}$ nije gornja međa familije $\mathscr{A}$.
Dakle, $A = \sup \mathscr{A}$.

Jedinstvenost uređaja slijedi iz činjenice da je, uz uređaj koji smo na $A$ definirali, $A$ segmentni skup, pa je svaki uređaj na njemu — produljenje. □

# Konačno na cilju !

**Teorem 18.14 (Teorem enumeracije[14])**

*Svaki je dobro uređen skup sličan jedinstvenom segmentnom skupu.*

Dokaz: Jedinstvenost slijedi iz teorema 18.5 ili korolara 18.6.

Egzistencija: Neka je $(X, <)$ DUS i neka je $a \in X$ t.d. je za svaki $x < a$, početni komad (segment) $X[x]$ sličan nekom segmentnom skupu $S_x$, i neka je $Z = \{S_x : x < a\}$ klasa svih takvih segmentnih skupova. Prema teoremu 18.5, svaka su dva slična segmentna skupa jednaka, pa je $S_x$ *jedinstven* segmentni skup sličan segmentu $X[x]$. Prema Aksiomu supstitucije, $Z$ je skup (skup $A$ iz aksioma supstitucije je $\{x : x < a\}$, a $f(x) = S_x$, što je skup). Iz prethodnog teorema 18.13 slijedi da je i unija $S_a = \bigcup\{S_x : x < a\}$ segmentni skup, a kako je svaki DUS sličan skupu svojih segmenata, teorem 17.11, zaključujemo da je $X[a] \simeq S_a$.

[14]Vidi definiciju 19.1.

# Završetak dokaza teorema 18.14

Tvrdnja: Svaki segment skupa $X$ sličan je nekom, a onda i jedinstvenom segmentnom skupu. Dokaz je transfinitnom indukcijom.

Kada tvrdnja ne bi bila istinita, postojao bi najmanji element $x_0 \in X$ t. d. $X[x_0]$ nije sličan nekom segmentnom skupu. Ali, prema upravo dokazanom, to nije moguće, jer ako su za sve $x < x_0$ segmenti $X[x]$ slični segmentnim skupovima $S_x$, onda je i $X[x_0]$ sličan uniji $\bigcup\{S_x : x < x_0\} = S_{x_0}$.

Dakle, za svaki segment $X[x]$ skupa $X$ postoji jedinstven segmentni skup $S_x$ koji mu je sličan. Ponovnom primjenom aksioma supstitucije zaključujemo da je $\{S_x : x \in X\}$ skup. Označimo ga s $\mathscr{A}$.

Prema teoremu 18.13, svi elementi skupa $\mathscr{A}$ čine segmentni skup, nazovimo ga $Y$, kojeg su segmenti upravo elementi od $\mathscr{A}$.

Kako je svaki DUS sličan skupu svih svojih segmenata, teorem 17.11, zaključujemo da je $Y \simeq X$. $\square$

## 5 ORDINALNI I KARDINALNI BROJEVI

- Ordinalni brojevi
- Kardinalni brojevi
- Brojevni razredi i viši kardinalni brojevi

# Ordinalni broj dobro uređenog skupa

Teorem enumeracije 18.14, omogućuje sljedeću definiciju:[15]

**Definicija 19.1**

Jedinstven segmentni skup sličan dobro uređenom skupu $(X, <)$, naziva se *ordinalni* ili *redni broj* skupa $X$ (točnije, skupa $(X, <)$).

**Napomena 19.2**

Različiti, tj. ne-slični DU skupovi, slični su jedinstvenim međusobno ne-sličnim segmentnim skupovima. S druge strane, različiti segmentni skupovi imaju različite redne tipove, pa se segmentni skupovi mogu identificirati s njihovim rednim tipovima. Stoga su, do na sličnost, DU skupovi karakterizirani svojim rednim tipom, pa se na ordinalni broj DU skupa može gledati i kao na njegov redni tip. Zato ćemo i ordinalni broj DU skupa $X$ označivati $\mathrm{t}X$ ili $\mathrm{t}(X)$.

[15] Zato se teorem 18.14 i naziva *teorem enumeracije* (vidi Vuković).

# Ordinalni brojevi prve i druge vrste

Prirodne brojeve $0, 1, 2, 3, \ldots$ smo u definiciji 3.6 definirali kao skupove $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\big\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\big\}$, ..., a to su upravo konačni segmentni skupovi, korolar 18.2. Stoga se i ordinalni brojevi konačnih DU skupova označuju arapskim brojevima $0, 1, 2, 3, \ldots$. Beskonačne ordinalne brojeve, kao i segmentne skupove kada na njih gledamo kao na ordinalne brojeve, označivat ćemo malim grčkim slovima. Skup svih konačnih ordinalnih brojeva označivat ćemo opet s $\omega$.

Svaki ordinalni broj $\alpha$ ima neposrednog sljedbenika: $\alpha^+ = \alpha \sqcup \{\alpha\}$, i svaki *konačan* ordinalni broj osim 0, ima neposrednog prethodnika. Ali nemaju svi ordinalni brojevi neposrednog prethodnika. Zato

**Definicija 19.3**

Za ordinalni broj $\alpha \neq 0$ kažemo da je *prve vrste* ako ima neposrednog prethodnika. Za ordinalni broj koji nema neposrednog prethodnika, kažemo da je *druge vrste* ili da je *granični ordinalni broj*.

# Uspoređivanje ordinalnih brojeva

**Definicija 19.4**

Za dva različita ordinalna broja $\alpha$ i $\beta$ kažemo da je $\alpha < \beta$ ako je $\alpha$ segment od $\beta$, tj. $\alpha \subset \beta$, ili ekvivalentno, $\alpha \in \beta$.

Iz teorema o usporedivosti segmentnih skupova, neposredno slijedi

**Teorem 19.5 (trihotomija za ordinalne brojeve)**

*Za ordinalne brojeve $\alpha$ i $\beta$ uvijek vrijedi ili $\alpha < \beta$, ili $\alpha = \beta$, ili $\beta < \alpha$.* $\square$

**Korolar 19.6**

*Neka su $X$ i $Y$ DU skupovi i neka su $\mathrm{t}X = \alpha$ i $\mathrm{t}Y = \beta$ njihovi ordinalni brojevi. Ako je $X \subseteq Y$ onda je $\alpha \leqslant \beta$.*

Dokaz: Kada ne bi bilo $\alpha \leqslant \beta$, bilo bi $\beta < \alpha$, pa bi $Y$ bio sličan segmentu svoga podskupa $X$, dakle i svom segmentu, što zbog korolara 17.8 nije moguće. $\square$

# Dobra uređenost skupova ordinalnih brojeva

Neposredna posljedica teorema 18.12 je

**Teorem 19.7 (o dobroj uređenosti skupova ordinalnih brojeva)**

*Svaki je skup ordinalnih brojeva dobro uređen relacijom* $<$. □

Nazovimo s $W$ klasu svih ordinalnih brojeva, tj. klasu svih segmentnih skupova. ***Je li*** $W$ ***skup ?***

Kao u teoremima 18.12 i 18.13, pokazuje se da je $W$ DU klasa, štoviše, segmentna klasa: svaki $\alpha \in W$ je segmentni skup i $\alpha = \{\xi \in W : \xi \subset \alpha\} = W[\alpha]$. Pritom $\xi \subset \alpha$ možemo zapisati i kao $\xi < \alpha$ ili kao $\xi \in \alpha$.

Primijetimo da je svaki segment klase $W$ skup — segmentni skup, tj. ordinalni broj.

# Burali-Fortijev paradoks

Dakle, za svaki ordinalni broj $\alpha$, klasa $W[\alpha]$ svih ordinalnih brojeva manjih od $\alpha$ je skup (jer je jednaka segmentnom skupu $\alpha$).
A je li klasa $W$ skup ? Nije.

**Teorem 19.8 (Burali-Fortijev paradoks, 1897)**

*Klasa $W$ svih ordinalnih brojeva je prava klasa, tj. $W$ nije skup.*

Dokaz: Kada bi klasa $W$ bila skup, bio bi to neki segmentni skup, tj. ordinalni broj, npr. $\beta$, dakle $\beta = W$. Ali, $\beta$ bi, kao ordinalni broj, bio i element skupa $W$, tj. $\beta \in W$, pa bi $W$ bio jednak svom segmentu, a to nije moguće prema korolaru 17.8. $\square$

# Transfinitni nizovi

Neka je $(A,<)$ dobro uređen skup, i neka je $\mathrm{t}(A,<) = \alpha$ njegov ordinalni broj. Prema teoremu 18.14, postoji ***jedinstven*** segmentni skup koji je sličan skupu $(A,<)$, pa je to upravo skup $W[\alpha] = \{\xi : \xi < \alpha\}$ svih ordinalnih brojeva manjih od $\alpha$ (uređen inkluzijom, odnosno relacijom produljenja).

Neka je $s\colon W[\alpha] \to A$ ***jedinstveno*** preslikavanje sličnosti (jedinstvenost slijedi iz korolara 17.6), i označimo $s(\xi) =: a_\xi$, $\xi < \alpha$.

**Korolar 19.9**

*Svaki se dobro uređen skup $(A,<)$ može zapisati kao $A = \{a_\xi : \xi < \alpha\}$, gdje je $\alpha = \mathrm{t}(A,<)$, ili, bolje, kao transfinitan niz*[16] $(a_\xi)_{\xi<\alpha}$, *odnosno $a_0, a_1, \ldots, a_\xi, \ldots, \quad \xi < \alpha$.* □

Primijetimo da su ovako definirani transfinitni nizovi strogo uzlazni, tj. za $\xi < \eta$ je $a_\xi < a_\eta$.

[16] Zapravo, termin *transfinitan* ima smisla samo kada je skup $A$ beskonačan.

# Zermelov teorem o dobrom uređenju

Kako bismo definirali kardinalne brojeve, trebat će nam već najavljen

**Teorem 19.10 (Zermelov teorem o dobrom uređenju, 1904)**

*Svaki se skup može dobro urediti.*

U dokazu ovog teorema koristit ćemo Zornovu lemu, a za čiji smo pak dokaz bili koristili Aksiom izbora. Sve su to egzistencijalni dokazi koji ne ukazuju na nikakav način da se, u ovom slučaju dobro uređenje, konstruira. Specijalno, ovaj teorem kaže da se i skup realnih brojeva može dobro urediti, ali još nikome nije uspjelo, i pitanje je hoće li ikada ikome uspjeti, zaista definirati neko konkretno dobro uređenje skupa $\mathbb{R}$.

# Dokaz Zermelovog teorema o dobrom uređenju

Kako znamo da je $\mathscr{A}$ zaista familija, tj. skup?

- Neka je $X$ neki skup a $\mathscr{A}$ familija parova $A = (Y, \propto)$ svih podskupova $Y \subseteq X$ i dobrih uređenja $\propto$ na $Y$. Familija $\mathscr{A}$ nije prazna jer joj, naprimjer, svaki jednočlan podskup od $X$ s trivijalnim (dobrim) uređenjem, pripada, kao i prazan skup $\emptyset$.

Uvedimo u $\mathscr{A}$ parcijalni uređaj relacijom produljenja (definicija 17.13): za $A_1, A_2 \in \mathscr{A}$ je $A_1 \prec A_2$ ako je $A_2$ produljenje od $A_1$, tj. $A_1$ je segment (početni komad) od $A_2$. Neka je $\mathscr{L} = \{A_\lambda : \lambda \in \Lambda\}$ lanac u $\mathscr{A}$, tj. za $\lambda \neq \mu$ je ili $A_\lambda$ produljenje od $A_\mu$ ili je $A_\mu$ produljenje od $A_\lambda$. Skup $B := \bigcup\{A_\lambda : \lambda \in \Lambda\} \subseteq X$ sadrži sve $A_\lambda$, produljenje je svakog od njih, i dobro je uređen (teorem 18.13). Stoga je $B \in \mathscr{A}$ i gornja je međa lanca $\mathscr{L}$. Dakle, svaki lanac u $\mathscr{A}$ ima gornju među pa, prema Zornovoj lemi, $\mathscr{A}$ ima barem jedan maksimalan element $(M, \ltimes)$.

Tvrdnja: $M = X$, tj. $\ltimes$ je dobro uređenje skupa $X$.

Zaista, kada bi postojao $x \in X \setminus M$ onda bi redna unija $M \sqcup \{x\}$ bio dobro uređen podskup od $X$, što se protivi maksimalnosti od $(M, \ltimes)$. $\square$

# Koliko ordinalnih brojeva pripada nekom skupu?

U nemogućnosti da u § 12 definiramo kardinalni broj kao „veličinu” nekog (beskonačnog) skupa, govorili smo o *kardinalnosti*. Za skupove $A$ i $B$ rekli smo da su *jednake kardinalnosti*, i pisali $\mathrm{k}A = \mathrm{k}B$, ako su oni ekvipotentni. Sada možemo zaista definirati kardinalne brojeve.

Neka je $A$ proizvoljan skup. Prema Zermelovom teoremu, skup $A$ se može dobro urediti, i to na više načina ako ima više od jednog elementa. Za $n$-člani skup taj broj je $n!$, ali svi su ti uređeni skupovi međusobno slični, i slični skupu $[1\,..\,n]$, pa imaju isti ordinalni broj, $n$.

Ali, za beskonačne skupove različita dobra uređenja ne moraju biti slična, tj. mogu imati različite ordinalne brojeve. Npr. skup $\mathbb{N}$ se može dobro urediti tako da su pripadni ordinalni brojevi $\omega$, $\omega + 2$, $\omega + \omega$, $\omega \cdot \omega = \omega^2$, $\omega^3 + \omega \cdot 7 + 5$, i mnogi drugi.

**Definicija 20.1**

Kažemo da skup $A$ *može primiti* ordinalni broj $\alpha$, ili da $\alpha$ *pripada* skupu $A$, ako postoji dobro uređenje skupa $A$ s ordinalnim brojem $\alpha$.

# Kardinalni broj

Primijetimo da ako se $A$ i $B$ mogu dobro urediti tako da budu slični, onda su oni ekvipotentni. Dakle, ako im pripada barem jedan zajednički ordinalni broj, onda su ekvipotentni, odnosno ako $A$ i $B$ nisu ekvipotentni, onda im ne pripada niti jedan zajednički ordinalni broj.

Svaki je ordinalni broj koji pripada skupu $A$, ekvipotentan skupu $A$.

Neka je $A$ neki skup a $\mathcal{O}(A)$ skup svih ordinalnih brojeva (= segmentnih skupova) koji pripadaju skupu $A$. Skup $\mathcal{O}(A)$ je dobro uređen, teorem 18.12, pa ima minimum, dakle najmanji segmentni skup, i on je ekvipotentan s $A$ (jer je to zapravo $A$ s nekim dobrim uređajem).

Kako znamo da je $\mathcal{O}(A)$ skup?

**Definicija 20.2**

*Kardinalni broj* skupa $A$, $\kappa A$, je najmanji ordinalni broj koji je ekvipotentan skupu $A$.

***Pokažimo da je ova definicija svrhovita***, tj. da ako su skupovi $A$ i $B$ ekvipotentni, onda su najmanji elementi skupova $\mathcal{O}(A)$ i $\mathcal{O}(B)$ jednaki.

# Ekvipotentni skupovi imaju jednake kardinalne brojeve

**Teorem 20.3**

*Ako su skupovi $A$ i $B$ ekvipotentni onda je $\mathcal{O}(A) = \mathcal{O}(B)$, pa su i najmanji elementi ovih skupova jednaki, tj. $\kappa A = \kappa B$.*

Dokaz: Neka je $(A, <)$ neko dobro uređenje skupa $A$ i neka je $\mathrm{t}(A, <) = \alpha \in \mathcal{O}(A)$. Kao segmentni skup, $\alpha = W[\alpha]$, pa skup $A$ možemo zapisati kao transfinitan niz $A = \{a_\lambda : \lambda < \alpha\}$ (korolar 19.9).
Neka je $f\colon A = \{a_\lambda : \lambda < \alpha\} \to B$ neka bijekcija.
Time je na skupu $B = \{f(a_\lambda) : \lambda < \alpha\}$ definiran i jedan dobar uređaj:

$$f(a_\lambda) \prec f(a_\mu) \overset{\text{def}}{\Leftrightarrow} \lambda < \mu$$

a preslikavanja $f\colon (A, <) \to (B, \prec)$ i $f^{-1}\colon (B, \prec) \to (A, <)$ su sličnosti.
Stoga je $\alpha = \mathrm{t}(A, <) = \mathrm{t}(B, \prec) \in \mathcal{O}(B)$, što pokazuje $\mathcal{O}(A) \subseteq \mathcal{O}(B)$.
Analogno se dokazuje obrnuta inkluzija. $\square$

NAPOMENA: Ako je $K$ konačan, npr. $n$-član skup, onda je skup $\mathcal{O}(K)$ jednočlan, pa je $\kappa(K)$ jednak ordinalnom broju skupa $[1\,..\,n]$, tj. $\kappa(K) = n$.

# Kardinalnost i kardinalni broj

**Korolar 20.4**

*Skupovi $A$ i $B$ su ekvipotentni ako i samo ako je $\kappa A = \kappa B$.*

Dokaz: $\Rightarrow$ To je upravo prethodni teorem 20.3.

$\Leftarrow$ Kardinalni broj skupa $A$ je ordinalni broj skupa $A$ uz neko dobro uređenje, pa, shvaćen kao segmentni skup, ekvipotentan je skupu $A$, tj. $A \sim \kappa A$. Dakle, $A \sim \kappa A = \kappa B \sim B$. $\square$

NAPOMENA: Ovaj korolar pokazuje da je, vjerojatno, *kardinalni broj* prava zamjena za *kardinalnost* iz definicije 12.1. Treba još samo vidjeti što je s uspoređivanjem kardinalnih brojeva.

# Uspoređivanje kardinalnih brojeva

Svaki kardinalni broj je ordinalni broj, pa se među kardinalne brojeve može uvesti uređaj ovako:

**Definicija 20.5**

Za kardinalni broj $\alpha$ kažemo da je *manji* od kardinalnog broja $\beta$, i pišemo $\alpha < \beta$, ako za $\alpha$ i $\beta$ shvaćene kao ordinalne brojeve vrijedi $\alpha < \beta$, tj. $\alpha \subset \beta$.

NAPOMENA: Ordinalni broj $\alpha$ je i kardinalni broj ako i samo ako nije ekvipotentan nekom ordinalnom broju $\lambda < \alpha$. Ali svaki ordinalni broj ima, jer je on segmentni skup, svoj kardinalni broj.

**Primjer 20.6**

$$\kappa(\omega) = \kappa(\omega + 2) = \kappa(\omega \cdot 3 + 5) = \kappa(\omega^3 + \omega \cdot 7 + 4) = \omega$$

# Kriterij za uspoređivanje kardinalnih brojeva

Kako želimo da kardinalni brojevi „vjerno" zamijene pojam kardinalnosti, treba se uvjeriti u to da i za uspoređivanje kardinalnih brojeva vrijedi isto što i za uspoređivanje kardinalnosti.

**Teorem 20.7**

*Za kardinalne brojeve $\alpha$ i $\beta$ sljedeće su tvrdnje ekvivalentne:*

(a) $\alpha \leqslant \beta$;

(b) *za svaka dva skupa $A$ i $B$ t.d. je $\kappa A = \alpha$ i $\kappa B = \beta$, za njihove kardinalnosti vrijedi $\mathrm{k}A \leqslant \mathrm{k}B$, tj. postoji injekcija $A \rightarrowtail B$;*

(c) *postoje skupovi $A$ i $B$ s $\kappa A = \alpha$ i $\kappa B = \beta$, t.d. da za njihove kardinalnosti vrijedi $\mathrm{k}A \leqslant \mathrm{k}B$, tj. da postoji injekcija $A \rightarrowtail B$.*

Dokaz:(a) $\Rightarrow$ (b) Neka su $A$ i $B$ t.d. je $\kappa A = \alpha$ i $\kappa B = \beta$. Ali $\alpha = W[\alpha]$ i $\beta = W[\beta]$ su ordinalni brojevi (segmentni skupovi) koji su ekvipotentni skupovima $A$ odnosno $B$, pa $\alpha < \beta$ znači da je $W[\alpha]$ segment (početni komad) od $W[\beta]$, a $\alpha = \beta$ znači da je $W[\alpha] = W[\beta]$, pa u oba slučaja postoji injekcija $W[\alpha] \rightarrowtail W[\beta]$, i ona inducira injekciju $A \rightarrowtail B$. $\triangle$

# Završetak dokaza

$(b) \Rightarrow (c)$ Ova implikacija je očita.

$(c) \Rightarrow (a)$ Neka su $A$ i $B$ skupovi za koje je $\kappa A = \alpha$ i $\kappa B = \beta$ t.d. je $\mathrm{k}A \leqslant \mathrm{k}B$, tj. postoji injekcija $f : A \rightarrowtail B$.
Pretpostavimo da je $\mathrm{k}A < \mathrm{k}B$, tj. da ne postoji injekcija $B \rightarrowtail A$.
Kako su $A$ i $B$ ekvipotentni segmentnim skupovima $\alpha$ odnosno $\beta$, to znači da ne postoji injekcija, dakle niti uzlazna injekcija, $\beta \rightarrowtail \alpha$, što znači da je $\beta \neq \alpha$ i da $\beta$ nije segment (početni komad) od $\alpha$, tj. $\beta \not< \alpha$. Dakle, zbog trihotomije za ordinalne brojeve, teorem 19.5, je $\alpha \leqslant \beta$. □

Zbog korolara 20.4 i prethodnog teorema, opravdano je za kardinalni broj rabiti istu oznaku k, $\mathrm{k}A$, kao i za kardinalnost.
Definicije „računskih” operacija za kardinalnosti i njihova svojstva promatrana u § 12, nepromijenjeno vrijede i za kardinalne brojeve.

# Trihotomija za kardinalne brojeve

Iz teorema 19.5 odnosno 19.7, neposredno slijede

**Teorem 20.8 (trihotomija za kardinalne brojeve)**

*Za kardinalne brojeve $\alpha$ i $\beta$ uvijek vrijedi ili $\alpha < \beta$, ili $\alpha = \beta$, ili $\beta < \alpha$.* □

**Teorem 20.9 (o dobroj uređenosti skupova kardinalnih brojeva)**

*Svaki je skup kardinalnih brojeva dobro uređen relacijom $<$.* □

# Brojevni razredi

Kardinalni broj skupa $A$ definirali smo kao najmanji element skupa $\mathcal{O}(A)$ svih ordinalnih brojeva koji pripadaju skupu $A$ (definicija 20.2), a teorem 20.3 pokazuje da ako je $\mathrm{k}A = \mathrm{k}B$ onda je $\mathcal{O}(A) = \mathcal{O}(B)$.

## Definicija 21.1

*Brojevni razred* $\mathcal{O}(\alpha)$ kardinalnog broja $\alpha$ je skup svih ordinalnih brojeva ekvipotentnih s $\alpha$.

Primijetimo da teorem 20.3 pokazuje da je $\mathcal{O}(\alpha) = \mathcal{O}(A)$ za svaki skup $A$ za koji je $\mathrm{k}A = \alpha$.

Napomena. Za svaki beskonačan kardinalni broj $\alpha$ je brojevni razred $\mathcal{O}(\alpha)$, kao skup ordinalnih brojeva, dobro uređen relacijom produljenja (teorem 18.12), i nema maksimuma.

Naime, za $\forall \xi \in \mathcal{O}(\alpha)$ je $\mathrm{k}(\underbrace{\xi + 1}_{:=\xi^+}) = \mathrm{k}(\xi)$, tj. $\xi{+}1 \in \mathcal{O}(\alpha)$, i $\xi{+}1 > \xi$.

# Skup $\mathcal{O}(\aleph_0)$ prebrojivo beskonačnih ordinalnih brojeva

Pozabavimo se najprije brojevnim razredom $\mathcal{O}(\aleph_0)$,
tj. skupom svih prebrojivo beskonačnih ordinalnih brojeva.

**Teorem 21.2**

*Za svaki prebrojiv podskup $S \subseteq \mathcal{O}(\aleph_0)$, prvi ordinalni broj koji dolazi iza svih ordinalnih brojeva iz $S$, također pripada skupu $\mathcal{O}(\aleph_0)$.*

Dokaz: Primijetimo najprije da iskaz teorema ima smisla, tj. da za svaki prebrojiv $S \subseteq \mathcal{O}(\aleph_0)$ postoji ***prvi*** ordinalni broj iza svih elemenata od $S$.
Zaista, ako skup $S$ ima najveći element, kažimo $\sigma$, onda je $\sigma + 1$ najmanji ordinalni broj koji je veći od svih elemenata iz $S$.
U tom slučaju $\sigma + 1$ je očito prebrojiv, tj. $\sigma + 1 \in \mathcal{O}(\aleph_0)$.
Pretpostavimo da skup $S$ nema najveći element.
Neka je $\beta$ neki neprebrojiv ordinalni broj.
Tada je $S = \{\alpha_n : n \in \mathbb{N}\} \subset W[\beta + 1]$, pa je odozgo omeđen,
te ima supremum, kažimo $\alpha$ (koji postoji, jer je to upravo minimum skupa onih ordinalnih brojeva koji su manji od $\beta + 1$ i veći od svih $\alpha_n$).
$\alpha$ je prvi, tj. najmanji ordinalni broj koji dolazi iza svih elemenata skupa $S$.

# Skup $\mathcal{O}(\aleph_0)$ nije prebrojiv

Tvrdnja: $W[\alpha] = \bigcup_{n\in\mathbb{N}} W[\alpha_n]$.

$\supseteq$ Za $\forall n$ je $\alpha_n < \alpha$ tj. $W[\alpha_n] \subset W[\alpha]$ pa je i $\bigcup_{n\in\mathbb{N}} W[\alpha_n] \subseteq W[\alpha]$.

$\subseteq$ Neka je $\xi \in W[\alpha]$ proizvoljan. Kako je $\alpha = \sup S$ i $S$ nema najveći element, postoji $n \in \mathbb{N}$ t.d. je $\xi < \alpha_n$, te je $\xi = W[\xi] \subseteq W[\alpha_n] \subseteq \bigcup_{n\in\mathbb{N}} W[\alpha_n]$. $\triangle$

Konačno, $W[a]$ je prebrojiva unija prebrojivih skupova, pa je i $\alpha = W[\alpha]$ prebrojiv skup, tj. $\alpha \in \mathcal{O}(\aleph_0)$. □

Neposredna posljedica je ovaj važan

**Korolar 21.3**

*Kardinalni broj skupa $\mathcal{O}(\aleph_0)$ veći je od $\aleph_0$.*

Dokaz: Kada bi skup $\mathcal{O}(\aleph_0)$ bio prebrojiv, bio bi, prema prethodnom teoremu, i prvi ordinalni broj koji je veći od svih ordinalnih brojeva iz $\mathcal{O}(\aleph_0)$, prebrojiv, dakle element od $\mathcal{O}(\aleph_0)$, pa bi on bio veći i od sebe sâmog. $\Rightarrow\Leftarrow$ □

# $\omega_1$: ordinalni broj skupa svih prebrojivih ordinalnih brojeva

**Definicija 21.4**

Ordinalni broj dobro uređenog skupa $\mathcal{O}(\aleph_0)$ označava se $\omega_1$ ili $\Omega$.

Dakle, $\omega_1 = \mathrm{t}\big(\mathcal{O}(\aleph_0)\big)$.

**Teorem 21.5**

*$\omega_1 = W[\omega_1]$, tj. $\omega_1$ je ordinalni broj DU skupa svih ordinalnih brojeva manjih od $\omega_1$, dakle, DU skupa svih prebrojivih ordinalnih brojeva, uključujući i konačne ordinalne brojeve.*

Dokaz: Svaki ordinalni broj $\alpha < \omega^2$ je oblika $\omega \cdot n + m$, $(n, m) \in \mathbb{N}_0 \times \mathbb{N}_0$, pri čemu je $\mathbb{N}_0 \times \mathbb{N}_0$ uređen leksikografski.

Tvrdnja: Redna unija $W[\omega] \sqcup \mathcal{O}(\aleph_0)$ jednaka je $W[\omega_1]$.

Zaista, definirajmo preslikavanje $f\colon W[\omega] \sqcup \mathcal{O}(\aleph_0) \to \mathcal{O}(\aleph_0)$

$$f(\alpha) = \begin{cases} \omega \cdot (n+1) + m \,, & \text{za } \alpha < \omega^2 \text{ oblika } \alpha = \omega \cdot n + m \\ \alpha & , \text{ za } \alpha \geqslant \omega^2 \end{cases}.$$

$f$ je očito preslikavanje sličnosti, pa je $\omega_1 = W[\omega_1]$. □

# $\aleph_1$

Svaki ordinalni broj $\alpha < \omega_1$ je prebrojiv, pa je $\omega_1$, kao najmanji neprebrojiv ordinalni broj, ujedno i kardinalni broj.

## Definicija 21.6

Kao kardinalni broj, $\omega_1$ se označava $\aleph_1$.
Dakle, $\aleph_1 = \mathrm{k}\big(\mathscr{O}(\aleph_0)\big) = \mathrm{k}\big(W[\omega_1]\big)$.

## Teorem 21.7

*$\aleph_1$ je prvi (najmanji) kardinalni broj veći od $\aleph_0$, tj. između $\aleph_0$ i $\aleph_1$ nema drugih kardinalnih brojeva.*

Dokaz: Neka je $\alpha < \aleph_1$. Kao ordinalni broj, $\alpha$ je manji od $\omega_1$, pa je, prema teoremu 21.5, $\alpha$ prebrojiv, tj. kao kardinalan broj je $\alpha \leqslant \aleph_0$. $\square$

## $0 < 1 < \cdots < n < \cdots < \aleph_0 < \aleph_1 < \aleph_2 < \cdots < \aleph_\xi < \cdots$

Svi ordinalni brojevi kojima je kardinalni broj jednak $\aleph_1$ čine brojevni razred $\mathscr{O}(\aleph_1)$, i, slično kao ranije, pokazuje se da je kardinalni broj skupa $\mathscr{O}(\aleph_1)$ veći od $\aleph_1$.

Ordinalni broj DU skupa $\mathscr{O}(\aleph_1)$ označuje se $\omega_2$, a kako je to i najmanji ordinalni broj koji je veći od svih elemenata skupa $\mathscr{O}(\aleph_1)$, on je ujedno i kardinalni broj, i kao takav, označuje se $\aleph_2$.

itd.

Svaki skup ordinalnih brojeva je dobro uređen, pa se time dobiva i dobro uređenje svakog skupa kardinalnih brojeva. Tako dobivamo

$$0 < 1 < \cdots < n < \cdots < \aleph_0 < \aleph_1 < \aleph_2 < \cdots < \aleph_\xi < \cdots$$

# Oznake: $\aleph_\xi$ *vs.* $\omega_\xi$

Zašto ordinalne brojeve $\omega_0 = \omega, \omega_1, \omega_2, \ldots, \omega_\xi, \ldots,$ kada na njih gledamo kao na kardinalne brojeve, označujemo $\aleph_0, \aleph_1, \aleph_2, \ldots, \aleph_\xi, \ldots$?

Jedan, vrlo jasan razlog su različita svojstva računskih operacija s ordinalnim i s kardinalnim brojevima.

**Primjer 21.8**

$$\aleph_0 \underbrace{+}_{\substack{\text{zbrajanje}\\ \text{kardinalnih brojeva}}} \aleph_0 = \aleph_0, \quad \text{dok je} \quad \omega \underbrace{+}_{\substack{\text{zbrajanje}\\ \text{ordinalnih brojeva}}} \omega = \omega \cdot 2 \neq \omega.$$