Teorija skupova

Vježbe

$\boxed{\text{Radna verzija!}}$

[23. veljače 2006.]

Vedran Čačić

Sadržaj

Dio 1

Uvod

POGLAVLJE 1

Par logičkih napomenâ

1. Implikacija

$p \rightarrow q \iff \neg p \vee q$ Implikacija nije ništa drugo nego disjunkcija (kojoj je prvi član negiran); dakle, samo u jednom slučaju je lažna: $\top \rightarrow \bot \iff \bot$. Preostale tri mogućnosti su istinite.

Negacija implikacije: $\neg(p \rightarrow q) \iff p \wedge \neg q$

Obrat i kontrapozicija: $p \rightarrow q \overset{\text{opć.}}{\not\Longleftrightarrow} q \rightarrow p \iff \neg p \rightarrow \neg q$

2. Ostalo

Jedinstvenost: $\exists! x \varphi(x) :\iff \exists x \forall y (\varphi(y) \leftrightarrow x = y)$

Poredak kvantifikatorâ je bitan: $\exists\forall \implies \forall\exists$, ali obrat općenito ne vrijedi.

Slobodne nastupe varijablî ne smijemo preimenovati, dok vezane smijemo:

- $\exists x(x \in y) \iff \exists z(z \in y) \iff y \neq \emptyset$
- to nije isto što i $\exists x(x \in z)$ (z nije prazan)
- također, $\exists x(x \in x)$ je nešto sasvim treće:
  "postoji objekt koji je element samog sebe"

Rješavanje jednadžbi možemo shvatiti kao pojednostavljivanje izraza za određeni skup: npr. $\{x \in \mathbb{R} : \frac{x-1}{x+1} \leq 0\}$ je samo kompliciranije ime za $\langle -1, 1]$.

POGLAVLJE 2

Operacije sa skupovima

1. Osnovne operacije, odnosi, zadavanje

Napomena: Za većinu matematičkih teorijâ, skupovi su sekundarni objekti. Na primjer, u realnoj analizi, primarni objekti su realni brojevi i označuju se obično malim slovima, dok su skupovi uglavnom skupovi brojeva i označuju se velikim slovima. No u teoriji skupova, skupovi su primarni objekti, i prirodno ih je označavati i malim slovima ako treba (velika slova onda možemo koristiti za skupove skupova, skupove skupova skupova, itd.).

Ako su a i b skupovi, možemo definirati nove skupove pomoću njih:

- $a \cap b := \{x : x \in a \wedge x \in b\}$ — presjek
- $a \cup b := \{x : x \in a \vee x \in b\}$ — unija
- $a \setminus b := \{x : x \in a \wedge x \notin b\}$ — razlika
- $a \triangle b := (a \cup b) \setminus (a \cap b) = (a \setminus b) \cup (b \setminus a)$ — simetrična razlika

kao i neke odnose između njih:

- $a \subseteq b :\iff \forall x(x \in a \to x \in b)$ — podskup
- Princip *ekstenzionalnosti*:
  $a = b :\iff \forall x(x \in a \leftrightarrow x \in b) \iff a \subseteq b \wedge b \subseteq a$ — jednakost (Važno: za skupove se $\in$ smatra osnovnom relacijom — pomoću nje se može definirati čak i jednakost)
- $a \subset b :\iff a \subseteq b \wedge a \neq b$ — pravi podskup

Za skupovne operacije vrijede brojni zakoni:

- Komutativnost i asocijativnost presjeka, unije, i simetrične razlike
- Idempotentnost presjeka i unije: $\star \cup \star = \star \cap \star = \star$
- Distributivnost presjeka prema uniji, i unije prema presjeku
- Distributivnost presjeka prema simetričnoj razlici — ostale distributivnosti ne vrijede općenito

Dokažite ih za DZ — ono što ne vrijedi opovrgnite kontraprimjerom!

Napomena: U teoriji skupova su skupovi skupova uobičajena stvar. Štoviše, kao što ćemo kasnije vidjeti, svi elementi skupova su zapravo skupovi.

$\mathcal{P}(a) := \{x : x \subseteq a\}$ — partitivni skup od a
Primijetimo, $x \in \mathcal{P}(a) \iff x \subseteq a$.

Zadavanje skupova:

- nabrajanjem elemenata — zgodno za konačne skupove (poput $\{\pi, e, \gamma\}$); primjenjivo i za beskonačne, ali treba osigurati dovoljno elemenata za razumijevanje strukture skupa
(npr. $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ — da, u teoriji skupova smatramo $0 \in \mathbb{N}$)
- svojstvom — vrlo općenito definiranje, čak preopćenito za neke svrhe: na taj način definirane "klase" ne moraju uopće biti skupovi (npr. $\{x : x \notin x\}$ nije skup — Russell); ipak, u slučaju "vađenja" elemenata s nekim svojstvom iz skupa, uvijek dobivamo skup (npr. $\{x : x \in \mathbb{C} \land x^2 = -1\}$ — često se piše skraćeno kao $\{x \in \mathbb{C} : x^2 = -1\}$)
- kao slika neke funkcije na nekom skupu;
na primjer, $\{x^2 : x \in \mathbb{Q}\}$ je dobro zadan skup — primijetimo da nismo morali specificirati iz kojeg su skupa ovi x^2.

2. Familije skupova. Generalizirani presjek i unija

Kao što rekosmo, skupovi skupova su uobičajena pojava u teoriji skupova. Ako je a skup čiji su elementi skupovi, vrijedi $a = \{b : b \in a\}$. Unija svih b-ova koji su u a je također tada skup, definiran s

$$\bigcup a := \bigcup_{b \in a} b := \{x : \exists b(b \in a \to x \in b)\}$$

Primijetimo, $x \in \bigcup a \iff \exists b(x \in b \in a)$.

Specijalno, ako je a dvočlani skup $a = \{r, s\}$, tada je $\bigcup a = r \cup s$ — dokažite!

Također, ako a nije prazan (sadrži bar jedan element), presjek svih elemenata od a je također skup, definiran s

$$\bigcap a := \bigcap_{b \in a} b := \{x : \forall b(b \in a \to x \in b)\}$$

Analogno, $\bigcap\{r, s\} = r \cap s$.

Po uzoru na oznaku $\bigcup_{b \in a} b$, možemo napraviti i $\bigcup_{b \in a} f(b)$, gdje je f bilo kakva skupovna funkcija (npr. $\mathcal{P}$ na odgovarajućem skupu) —

prvo napravimo skup $s := \{f(b) : b \in a\}$ (slika funkcije f na skupu a), a onda je traženi skup upravo $\bigcup s$.

Često se tada oznake sugestivno promijene: b se zove *indeks* ι, a se zove *skup indeksa* I, dok se vrijednost $f(\iota)$ općenito označava s A_ι. Skup $\{A_\iota : \iota \in I\}$ (ponekad i sama funkcija $\iota \mapsto A_\iota$ restringirana na I) tada se zove *familija skupova.* Imamo

$$x \in \bigcup_{\iota \in I} A_\iota \iff \exists \iota \in I(x \in A_\iota)$$

3. Zadaci

(1) Je li $\mathcal{P}(a) \cap \mathcal{P}(b) = \mathcal{P}(a \cap b)$?
Rj.: Jest. Za proizvoljan x, dokažimo da je $x \in \mathcal{P}(a) \cap \mathcal{P}(b) \leftrightarrow x \in \mathcal{P}(a \cap b)$. To se naravno svodi na $x \subseteq a \wedge x \subseteq b \leftrightarrow x \subseteq a \cap b$, što se lako dokaže.

(2) Je li $\mathcal{P}(a) \setminus \mathcal{P}(b) = \mathcal{P}(a \setminus b)$?
Rj.: Nije (nikada), jer $\emptyset \in \mathcal{P}(\star)$ za svaki $\star$. Dakle $\emptyset$ je element desne strane, a nije element lijeve.

(3) Je li $\mathcal{P}(a) \cup \mathcal{P}(b) = \mathcal{P}(a \cup b)$?
Rj.: Općenito nije, npr. za $a := \{1\} \wedge b := \{2\}$.
Ponekad jest, npr. kad je $a \subseteq b$.

(4) $\mathcal{P}(a) = \mathcal{P}(b) \iff a = b$ — DZ

(5) Vrijedi li $a \in b \iff \mathcal{P}(a) \in \mathcal{P}(b)$?
Rj.: Jedan smjer vrijedi: ako je $\mathcal{P}(a) \in \mathcal{P}(b)$,
to znači $\mathcal{P}(a) \subseteq b$, pa su svi elementi od $\mathcal{P}(a)$ ujedno u b.
Budući da je $a \in \mathcal{P}(a)$ (a je jedan takav), vrijedi $a \in b$.
Drugi smjer ne vrijedi: na primjer, za $a := \{1\} \wedge b := \{\{1\}\}$.

(6) $\forall a(\{\emptyset, \{\emptyset\}\} \in \mathcal{PPP}(a))$
Rj.: Znamo $\emptyset \in \mathcal{P}(\star)$, dakle specijalno $\emptyset \in \mathcal{P}(a)$. To znači $\{\emptyset\} \subseteq \mathcal{P}(a)$ (jer su svi njegovi elementi u $\mathcal{P}(a)$), odnosno $\{\emptyset\} \in \mathcal{PP}(a)$. Također iz $\emptyset \in \mathcal{P}(\star)$ za $\star := \mathcal{P}(a)$ imamo $\emptyset \in \mathcal{PP}(a)$, što zajedno s gornjim daje da su svi elementi od $\{\emptyset, \{\emptyset\}\}$ u $\mathcal{PP}(a)$. Dakle, $\{\emptyset, \{\emptyset\}\}$ je podskup od $\mathcal{PP}(a)$, odnosno element od $\mathcal{PPP}(a)$.

(7) Izračunajte $\mathcal{P}(\emptyset) \cap \mathcal{PP}(\emptyset) \cap \mathcal{PPP}(\emptyset)$.
Rj.: Budući da je prvi operand $\mathcal{P}(\emptyset) = \{\emptyset\}$, a $\emptyset$ se, znamo, nalazi i u ostalim $\mathcal{P}$-ovima, presjek je upravo $\{\emptyset\}$.

(8) Što su $\bigcap a$ i $\bigcup a$ ako je a jednočlan? Što je $\bigcup \emptyset$?
Rj.: $(\bigcup\{\star\} = \bigcap\{\star\} = \star \quad \wedge \quad \bigcup \emptyset = \emptyset)$

(9) Za proizvoljan skup a, kakvi odnosi vrijede između
a, $\bigcup \mathcal{P}(a)$ i $\mathcal{P}(\bigcup a)$?
Rj.: $a = \bigcup \mathcal{P}(a) \subseteq \mathcal{P}(\bigcup a)$.
Dokažimo prvu jednakost. Trebamo dokazati $a \subseteq \bigcup \mathcal{P}(a)$ i $\bigcup \mathcal{P}(a) \subseteq a$. Za prvu inkluziju, uzmimo proizvoljni $x \in a$.

Budući da je $a \in \mathcal{P}(a)$, dobivamo da postoji $b(\!(= a)\!) \in \mathcal{P}(a)$ takav da je $x \in b$, odnosno $x \in \bigcup \mathcal{P}(a)$.
Za drugu inkluziju, neka je $x \in \bigcup \mathcal{P}(a)$. To znači $\exists r(r \in \mathcal{P}(a) \wedge x \in r)$. No $r \in \mathcal{P}(a)$ znači $r \subseteq a$, pa $x \in r$ povlači $x \in a$.
Za $a \subseteq \mathcal{P}(\bigcup a)$, neka je $x \in a$ proizvoljan. Svaki element od x je time ujedno element od $\bigcup a$, pa je $x \subseteq \bigcup a$, odnosno $x \in \mathcal{P}(\bigcup a)$.
Inkluzija $\mathcal{P}(\bigcup a) \subseteq a$ općenito ne vrijedi, jer $\emptyset$ ne mora nužno biti element od a (npr. za $a := \emptyset$). (\!(Može se i kardinalnim argumentom.)\!)

4. Još zadataka s generaliziranim unijama i presjecima

Dokažimo distributivnost:

$$\bigcup_{i \in I} A_i \cap \bigcup_{j \in J} B_j = \bigcup_{i \in I} \bigcup_{j \in J} (A_i \cap B_j)$$

<u>*Rj.:*</u> Ako je $x \in \bigcup_{i \in I} A_i \cap \bigcup_{j \in J} B_j$, to znači $x \in \bigcup_{i \in I} A_i$ i $x \in \bigcup_{j \in J} B_j$. Ovo prvo znači da postoji $i_0 \in I$ takav da je $x \in A_{i_0}$, a ovo drugo da postoji $j_0 \in J$ sa svojstvom $x \in B_{j_0}$. To dvoje daje $x \in A_{i_0} \cap B_{j_0}$. Sad idemo unatrag: postoji $j_0 \in J$ takav da je $x \in A_{i_0} \cap B_{j_0}$, znači da je $x \in \bigcup_{j \in J} A_{i_0} \cap B_j$. Budući da to vrijedi za neki $i_0 \in I$, imamo $x \in \bigcup_{i \in I} \bigcup_{j \in J} (A_i \cap B_j)$.
Za drugi smjer, $x \in \bigcup_{i \in I} \bigcup_{j \in J} (A_i \cap B_j)$ znači da, kao gore, postoje $i_0 \in I$ i $j_0 \in J$ takvi da je $x \in A_{i_0} \cap B_{j_0}$. No sada iz $x \in A_{i_0}$ možemo zaključiti $x \in \bigcup_{i \in I} A_i$, a jednako tako iz $x \in B_{j_0}$ možemo zaključiti $x \in \bigcup_{j \in J} B_j$. To dvoje zajedno daje $x \in \bigcup_{i \in I} A_i \cap \bigcup_{j \in J} B_j$, što smo i trebali.

Vrijedi i druga (dualna) distributivnost,

$$\bigcap_{i \in I} A_i \cup \bigcap_{j \in J} B_j = \bigcap_{i \in I} \bigcap_{j \in J} (A_i \cup B_j)$$

<u>*Rj.:*</u> Za dokaz, prvo uzmimo $x \in \bigcap_{i \in I} A_i \cup \bigcap_{j \in J} B_j$. To znači $x \in \bigcap_{i \in I} A_i$ ili $x \in \bigcap_{j \in J} B_j$. Tvrdnja je simetrična zamjenom A-ova i B-ova (te I i J), pa BSOMP ovo prvo. Dakle, x je u svim A_i-ovima. No to znači da se za proizvoljni j, x nalazi i u $A_i \cup B_j$, odnosno $x \in \bigcap_{j \in J} A_i \cup B_j$ za svako $i \in I$, što smo i trebali.
Ako je x element desne strane, imamo da za sve mogućnosti $i \in I$ i $j \in J$, vrijedi $x \in A_i$ ili $x \in B_j$. Ako je x u svim A_i-ovima, imamo tvrdnju. U suprotnom, recimo $x \notin A_{i_0}$, i pogledajmo sve skupove oblika $A_{i_0} \cup B_j$ (za sve $j \in J$). x je u svima njima, a nije u A_{i_0}, dakle je u svim B_j-ovima, i opet imamo tvrdnju.

POGLAVLJE 3

Funkcije

1. Uređeni parovi i Kartezijevi produkti

Za skupove x i y, definiramo *uređen* par (x, y) kao skup $\{\{x\}, \{x, y\}\}$. Glavno svojstvo uređenih parova je:

$$(a, b) = (c, d) \iff a = c \wedge b = d$$

Dokažimo to!
Rj.: Smjer ($\Leftarrow$) je trivijalan, jednom kad primijetimo da su skupovi u potpunosti određeni svojim elementima: tvrdnju "ako je $x = x'$ i $y = y'$, tada je $\{x, y\} = \{x', y'\}$ primijenimo dva puta.
Za drugi smjer, treba više pisati. Imamo da je svaki element od (a, b) također element od (c, d). Ti elementi su $\{a\}$ i $\{a, b\}$. To što je $\{a\} \in (c, d)$ znači $\{a\} = \{c\}$ ili $\{a\} = \{c, d\}$. U prvom slučaju je $a = c$, a u drugom je $a = c = d$, dakle u svakom slučaju $a = c$. Sada iz $\{a, b\} \in (c, d)$ slično, i koristeći već dokazano $a = c$, dobijemo $b = d$.

Projekcije (x i y) se iz uređenog para (x, y) mogu dobiti pomoću skupovnih operacijâ:

$$
\begin{array}{ll}
(1) & \bigcup\bigcap(x, y) = \bigcup(\{x\} \cap \{x, y\}) = \bigcup\{x\} = x \\
(2) & \bigcap\bigcup(x, y) = \bigcap\{x, y\} = x \cap y \\
(3) & \bigcup\bigcup(x, y) = x \cup y \\
(4) & \bigcap\bigcup(x, y) \cup (\bigcup\bigcup(x, y) \setminus \bigcup\bigcap(x, y)) = \\
 & = (x \cap y) \cup ((x \cup y) \setminus x) = (y \cap x) \cup (y \setminus x) = y
\end{array}
$$

(dokažite sve skupovne jednakosti korištene u gornjem redu!)

Za skupove a i b, definiramo *Kartezijev produkt*:

$$A \times B := \{(x, y) : x \in a \wedge y \in b\}$$

Ako je $x \in a$ i $y \in b$, tada su oba u $a \cup b$. Dakle $\{x\}$ i $\{x, y\}$ su podskupovi od $a \cup b$, odnosno elementi od $\mathcal{P}(a \cup b)$. To znači da je (x, y) podskup od $\mathcal{P}(a \cup b)$, pa je element od $\mathcal{P}\mathcal{P}(a \cup b)$. Svaki uređeni par elemenata od a i b se nalazi u tom skupu, pa je Kartezijev produkt $a \times b$ podskup tog skupa: $a \times b \subseteq \mathcal{P}\mathcal{P}(a \cup b)$, odnosno

$$a \times b \in \mathcal{P}\mathcal{P}\mathcal{P}(\bigcup\{a, b\})$$

Dokažite (pogledajte bilješke iz EM1) sljedeća svojstva Kartezijevog produkta:

- Kartezijev produkt je distributivan prema uniji, presjeku i skupovnoj razlici.
- Monoton je: $a \subseteq b \wedge c \subseteq d \Longrightarrow a \times c \subseteq b \times d$.
- Prazan skup ima svojstvo nule: $a \times \emptyset = \emptyset \times a = \emptyset$.
- Dopušta kraćenje: $a \times b = a \times c$, uz $a \neq \emptyset$, povlači $b = c$. (Uputa: ako je $x \in a$ i $y \in b \setminus c$, tada je $(x, y) \in a \times b \setminus a \times c$.)

Za skup A, *(Kartezijev) kvadrat* skupa A, A^2, definira se kao Kartezijev produkt A sa samim sobom:

$$A^2 := \{(a, b); a \in A \wedge b \in A\} .$$

Kartezijev kvadrat singletona je

$$\{\star\}^2 = \{\star\} \times \{\star\} = \{(\star, \star)\} = \{\{\{\star\}, \{\star, \star\}\}\} = \{\{\{\star\}, \{\star\}\}\} = \Big\{\{\{\star\}\}\Big\}$$

Kartezijev kvadrat praznog skupa je, naravno, prazan (općenito, Kartezijev produkt praznog skupa s bilo kojim skupom je prazan). Dakle, $\emptyset$ je primjer skupa koji je jednak svom Kartezijevom kvadratu. No za dokazati da je to *jedini* takav skup, moramo imati snažniju aksiomatiku — na primjer, aksiom utemeljenosti.

Relacija između skupova A i B je podskup njihovog Kartezijevog produkta: $\rho \subseteq A \times B$. Dakle, to je skup nekih uređenih parova (x, y), gdje je $x \in A$ i $y \in B$. Ako je $(x, y) \in \rho$, još kažemo “x i y su u relaciji ρ”, i pišemo skraćeno $x \rho y$.

Binarna relacija na skupu A je podskup njegovog Kartezijevog kvadrata: $\rho \subseteq A^2$. Dakle, to je relacija između skupa i njega samog, odnosno skup nekih uređenih parova elemenata od A. Binarne relacije mogu imati mnoga specijalna svojstva, o kojima će biti više riječi kasnije.

Sada je lako precizno definirati funkciju — to je relacija između domene i kodomene, koja ima svojstvo da za svaki x iz domene postoji jedinstveni y iz kodomene koji je s njim u relaciji:

$$\big(f : D \to K\big) :\Longleftrightarrow\ f \subseteq D \times K\ \wedge\ (\forall x \in D)(\exists! y \in K)((x, y) \in f)$$

Važna posljedica toga je da u teoriji skupova obično funkciju s proširenom kodomenom smatramo istom funkcijom: to je jednostavno isti skup, samo što je jednom podskup od $D \times K$, a drugi put od $D \times K'$. Na primjer, $f = \{(1, 5), (2, 6)\}$ možemo promatrati kao funkciju s $\{1, 2\}$ u $\{5, 6\}$, no jednako tako je možemo promatrati i kao funkciju s $\{1, 2\}$ u $\{1, 2, 3, 4, 5, 6\}$, ili čak u $\mathbb{N}$.

2. Injekcije, surjekcije, bijekcije

Bitno svojstvo funkcije $f : a \to b$:

$$\forall x \in a \; \exists! f(x) \in b$$

— važno je i postojanje i jedinstvenost!

Ako je $f : a \to b$, a se zove *domena*, a b *kodomena* funkcije f. Pišemo $a =: \mathsf{dom}(f)$. Kodomena nije toliko bitna, što slijedi iz napomene na kraju prethodne točke — skupovno jedna te ista funkcija može imati različite kodomene.

Skup svih funkcijâ s a u b označavamo s b^a (pazite na redoslijed!). Alternativna oznaka je ${}^b a$ — primijetite da je u svakom slučaju domena eksponent, a kodomena baza.

Slika skupa: ako je $f : A \to B$ i $C \subseteq A$,

$$f^{\rangle}(C) := \{f(x) : x \in C\}$$

(standardna oznaka za to u "uobičajenoj" matematici je samo $f(C)$, no u teoriji skupova je sasvim moguće da je isti C ujedno i podskup i element domene, pa tada nije jasno označava li $f(C)$ vrijednost funkcije, ili sliku funkcije. Naravno, kad nema mogućnosti zabune, može se i u teoriji skupova pisati jednostavno $f(C)$.)

Slika funkcije je specijalni slučaj gornjeg:

$$\mathsf{im}(f) := f^{\rangle}(\mathsf{dom}\, f) = \{f(x) : x \in \mathsf{dom}\, f\}$$

Restrikcija funkcije: ako je $f : A \to B$ i $C \subseteq A$, $f|_C$ je funkcija s domenom C (i kodomenom B), definirana istim pravilom kao f.

DZ: dokažite: $f^{\rangle}(C) = \mathsf{im}(f|_C)$.

Praslika skupa: ako je $f : A \to B$ i $D \subseteq B$,

$$f^{\langle}(D) := \{x \in \mathsf{dom}(f) : f(x) \in D\}$$

("standardna" oznaka je $f^{-1}(D)$, no to može dovesti do zabune s oznakom za vrijednost inverza funkcije. Primijetimo da je $f^{\langle}(D)$ dobro definirano bez obzira na to je li f bijekcija.)

Primijetimo, ako je $f : a \to b$,
tada je $f^{\rangle} : \mathcal{P}(a) \to \mathcal{P}(b)$, a $f^{\langle} : \mathcal{P}(b) \to \mathcal{P}(a)$.

Za funkciju $f \in b^a$ kažemo da je

- *injekcija* ako $\forall x_{1,2} \in a \; (f(x_1) = f(x_2) \to x_1 = x_2)$
- *surjekcija* (*na* b) ako $\forall y \in b \; \exists x \in a \; (y = f(x))$
- *bijekcija* ako je injekcija i surjekcija

3. Primjeri

(1) $(n \mapsto 2n) : \mathbb{N} \to 2\mathbb{N}$ je bijekcija
(2) $\mathsf{tg} : \langle -\frac{\pi}{2}, \frac{\pi}{2} \rangle \to \mathbb{R}$ je bijekcija
(3) $\mathsf{sin} : \mathbb{R} \to [-1, 1]$ je surjekcija, ali nije injekcija
(4) $\mathsf{exp} : \mathbb{R} \to \mathbb{R}$ je injekcija, ali nije surjekcija
(5) Za svaki S, $\chi : \mathcal{P}(S) \to \{0,1\}^S$ je bijekcija (podskupu $A \subseteq S$ pridruži njegovu karakterističnu funkciju $\chi_A : S \to \{0,1\}$)

Dokažite to za domaću zadaću!

Ako je domena prazna: *jedina* funkcija s praznom domenom je upravo $\emptyset : \emptyset \to K$ (kodomena je proizvoljna, no slika joj je uvijek $\emptyset$) — ona je tada injekcija, a surjekcija je akko je $K = \emptyset$. Imamo dakle $K^\emptyset = \{\emptyset\}$ za svaki K, i specijalno $\emptyset^\emptyset = \{\emptyset\}$.

Ako je domena neprazna, a kodomena prazna: takvih funkcijâ nema! Za $D \neq \emptyset$, imamo $\emptyset^D = \emptyset$. Primijetimo bitnu razliku između ova dva slučaja!

4. Zadaci

(1) Funkcija je istodobno konstanta i bijekcija ako i samo ako su joj domena i kodomena jednočlani.
Rj.: ($\Leftarrow$) Ako je $f : \{a\} \to \{b\}$, $f(a)$ mora biti neki element od $\{b\}$, dakle mora biti $f(a) = b$. Tada je f konstanta (za sve x iz domene, $f(x) = b$), injekcija ("svi" elementi domene su jednaki), i surjekcija (za svaki element kodomene postoji original — jedini takav je b, a za njega postoji a).
($\Rightarrow$) Ako je $f : A \to B$ konstanta, to znači da postoji b iz kodomene takav da je $\forall x \in A(f(x) = b$. Kad bi domena bila prazna, taj b ne bi uopće bio pogođen, pa f ne bi bila surjekcija. Kad bi u domeni postojala bar dva elementa, recimo x_1 i x_2, bili bi različiti s istim slikama, pa f ne bi bila injekcija. Kad bi u kodomeni postojao još neki element osim b, on ne bi bio u slici (jer se svi $x \in A$ preslikaju u b), pa f ne bi bila surjekcija.
Dakle, i A i B moraju sadržavati točno jedan element.
(2) Kompozicija injekcijâ je injekcija.
Kompozicija surjekcijâ je surjekcija.
Ako znamo da je $f \circ g$ bijekcija, što možemo zaključiti o f i g? (DZ — na ovo posljednje potražite odgovor na Forumu.)
(3) Neka je $f : A \to A$ takva da je za svaki $n \in \mathbb{N}$, $f^n = \mathsf{id}_A$. Dokažite da je f bijekcija.
(f^n označava n-struku kompoziciju f sa samom sobom. id_A označava identitetu na A: funkciju iz A^A, definiranu s $x \mapsto x$.)

<u>*Rj.:*</u> Za $n = 2$, imamo $f_\circ^2 = f \circ f = \mathsf{id}_A$. To znači da je f sama sebi i lijevi i desni inverz, pa je bijekcija.
((Štoviše, iz $\mathsf{id}_A = f_\circ^3 = f \circ f \circ f = \mathsf{id}_A \circ f = f$ zaključujemo da mora biti $f = \mathsf{id}_A$.))

(4) Neka je $h \in A^A$. Dokažite: h je surjekcija akko za sve f i g iz A^A vrijedi $f \circ h = g \circ h \to f = g$.
<u>*Rj.:*</u> ($\Rightarrow$) Imamo da za svaki $a \in A$ vrijedi $f(h(a)) = g(h(a))$, odnosno za svaki $b \in \mathsf{im}\, h = A$, $f(b) = g(b)$.
($\neg \Rightarrow \neg$) Pretpostavimo da h nije surjekcija: neka je $a \in A$ neki element koji nije u slici od h, i $b := h(a)$. Naravno, $b \neq a$ jer b *jest* u slici od h. Definirajmo f kao konstantu b, a g kao funkciju koja preslikava $a \mapsto a$, a sve ostale elemente u b. Vrijedi $f \neq g$ (jer je $f(a) = b \neq a = g(a)$), ali (dokažite!) $f \circ h = f = g \circ h$.

(5) Neka je $h \in A^A$. Dokažite: h je injekcija akko za sve f i g iz A^A vrijedi $h \circ f = h \circ g \to f = g$.
(DZ — prilično analogno prethodnom zadatku.)

(6) Ako $f : A \to B$ ima desni inverz (funkciju $g : B \to A$ takvu da je $f \circ g = \mathsf{id}_B$), tada je surjekcija. (Obrat vrijedi uz pretpostavku AC!)
<u>*Rj.:*</u> Ako vrijedi $(\forall b \in B)(f(g(b)) = b)$, tada očito svaki element $b \in B$ ima original — na primjer $g(b)$.

(7) Neka je $f : A \to B$, te X i Y podskupovi od A. Tada vrijedi
- $f^\rangle(X \cup Y) = f^\rangle(X) \cup f^\rangle(Y)$
- $f^\rangle(X \cap Y) \subseteq f^\rangle(X) \cap f^\rangle(Y)$ (ali $\supseteq$ općenito nije)
- $f^\rangle(X \setminus Y) \supseteq f^\rangle(X) \setminus f^\rangle(Y)$ (ali $\subseteq$ općenito nije)

Neka je $f : A \to B$, te X i Y podskupovi od B. Tada vrijedi
- $f^\langle(X \cup Y) = f^\langle(X) \cup f^\langle(Y)$
- $f^\langle(X \cap Y) = f^\langle(X) \cap f^\langle(Y)$
- $f^\langle(X \setminus Y) = f^\langle(X) \setminus f^\langle(Y)$

(DZ — rješenja potražite u bilješkama iz MA1!)

(8)* $f^\langle$ je surjekcija akko je f injekcija, i
$f^\langle$ je injekcija akko je f surjekcija.

(9) Ako je $A \subseteq B$, tada za svaki S vrijedi $A^S \subseteq B^S$. (U teoriji skupova kodomenu ne smatramo esencijalnim dijelom funkcije: $\mathsf{sin} : \mathbb{R} \to \mathbb{R}$ i $\mathsf{sin} : \mathbb{R} \to \mathbb{R} \cup \{i\}$ smatramo jednom te istom funkcijom. Pogledajte i napomenu nakon stroge definicije funkcije.)

(10) Ako je $f : A \to B$, i $C \subseteq A$, vrijedi $C \subseteq f^\langle(f^\rangle(C))$, no jednakost ne vrijedi općenito.
<u>*Rj.:*</u> ($\subseteq$) Za proizvoljni $c \in C$ i $d := f(c)$, vrijedi $d \in f^\rangle(C)$, pa c ima svojstvo da se njegova slika nalazi u $f^\rangle(C)$. Dakle $c \in f^\langle(f^\rangle(C))$.

($\not\supseteq$) Za $\mathsf{sin} : \mathbb{R} \to \mathbb{R}$, i $C := [-\frac{\pi}{2}, \frac{\pi}{2}]$, imamo $\mathsf{sin}^{\rangle}(C) = [-1, 1]$, a $\mathsf{sin}^{\langle}([-1, 1]) = \mathbb{R} \supset C$.

(11) Ako je $f : A \to B$, te $C \subseteq A \wedge D \subseteq B$, tada $f^{\rangle}(C) \subseteq D \iff C \subseteq f^{\langle}(D)$.
<u>*Rj.:*</u> Obje tvrdnje znače $(\forall x \in C)(f(x) \in D)$.

Dio 2

Kardinalni i ordinalni brojevi

POGLAVLJE 4

Beskonačna kombinatorika

1. Ekvipotentni skupovi

Možemo reći da je teorija skupova nastala kada je Cantor, našavši način kako brojiti beskonačne skupove, učinio beskonačnost predmetom matematički strogog proučavanja. Naime, brojenje je uspostavljanje bijekcije s nekim unaprijed poznatim skupom (*brojem*). Obično koristimo konačne brojeve, za prebrajanje konačnih skupova. Na primjer, konačan broj 2 možemo definirati kao skup $\{\emptyset, \{\emptyset\}\}$, i onda za (npr.) skup orijentacijâ na nekom pravcu možemo reći da ima 2 elementa, jer je jednostavno uspostaviti bijekciju između skupa tih orijentacijâ i fiksiranog (dogovorenog) broja 2.

No za prebrajanje beskonačnih skupova, trebaju nam beskonačni brojevi. Na primjer, beskonačan broj $\aleph_0$ možemo definirati kao skup $\mathbb{N}$, i tada za (npr.) skup svih riječî sastavljenih samo od slova a možemo reći da ima $\aleph_0$ elemenata, jer je jednostavno uspostaviti bijekciju između skupa takvih riječî i upravo dogovorenog broja $\aleph_0$ (naravno, svakoj riječi pridružimo njenu duljinu).

To ćemo u ovom dijelu i činiti: prebrajati beskonačne skupove (uspostavljati bijekcije s nekim drugim beskonačnim skupovima), pokušati definirati brojeve (tzv. *kardinalne brojeve*) koji nam za to mogu služiti, definirati operacije na tim brojevima, i proučavati njihova svojstva.

Pri tome treba imati na umu osnovno svojstvo beskonačnih skupova:

> Skup je beskonačan akko postoji bijekcija
> između njega i nekog njegovog pravog podskupa.

Dakle, skup može imati jednako mnogo elemenata kao i njegov pravi podskup. Štoviše, to upravo karakterizira beskonačne skupove. Na primjer, $\aleph_0$ je beskonačan (odnosno skup $\mathbb{N}$ je beskonačan) jer postoji njegov pravi podskup $\mathbb{N}_+ := \mathbb{N} \setminus \{0\}$, koji također ima $\aleph_0$ elemenata: bijekcija je $n \mapsto n - 1$.
S druge strane, gore spomenuti broj 2 (odnosno skup $\{\emptyset, \{\emptyset\}\}$) je konačan, jer svaki njegov pravi podskup ima strogo manje elemenata: $\{\emptyset\}$ i $\{\{\emptyset\}\}$ imaju po 1 element, dok $\emptyset$ ima 0 elemenata.

Formalizirajmo to:

Za dva skupa kažemo da su *ekvipotentni* ako postoji bijekcija s jednog na drugi:

$$A \sim B :\iff (\exists f \in B^A)(f \text{ je bijekcija})$$

Za skup kažemo da je *prebrojiv* (ili *strogo prebrojiv*) ako je ekvipotentan s $\mathbb{N}$ (tj. ako ima $\aleph_0$ elemenata).

Za skup kažemo da je *najviše prebrojiv* ako je konačan ili prebrojiv. Inače (dakle ako je beskonačan i nije prebrojiv) kažemo da je *neprebrojiv.*

Ako je $f : A \to B$ injekcija, tada je $f : A \to \operatorname{im} f$ bijekcija (surjektivnost smo postigli proglasivši sliku kodomenom). To znači da je $\operatorname{dom} f \sim \operatorname{im} f$, kad god je f injekcija.

2. Primjeri

Skup nepozitivnih cijelih brojeva je prebrojiv.
($n \mapsto -n$ je bijekcija između njih.)

Skup neparnih prirodnih brojeva je prebrojiv.
($n \mapsto 2n + 1$ je tražena bijekcija.)

$\mathbb{R} \sim \mathbb{R}^+$ (exp je injekcija na $\mathbb{R}$, čija je slika $\mathbb{R}^+$.)

$\mathbb{R}^2 \sim \mathbb{C}$ ($(x, y) \mapsto x + iy$ je bijekcija.)

Svaka dva segmenta (ili otvoreni, ili poluotvoreni, ili zatvoreni intervali) u $\mathbb{R}$ su ekvipotentni. (Afina funkcija je bijekcija.)

⦅(Zapravo, možemo reći "svi segmenti u $\mathbb{R}$ su ekvipotentni", jer ekvipotentnost ima svojstva relacije ekvivalencije: refleksivnost, simetričnost i tranzitivnost.)⦆

Sve kružnice u ravnini su ekvipotentne.
(DZ – traži se prikladno odabrana kompozicija translacije i homotetije.)

Da bismo rješavali kompliciranije zadatke, treba nam sljedeći pojam:

> Za skupove A i B, kažemo da je A *(kardinalno) ispred* B, i pišemo $A \lesssim B$, ako postoji injekcija s A u B, odnosno ako je A ekvipotentan nekom podskupu od B (dokažite da je to dvoje ekvivalentno).

kao i sljedeći teorem:

(Cantor–Bernstein) Ako je A kardinalno ispred B,
i B kardinalno ispred A, tada su A i B ekvipotentni:

$$A \lesssim B \wedge B \lesssim A \Longrightarrow A \sim B$$

Sada možemo lako dokazati i tvrdnje poput:

$[0,1] \sim \langle 0,1\rangle$
<u>*Rj.:*</u> Po Cantor–Bernsteinovom teoremu, dovoljno je naći injekcije u oba smjera. U tu svrhu mogu poslužiti $f : [0,1] \to \langle 0,1\rangle; x \mapsto (x+1)/3$, i $g : \langle 0,1\rangle \to [0,1]; x \mapsto x$ (ovo posljednje pokazuje da je podskup nekog skupa uvijek kardinalno ispred njega).

Ako je $A \subseteq B \subseteq C$ i $A \sim C$, tada je i $B \sim C$
(tj. sva tri skupa su ekvipotentni).
<u>*Rj.:*</u> Označimo s f bijekciju između A i C.
Tada su $\mathsf{id}_B : B \to C$ i $f^{-1} : C \to B$ tražene injekcije.

$\langle 0,1\rangle \sim [0,1\rangle \sim \langle 0,1] \sim [0,1]$
<u>*Rj.:*</u> Direktno iz prethodnog.
Pokušajte direktno konstruirati potrebne bijekcije.

Svi netrivijalni (s različitim krajevima) ograničeni intervali u $\mathbb{R}$ su ekvipotentni.
<u>*Rj.:*</u> Svaki je, afinom funkcijom, ekvipotentan odgovarajućem intervalu od 0 do 1.

$\mathbb{R} \sim \langle -\frac{\pi}{2}, \frac{\pi}{2}\rangle$ ($\mathsf{arc\,tg}$ je bijekcija)

Svaki interval (s bar dvije točke) je ekvipotentan s $\mathbb{R}$.
<u>*Rj.:*</u> Ako interval I sadrži bar dvije točke a i b, tada sadrži i cijeli podinterval $\langle a,b\rangle$, koji je afinom funkcijom ekvipotentan s $\langle -\frac{\pi}{2}, \frac{\pi}{2}\rangle$, a time i s cijelim $\mathbb{R}$. Inkluzija $\langle a,b\rangle \subseteq I \subseteq \mathbb{R}$ sada daje tvrdnju.

Svi intervali (s bar po 2 točke) u $\mathbb{R}$ su ekvipotentni.
<u>*Rj.:*</u> Direktno iz tranzitivnosti ekvipotentnosti.

Kardinalni broj skupa $\mathbb{R}$ zovemo *kontinuum*, i označavamo s $\mathfrak{c}$. Dakle, gornja tvrdnja kaže da svi netrivijalni intervali u $\mathbb{R}$ imaju kontinuum elemenata.

$\mathbb{N}^2$ je prebrojiv. Općenitije, $\mathbb{N}^n$ je prebrojiv za svaki $n \in \mathbb{N}$ od 1 nadalje.
<u>*Rj.:*</u> $f : \mathbb{N}^n \to \mathbb{N}; (i_1, i_2, \ldots, i_n) \mapsto 2^{i_1} 3^{i_2} \cdot \ldots \cdot {p_n}^{i_n}$ (s p_k je označen k-ti prosti broj po veličini) je jedna injekcija. $g : \mathbb{N} \to \mathbb{N}^n; k \mapsto (k, k, \ldots, k)$ je druga.

$\mathbb{N}^* := \bigcup_{n\in\mathbb{N}} \mathbb{N}^n$ je prebrojiv.
<u>*Rj.:*</u> $f : \mathbb{N}^* \to \mathbb{N}; (i_1, i_2, \ldots, i_n) \mapsto 2^{i_1+1} 3^{i_2+1} \cdot \ldots \cdot {p_n}^{i_n+1}$ je jedna injekcija. $g : \mathbb{N} \to \mathbb{N}^*; k \mapsto (k)$ je druga.

Štoviše, A^* je prebrojiv za svaki prebrojivi A — dokažite to!

$\mathbb{Z}$ je prebrojiv.
Rj.: Budući da je $\mathbb{N} \subset \mathbb{Z}$ (dakle i $\mathbb{N} \lesssim \mathbb{Z}$), sve što nam treba je injekcija sa $\mathbb{Z}$ u neki prebrojivi skup. Lako se provjeri da je $m \mapsto (2+\mathsf{sgn}\, m, |m|)$ injekcija sa $\mathbb{Z}$ u $\mathbb{N}^2$.

$\mathbb{Q}$ je prebrojiv.
Rj.: Kao gore, dovoljno je primijetiti da je $p/q \mapsto (p, q)$, gdje su p i q relativno prosti, injekcija s $\mathbb{Q}$ u $\mathbb{Z} \times \mathbb{N}$.

Naravno, $\mathbb{Z} \times \mathbb{N}$ je prebrojiv, što možemo opet dokazati metodom dvije injekcije, no možda to možemo i direktno, računajući s $\aleph_0$ kao i s ostalim brojevima? Pokazuje se da možemo, i time ćemo se sada baviti.

3. Računanje s kardinalnim brojevima

Iako ne znamo strogo što su kardinalni brojevi, znamo puno o njima. To su neki objekti (nesumnjivo skupovi) pridruženi skupovima, koji govore koliko elemenata oni imaju. Preciznije, kad skupu A pridružimo njegov kardinalni broj κ (u oznaci $\kappa = \mathsf{card}\, A$), time želimo reći "Skup A ima κ elemenata". Pri tome κ može biti konačan, poput

$$0 = \mathsf{card}\, \emptyset$$

$$1 = \mathsf{card}\{0\}$$

$$2 = \mathsf{card}\{0, 1\}$$

$$\vdots$$

— ili može biti beskonačan, poput $\aleph_0 = \mathsf{card}\, \mathbb{N}$ ili $\mathfrak{c} = \mathsf{card}\, \mathbb{R}$.

Kardinalne brojeve možemo uspoređivati, i računati s njima — za dva kardinalna broja $\kappa = \mathsf{card}\, A$ i $\mu = \mathsf{card}\, B$:

- kažemo da su jednaki, ako su skupovi A i B ekvipotentni ($\kappa = \mu :\iff A \sim B$).
- kažemo da je κ manji ili jednak μ ako je skup A kardinalno prije B ($\kappa \leq \mu :\iff A \lesssim B$).
- kažemo da je κ strogo manji od μ ako je A kardinalno prije B, ali nije ekvipotentan s njim ($\kappa < \mu :\iff A \lesssim B \wedge A \not\sim B$).
- definiramo njihov zbroj kao kardinalni broj unije A i B, pod pretpostavkom da su A i B disjunktni ($\kappa + \mu := \mathsf{card}(A \dot\cup B)$).
- definiramo njihov produkt kao kardinalni broj Kartezijevog produkta skupova A i B ($\kappa \cdot \mu := \mathsf{card}(A \times B)$).
- definiramo potenciju s bazom κ i eksponentom μ kao broj funkcijâ s B u A ($\kappa^\mu := \mathsf{card}\, A^B$).

Samo jedna mala napomena u vezi zbroja: što ako A i B *nisu* disjunktni? Izlazi da se uvijek mogu naći skupovi s istim kardinalnim brojevima, koji *jesu* disjunktni — specijalno, skupovi $A \times \{0\} \sim A$ i $B \times \{1\} \sim B$ su takvi. Onda se $\kappa + \mu$ definira kao kardinalni broj *njihove* unije.

Gornji odlomak, i definicija množenja kardinalnih brojeva, daju nam

$$\kappa \cdot 1 = \mathsf{card}\, A \cdot \mathsf{card}\{0\} = \mathsf{card}(A \times \{0\}) = \mathsf{card}\, A = \kappa\ ,$$

odnosno 1 (kao kardinalni broj jednočlanih skupova) je neutralni element za množenje kardinalnih brojeva. Jednako tako, 0 je neutralni element za zbrajanje ($\emptyset$ je disjunktan sa svakim skupom). Također, vrijede i mnogi drugi zakoni: asocijativnost i komutativnost zbrajanja i množenja, distributivnost množenja prema zbrajanju, kao i svojstvo nule: $\kappa \cdot 0 = 0$. Također, za potenciranje vrijedi:

$$\kappa^{\mu_1+\mu_2} = \kappa^{\mu_1} \cdot \kappa^{\mu_2}$$

$$(\kappa^{\mu_1})^{\mu_2} = \kappa^{\mu_1 \cdot \mu_2}$$

$$(\kappa_1 \cdot \kappa_2)^{\mu} = {\kappa_1}^{\mu} \cdot {\kappa_2}^{\mu}$$

$$\kappa_1 \le \kappa_2 \Longrightarrow {\kappa_1}^{\mu} \le {\kappa_2}^{\mu}$$

$$\mu_1 \le \mu_2 \wedge \kappa \ne 0 \Longrightarrow \kappa^{\mu_1} \le \kappa^{\mu_2}$$

(za dokaz vidjeti bilješke iz kombinatorike — "kombinatorni dokazi" obično prolaze i u beskonačnim slučajevima)

Dokažimo samo zadnju tvrdnju, za ilustraciju zašto nam treba pretpostavka $\kappa \ne 0$: neka je $\kappa = \mathsf{card}\, A$, $\mu_1 = \mathsf{card}\, B$ i $\mu_2 = \mathsf{card}\, C$. Imamo pretpostavku $A \not\sim \emptyset$ (što zapravo znači da je A neprazan), te da je $\mathsf{card}\, B \le \mathsf{card}\, C$, što znači da imamo injekciju $f : B \to C$. Sliku od f označimo s D — to je podskup od C ekvipotentan s B.

Trebamo dokazati da je $\mathsf{card}\, A^B \le \mathsf{card}\, A^C$, odnosno naći neku injekciju s A^B u A^C. Ako uzmemo neku funkciju iz A^B (dakle $g : B \to A$), njoj trebamo (injektivno) pridružiti neku funkciju s C u A. Naravno, budući da je f bijekcija između B i D, lako je vidjeti da možemo pridružiti $g \mapsto g' := g \circ f^{-1}$, funkciju s D u A, i to je injektivno pridruživanje. No kako proširiti g' na preostale elemente iz $C \setminus D$, ako ih ima? Budući da je A neprazan, postoji neki $a \in A$. Njega možemo pridružiti svim ostalim elementima iz C, i na taj način dobiti funkciju iz A^C, koju možemo pridružiti funkciji g.

Štoviše, ne samo da dokaz ne prolazi, nego ni tvrdnja ne vrijedi općenito za $\kappa = 0$: na primjer, $0 \le 2$, ali $1 = 0^0 \not\le 0^2 = 0$. No u svim ostalim slučajevima, isključujući $0^0 = 1$, potenciranje je monotona operacija.

I ostale operacije su monotone:

$$\kappa_1 \le \kappa_2 \Longrightarrow \kappa_1 + \mu \le \kappa_2 + \mu \wedge \kappa_1 \cdot \mu \le \kappa_2 \cdot \mu$$

— no treba napomenuti da *nisu strogo monotone*: na primjer, $1 < 2$, ali $\aleph_0 + 1 = \aleph_0 = \aleph_0 + 2$ (dokažite!).

Monotonost, zajedno s dosad dokazanim svojstvima, kao i važnom vezom između $\aleph_0$ i $\mathfrak{c}$, koju ćemo upravo dokazati, omogućit će nam brojne korisne zaključke o kardinalnim brojevima.

Dokažimo: $\mathfrak{c} = 2^{\aleph_0}$.

Dokaz. Na lijevoj strani je $\mathsf{card}\,\mathbb{R}$, a na desnoj je $\mathsf{card}(\{0,1\}^{\mathbb{N}})$, za što smo prije vidjeli da je jednako $\mathsf{card}\,\mathcal{P}(\mathbb{N})$ (općenito, kardinalni broj partitivnog skupa nekog prebrojivog skupa). Trebamo konstruirati dvije injekcije:

Ako realnom broju x pridružimo skup svih racionalnih brojeva koji su manji od njega (dakle, $f(x) := \mathbb{Q} \cap \langle -\infty, x\rangle$), to će biti preslikavanje $f : \mathbb{R} \to \mathcal{P}(\mathbb{Q})$. Također će biti injektivno: ako su x i y dva različita realna broja (BSOMP $x < y$), tada postoji racionalan broj q takav da je $x < q < y$. Tada će biti $q \in f(y)$, ali $q \notin f(x)$, dakle bit će $f(x) \neq f(y)$. To znači da je f injekcija, odnosno da je $\mathfrak{c} = \mathsf{card}\,\mathbb{R} \leq \mathsf{card}\,\mathcal{P}(\mathbb{Q}) = 2^{\aleph_0}$.

S druge strane, ako podskupu $A \subseteq \mathbb{N}$ pridružimo realan broj $g(A) := \sum_{n\in A} 3^{-n}$ (taj red s pozitivnim članovima konvergira, jer je majoriran geometrijskim redom s kvocijentom $\frac{1}{3}$), to je također injekcija: ako su A i B dva različita podskupa od $\mathbb{N}$, tada s c označimo najmanji prirodni broj koji jest u jednom od njih, ali nije u drugom. Dakle, $c := \min(A \triangle B)$, i BSOMP $c \in A \setminus B$. Sada se lako vidi, koristeći činjenicu da se A i B podudaraju na $0, 1, 2, \ldots, c-1$, da je $g(A) > g(B)$, dakle g je injekcija, odnosno $\mathfrak{c} = \mathsf{card}\,\mathbb{R} \geq \mathsf{card}\,\mathcal{P}(\mathbb{N}) = 2^{\aleph_0}$. □

Sada možemo dokazati brojne jednakosti među kardinalnim brojevima:

$1 + 1 = 2$
<u>Rj.:</u> $1 = \mathsf{card}\{0\}$, što znači da nam trebaju dvije disjunktne kopije od $\{0\}$, na primjer $\{0\} \times \{0\} = \{(0,0)\}$ i $\{0\} \times \{1\} = \{(0,1)\}$. Njihova unija je $\{(0,0),(0,1)\}$, a taj skup je trivijalno ekvipotentan s $\{0,1\}$ ($x \mapsto (0,x)$ je bijekcija između njih).

${\aleph_0}^2 = \aleph_0$
<u>Rj.:</u> Direktno iz $\mathbb{N}^2 \sim \mathbb{N}$, što smo dokazali. Ili: injekcija $(x,y) \mapsto 2^x \cdot 3^y$ nam daje ${\aleph_0}^2 \leq \aleph_0$, a također imamo $\aleph_0 = \aleph_0 \cdot 1 \leq \aleph_0 \cdot \aleph_0 = {\aleph_0}^2$ (primijetite kako smo iskoristili monotonost množenja: iz $1 \leq \aleph_0$ množenjem s $\aleph_0$ slijedi nejednakost koja nam treba).

$\aleph_0 + \aleph_0 = \aleph_0$
<u>Rj.:</u> Po distributivnosti, $\aleph_0 + \aleph_0 = \aleph_0 \cdot 1 + \aleph_0 \cdot 1 = \aleph_0 \cdot (1+1) = \aleph_0 \cdot 2$.

Dakle, treba dokazati $\aleph_0 \cdot 2 = \aleph_0$. No to slijedi iz $1 \leq 2 \leq \aleph_0$ množenjem s $\aleph_0$: dobijemo $\aleph_0 \leq 2 \cdot \aleph_0 \leq \aleph_0 \cdot \aleph_0 = \aleph_0$.

$\mathfrak{c}^{\aleph_0} = \mathfrak{c}$ — odnosno, svih realnih (ili kompleksnih, ili nad nekim intervalom, itd.) nizova ima kontinuum)
Rj.: Znamo da je $\mathfrak{c} = 2^{\aleph_0}$. Dignimo to na $\aleph_0$:
$\mathfrak{c}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} = \mathfrak{c}$.

Za svaki kardinalni broj κ između 2 i $\mathfrak{c}$, vrijedi $\kappa^{\aleph_0} = \mathfrak{c}$
(odnosno, ako skup S ima bar 2 elementa, a najviše kontinuum elemenata, tada nizova nad S ima kontinuum).
Specijalno, ${\aleph_0}^{\aleph_0} = \mathfrak{c}$.
Rj.: Direktno iz prethodnog zadatka: $2 \leq \kappa \leq \mathfrak{c}$ dignemo na $\aleph_0$, i iskoristimo monotonost potenciranja za nenul-baze.

$\mathfrak{c}^2 = \mathfrak{c}$ (kompleksnih brojeva ima kontinuum)
Rj.: Imamo $\mathfrak{c}^2 = (2^{\aleph_0})^2 = 2^{\aleph_0 \cdot 2} = 2^{\aleph_0}$

$\mathfrak{c}^{\mathfrak{c}} = 2^{\mathfrak{c}}$ (funkcijâ s $\mathbb{R}$ u $\mathbb{R}$ ima koliko i podskupova od $\mathbb{R}$)
Rj.: Imamo $2 \leq \mathfrak{c} \leq 2^{\mathfrak{c}}$ (zadnja nejednakost je posljedica Cantorovog teorema). Dignuvši to na $\mathfrak{c}$, dobijemo $2^{\mathfrak{c}} \leq \mathfrak{c}^{\mathfrak{c}} \leq (2^{\mathfrak{c}})^{\mathfrak{c}} = 2^{\mathfrak{c} \cdot \mathfrak{c}} = 2^{\mathfrak{c}^2} 2^{\mathfrak{c}}$.

Još neki rezultati operacijâ s kardinalnim brojevima, za DZ:

$$2^2 = 2 \cdot 2 = 2 + 2 = 4$$
$$\mathfrak{c} \cdot 2 = \mathfrak{c} \cdot \aleph_0 = \mathfrak{c}$$
$$\mathfrak{c} + \aleph_0 = \mathfrak{c}$$
$${\aleph_0}^{\mathfrak{c}} = 2^{\mathfrak{c}}$$

4. Kardinalni brojevi još nekih skupova

Dokažimo: Svaki beskonačan podskup od $\mathbb{N}$ je prebrojiv.

Dokaz. Neka je $S \subseteq \mathbb{N}$ beskonačan. Funkciju $f : \mathbb{N} \to S$ definiramo totalnom indukcijom:

$$f(n) := \min(S \setminus \{f(0), f(1), \ldots, f(n-1)\})$$

(specijalno, $f(0) = \min S$). Budući da je S beskonačan, u svakom koraku će još ostati nepridruženih elemenata od S, a budući da je $S \subseteq \mathbb{N}$, od svih njih će postojati najmanji.

Da je f injekcija, vidi se ovako: ako su i i j različiti prirodni brojevi, BSOMP $i < j$. No to znači da je

$$f(j) = \min(S \setminus \{f(0), \ldots, f(i), \ldots, f(j-1)\}) ,$$

odnosno, $f(i)$ je isključen prilikom odabira vrijednosti za $f(j)$. To znači da je $f(i) \neq f(j)$.

Surjektivnost od f se vidi tako da se (matematičkom indukcijom) pokaže da je svaki $n \in S$ već među $f(0)$, $f(1)$,..., $f(n)$. $\square$

$\mathsf{card}\,\mathbb{P} = \aleph_0$
Rj.: Direktna posljedica prethodno dokazanog.

$\mathsf{card}\,\mathbb{A} = \aleph_0$
Rj.:
($\mathbb{A}$ označava skup svih (realnih) algebarskih brojeva, odnosno svih realnih brojeva koji su nultočke polinomâ s cjelobrojnim koeficijentima.)

Jedna nejednakost je očita: budući da je svaki racionalni broj algebarski (m/n je nultočka od $n \cdot x - m$), imamo $\aleph_0 = \mathsf{card}\,\mathbb{Q} \leq \mathsf{card}\,\mathbb{A}$.
Za drugu nejednakost, treba nam injekcija s $\mathbb{A}$ u neki prebrojivi skup. Uzmimo $\mathbb{N}^*$, za koji znamo da je prebrojiv, i realizirajmo preslikavanje ovako:
uzmimo proizvoljni $x \in \mathbb{A}$. Znamo da je x nultočka nekog polinoma s cjelobrojnim koeficijentima $p(x) = a_n x^n + \ldots + a_0$. Taj polinom, osim x, može imati i druge realne nultočke: budući da ih ima konačno mnogo, možemo ih poredati po veličini. Neka je x m-ta od njih. Dakle, broju x možemo pridružiti $(2n+3)$-torku

$$(m, |a_n|, 1 + \mathsf{sgn}\,a_n, |a_{n-1}|, 1 + \mathsf{sgn}\,a_{n-1}, \ldots, |a_0|, 1 + \mathsf{sgn}\,a_0) \in \mathbb{N}^*$$

koja ga na jednoznačan način određuje — jedini problem je što to možemo učiniti na više načina — jedan algebarski broj je nultočka mnogih polinomâ. Ipak, kao što ćemo kasnije vidjeti, skup $\mathbb{N}^*$ ima dobro svojstvo da se među svim reprezentacijama gornjeg oblika može odabrati *najmanja* s obzirom na neki uređaj, pa tako imamo pridruživanje. Da nema tog dobrog svojstva, također bismo mogli odabrati po jednu reprezentaciju za svaki algebarski broj, ali bi to u općem slučaju zahtijevalo korištenje aksioma izbora.

(DZ: dokažite, na sličan način, da je $\mathbb{Q}[x]$ — skup polinoma u jednoj varijabli s racionalnim koeficijentima — prebrojiv.)

Svih poligona u ravnini, s vrhovima iz $\mathbb{Q}^2$, ima prebrojivo mnogo.
Rj.: Kao i gore, možemo vidjeti da je $\mathbb{Q}^2$ ne samo prebrojiv, već jednom kad imamo konkretnu bijekciju $q : \mathbb{Q}^2 \leftrightarrow \mathbb{N}$, možemo točke iz $\mathbb{Q}^2$ *urediti* po vrijednostima funkcije q (više o uređajima u sljedećem poglavlju). Budući da su vrijednosti od f prirodni brojevi, moguće je za svaki poligon naći njegov "prvi" vrh — preciznije, onaj kojem je vrijednost funkcije q najmanja.
Jednom kad to imamo, lako je konstruirati injekciju sa skupa koji promatramo, u $\mathbb{Q}^*$: svakom poligonu P nađemo prvi vrh (x_1, y_1), i krećući se od njega u pozitivnom smjeru pišemo redom koordinate vrhova:

$$P \mapsto (x_1, y_1, x_2, y_2, \ldots, x_n, y_n) \in \mathbb{Q}^* .$$

Drugu injekciju je vrlo jednostavno konstruirati: prirodnom broju n pridružimo trokut s vrhovima $(0,0)$, $(1,0)$ i $(0,n)$.

Svih intervalâ (otvorenih, poluotvorenih, poluzatvorenih i zatvorenih) u $\mathbb{R}$, *s racionalnim krajevima*, ima prebrojivo mnogo.
Rj.: Označimo skup svih tih intervalâ sa $\mathcal{I}$. Injekciju sa $\mathcal{I}$ u prebrojivi skup možemo konstruirati na primjer ovako (po slučajevima):

$$f : \mathcal{I} \to \mathbb{Q}^3$$
$$f(\langle a,b\rangle) := (1,a,b)$$
$$f(\langle a,b]) := (2,a,b)$$
$$f([a,b]) := (3,a,b)$$
$$f([a,b\rangle) := (4,a,b)$$

Vidimo da vrijednost funkcije f ovisi i o tipu intervalâ, i o njegovim krajevima. Budući da različiti intervali imaju ili različit tip, ili različite krajeve (kažemo da je interval *jednoznačno određen* svojim tipom i krajevima), vidimo da je f injekcija.
Druga injekcija je na primjer $g : \mathbb{Q} \to \mathcal{I}\ ;\ g(r) := [0,r]$.

DZ: dokažite da *svih* intervalâ u $\mathbb{R}$ (bez ograničenja na racionalnost krajeva), ima kontinuum.

Konačnih podskupova od $\mathbb{N}$ ima prebrojivo mnogo.
Rj.: Svaki konačni podskup $X \subset \mathbb{N}$ možemo urediti po veličini: recimo $X = \{a_1,\dots,a_k\}$, gdje je $a_1 < a_2 < \ldots < a_k$. Ako sada pridružimo $X \mapsto (a_1,\dots,a_k)$, vidimo da smo dobili injekciju s našeg skupa (možemo ga označiti s $\mathcal{P}_{kon}(\mathbb{N})$) u prebrojiv skup $\mathbb{N}^*$.
S druge strane, $g : \mathbb{N} \to \mathcal{P}_{kon}(\mathbb{N})\ ;\ g(n) := \{n\}$ je injekcija.

Beskonačnih podskupova od $\mathbb{N}$ (zapravo od bilo kojeg prebrojivog skupa) ima kontinuum.
Rj.: Skup svih beskonačnih podskupova od $\mathbb{N}$ označimo s $\mathcal{P}_{\neg kon}(\mathbb{N})$. Dokazat ćemo da je taj skup ekvipotentan s $\mathcal{P}(\mathbf{N})$, gdje je $\mathbf{N} = \mathbb{N} \setminus \{0\}$. Jedna injekcija je $f : \mathcal{P}_{\neg kon}(\mathbb{N}) \to \mathcal{P}(\mathbf{N})\ ;\ A \mapsto \{x+1\,;\,x \in A\}$ (jednostavno skup translatiramo za 1 u desno). Ako smo krenuli od (beskonačnog) podskupa od $\mathbb{N}$, dobit ćemo podskup od $\mathbf{N}$, i to je injekcija (jer je $x \mapsto x+1$ injekcija).
Druga injekcija je zanimljivija:

$$g : \mathcal{P}(\mathbf{N}) \to P_{\neg kon}(\mathbb{N})\ ;\ A \mapsto \begin{cases} A & , A \text{ beskonačan} \\ \mathbb{N} \setminus A & , A \text{ konačan} \end{cases} .$$

Njene vrijednosti su očito sve beskonačni podskupovi od $\mathbb{N}$, no kako znamo da je injekcija? Pretpostavimo $g(A) = g(B)$, za neke A i B podskupove od $\mathbf{N}$. Ako su A i B beskonačni, to direktno znači da je $A = g(A) = g(B) = B$. Ako su pak oba konačni, iz $A = \mathbb{N} \setminus g(A) = \mathbb{N} \setminus g(B) = B$ vidimo da je $A = B$.

No što ako je jedan konačan, a drugi beskonačan (BSOMP A konačan, B beskonačan)? Tada se lako vidi $0 \in \mathbb{N} \setminus \mathsf{N} \subseteq \mathbb{N} \setminus A = g(A)$, te $0 \notin \mathsf{N} \Longrightarrow 0 \notin B = g(B)$, pa nikako ne može biti $g(A) = g(B)$ (jedan ima 0 kao element, a drugi nema).

5. Primjeri iz analize

Ovdje ćemo se obično baviti skupovima funkcijâ. Prisjetimo se, svih funkcija iz A u B ima $\mathsf{card}\, B^A = (\mathsf{card}\, B)^{\mathsf{card}\, A}$. Korolari toga, koje smo već spomenuli:

- cjelobrojnih/racionalnih/realnih/kompleksnih nizova ima $\mathfrak{c}$;
- realnih funkcijâ s domenom $\mathbb{Q}$ ima $\mathfrak{c}$;
- realnih funkcijâ s domenom $\mathbb{R}$ ima $2^{\mathfrak{c}}$.

Sada idemo na kompliciranije primjere.

Realnih funkcijâ realne varijable (dakle, onih kojima je kodomena $\mathbb{R}$, a domena proizvoljni neprazni podskup od $\mathbb{R}$) ima $2^{\mathfrak{c}}$.
<u>*Rj.:*</u> Skup svih takvih označimo s $F({}^{\subseteq}\mathbb{R})$. Očito ih ima bar $2^{\mathfrak{c}}$, jer je $\mathbb{R}^{\mathbb{R}} \subset F({}^{\subseteq}\mathbb{R})$. S druge strane, imamo injekciju

$$g : F({}^{\subseteq}\mathbb{R}) \to \mathcal{P}(\mathbb{R}) \times \mathbb{R}^{\mathbb{R}} \; ; \; g(f) := (\mathsf{dom}\, f, \tilde{f}) \; ,$$

gdje je $\tilde{f}$ funkcija f proširena (recimo nulom) na cijeli $\mathbb{R}$. Iz toga imamo

$$\mathsf{card}\, F({}^{\subseteq}\mathbb{R}) \leq \mathsf{card}(\mathcal{P}(\mathbb{R}) \times \mathbb{R}^{\mathbb{R}}) = 2^{\mathfrak{c}} \cdot 2^{\mathfrak{c}} = 2^{\mathfrak{c}+\mathfrak{c}} = 2^{\mathfrak{c}} \; .$$

Drugi način: možemo direktno naći bijekciju.

$$h : F({}^{\subseteq}R) \leftrightarrow (\mathbb{R} \cup \{i\})^{\mathbb{R}} \; ; \; h(f) := f^* \; ,$$

gdje je $f^*(x) := f(x)$ ako je $x \in \mathsf{dom}\, f$, a i inače.

Neprekidnih funkcijâ sa $\mathbb{R}$ u $\mathbb{R}$ ima $\mathfrak{c}$: $\mathsf{card}\, C(\mathbb{R}) = \mathfrak{c}$.
<u>*Rj.:*</u> Koristimo teorem iz analize, koji kaže da je proširenje neprekidne funkcije s $\mathbb{Q}$ u $\mathbb{R}$ po neprekidnosti, jedinstveno. To znači da je preslikavanje

$$|_{\mathbb{Q}} : C(\mathbb{R}) \to \mathbb{R}^{\mathbb{Q}} \; ; \; f \mapsto f|_{\mathbb{Q}} \; ,$$

injekcija. (Naime, ako je $f|_{\mathbb{Q}} = g|_{\mathbb{Q}}$, te su f i g neprekidne s domenom $\mathbb{R}$, tada je za svaki $\mathbb{R} \ni x = \lim_n q_n$, $f(x) = \lim_n f(q_n) = \lim_n g(q_n) = g(x)$.)
Dakle, $\mathsf{card}\, C(\mathbb{R}) \leq \mathsf{card}\, \mathbb{R}^{\mathbb{Q}} = \mathfrak{c}^{\aleph_0} = \mathfrak{c}$.
S druge strane, svakom realnom broju x možemo pridružiti konstantnu funkciju c_x, $c_x(y) = x$ za svaki $y \in \mathbb{R}$. To (pridruživanje $x \mapsto c_x$) je očito injekcija s $\mathbb{R}$ u $C(\mathbb{R})$, te je $\mathfrak{c} = \mathsf{card}\, \mathbb{R} \leq \mathsf{card}\, C(\mathbb{R})$.

Ograničenih funkcijâ sa $\mathbb{R}$ u $\mathbb{R}$ ima $\mathsf{card}\, B(\mathbb{R}) = 2^{\mathfrak{c}}$.
<u>*Rj.:*</u> Uočivši da su sve funkcije s $\mathbb{R}$ u $[0, 1]$ ograničene, i uzevši u obzir napomenu o irelevantnosti proširenja kodomene (funkcija s A u B je

ujedno i funkcija s A u C za svaki $C \supseteq B$), imamo $[0,1]^{\mathbb{R}} \subseteq B(\mathbb{R}) \subseteq \mathbb{R}^{\mathbb{R}}$. Uzevši kardinalne brojeve tih skupova, dobijemo

$$2^{\mathfrak{c}} \leq \mathsf{card}\, B(\mathbb{R}) \leq 2^{\mathfrak{c}}\ .$$

DZ: koliko ima ograničenih i neprekidnih funkcija: $\mathsf{card}\, BC(\mathbb{R}) = ?$

DZ: koliko ima derivabilnih funkcijâ s $\mathbb{R}$ u $\mathbb{R}$: $\mathsf{card}\, D(\mathbb{R}) = ?$

Periodičkih funkcijâ s $\mathbb{R}$ u $\mathbb{R}$ ima $\mathsf{card}\, P(\mathbb{R}) = 2^{\mathfrak{c}}$.
Rj.: Očito $P(\mathbb{R}) \subseteq \mathbb{R}^{\mathbb{R}}$, pa $\mathsf{card}\, P(\mathbb{R}) \leq 2^{\mathfrak{c}}$. Za drugu nejednakost, primijetimo da svakoj realnoj funkciji $f : [0,1\rangle \to \mathbb{R}$ prirodno odgovara funkcija perioda 1, definirana s $g(x) = f(\mathit{rd}(x))$, gdje smo označili s $\mathit{rd}(x) := x - \lfloor x \rfloor = x \bmod 1$, razlomljeni dio od x. Lako se vidi da je $f \mapsto f \circ \mathit{rd}$ injekcija s $\mathbb{R}^{[0,1\rangle}$ u $P(\mathbb{R})$, te imamo i $\mathsf{card}\, P(\mathbb{R}) \geq 2^{\mathfrak{c}}$.

(Strogo) konveksnih funkcijâ s $\mathbb{R}$ u $\mathbb{R}$ ima $\mathsf{card}\, K(\mathbb{R}) = \mathfrak{c}$.
Rj.: Iz analize znamo da su sve konveksne funkcije ujedno neprekidne: $K(\mathbb{R}) \subseteq C(\mathbb{R})$, pa je traženi kardinalni broj manji ili jednak prije određenom $\mathsf{card}\, C(\mathbb{R}) = \mathfrak{c}$. S druge strane, svakom pozitivnom broju a možemo jednostavno injektivno pridružiti konveksnu (kvadratnu) funkciju $x \mapsto a \cdot x^2$. Dakle konveksnih funkcijâ ima bar koliko i pozitivnih realnih brojeva, a to je $\mathsf{card}\, \mathbb{R}^+ = \mathfrak{c}$.

Surjekcijâ s $\mathbb{R}$ na $\mathbb{R}$ ima $\mathsf{card}\, S(\mathbb{R}) = 2^{\mathfrak{c}}$.
Rj.: Očito ih nema više od toga (jer $S(\mathbb{R}) \subseteq \mathbb{R}^{\mathbb{R}}$). Da ih ima bar toliko, može se vidjeti ovako: preslikavanje koje svakoj funkciji $f : \mathbb{R}_0^- \to \mathbb{R}$ pridružuje surjekciju $f \cup \ln$ (proučite kako djeluje ta funkcija, te se uvjerite da je ona zaista element od $S(\mathbb{R})$!), je injekcija. Dakle $\mathsf{card}\, S(\mathbb{R}) \geq \mathsf{card}\, \mathbb{R}^{\mathbb{R}_0^-} = 2^{\mathfrak{c}}$.
Objašnjenje: jednostavno smo funkciju f proširili ln-om. Dobili smo funkciju koja na nepozitivnim brojevima djeluje kao f, a na pozitivnim kao ln. To je surjekcija jer je već ln "pokupio" sve realne brojeve u kodomeni.

Konvergentnih nizova ima $\mathfrak{c}$.
Rj.: Znamo da ih ima manje ili jednako nego svih nizova, dakle najviše $\mathfrak{c}$. S druge strane, za svaki $x \in \mathbb{R}$ postoji konstantni niz $(x, x, x, \ldots)$, koji je očito konvergentan (limes mu je x), i to pridruživanje $(x \mapsto (x, x, x, \ldots))$ je injekcija s $\mathbb{R}$ u skup konvergentnih nizova. Dakle, ima ih bar $\mathsf{card}\, \mathbb{R} = \mathfrak{c}$.

Nizova s limesom 6 ima $\mathfrak{c}$.
Rj.: Sigurno ih nema više nego svih konvergentnih nizova, dakle $\leq \mathfrak{c}$. S druge strane, svakom realnom x možemo injektivno pridružiti niz koji konvergira k 6, ovako: $x \mapsto (6 - x, 6 - \frac{x}{2}, 6 - \frac{x}{3}, \ldots)$ (ili jednostavnije, $x \mapsto (x, 6, 6, 6, \ldots)$ — primijetimo da je i ovo injekcija, iako se dobiveni nizovi podudaraju svuda osim u prvom mjestu).

Za netrivijalne konačnodimenzionalne realne vektorske prostore V i W, linearnih operatorâ s V u W ima $\mathsf{card}\, \mathit{Hom}(V, W) = \mathfrak{c}$.

<u>*Rj.:*</u> Znamo da svaki konačnodimenzionalni vektorski prostor ima bazu, pa fiksirajmo baze $e = (e_0, \ldots, e_{n-1})$ u V i $f = (f_0, \ldots, f_{m-1})$ u W. Također znamo da je koordinatizacija $A \mapsto A(e, f)$ izomorfizam, dakle specijalno bijekcija, između $\mathit{Hom}(V, W)$ i $\mathbb{R}^{m \times n}$, odnosno linearnih operatorâ s V u W ima točno koliko i realnih matricâ tipa $m \times n$, a to je $\mathsf{card}\, \mathbb{R}^{\mathsf{card}(m \times n)} = \mathfrak{c}^{m \cdot n} = \mathfrak{c}$ (jer su V i W netrivijalni, $m \cdot n \geq 1$).

Uz oznake kao u prethodnom zadatku, koliko ima *regularnih* linearnih operatora s V na W?

<u>*Rj.:*</u> Ako je $m \neq n$ (odnosno $V \ncong W$), odgovor je 0: nema izomorfizma između V i W. S druge strane, ako je $m = n$ (BSOMP $V = W$), odgovor je $\mathfrak{c}$: $\leq \mathfrak{c}$ zbog prethodnog zadatka (nema ih više nego *svih* linearnih operatorâ), a $\geq \mathfrak{c}$ jer svakom realnom skalaru $\alpha \neq 0$ možemo pridružiti (injektivno) regularni operator $\alpha \cdot I$. Dakle $\mathsf{card}\, \mathit{GL}(V) = \mathsf{card}\, \mathit{GL}(n, \mathbb{R}) \geq \mathsf{card}\, \mathbb{R} \setminus \{0\} = \mathfrak{c}$.

POGLAVLJE 5

Relacije i uređaji

1. Osnovno o relacijama

Ponovimo:

- Uređen par skupova a i b, (a, b), definira se kao $\{\{a\}, \{a, b\}\}$. Dva uređena para su jednaka ako su im prve komponente jednake, i druge komponente jednake. Komponente a i b se mogu dobiti iz (a, b) pomoću generaliziranih skupovnih operacijâ.
- Kartezijev produkt skupova A i B, $A \times B$, je skup svih uređenih parova kojima je prva komponenta iz A, a druga iz B. $A \times B$ je element od $\mathcal{PPP}(\bigcup\{A, B\})$. Operacija Kartezijevog produkta je distributivna prema elementarnim skupovnim operacijama, i koristi se za definiranje produkta kardinalnih brojeva.
- Relacija između skupova A i B je podskup njihovog Kartezijevog produkta: $\rho \subseteq A \times B$. Dakle, za svaki par (a, b), pri čemu je $a \in A \wedge b \in B$, možemo pitati je li on u ρ. Ako jest, pišemo $a\rho b$; u suprotnom, pišemo $a \not\rho\, b$.
- Binarna relacija na skupu A je relacija između A i A, odnosno podskup Kartezijevog kvadrata $A \times A = A^2$. Iako se svaka relacija između A i B može promatrati kao binarna relacija na $A \cup B$ (dokažite!), ipak je prirodno binarne relacije gledati kao relacije između objekata iste "vrste".

Ubuduće će nas zanimati samo binarne relacije.

Binarna relacija ρ na skupu A može imati sljedeća svojstva (sve izjave su univerzalno kvantificirane po A, odnosno za varijable se pretpostavlja da označavaju proizvoljne elemente od A):

- ρ je *refleksivna* ako vrijedi $x\rho x$ (za svaki x iz A);
- ρ je *irefleksivna* ako vrijedi $x \not\rho\, x$ (opet, za svaki $x \in A$);
- ρ je *simetrična* ako vrijedi $x\rho y \Rightarrow y\rho x$;
- ρ je *asimetrična* ako vrijedi $x\rho y \Rightarrow y \not\rho\, x$;
- ρ je *antisimetrična* ako vrijedi $x\rho y \wedge y\rho x \Rightarrow x = y$;
- ρ je *tranzitivna* ako vrijedi $x\rho y \wedge y\rho z \Rightarrow x\rho z$;
- ρ je *itranzitivna* ako vrijedi $x\rho y \wedge y\rho z \Rightarrow x \not\rho\, z$;
- ρ je *koneksna* ako vrijedi $x\rho y \vee y\rho x \vee x = y$;

Pokažimo prvo da su mnoga od tih svojstava međusobno povezana:

Irefleksivnost $\wedge$ tranzitivnost $\Rightarrow$ asimetričnost.
Rj.: Pretpostavimo da je ρ na A irefleksivna i tranzitivna, te da nije asimetrična. Ovo zadnje znači da postoje a i b iz A, takvi da je $a\rho b \wedge b\rho a$. Po tranzitivnosti bi tada trebalo biti $a\rho a$ (kao i $b\rho b$), a to je u kontradikciji s irefleksivnošću.

Asimetričnost $\Rightarrow$ antisimetričnost $\wedge$ irefleksivnost.
Rj.: Kad bi bilo $a\rho b \wedge b\rho a$ za asimetričnu relaciju ρ, to bi značilo $a\rho b \wedge \neg(a\rho b)$, što je kontradikcija — iz čega slijedi bilo što, pa tako i $a = b$.
Kad bi, za neki $a \in A$, bilo $a\rho a$, po asimetričnosti bi bilo i $\neg(a\rho a)$, što je kontradikcija. Dakle vrijedi i irefleksivnost.

Refleksivnost $\wedge$ simetričnost $\wedge$ koneksnost $\Rightarrow$ univerzalnost ($\rho = A^2$).
Uzmimo proizvoljne a i b iz A. Tada po koneksnosti imamo tri slučaja:

1. $a\rho b$.
2. $b\rho a$. Tada je po simetričnosti i $a\rho b$.
3. $a = b$. Tada je po refleksivnosti $a\rho a$, dakle i $a\rho b$.

Dakle, uvijek je $a\rho b$, za sve a i b iz A, odnosno $\rho = A^2$.

Simetričnost $\wedge$ tranzitivnost $\Rightarrow$ reducirana refleksivnost (postoji skup na kojem je ρ refleksivna relacija).
Rj.: Ako s B označimo skup samo onih elemenata od A koji se zaista pojavljuju u relaciji ρ (zbog simetričnosti, to možemo dobiti i kao $B := \{x \in A : (\exists y \in A)(x\rho y)\}$ — uočite sličnost s definicijom slike funkcije), tada je ρ binarna relacija i na B. Štoviše, ako je $b \in B$ proizvoljan, postoji $a \in A$ takav da je $b\rho a$. Po simetričnosti je tada i $a\rho b$, te po tranzitivnosti $b\rho b$. Dakle ρ je refleksivna na B.

2. Parcijalni uređaji

Relacije nam služe da opišemo odnose elemenata. Promotrimo neke jednostavne odnose među skupovima, i pogledajmo koja svojstva oni imaju. Po uzoru na njih, definirajmo skupine gornjih svojstava koje ćemo smatrati "dobrima".

- "Biti podskup". Ako je S bilo kakav skup, za proizvoljne njegove elemente a i b možemo pitati je li $a \subseteq b$. Dakle, imamo relaciju $\subseteq$ na skupu S. Lako se vidi da je ona refleksivna, antisimetrična i tranzitivna. S obzirom na to da nam $\subseteq$ služi da u(spo)ređujemo skupove (kažemo koji je "veći" a koji "manji"), općenito relaciju s ta tri svojstva zovemo *refleksivni parcijalni uređaj*, skraćeno RPU. ('parcijalni' jer ne možemo

svaka dva skupa "usporediti", na primjer $\{1\}$ i $\{2\}$). Općenito o takvim relacijama razmišljamo pomoću fraze "manje ili jednako", i bilježimo ih simbolima poput $\preceq$.
- "Biti pravi podskup". Kao i gore, samo sada imamo relaciju $\subset$ na S. Također je antisimetrična (štoviše, asimetrična) i tranzitivna, no za razliku od $\subseteq$, relacija $\subset$ je irefleksivna. Jednako nam tako može služiti za uređivanje skupova, i jednako tako ne možemo uvijek svaka dva skupa usporediti, pa općenito relaciju koja je irefleksivna i tranzitivna (vidjeli smo da to povlači a(nti)simetričnost) zovemo *irefleksivni parcijalni uređaj*, skraćeno IPU. Općenito o takvim relacijama razmišljamo pomoću fraze "strogo manje", i bilježimo ih simbolima poput $\prec$.
- "Biti ekvipotentan". Ako promotrimo relaciju $\sim$ na skupu S, odnosno za svaka dva njegova elementa se pitamo jesu li ekvipotentni, vidimo da ona ima svojstva refleksivnosti, simetričnosti i tranzitivnosti. Ona nam također služi za uspoređivanje skupova, ali drugačije: ne tako da kaže koji je od dva skupa "veći" a koji je "manji", već koja dva su po nečem "jednaki" (ovdje po kardinalitetu, odnosno broju elemenata). Binarnu relaciju s ta tri svojstva zovemo *relacija ekvivalencije*, skraćeno REQ. Općenito o takvim relacijama razmišljamo pomoću fraze "jednako", i bilježimo ih simbolima poput $\sim$. Ponovite iz Elementarne matematike što znate o particijama i vezi particijâ s relacijama ekvivalencije!

Primijetimo sljedeću stvar o RPU i IPU: ako na skupu A imamo neki IPU $\prec$, njemu prirodno odgovara jedan RPU na A, definiran formulom $a \preceq b :\iff a \prec b \lor a = b$. Također, ako imamo zadan RPU, recimo $\preceq$, na skupu A, jednako lako možemo definirati pripadni IPU: $a \prec b :\iff a \preceq b \land a \neq b$. Drugim riječima, između skupa svih RPU na A i skupa svih IPU na A postoji prirodna bijekcija $\preceq \mapsto \prec$. To nas dovodi do zaključka da su RPU i IPU samo dva načina za opisati jedan te isti koncept (parcijalni uređaj elemenata od A), baš kao što su relacije ekvivalencije i particije dva načina za opisati jedan te isti koncept (poistovjećivanje pojedinih elemenata nekog skupa). Kao posljedica toga, često se jednostavno govori o parcijalnom uređaju, a iz tipa oznake ($\prec$ ili $\preceq$), ili konteksta zadatka, treba odrediti misli li se na refleksivni ili irefleksivni parcijalni uređaj. Ako je potpuno svejedno, podrazumijeva se IPU.

Ako je R parcijalni uređaj na skupu A, često se promatra *struktura* (A, R) skupa s parcijalnim uređajem na njemu, i kaže se da je to *parcijalno uređen skup*, skraćeno PUS.

U PUSovima možemo definirati mnoge druge pojmove preko uređaja. Kao što je već rečeno, koristit ćemo IPU ili RPU, kako nam već više odgovara za pojedinu definiciju.

Neka je $(A, \prec)$ PUS. ($\prec$ je IPU: pripadni RPU označimo s $\preceq$. Naravno, $b \succ a$ znači $a \prec b$, i $b \succeq a$ znači $a \preceq b$.) Neka je također B neki podskup od A, i a neki element od A. Kažemo:

- a je *donja međa* za B ako $(\forall b \in B)(a \preceq b)$.
- a je *gornja međa* za B ako $(\forall b \in B)(a \succeq b)$.
- a je *najmanji element* od B ako je a donja međa za B, i $a \in B$.
- a je *najveći element* od B ako je a gornja međa za B, i $a \in B$.
- a je *minimalni element* od B ako $a \in B \wedge \neg(\exists b \in B)(b \prec a)$.
- a je *maksimalni element* od B ako $a \in B \wedge \neg(\exists b \in B)(b \succ a)$.
- a je *infimum* za B ako je a najveća donja međa za B.
- a je *supremum* za B ako je a najmanja gornja međa za B.
- *početni komad* (u A) od a je $p_A(a) := \{b \in A : b \prec a\}$.
- *prethodnik* od a je bilo koji element od $p_A(a)$.
- *neposredni prethodnik* od a je maksimalni element od $p_A(a)$.
- B je *gust* (u A) ako $(\forall (a_1, a_2) \in \prec)(\exists B \in B)(a_1 \prec b \wedge b \prec a_2)$.
- B je *kofinalan* (u A) ako $(\forall a \in A)(\exists b \in B)(b \succeq a)$.

Primijetimo bitnu razliku između definicije najmanjeg i minimalnog (te analogno najvećeg i maksimalnog) elementa: najmanji je onaj element danog skupa, koji je "manji" od svih ostalih, dok je minimalan onaj od kojeg nema "manjih" u tom skupu. Za parcijalne uređaje, to općenito nije isto: za dani element $a \in B$, elemente skupa B možemo u odnosu na njega podijeliti u četiri skupine:

(1) oni jednaki a. Naravno, to je samo a: skup takvih je $\{a\}$.
(2) oni "manji" od a. Skup takvih je početni komad u B od a, odnosno $p_{(B, \prec \cap B^2)}(a)$.
(3) oni "veći" od a. Skup takvih je također početni komad od a, ali u obrnuto uređenom skupu, $p_{(B, \succ \cap B^2)}(a)$.
(4) svi ostali — dakle, oni neusporedivi s a.

Najmanji je onaj element za kojeg su druga i četvrta skupina prazne (dakle, svi elementi od B, osim njega, su u trećoj skupini). Minimalan je onaj za kojeg je druga skupina prazna (ali četvrta ne mora biti). Iz toga direktno slijedi da je najmanji element ujedno i minimalan, no obrat ne vrijedi općenito. Također, tamo gdje nema neusporedivih elemenata (više o tome kasnije), ta dva pojma se podudaraju.

Jednako tako, najveći je onaj element za kojeg su treća i četvrta skupina prazne, dok je maksimalan onaj za kojeg je treća skupina prazna. Vrijede analogni zaključci: "biti najveći" povlači "biti maksimalan", ali obrat ne vrijedi općenito — ipak, vrijedi ako nema neusporedivih elemenata.

Štoviše, najmanji (i najveći) element je jedinstven (ako postoji): ako su a i b dva takva, vrijedi $a \preceq b$ jer je a najmanji, i $b \preceq a$ jer je b najmanji, pa po antisimetričnosti imamo $a = b$. Zato možemo imati oznaku za najmanji i najveći element (ako su definirani): $\mathsf{najm}\, B$ i $\mathsf{najv}\, B$. Naravno, minimalni (maksimalni) element ne mora biti jedinstven: ako imamo dva neusporediva elementa a i b, oba su minimalni (i maksimalni) elementi skupa $\{a, b\}$.

Budući da je infimum od B jednostavno najveći element skupa svih donjih međâ za B, on je također jedinstven, pa možemo imati oznaku $\inf B$. Analogno za supremum, $\sup B$.

DZ: je li neposredni prethodnik zadanog elementa nužno jedinstven? Dajte dokaz ili kontraprimjer.

Ako su $(A, \prec)$ i $(B, \lhd)$ dva PUSa, na Kartezijevom produktu $A \times B$ možemo definirati parcijalni uređaj $\dashv$ formulom

$$(a_1, b_1) \dashv (a_2, b_2) :\iff a_1 \prec a_2 \land b_1 \lhd b_2 \,.$$

$\dashv$ se zove *produktni uređaj*, i prirodni je način da se Kartezijev produkt parcijalno uredi. No nedostaju mu mnoga dobra svojstva: na primjer, njegov pripadni RPU nije ekvivalentno definiran kao produkt pripadnih RPUova $\preceq$ i $\unlhd$. Konkretno, na primjer, ako je $b_1 \neq b_2$, parovi (a, b_1) i (a, b_2) su neusporedivi u irefleksivnom produktnom uređaju (provjerite!).
Bolje načine za urediti Kartezijev produkt ćemo promotriti kasnije.

3. Primjeri

(1) Ako su Σ i Π dvije particije skupa X, kažemo da je Σ *finija* od Π, ako vrijedi

$$(\forall A \in \Sigma)(\exists B \in \Pi)(A \subseteq B)$$

(na primjer, particija $\{\{1,2\},\{3,5\},\{4\}\}$ skupa $\{1,2,3,4,5\}$ je finija od particije $\{\{1,2\},\{3,4,5\}\}$). Tada je "biti finija" parcijalni uređaj na skupu svih particijâ od X.

<u>*Rj.:*</u> Ovdje se očito radi o RPU: particija *jest* finija od same sebe, po gornjoj definiciji. Dakle, treba provjeriti tri svojstva:

refleksivnost: Ako je Σ proizvoljna particija od X, za svaki blok $A \in \Sigma$ postoji taj isti blok (nazovimo ga) $B = A \in \Sigma$, tako da je $A = B$, specijalno $A \subseteq B$.

antisimetričnost: Neka je Σ finija od Π, i Π finija od Σ. Za svaki blok $A \in \Sigma$, postoji blok $B \in \Pi$ takav da je $A \subseteq B$. Za taj blok B, budući da je Π finija od Σ, postoji blok $C \in \Sigma$

takav da je $B \subseteq C$. Sveukupno imamo $A \subseteq C$, te kad bi bilo $A \subset C$, morali bismo imati (svojstva particije!) $\emptyset \neq A = A \cap C = \emptyset$, što je kontradikcija. Dakle $A = C$, pa i $A = B$, odnosno, svaki element od Σ je u Π: $\Sigma \subseteq \Pi$. Analogno bismo dobili i $\Pi \subseteq \Sigma$.

tranzitivnost: Neka je Σ finija od Π, i Π finija od Ω. Kao gore, ako za svaki blok $A \in \Sigma$ postoji nadskup $B \in \Pi$, a za njega postoji nadskup $C \in \Omega$, imamo $A \subseteq C$, te time da je Σ finija od Ω (za svaki A postoji C).

(2) Standardni uređaj na $\mathbb{R}^{\mathbb{R}}$,

$$f \leq g :\iff (\forall x \in \mathbb{R})(f(x) \leq g(x)) ,$$

je RPU. Naravno, postoje neusporedivi elementi: na primjer, identiteta $f(x) := x$ i promjena predznaka $g(x) := -x$ su neusporedive — za pozitivne x je $f(x) > g(x)$, dok je za negativne $f(x) < g(x)$.

(3) $\subset$ na skupu $S := \mathcal{P}(\{0, 1, 2\}) \setminus \{\emptyset\}$ je IPU. (Već je rečeno, $\subset$ je prototip IPUa na familijama skupova, i često se podrazumijeva kao parcijalni uređaj ako on nije naveden.) Vrijede sljedeće tvrdnje:

- $\{0\}$ i $\{1\}$ su neusporedivi.
- $\{0, 1\}$ i $\{1, 2\}$ su neusporedivi.
- $\{0, 1\}$ i $\{1\}$ su usporedivi: $\{1\} \subset \{0, 1\}$.
- Singletoni ($\{0\}$, $\{1\}$ i $\{2\}$) su minimalni elementi od S.
- Ne postoji najmanji element od S.
- Najveći element od S je $\mathsf{najv}\, S = \{1, 2, 3\}$.
- $\mathsf{najm}\{\{2\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\} = \{2\}$.
- $\{1, 2\}$ je gornja međa za $\{\{1\}\}$.
- $\{0, 2\}$ nije gornja međa za $\{\{1\}\}$.
- $\inf\{\{1\}, \{2\}\}$ ne postoji (u S).
- $\inf\{\{1, 2\}, \{0, 1\}\} = \{1\}$.
- $\sup S = \{0, 1, 2\}$.
- $\inf \emptyset = \{0, 1, 2\}$ (u S).

Eventualno treba objasniti posljednji redak: donja međa za $\emptyset$ je bilo koji element koji nije manji ili jednak od svih elemenata praznog skupa — dakle bilo koji element od S. Najveća donja međa je tada najveći element od S, a to je $\{0, 1, 2\}$.

(4) Na skupu $S := \{1, 2, 3, 4, 5, 6\}$, relacija

$$\delta := \{(1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (2, 4), (2, 6), (3, 6)\}$$

je IPU (pažljiviji čitatelj će u δ prepoznati restrikciju relacije stroge djeljivosti). 1 je najmanji element. 4, 5 i 6 su maksimalni elementi — najvećeg elementa nema. Infimum skupa $\{2, 4, 6\}$

je 2, dok supremum tog skupa ne postoji (u S). $\inf\{4,5\}=1$.

(5) Promotrimo PUS $(\mathbb{N}\setminus\{0,1\},|\,)$ (prirodni brojevi od 2 nadalje, s refleksivnom relacijom djeljivosti). Minimalni elementi su upravo prosti brojevi, i oni su međusobno neusporedivi. Najmanjeg elementa nema. Maksimalnih elemenata nema (svaki broj n dijeli na primjer $2n$), pa nema ni najvećeg. Supremum konačnog nepraznog skupa je najmanji zajednički višekratnik brojeva u tom skupu.

(6) Promotrimo strukturu $(\mathbb{Z},|\,)$.
Ovdje ne možemo pričati o pojedinim elementima kao o maksimalnim/minimalnim/najvećim/najmanjim, budući da $|$ na $\mathbb{Z}$ nije RPU (niti IPU): ne zadovoljava svojstvo antisimetričnosti. Naime, $6|-6$ i $-6|6$, ali $6\neq-6$.

(7) Malo bolje uređen skup od PUSa je tzv. "usmjereni skup", u kojem svaki dvočlani podskup ima gornju među. Dakle, *usmjeren skup* je PUS $(A,\prec)$ koji ima svojstvo

$$(\forall a\in A)(\forall b\in A)(\exists g\in A)(g\succeq a\wedge g\succeq b)\ .$$

Primijetimo: ako nemamo neusporedivih elemenata, a i b ćemo uvijek moći usporediti, pa će onaj veći biti dobar g. No usmjerenost je slabije svojstvo od toga (vidjeti (5) za primjer usmjerenog skupa s neusporedivim elementima). Ipak vrijedi: U usmjerenom skupu je maksimalni element, ako postoji, jedinstven — štoviše, najveći. Dokažimo to!
Rj.: Neka je PUS $(A,\prec)$ usmjeren, i $a\in A$ maksimalan. Dakle, ne postoji $b\succ a$ u A. Pretpostavimo da a nije najveći — dakle, $\neg(\forall c\in A)(a\succeq c)$, odnosno $(\exists c\in A)(a\not\succeq c)$. Uzmimo jedan takav c. Očito $c\neq a$. Zbog usmjerenosti, skup $\{c,a\}$ ima gornju među, neka je to b. Dakle vrijedi $b\succeq a$, što znači $b\succ a\vee b=a$. Oba slučaja vode na kontradikciju: $b\succ a$ jer je a maksimalan, a $b=a$ jer bi onda trebalo biti $a=b\succeq c$.

(8) Svaki kofinalan podskup usmjerenog PUSa je također usmjeren.
Rj.: Neka je $(A,\prec)$ usmjeren PUS, i neka je $B\subseteq A$ kofinalan. Ako je $\{b,c\}$ dvočlani podskup od B, to je ujedno i dvočlani podskup od A, pa ima gornju među u A: $a\in A$ takav da je $a\succeq b\wedge a\succeq c$. Budući da je B kofinalan, za taj a postoji $g\in B$ takav da je $g\succeq a$, a onda po tranzitivnosti i $g\succeq b\wedge g\succeq c$. Dakle, svaki dvočlani podskup od B ima gornju među u B.

(9) Neka je S proizvoljan skup. Promotrimo (refleksivno uređen) PUS $(\mathcal{P}(S), \subseteq)$. Njegov najveći element je S, dok je najmanji element $\emptyset$. Za proizvoljnu familiju $\mathcal{F} \subseteq \mathcal{P}(S)$, gornja međa od $\mathcal{F}$ je bilo koji podskup od S koji sadrži (kao podskupove) sve $F \in \mathcal{F}$. Najmanja gornja međa je onda $\sup \mathcal{F} = \bigcup F$. Analogno, za $\mathcal{F} \neq \emptyset$, $\inf \mathcal{F} = \bigcap F$, dok je $\inf \emptyset = S$ (u $\mathcal{P}(S)$). Vidimo da u promatranom PUSu svaki podskup ima i infimum i supremum. Takav PUS se zove *(uređajno) potpun*. Primijetimo razliku od potpunosti skupa $\mathbb{R}$ u analizi, gdje samo neprazni ograničeni skupovi imaju infimum/supremum. No kad bismo $\mathbb{R}$ proširili s još dva elementa, $+\infty$ i $-\infty$, te definirali $(\forall x \in \mathbb{R})(-\infty < x \wedge x < +\infty)$, tako dobiven skup bi bio uređajno potpun.

(10)* Za uređajnu potpunost dovoljno je tražiti samo jedan od gornja dva uvjeta: "svaki podskup ima infimum" je ekvivalentno sa "svaki podskup ima supremum". Ideja dokaza: supremum nekog skupa je infimum skupa njegovih gornjih međâ.

4. Totalno uređeni skupovi. Sličnosti

Vidjeli smo da mnoge pojmove ne možemo prirodno i intuitivno definirati u PUSovima — smetaju nam neusporedivi elementi. Usmjereni skupovi su donekle bolji, ali još uvijek ne dovoljno. Zato ćemo se ubuduće ograničiti na proučavanje skupova u kojima nema neusporedivih elemenata. (Poslije ćemo promatrati još bolje uređaje.)

Totalno uređen skup (skraćeno TUS) je PUS $(A, \prec)$, koji ima dodatno svojstvo $(\forall a \in A)(\forall b \in A)(a \prec b \vee a = b \vee b \prec a)$. Za pripadni RPU tada vrijedi $(\forall a \in A)(\forall b \in A)(a \preceq b \vee b \preceq a)$. Dakle, u TUSovima nema neusporedivih elemenata, i kao posljedica toga pojmovi najmanjeg i minimalnog, te najvećeg i maksimalnog, elementa se podudaraju. Ako postoje za skup $B \subseteq A$, zovemo ih jednostavno *minimum* i *maksimum* od B, i označavamo s $\min B$ i $\max B$. Štoviše, kao što se lako dokaže indukcijom po broju elemenata, svaki konačan podskup TUSa ima minimum i maksimum. Svi TUSovi su također usmjereni: za gornju među skupa $\{a, b\}$ možemo uzeti $\max\{a, b\}$.

Imajući TUSove, možemo definirati totalan uređaj i na Kartezijevom produktu (dakle puno bolje nego produktni uređaj), i to na dva važna načina. Neka su $(A, <_A)$ i $(B, <_B)$ dva TUSa. Definiramo sljedeće uređaje na $A \times B$:

- *Leksikografski uređaj* je definiran formulom

$$(a_1, b_1) <_L (a_2, b_2) :\iff a_1 < a_2 \vee (a_1 = a_2 \wedge b_1 < b_2) .$$

- *Antileksikografski uređaj* je definiran formulom

$$(a_1, b_1) < (a_2, b_2) :\Longleftrightarrow\ b_1 < b_2 \vee (b_1 = b_2 \wedge a_1 < a_2)\ .$$

Usprkos nazivu, koji potječe od duge prakse uređivanja riječî u rječnicima, antileksikografski uređaj je prirodniji uređaj na produktu TUSova, što će postati jasnije uskoro. Zato se antileksikografski uređaj često podrazumijeva kada se govori o produktu dva TUSa.

Primijetimo da oba gornja uređaja, i leksikografski i antileksikografski, proširuju produktni uređaj: ako je jedan par manji od drugog u produktnom uređaju, bit će i leksikografski i antileksikografski manji od njega. Dakle, gornja dva uređaja se razlikuju samo po tome kako uređuju parove koji su bili neusporedivi u produktnom uređaju.

Dokažimo da je antileksikografski uređaj zaista totalni uređaj:

irefleksivnost: Pokušajmo usporediti (a, b) s (a, b). Niti vrijedi $b <_B b$ (irefleksivnost od $<_B$), niti vrijedi $b = b \wedge a <_A a$ (irefleksivnost od $<_A$), pa vidimo da $(a, b) \not< (a, b)$.

tranzitivnost: Neka je $(a, b) < (c, d)$ i $(c, d) < (e, f)$. Svaka od tih nejednakosti vodi na dva slučaja, pa ukupno imamo četiri mogućnosti:

- $b <_B d \wedge d <_B f$. Po tranzitivnosti od $<_B$, imamo $b <_B f$, a iz toga $(a, b) < (e, f)$.
- $b <_B d \wedge (d = f \wedge c <_A e)$. Opet imamo $b <_B d = f$, odnosno $b <_B f$, iz čega $(a, b) < (e, f)$.
- $(b = d \wedge a <_A c) \wedge d <_B f$. Imamo $b = d <_B f$, i opet $b <_B f$.
- $b = d \wedge a <_A c \wedge d = f \wedge c <_A e$. Po tranzitivnosti od $<_A$, imamo $b = f \wedge a <_A e$, odnosno $(a, b) < (e, f)$.

totalnost: Neka je $(a, b) \neq (c, d)$. To znači $a \neq c \vee b \neq d$. Ako je $b \neq d$, zbog totalnosti od $<_B$ imamo $b <_B d \vee d <_B b$. U prvom slučaju je $(a, b) < (c, d)$, a u drugom je $(c, d) < (a, b)$. Ako je pak $b = d$, tada mora biti $a \neq c$, odnosno zbog totalnosti od $<_A$, $a <_A c \vee c <_A a$. Opet, u prvom slučaju je $b = d \wedge a <_A c$, odnosno $(a, b) < (c, d)$, dok je u drugom $(c, d) < (a, b)$. Dakle, svaka dva para se mogu usporediti antileksikografski.

No glavna snaga TUSova nije u produktima, već u preslikavanjima. Za TUSove kao strukture se može prirodno definirati pojam homomorfizma, koji se u tom slučaju zove "sličnost", i odgovara pojmu strogo rastuće surjekcije u analizi.

Neka su $(A, <_A)$ i $(B, <_B)$ dva TUSa. Preslikavanje $f : A \to B$ zovemo *sličnost* između A i B, ako je f bijekcija koja čuva uređaj:

$$a <_A a' \Longrightarrow f(a) <_B f(a')\ .$$

Ako postoji sličnost između ta dva TUSa, kažemo da su oni *slični*, i pišemo $(A, <_A) \simeq (B, <_B)$. Ako se na A i B podrazumijevaju uređaji (na primjer $\subset$), pišemo samo $A \simeq B$.

Primijetimo da je sličnost strogo jača od ekvipotentnosti: ako između dva TUSa postoji sličnost, ona je bijekcija, te ta dva TUSa imaju isti broj elemenata. No obrat ne mora vrijediti: na primjer, nemoguće je naći sličnost između TUSa $(\mathbb{N}, <)$ i $(\mathbb{N}, >)$, iako je trivijalno $\mathbb{N} \sim \mathbb{N}$. Malo zanimljiviji primjer: $\mathbb{Z}$ i $\mathbb{Q}$, sa standardnim uređajima, nisu slični, iako su ekvipotentni (oba su prebrojivi). Naravno, za $\mathbb{Q}$ i $\mathbb{R}$ odmah znamo da nisu slični — budući da nisu ekvipotentni. Možda je zanimljivo reći i da su za konačne TUSove ta dva pojma ekvivalentna: konačni TUSovi su slični ako i samo ako su ekvipotentni.

Dokažimo da sličnost TUSova, iako se u definiciji traži samo jedan smjer, zapravo čuva uređaj u oba smjera: odnosno, ako za sličnost f vrijedi $f(a) <_B f(a')$, tada vrijedi i $a <_A a'$.
Rj.: Pretpostavimo suprotno: $a \not<_A a'$. Zbog totalnosti od $<_A$, tada mora biti $a = a'$ ili $a' <_A a$. U prvom slučaju je $f(a) = f(a')$, pa ne može biti $f(a) <_B f(a')$ zbog irefleksivnosti. U drugom slučaju je $f(a') <_B f(a)$, pa opet ne može biti $f(a) <_B f(a')$, ovaj put zbog antisimetričnosti.

DZ: sličnim argumentom dokažite da je umjesto bijektivnosti dovoljno tražiti surjektivnost: funkcija koja čuva uređaj je nužno injekcija.

Ako mislimo da su dva TUSa slični, jedan način (iako ne uvijek najlakši — više kasnije) kako to dokazati je da jednostavno nađemo sličnost: bijekciju koja čuva uređaj. Na primjer:

Ako je $a < b$ i $c < d$ za realne brojeve a, b, c i d, tada je, uz standardni uređaj, $\langle a, b\rangle \simeq \langle c, d\rangle$.
Rj.: Funkcija $x \mapsto b + \frac{d-b}{c-a}(x-a)$ (jednadžba pravca kroz (a, c) i (b, d)!) je sličnost.

(uz standardni uređaj) $\mathbb{R} \simeq \mathbb{R}^+ := \langle 0, +\infty\rangle$
Rj.: exp je jedna tražena sličnost. DZ: nađite ih još!

$\mathbb{R}^+ \simeq \mathbb{R}^-$
Rj.: $x \mapsto -\frac{1}{x}$ je jedna sličnost.

$\mathbb{R} \simeq \langle -1, 1\rangle$
Rj.: $\frac{2}{\pi} \cdot \mathsf{arc\,tg}$ je jedna sličnost.

$\mathbb{Q} \simeq \langle -1, 1\rangle \cap \mathbb{Q}$
Rj.: Ne, $(\frac{2}{\pi} \cdot \mathsf{arc\,tg})|_{\mathbb{Q}}$ nije tražena sličnost (zašto?). Treba nam strogo rastuća surjekcija na racionalne brojeve između -1 i 1. Jedna takva dana je formulom $x \mapsto \frac{x}{1+|x|}$ — dokažite da je to tražena sličnost!

$\langle 0,2\rangle \simeq \langle 0,1] \cup \langle 2,3]$.

Rj.: Jedna sličnost je zadana s $f(x) := \begin{cases} x & , \ x \leq 1 \\ x+1 \, , & x > 1 \end{cases}$.

DZ: $\mathbb{R} \simeq \mathbb{R} \setminus [0,1\rangle$.

DZ: $[0,1] \simeq [0,1] \setminus \langle \frac{1}{3}, \frac{2}{3}] \simeq [0,1] \setminus (\langle \frac{1}{3}, \frac{2}{3}] \cup \langle \frac{1}{9}, \frac{2}{9}] \cup \langle \frac{7}{9}, \frac{8}{9}])$ (i tako dalje).

5. Invarijante sličnosti

No kako dokazati da dva TUSa *nisu* slični? Pokazuje se da je to najefikasnije raditi pomoću invarijanata. Naime, sličnost je, kao i ekvipotentnost, relacija ekvivalencije na bilo kojem skupu TUSova (iako *svi* TUSovi zajedno ne čine skup), te za neku klasu TUSova možemo reći da su svi oni međusobno slični (na primjer, svi tročlani TUSovi su međusobno slični). Invarijanta sličnosti je onda svojstvo koje svi međusobno slični TUSovi ili istodobno imaju, ili istodobno nemaju. Preciznije:

Za svojstvo TUSova P kažemo da je *invarijanta sličnosti* ako, za sve TUSove A i B, $A \simeq B \wedge P(A) \Rightarrow P(B)$. Postoje mnoge invarijante sličnosti, i dokazi da je nešto invarijanta sličnosti obično su jednostavni, iako znaju biti dugački (vidjeti dolje). Ako nađemo neku invarijantu sličnosti P takvu da jedan TUS ima svojstvo P, a drugi ga nema, odmah znamo da ta dva TUSa ne mogu biti slični.

Već smo vidjeli primjer trivijalne invarijante sličnosti: kardinalni brojevi. Ako dva skupa imaju različite kardinalne brojeve (npr. jedan je prebrojiv, a drugi nije; ili je jedan konačan, a drugi beskonačan), znamo da nisu slični. Invarijante sličnosti su obično svojstva iskazana pomoću broja elemenata, i uređaja — odnosno, onog što sličnosti čuvaju. Na primjer:

Svojstvo "imati najveći element (maksimum)" je invarijanta sličnosti.
Rj.: Trebamo dokazati da ako TUS $(A, <_A)$ ima najveći element (recimo a), te $(A, <_A) \simeq (B, <_B)$, tada i B mora imati najveći element. Označimo sličnost između A i B s f. Tvrdimo da je $f(a)$ najveći element od B. Zaista, uzmimo proizvoljni $b \in B$, različit od $f(a)$. Taj b je, zbog surjektivnosti od f, slika nekog $c \in A$. Također, zbog injektivnosti od f, $c \neq a$. Budući da je $a = \max A$, znamo da je $c <_A a$. Sada po sličnosti f, $f(c) <_B f(a)$, odnosno $b <_B f(a)$. Budući da to vrijedi za proizvoljni $b \in B \setminus \{f(a)\}$, zaključujemo da je $f(a)$ najveći element u B.

Svojstvo "biti gust" (gustoća) je invarijanta sličnosti.
Rj.: Neka je TUS $(A, <_A)$ gust, $(B, <_B)$ neki TUS sličan s $(A, <_A)$, i $f : A \to B$ sličnost. Trebamo dokazati da je $(B, <_B)$ gust. Uzmimo

proizvoljni par $(b_1, b_2) \in <_B$ (dakle, $b_{1,2} \in B$ takve da vrijedi $b_1 <_B b_2$). Po surjektivnosti, ti b_1 i b_2 su slike po f nekih elemenata a_1 i a_2 iz A. Budući da, kao što smo vidjeli, f čuva uređaj i u suprotnom smjeru, iz $b_1 <_B b_2$ možemo zaključiti $a_1 <_A a_2$. Sada, budući da je $(A, <_A)$ gust, između a_1 i a_2 postoji neki element a (dakle, $a \in A$ takav da vrijedi $a_1 <_A a <_A a_2$). No tada je, po sličnosti, $b_1 <_B f(b) <_B b_2$, odnosno $f(b)$ je element između b_1 i b_2 koji smo trebali naći. Budući da to vrijedi za proizvoljne $b_1 <_B b_2$, zaključujemo da je B gust.

Uređajna potpunost je invarijanta sličnosti.
Rj.: Dovoljno je vidjeti da je "svaki podskup ima supremum" invarijanta sličnosti (tvrdnja za infimum onda slijedi iz toga, ili po simetričnosti argumenta). Pa neka u TUSu $(A, <_A)$ svaki podskup ima supremum, i neka je f sličnost između $(A, <_A)$ i $(B, <_B)$. Neka je $D \subseteq B$ proizvoljni podskup od B. Taj D je slika po f nekog podskupa $C \subseteq A$ (preciznije, $C := f^{\langle}(D)$). U skupu A, podskup C ima supremum — označimo ga s c. Tvrdimo da je $f(c) = \sup D$.
Treba vidjeti da je $f(c)$ gornja međa za D, i da je najmanja takva. Ovo prvo se vidi lako: neka je $b \in D$ proizvoljni element. On je slika nekog $a \in A$, a po definiciji skupa C, mora biti $a \in C$. Dakle $a \leq_A c = \sup C$, pa je i $b \leq_B f(c)$ (lako se vidi, primjenom injektivnosti, da sličnost čuva i pripadni RPU, i to u oba smjera — dokažite!).
Još je ostalo vidjeti da je $f(c)$ najmanja gornja međa za D. Pa pretpostavimo da postoji neka manja, $e <_B f(c)$. Taj $e \in B$ je slika nekog $a \in A$, i sad se sličnim argumentom kao u gornjem odlomku dokaže da iz "e je gornja međa za D" slijedi "a je gornja međa za C". No tada mora biti $a \geq_A c$ (jer je c najmanja gornja međa za C, te po sličnosti $e \geq_B f(c)$, što je u kontradikciji s pretpostavkom $e <_B f(c)$. Dakle $f(c) = \sup D$.

Svojstvo "svaki početni komad je konačan" je invarijatna sličnosti.
Rj.: Neka je u TUSu $(A, <_A)$ svaki početni komad konačan, i neka je $f : (A, <_A) \simeq (B, <_B)$ (često se skraćeno tako piše) sličnost TUSova. Uzmimo proizvoljni početni komad $p_B(b)$ u B. Taj početni komad je jednostavno skup svih elemenata u B, manjih od nekog fiksnog elementa $b \in B$. No b je slika nekog $a \in A$, i po sličnosti vrijedi: za svaki $c \in A$, $c <_A a$ ako i samo ako je $f(c) <_B b$ — odnosno, $c \in p_A(a) \iff f(c) \in p_B(b)$. Zbog bijektivnosti od f, dobijemo i da je restrikcija $f|_{p_A(a)}$ također bijekcija, između $p_A(a)$ i $p_B(b)$. Dakle ta dva početna komada imaju jednak broj elemenata — a budući da je po pretpostavci $p_A(a)$ konačan, mora takav biti i $p_B(b)$.

Kao što vidimo, svi dokazi invarijantnosti su poprilično "na isti kalup" — što i nije tako slučajno, ako smo upoznati s teorijom koja stoji iza Bethovog teorema definabilnosti. Dokažite da su sljedeća svojstva također invarijante sličnosti:

- Postojanje "predzadnjeg" elementa: takvog da postoji točno jedan element veći od njega.
- "Svaki neprazan podskup ima najmanji element" (*dobar uređaj* — svojstvo koje će nam biti vrlo bitno kasnije).
- "Svaki element ima neposrednog prethodnika ako nije najmanji, i neposrednog sljedbenika ako nije najveći" (*diskretan uređaj*).
- "$\mathbb{R}$-potpunost": svaki neprazan podskup koji ima gornju među, ima supremum.
- "Postoji samo konačno mnogo elemenata koji nemaju neposrednog prethodnika."
- "Između svaka dva elementa postoji samo konačno mnogo elemenata" (*lokalno konačan uređaj*).

Pokažimo sada kako se koriste invarijante sličnosti:

$\mathbb{N} \not\simeq \mathbb{Z}^-$ (ili $(\mathbb{N},<) \not\simeq (\mathbb{N},>)$)
Rj.: $\mathbb{N}$ ima najmanji element (konkretno, 0), dok $\mathbb{Z}^-$ nema (za svaki $a \in \mathbb{Z}^-$ postoji manji $a-1 \in \mathbb{Z}^-$). Budući da je postojanje najmanjeg elementa invarijanta sličnosti, ta dva TUSa ne mogu biti slični.

$\mathbb{Q} \not\simeq \mathbb{Z}$
Rj.: $\mathbb{Q}$ je gust: za svaka dva $a < b$ u $\mathbb{Q}$, postoji $\frac{a+b}{2} \in \mathbb{Q}$ takav da je $a < \frac{a+b}{2} < b$. $\mathbb{Z}$ nije gust: recimo, između $0 \in \mathbb{Z}$ i $1 \in \mathbb{Z}$ ne postoji nijedan cijeli broj. Gustoća je invarijanta sličnosti, dakle $\mathbb{Q}$ ne može biti sličan $\mathbb{Z}$.

$\mathbb{N} \not\simeq \mathbb{N}^2$ (sjetimo se, $\mathbb{N}^2$ je Kartezijev kvadrat — na njemu podrazumijevamo antileksikografski uređaj)
Rj.: U $\mathbb{N}$ postoji samo jedan element bez neposrednog prethodnika: 0 (svaki $n \in \mathbb{N} \setminus \{0\}$ ima neposrednog prethodnika: $n-1 \in \mathbb{N}$). U $\mathbb{N}^2$ pak, postoji beskonačno mnogo elemenata bez neposrednog prethodnika: to su svi parovi iz $\mathbb{N}^2$ oblika $(0,n)$. Zaista, budući da od 0 nema manjih elemenata u $\mathbb{N}$, svaki antileksikografski prethodnik od $(0,n)$ mora biti oblika (a,m), pri čemu je $m < n$. No nijedan od njih nije neposredan, jer postoji veći $(a+1,m)$ koji je također prethodnik od $(0,n)$. Budući da je "postoji samo konačno mnogo elemenata bez neposrednog prethodnika" invarijanta sličnosti, nužno slijedi $\mathbb{N} \not\simeq \mathbb{N}^2$.

$\mathbb{R} \not\simeq \mathbb{R} \setminus \mathbb{Q}$
Rj.: U $\mathbb{R}$, kao što znamo, svaki ograničen neprazan podskup ima supremum. Dokažimo da to u $\mathbb{R} \setminus \mathbb{Q}$ nije slučaj. Budući da je to svojstvo invarijanta sličnosti, iz toga će odmah slijediti tražena ne-sličnost. Promotrimo skup $[0,2] \setminus \mathbb{Q}$. To je očito podskup od $\mathbb{R} \setminus \mathbb{Q}$, i neprazan je (recimo, sadrži element $\sqrt{2}$). Također je ograničen — recimo, gornja međa mu je $\sqrt{5} \in \mathbb{R} \setminus \mathbb{Q}$ (primijetimo da ne možemo reći npr. "gornja

međa mu je 3", jer $3 \notin \mathbb{R} \setminus \mathbb{Q}$), a donja $-\sqrt{5} \in \mathbb{R} \setminus \mathbb{Q}$. No, taj skup nema supremum u $\mathbb{R} \setminus \mathbb{Q}$ — za svaku gornju među $g \in \mathbb{R} \setminus \mathbb{Q}$ skupa $[0,2] \setminus \mathbb{Q}$, možemo napraviti sljedeće:
Promotrimo broj $\frac{g}{2}+1$. Lako se vidi da je to iracionalan pozitivan broj između 2 i g. Ako je $g < 2$, to je element od $[0,2] \setminus \mathbb{Q}$, veći od g, dakle kontraprimjer za tvrdnju da je g gornja međa tog skupa. Ako je pak $g > 2$, to je također gornja međa za taj skup, manja od g. Naravno, ne može biti $g = 2$, jer $g \notin \mathbb{Q}$. Dakle, ne postoji najmanja gornja međa, u $\mathbb{R} \setminus \mathbb{Q}$, za skup $[0,2] \setminus \mathbb{Q}$.

$\mathbb{R} \not\simeq \mathbb{R} \times 2$ (($= \mathbb{R} \times \{0,1\}$, s antileksikografskim uređajem))
Rj.: Također, dokazat ćemo da ovaj desni skup nije $\mathbb{R}$-potpun. Pogledajmo prvo kako on izgleda: u njemu imamo dvije vrste parova — one oblika $(r,0)$, i one oblika $(r,1)$. Nazovimo prve "crveni", a druge "plavi". Antileksikografski uređaj kaže da su svi crveni manji od svih plavih, te da se crveni međusobno, kao i plavi međusobno, uspoređuju kao i realni brojevi (njihove prve komponente). Efektivno, imamo dvije kopije od $\mathbb{R}$ ("crveni $\mathbb{R}$" i "plavi $\mathbb{R}$"), svaka s prirodnim uređajem, posložene jedna do druge. Sada je jasno gdje neće biti supremuma: "crveni $\mathbb{R}$" (precizno, $\mathbb{R} \times \{0\}$) je podskup od $\mathbb{R} \times 2$, neprazan (na primjer, $(0,0) \in \mathbb{R} \times \{0\}$) i ograničen odozgo (na primjer, svaki $(r,0)$ je manji od $(0,1)$), no nema najmanju gornju među: svaka gornja međa mora biti "plava" (dokažite!), oblika $(r,1)$, a onda za nju postoji još manja gornja međa $(r-1,1)$.

$\mathbb{R} \not\simeq 2 \times \mathbb{R}$
Rj.: Opet imamo u desnom skupu dvije vrste točaka, no sad se prvo uspoređuju po svojoj realnoj vrijednosti, a tek ako su realne vrijednosti jednake, kažemo da je crvena manja od plave. Ovaj skup očito nije sličan $\mathbb{R}$, jer uopće nije gust: na primjer, $(0,0)$ i $(1,0)$ ("crvena" i "plava" nula) su međusobno susjedni elementi, i nema nijednog elementa od $2 \times \mathbb{R}$ između njih.

$\mathbb{R} \times 2 \not\simeq 2 \times \mathbb{R}$ (odnosno, $(\mathbb{R} \times 2, <) \not\simeq (\mathbb{R} \times 2, <_L)$)
Rj.: Budući da smo vidjeli da desni skup nije gust, dovoljno je vidjeti da lijevi jest. Uzmimo u $\mathbb{R} \times 2$ dva elementa $(a,b) < (c,d)$. Ako su oba "iste boje" ($b = d$), tada između njih postoji aritmetička sredina $(\frac{a+c}{2}, b)$ iste boje. Ako su različitih bojâ, manji mora biti crveni, a veći plavi: $b = 0 \wedge d = 1$. No tada je recimo element $(a+1,0)$ sigurno veći od $(a,0) = (a,b)$, a manji od $(c,1) = (c,d)$.

$\mathbb{Z} \not\simeq \mathbb{Z} \times 2$
Rj.: Skup $\mathbb{Z}$ je lokalno konačan: između $a \in \mathbb{Z}$ i $b \in \mathbb{Z}$ ima samo konačno mnogo, konkretno $|a-b|+1$, elemenata. S druge strane, skup $\mathbb{Z} \times 2$ nije lokalno konačan: između $(-1,0)$ i $(-1,1)$ nalaze se svi elementi oblika $(n,0)$, za $n \in \mathbb{N}$ — njih beskonačno mnogo.

$\mathbb{Z}\times\mathbb{N}\not\simeq\mathbb{N}\times\mathbb{Z}$
Rj.: U $\mathbb{Z}\times\mathbb{N}$ svaki element (z,n) ima neposrednog prethodnika: to je $(z-1,n)$. No u $\mathbb{N}\times\mathbb{Z}$ postoje elementi bez neposrednog prethodnika (štoviše, njih beskonačno mnogo): $(0,z)$, za proizvoljni $z\in\mathbb{Z}$.

6. Nekoliko težih zadataka

(1) Za svaki prirodni n, svi PUSovi kardinaliteta n su međusobno slični (odnosno, za konačne skupove je ekvipotentnost ekvivalentna sličnosti).
Rj.: Indukcijom po n, dokazat ćemo da je svaki skup s n elemenata sličan standardnom skupu $n:=\{0,1,\ldots,n-1\}$, sa standardnim uređajem $<$. Baza je trivijalna: svi skupovi s 0 elemenata su čak jednaki (prazan skup je jedinstven), pa su pogotovo slični ($\emptyset$ je sličnost). Pretpostavimo da tvrdnja vrijedi za neki prirodni k. Ako je A proizvoljni skup s $k+1$ elemenata, tada A ima maksimalni element (što se također može dokazati matematičkom indukcijom po k — DZ), označimo ga s a. Skup $A\setminus\{a\}$ sada ima k elemenata, pa je po pretpostavci indukcije sličan sa standardno uređenim $\{0,\ldots,k-1\}$. Ako tu sličnost označimo s $f:A\setminus\{a\}\simeq k$, tvrdimo da je $f_+:=f\cup\{(a,k)\}$ sličnost između A i $k+1$. Zaista, za svaka dva (različita, dakle BSOMP $b<_A c$) elementa b i c iz A, vrijedi jedno od sljedećeg:
- Nijedan od njih nije a. Tada su oba u $A\setminus\{a\}$, pa po pretpostavci indukcije $f(b)<f(c)$, a time i $f_+(b)<f_+(c)$ (jer je f_+ proširenje od f).
- Jedan od njih je a (ne mogu biti oba, jer smo uzeli različite). Budući da smo pretpostavili $b<_A c$, mora biti $c=a$. No tada je $f_+(b)=f(b)$ (jer je $b\in A\setminus\{a\}$), a to je najviše $k-1$ (jer je to maksimum kodomene od f), što je strogo manje od $k=f_+(a)=f_+(c)$, što smo i trebali dokazati.

(2) Neka je A proizvoljan skup. Ako promotrimo skup $\mathcal{U}(A)$ svih (irefleksivnih) parcijalnih uređajâ na A, tada je taj skup prirodno uređen relacijom $\subset$ ("jedan uređaj je pravi podskup drugog" znači da u drugom uređaju možemo usporediti sve elemente koje smo mogli i u prvom, s jednakim ishodom, i još neke elemente koji su u prvom uređaju bili neusporedivi). Tada su maksimalni elementi PUSa $(\mathcal{U}(A),\subset)$ upravo totalni uređaji na A.
Rj.: Jedan smjer je jasan: ako je $<$ totalni uređaj na A, tada je maksimalan: kad bi $\tilde{<}$ bio njegov pravi nadskup, bilo bi $(x,y)\in\tilde{<}$ i $(x,y)\notin<$ za neke x i y. Budući da je $\tilde{<}$

irefleksivan, imamo $x \neq y$, a kako vrijedi $x \not< y$, mora biti $y < x$ (jer je $<$ totalan), pa i $y \tilde{<} x$ (jer je $\tilde{<}$ nadskup od $<$), što je u kontradikciji s antisimetričnošću od $\tilde{<}$.

Za drugi smjer treba malo više pisati: neka je $<$ maksimalni element u $\mathcal{U}(A)$. Treba dokazati da je totalan. Pretpostavimo da nije, i neka su x i y dva neusporediva elementa s obzirom na $<$. Konstruirajmo novi uređaj ovako:

$$\tilde{<} \;:=\; \{a \in A\,;\, a \leq x\} \times \{b \in A\,;\, b \geq y\} \bigcup <$$

— odnosno, u $<$ ubacimo još sve parove oblika (a, b), gdje je $a \leq x \wedge b \geq y$. Primijetimo da smo time ubacili i par (x, y), ali potencijalno i mnoge druge. $\tilde{<}$ je svakako binarna relacija na A (podskup od A^2). Dokažimo da je to IPU na A:

irefleksivnost Pretpostavimo da je $z \tilde{<} z$ za neki z. Budući da nije $z < z$ ($<$ je irefleksivna relacija), jedino je moguće $z \leq x \wedge z \geq y$, no to bi po tranzitivnosti dalo $y \leq x$, što je kontradikcija s neusporedivošću x i y. Dakle, takav z ne postoji, pa imamo irefleksivnost.

tranzitivnost Neka je $p \tilde{<} q \wedge q \tilde{<} r$ za proizvoljne p, q i r iz A. Ako su oba para (p, q) i (q, r) već u $<$, imamo $p < r$ po tranzitivnosti od $<$, pa i $p \tilde{<} r$. Oba ne mogu biti novododani, jer bi to vodilo na $q \leq x \wedge q \geq y$, što je kontradikcija kao u prošlom odlomku. Dakle, još je ostao slučaj kada je jedan novododan, a drugi je u $<$ — BSOMP $p \leq x \wedge q \geq y \wedge q < r$. Sada imamo $y \leq q < r$ odnosno $y < r$, što zajedno s $p \leq x$ daje $p \tilde{<} r$.

Dakle, $\tilde{<} \in \mathcal{U}(A)$. Po definiciji, $< \subseteq \tilde{<}$. Budući da je trivijalno $x \tilde{<} y$ ali $x \not< y$, vrijedi $\tilde{<} \supset <$, što je u kontradikciji s pretpostavkom da je $<$ maksimalan element u $\mathcal{U}(A)$.

(3) Neka je $(A, <)$ proizvoljan TUS. Dokažite da postoji TUS $(B, \subset)$ (sa standardnim uređajem "biti pravi podskup"), sličan s A.

<u>*Rj.:*</u> Za B uzmimo skup svih početnih komada u A, dakle $\{p_A(a)\,;\, a \in A\}$; a za sličnost preslikavanje p_A koje svakom $a \in A$ pridružuje njegov početni komad $p_A(a)$. To preslikavanje je surjekcija po definiciji: B je definiran kao slika od p_A. Treba još vidjeti da je injekcija, i da čuva uređaj (iz toga će odmah slijediti da je B TUS).

Ako su $x \neq y$ dva različita elementa iz A, oni su usporedivi (jer je A TUS), pa BSOMP $x < y$. No to znači $x \in p_A(y)$. S druge strane, $x \notin p_A(x)$ (irefleksivnost), pa vidimo da su $p_A(x)$ i $p_A(y)$ različiti. Dakle, p_A je injekcija.

Štoviše, ako je $x < y$, za svaki element $z \in p_A(x)$ vrijedi $z < x < y$, odnosno po tranzitivnosti $z < y$, dakle $z \in p_A(y)$.

Drugim riječima, $p_A(x) \subseteq p_A(y)$, a u gornjem odlomku smo vidjeli da nisu jednaki (zbog $x \neq y$), dakle $p_A(x) \subset p_A(y)$, što smo i trebali dokazati.

7. Uređajni tipovi i karakterizacije

Vidjeli smo da se dva skupa mogu pokazati sličnim našavši konkretnu sličnost između njih (i dokazavši da je to sličnost), te da se mogu pokazati ne-sličnim našavši invarijantu sličnosti koju jedan ima, a drugi nema. No što ako ne možemo naći ni jedno ni drugo? Na primjer, promotrimo skupove $\mathbb{Q}$ i $\mathbb{A}$ (racionalnih i algebarskih brojeva). Prebrojivi su oba. Ograničeni — nijedan. Diskretni — nijedan. Lokalno konačni — nijedan. Gusti — oba. Na svim invarijantama sličnosti koje nam padaju na pamet, podudaraju se. Pa ipak, ne čini se da možemo naći neku konkretnu sličnost između ta dva TUSa. Kako riješiti taj problem?

Pokazuje se da obično ne moramo proučavati bezbrojne invarijante sličnosti: za svaki od "lijepih" TUSova kojima ćemo se baviti ($\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ i $\mathbb{R}$), postoji nekoliko "reprezentativnih" invarijanata sličnosti, u kojima je dovoljno da se neki TUS podudara s danim "lijepim" TUSom, pa da mu bude sličan. Uskoro ćemo navesti te reprezentativne invarijante sličnosti, samo prvo donekle formalizirajmo pojam "svi međusobno slični TUSovi" koji nam je trebao još za invarijante sličnosti.

Za dva TUSa $(A, <_A)$ i $(B, <_B)$ kažemo da imaju isti *uređajni (ordinalni) tip*, i pišemo $\tau(A, <_A) = \tau(B, <_B)$, ako su slični. Primijetimo da je to dobro definirano, jer je svaki TUS sličan samom sebi (identiteta je sličnost), sličnost TUSova se može invertirati (i inverz sličnosti je sličnost, kao što smo dokazali), te vrijedi tranzitivnost, jer je kompozicija sličnostî ponovo sličnost. Također primijetimo kako je to analogno definiciji kardinalnih brojeva: ne kažemo *što* su kardinalni brojevi, već definiramo kad dva skupa imaju isti kardinalni broj (ekvipotentni su).

Sjetimo se, kod kardinalnih brojeva imali smo nekoliko međusobno ne-ekvipotentnih skupova, čije kardinalne brojeve smo označili posebnim simbolima: 0 za $\emptyset$, 1 za $\{0\}$, 2 za $\{0, 1\}$, i tako dalje; zatim $\aleph_0$ za $\mathbb{N}$, te $\mathfrak{c}$ za $\mathbb{R}$. Ovdje također imamo nekoliko međusobno ne-sličnih TUSova, čije ordinalne tipove označujemo posebnim simbolima:

- $\omega := \tau(\mathbb{N}, <)$
- $\pi := \tau(\mathbb{Z}, <)$
- $\eta := \tau(\mathbb{Q}, <)$
- $\lambda := \tau(\mathbb{R}, <)$

Sada, na primjer, kad želimo reći da je neki TUS sličan $\mathbb{Q}$ (sa standardnim uređajem), možemo reći da je njegov uređajni tip jednak η.

Teoremi o uređajnoj karakterizaciji (nabrajanje reprezentativnih invarijanata za svaki od gornjih tipova) glase:

- Ako je TUS $(A, <_A)$ konačan (dakle, $\mathsf{card}\, A = n \in \mathbb{N}$), tada je $\tau(A, <_A) = n$.
- Ako je TUS $(A, <_A)$ beskonačan, i svaki početni komad mu je konačan, tada je $\tau(A, <_A) = \omega$.
- Ako je TUS $(A, <_A)$ prebrojiv, obostrano neograničen (nema ni najmanjeg ni najvećeg elementa), i lokalno konačan, tada je $\tau(A, <_A) = \pi$.
- Ako je TUS $(A, <_A)$ prebrojiv, obostrano neograničen i gust, tada je $\tau(A, <_A) = \eta$.
- Ako je TUS $(A, <_A)$ beskonačan (dovoljno je da je neprazan), obostrano neograničen, $\mathbb{R}$-potpun i separabilan (sadrži prebrojiv gust podskup), tada je $\tau(A, <_A) = \lambda$.

Sada je lako vidjeti: $\mathbb{Q} \simeq \mathbb{A}$
Rj.: Tip od $\mathbb{Q}$ je η po definiciji. Treba još vidjeti da je $\tau(\mathbb{A}, <) = \eta$. Znamo otprije da je $\mathbb{A}$ prebrojiv. Za proizvoljan $a \in \mathbb{A}$, $a-1$ je također algebarski, i manji od a, dok je $a+1$ također algebarski, i veći od a — dakle, $\mathbb{A}$ nema ni najmanji ni najveći element. Također, za a i b algebarske takve da je $a < b$, sigurno postoji racionalan broj q između njih (štoviše, između svaka dva realna broja postoji racionalan). No q je algebarski (m/n je rješenje jednadžbe $nx - m = 0$), pa je $\mathbb{A}$ gust. Teorem o uređajnoj karakterizaciji tipa η sada daje sličnost.

DZ: dokažite primjenom teoremâ o uređajnoj karakterizaciji:
$\mathbb{P} \simeq \mathbb{N}$
$3\mathbb{Z} \simeq \mathbb{Z}$
$\mathbb{Q} \setminus \mathbb{N} \simeq \mathbb{Q}$

8. Računanje s uređajnim tipovima

Prisjetimo se, za kardinalne brojeve smo mogli definirati jednakost, uspoređivanje, zbrajanje, množenje i potenciranje. Za ordinalne tipove ne možemo to sve definirati (bar ne tako da ima lijepa svojstva), no nešto možemo. Primjerice, jednakost ordinalnih tipova smo definirali već u prethodnoj točki. Sada ćemo definirati množenje i zbrajanje.

Podsjetimo se definicijâ množenja i zbrajanja kardinalnih brojeva: za $\kappa = \mathsf{card}\, A \land \mu = \mathsf{card}\, B$, bilo je definirano $\kappa \cdot \mu := \mathsf{card}(A \times B)$, te $\kappa + \mu := \mathsf{card}(A \times \{0\} \cup B \times \{1\})$. Specijalno, ako su A i B bili disjunktni, zbroj smo mogli definirati i jednostavnije, kao $\mathsf{card}(A \cup B)$.

Da bismo to pretvorili u definicije za ordinalne tipove, moramo još specificirati uređaj na gornjim skupovima $A \times B$ i $A \times \{0\} \cup B \times \{1\}$.

No to su oba skupovi uređenih parova, a na uređenim parovima znamo da postoji prirodan uređaj: antileksikografski. Dakle:

Neka su σ i ν dva ordinalna tipa, $\sigma := \tau(A,<)$ i $\nu := \tau(B,<)$. Tada definiramo $\sigma \cdot \nu := \tau(A \times B, <)$, te $\sigma + \nu := \tau(A \times \{0\} \cup B \times \{1\}, <)$, s antileksikografskim uređajima.

Pogledajmo zbroj preciznije. Promatrajući $A \times \{0\}$ i $B \times \{1\}$, možemo reći da smo obojali sve elemente od A u crveno, te sve elemente od B u plavo. Uspoređujući ih antileksikografski, prvo uspoređujemo njihovu boju: budući da je $0 < 1$, vidimo da su svi crveni prije svih plavih. Ako su pak iste boje, uspoređujemo ih kako već znamo: dva crvena uređajem u A, a dva plava uređajem u B. U specijalnom slučaju, kada su A i B disjunktni, njihove elemente uopće ne moramo bojati ("obojani" su već time kojem skupu pripadaju): u zbroju, prvo dolaze svi elementi iz A (uređeni kao što su bili u A), a nakon toga svi elementi iz B (uređeni kao što su bili u B). Na neki način, novi uređaj je $<_A \cup <_B \cup A \times B$.

Postoji još jedna unarna operacija na ordinalnim tipovima: ako je $\sigma := \tau(A,<)$, definiramo *reverzni tip* (ponekad se zove i "inverzni", ali treba imati na umu da to nije inverzni element s obzirom na gornje operacije) od σ kao $\sigma^* := \tau(A,>)$, dakle uređajni tip obrnuto uređenog skupa. Na primjer, $\omega^* = \tau(\mathbb{N},>)$, i vidjeli smo da je različit od ω, no svi ostali spomenuti tipovi (π, η, λ, kao i svi konačni) su jednaki svojim reverznim tipovima (DZ).

Vrijede brojni zakoni koji vežu te operacije
(podrazumijevamo da su $\rho = \tau(A,<)$, $\sigma = \tau(B,<)$, te $(\nu = \tau(C,<)$ proizvoljni uređajni tipovi):

(1) Zbrajanje je asocijativno: $(\rho+\sigma)+\nu = \rho+(\sigma+\nu)$. Zaista, s $x \mapsto \begin{cases} (a,0) & , x = ((a,0),0) \\ ((b,0),1) & , x = ((b,1),0) \\ ((c,1),1) & , x = (c,1) \end{cases}$ je dana sličnost između $\Big(A \times \{0\} \cup B \times \{1\}\Big) \times \{0\} \cup C \times \{1\}$ i
$A \times \{0\} \cup \Big(B \times \{0\} \cup C \times \{1\}\Big) \times \{1\}$ (provjerite!).
(2) Množenje je asocijativno: $(\rho \cdot \sigma) \cdot \nu = \rho \cdot (\sigma \cdot \nu)$. Zaista, $((a,b),c) \mapsto (a,(b,c))$ je sličnost između TUSova $(A \times B) \times C$ i $A \times (B \times C)$.
(3) $0 = \emptyset$ je neutralni element za zbrajanje. Primijetimo, $A \times \{0\} \cup \emptyset \times \{1\}$ je zapravo $A \times \{0\}$, a $\emptyset \times \{0\} \cup A \times \{1\}$ je $A \times \{1\}$, te je prva projekcija sličnost bilo kojeg od tih skupova s A.
(4) $1 = \{0\}$ je neutralni element za množenje: $a \mapsto (a,0)$ odnosno $a \mapsto (0,a)$ je sličnost između A i $A \times 1$ odnosno $1 \times A$.

(5) Vrijedi jedna distributivnost množenja (slijeva) prema zbrajanju: $\rho \cdot \sigma + \rho \cdot \nu = \rho \cdot (\sigma + \nu)$. Zanimljivo je da se sličnost (između kojih skupova?) dobiva istim "pravilom" kao i za dokazivanje asocijativnosti množenja: $((a, d), j) \mapsto (a, (d, j))$.
(6) DZ: kako se reverz ponaša s obzirom na zbrajanje i množenje? Dokažite. (Rješenje: $(\rho + \sigma)^* = \sigma^* + \rho^*$, te $(\rho \cdot \sigma)^* = \rho^* \cdot \sigma^*$.)

Također, mnoga svojstva danih operacijâ *ne* vrijede:

(1) Ne vrijede zakoni kraćenja: na primjer, $1 + \omega = \omega$ (dakle $1 + \omega = 0 + \omega$, a $1 \neq 0$). Zaista, s $(a, b) \mapsto a + b$ je dana sličnost između $1 \times \{0\} \cup \mathbb{N} \times \{1\}$ i $\mathbb{N}$. Također, $\omega^* + 1 = \omega^*$. Ne vrijede ni za množenje: na primjer, $2 \cdot \omega = \omega$ (sličnost je $(a, b) \mapsto a + 2b$). Da ne vrijedi ni drugi zakon kraćenja za množenje, vidi se iz $\eta \cdot \eta = \eta$, što se može dokazati primjenom teorema o uređajnoj karakterizaciji: leksikografski uređen $\mathbb{Q}^2$ je prebrojiv, obostrano neograničen i gust (dokažite!), dakle tipa η.
(2) Ne vrijedi komutativnost zbrajanja. Naime, vidjeli smo gore $1 + \omega = \omega$, no $\omega + 1 \neq \omega$ (primjena invarijanata sličnosti: $\mathbb{N} \times \{0\} \cup 1 \times \{1\}$ ima najveći element $(0, 1)$, dok ga $\mathbb{N}$ nema. Ne vrijedi ni komutativnost množenja. Gore smo vidjeli $2 \cdot \omega = \omega$, preostaje vidjeti $\omega \cdot 2 \neq \omega$ — a to je zato što je početni komad $p_{\omega \cdot 2}(0, 1) = \mathbb{N} \times \{0\}$ beskonačan, dok su u $\mathbb{N}$ svi početni komadi konačni.
(3) Ne vrijedi druga distributivnost množenja (zdesna) prema zbrajanju: specijalno, $\omega \cdot 2 + 1 \cdot 2 \neq (\omega + 1) \cdot 2$. Dokažite to! Uputa: skup predstavnik lijeve strane ima predzadnji element, dok ga skup predstavnik desne strane nema.

Sada vidimo da mnoge dosadašnje zadatke možemo zapisati kao nejednakosti s ordinalnim tipovima: na primjer, dosad smo vidjeli da vrijedi:

- $\omega \neq \omega \cdot \omega$,
- λ, $\lambda \cdot 2$ i $2 \cdot \lambda$ su svi međusobno različiti,
- $\pi \neq \pi \cdot 2$,
- $\omega \cdot \pi \neq \pi \cdot \omega$ (još jedan kontraprimjer komutativnosti množenja).

Primjenom teorema o uređajnoj karakterizaciji, ili nalaženjem konkretnih sličnosti (učinite to!), može se vidjeti da vrijedi:

- $\omega^* + \omega = \pi = 2 \cdot \pi$,
- $\eta + \eta = \eta \cdot \eta = \eta$,
- $\lambda + 1 + \lambda = (1 + \lambda) \cdot \pi = \lambda$.

POGLAVLJE 6

Ordinali

1. Motivacija i pregled

Vidjeli smo da ordinalni tipovi imaju svoju aritmetiku, koja u nekom pogledu profinjuje aritmetiku kardinalnih brojeva: na primjer, unutar kardinalnog broja $\aleph_0$ našli smo bogatstvo raznih ordinalnih tipova — ω, π, η, i njihovih izvedenicâ, od kojih su mnogi međusobno bitno različiti.

Ipak, neke stvari koje smo imali definirane za kardinalne brojeve, poput uspoređivanja po veličini i potenciranja, nedostaju. Možda bismo i mogli reći da je u nekom smislu π "manji" od η, no kako usporediti na primjer ω i ω^*? Nekako se čini da postoje "nepopravljivo neusporedivi" ordinalni tipovi.

Da bismo to riješili, trebamo se usredotočiti na skupove koji su još bolje uređeni od općenitih TUSova. Mnogi ordinalni tipovi će pri tome otpasti, no na onom što ostane (ordinalni tipovi koji preostanu zvat će se *ordinalni brojevi* ili *redni brojevi*) imat ćemo jako dobru strukturu, koja će u izvjesnom smislu biti "najbolja moguća" za ono što želimo postići: aritmetiku beskonačnosti.

Vidjet ćemo da će taj pristup imati još jednu pozitivnu stranu: umjesto "poludefinicijâ" tipa "kažemo da skupovi imaju jednak kardinalni broj ako i samo ako su ekvipotentni, ali nigdje ne definiramo što kardinalni broj jest", za ordinalne brojeve imat ćemo konkretne skupove (zovu se *ordinali*) koji će ih predstavljati. Tako ćemo moći preciznije formalizirati i mnoge pojmove koji u sebi nose ideju "nadograđivanja u beskonačnost", jedan od kojih je svakako i sama kumulativna hijerarhija (više o tome na predavanjima).

Štoviše, tako izgrađena teorija ordinalâ bit će dovoljno snažna da se u njoj može strogo definirati čak i pojam kardinalnog broja (no da bismo vidjeli da se on podudara s onim što smo intuitivno napravili u poglavlju na početku ovog dijela, trebat će nam aksiom izbora). Uvid u to može se vidjeti na primjeru konačnih skupova: iako općenite kardinalne brojeve još ne znamo definirati unutar teorije skupova, konačni kardinalni brojevi su upravo prirodni brojevi (uključujući nulu), za koje smo vidjeli da postoje prirodne definicije: $n := \{0, 1, \ldots, n-1\}$. Iako se na prvi pogled takva definicija čini cirkularnom, pokazuje se da nije, i upravo svojstvo koje omogućuje da se takve definicije mogu "legalno" provoditi, bit će ono što razlikuje *dobro uređene skupove*, kojima ćemo se ubuduće baviti, od uobičajenih TUSova.

Naravno, u slučaju prirodnih brojeva, radi se o principu rekurzivne definicije, koji se zasniva na istoj ideji kao i princip matematičke indukcije. Pokazat će se da, kad prirodne brojeve proširimo na općenite ordinale, ista ideja i dalje funkcionira, i omogućuje *princip transfinitne indukcije* i *definicije transfinitnom rekurzijom* — što će nama biti prilično bitno, jer omogućuje rješavanje široke klase zadataka, na sličan način kao i matematička indukcija na prirodnim brojevima.

2. Dobro uređeni skupovi

Za PUS $(A, <)$ kažemo da je *dobro uređen* (skraćeno *DUS*), ako svaki njegov neprazan podskup ima najmanji element. Lako je vidjeti da je svaki DUS totalno uređen: kad bi x i y bili njegovi neusporedivi elementi, tada njegov dvočlani podskup $\{x, y\}$ ne bi mogao imati najmanji element. Zbog tog svojstva, kao i činjenice da se u TUSovima podudaraju pojmovi najmanjeg i minimalnog elementa, često se navodi ekvivalentna definicija: DUS je TUS u kojem svaki neprazan podskup ima minimum. Treba samo napomenuti da to nije ekvivalentno zahtjevu da svaki podskup ima minimalan element, ako a priori ne znamo da se radi o TUSu. Takvi skupovi (koji nisu nužno totalno uređeni, ali su parcijalno uređeni i svaki neprazan podskup im ima minimalan element) zovu se *dobro utemeljeni skupovi* — no skraćenica DUS se ovdje odnosi na dobro *uređene* skupove.

Budući da su DUSovi samo specijalni TUSovi, na njima je moguće promatrati sličnosti, invarijante i ordinalne tipove. Važna činjenica je da je "biti DUS" invarijanta sličnosti, tako da za svaka dva skupa koji imaju isti ordinalni tip, ili su oba DUSovi, ili nijedan od njih nije DUS. Drugim riječima, sâmi ordinalni tipovi se dijele u dvije skupine: ordinalni tipovi DUSova, i ordinalni tipovi skupova koji nisu DUSovi. Ubuduće ćemo se fokusirati na ove prve, i zvat ćemo ih *ordinalni brojevi*.

Svi konačni ordinalni tipovi (0, 1, 2,...) su ujedno i ordinalni brojevi, što se lako vidi matematičkom indukcijom: 0 je ordinalni broj jer TUS tipa 0 uopće nema nepraznih podskupova, a ako je k ordinalni broj, neprazni podskup B TUSa A tipa $k+1$, za koji smo dokazali da ima najveći element $\max A =: a$, je ili $\{a\}$, ili ima neprazan presjek s $A \setminus \{a\}$. U svakom slučaju ima najmanji element: u prvom slučaju je to a, njegov jedini element, a u drugom je to upravo $\min(B \setminus \{a\})$ (koji postoji po pretpostavci indukcije, jer je $B \setminus \{a\}$ neprazan podskup skupa $A \setminus \{a\}$ tipa k — te je manji i od a, jer je a najveći element).

Postoje li beskonačni DUSovi? Naravno, postoje — najpoznatiji primjer je skup prirodnih brojeva $\mathbb{N}$. Da je to DUS, lako se vidi jednom kad smo vidjeli (u prošlom odlomku) da su njegovi elementi ordinali: svaki neprazan podskup $A \subseteq \mathbb{N}$ ima bar jedan element $n = \{0, \ldots, n-1\}$. Ako n nije najmanji element od A, to znači da u A postoje elementi manji od n, odnosno da je $A \cap n$ neprazan podskup od n, i kao takav ima najmanji element, koji je ujedno i najmanji element od A. U svakom slučaju, dakle, A ima najmanji element — odnosno, $\mathbb{N}$ je, uz standardni uređaj, DUS, te je ω ordinal.

Primijetimo frazu "uz standardni uređaj" u gornjem odlomku. Dakako, mi znamo što je standardni uređaj za prirodne brojeve, no čini se da je on definiran "naknadno", nakon što smo prirodne brojeve već izgradili. S druge strane, skupovi već imaju svoj intrinsični uređaj, relaciju $\subset$. Lako je vidjeti da se, na prirodnim brojevima, relacija $\subset$ podudara s njihovim standardnim uređajem — što znači da ne moramo specificirati nikakav poseban uređaj za DUSove prirodnih brojeva; najprirodniji uređaj na njima već je zapisan u samim elementima, preko relacije $\subset$.

Štoviše, pokazuje se da vrijedi i bolje od toga: osnovna relacija u teoriji skupova, relacija $\in$ ("biti element"), može se upotrijebiti za uređivanje ordinalâ, budući da je ona na svakom ordinalu tranzitivna i koneksna (dokaz na predavanjima) — irefleksivnost i dobra utemeljenost propisani su aksiomom utemeljenosti. To je bolje od relacije $\subset$ zato što se može obrnuti: iako svaki podskup proizvoljnog ordinala ne mora biti ordinal, svaki *element* proizvoljnog ordinala ponovo je (manji) ordinal. Na taj način, ordinal je upravo skup svih manjih ordinala, izgrađen na takav način da to ne bude cirkularno.

3. Hijerarhija ordinalâ

Pogledajmo kako to izgleda u početku: želimo konstruirati neki ordinal α. To mora biti skup svih manjih ordinalâ, a budući da još nemamo nijedan ordinal, jedini način da to ne bude cirkularno je da bude $\alpha = \emptyset$. To je najmanji ordinal, i kao što već znamo, označava se s 0.

Nakon toga, ako želimo konstruirati novi ordinal, to ne smije biti $\emptyset$ ("svi prazni skupovi su međusobno jednaki", a mi želimo novi ordinal) — dakle, mora sadržavati neki element β. Po gornjem principu, to mora biti (manji) ordinal, a jedini koji zasad imamo je $\emptyset$. Odnosno, $\emptyset$ jedini dolazi u obzir za "članstvo" u našem novom ordinalu, koji onda mora biti $\{\emptyset\}$. To je sljedeći ordinal nakon 0, i znamo da se označava s 1.

Sljedeći korak: novi ordinal treba biti skup svih manjih ordinalâ. 0 je manja od svakog ordinala, a 1 je manji od svakog osim 0. S druge strane, jedino oni dolaze u obzir za članstvo u ordinalu kojeg upravo izgrađujemo, ako želimo izbjeći cirkularnost. Dakle, novi ordinal je $\{0,1\}$, prvi nakon (0 i) 1, i zove se 2.

I tako dalje... prirodno dobivamo $3 := \{0,1,2\}$, $4 := \{0,1,2,3\}$, i ostale prirodne brojeve kao ordinale, zadržavajući princip da novoizgrađeni ordinal mora biti skup svih do tada izgrađenih ordinalâ, koji će onda biti jedini koji su manji od njega. Na taj način gledano, nakon što smo izgradili sve prirodne brojeve, prirodni sljedeći korak je uzeti skup svih njih, uređen standardno, i nazvati ga ω. Primijetimo da je ω *skup svih konačnih* ordinalâ, a isto tako je i *prvi beskonačni* ordinal.

Koje ordinale dosad imamo izgrađene? Sve prirodne brojeve (0, 1, 2,...), kao i ω, koji je od svih njih najveći. Ako sad uzmemo skup svih do sad izgrađenih ordinalâ, $\{0,1,2,\ldots,\omega\} = \omega \cup \{\omega\}$, uređen upravo opisanom relacijom, vidimo da je to DUS: jer svaki njegov neprazan podskup je ili $\{\omega\}$, ili ima neprazan presjek s $\{0,1,2,\ldots\}$. U prvom slučaju mu je najmanji element ω, a u drugom je to najmanji element tog presjeka. Vidimo ne samo da smo dobili DUS, već vidimo da je način dokazivanja potpuno paralelan s onim kojim smo dokazali dobru uređenost za sljedbenike prirodnih brojeva (matematičkom indukcijom).

Lako je to i generalizirati (jednom kad uočimo $4 = 3\cup\{3\}$, $3 = 2\cup\{2\}$, i slično): za proizvoljni ordinal α, skup $\alpha \cup \{\alpha\}$ je ponovo ordinal, koji se označava s α^+, i zove *(ordinalni) sljedbenik* od α. Dakle, gore dobiveni ordinal je ω^+, koji se još i označava s $\omega + 1$, po uzoru na $3^+ = 3+1 (= 4)$, $2^+ = 2+1 (= 3)$, itd. Primijetimo sličnost (i različitost) sa zbrajanjem ordinalnih *tipova*: $\omega + 1$ bio bi ordinalni tip disjunktne unije dva skupa A i B, od kojih je A tipa ω, a B tipa 1 (dakle, ima samo jedan element x), uređene tako da su svi elementi prvog skupa prije x, a međusobno su uređeni kao što su bili uređeni u A. To se događa i ovdje — jedino što u slučaju ordinalâ, imamo točno precizirano što je A, a što B ($A = \omega \land B = \{\omega\}$), te nam ista relacija koja nam je služila za uređaj u A ("biti element"), služi i u $A\cup B$. To ujedno znači da se moramo oprostiti s antileksikografskim uređajem kao metodom uređivanja ordinalâ (jer u $A \cup B$ više nisu parovi), no o tome više kasnije.

Sada možemo nastaviti i dalje: novi ordinal bit će $\{0,1,2,\ldots,\omega,\omega^+\} = \omega^+\cup\{\omega^+\}$, odnosno sljedbenik od ω^+, kojeg je onda prirodno označiti s $\omega + 2$. Primijetimo da je i to u skladu sa zbrajanjem ordinalnih tipova: tip od $\{0,1,2,\ldots\}$ je ω, dok je tip njemu disjunktnog skupa $\{\omega,\omega^+\}$ jednak 2. Gornji ordinal je njihova unija, uređena tako da svi elementi prvog skupa budu prije svih elemenata drugog.

Sljedeći ordinal je $\{0, 1, 2, \dots, \omega, \omega + 1, \omega + 2\}$, sljedbenik od $\omega + 2$, i označava se s $\omega+3$. Jasno je da sada možemo istim postupkom izgraditi sve ordinale oblika $\omega + n$, za prirodni n.

Nakon što to učinimo, skup svih do tad izgrađenih ordinalâ bit će $\{0, 1, 2, \dots, \omega, \omega + 1, \omega + 2, \dots\}$, odnosno disjunktna unija dva skupa, oba tipa ω, uređena tako da su svi elementi prvog (oblika n) prije svih elemenata drugog (oblika $\omega + n$). To je dakle $\omega + \omega$, koji se često označava i s $\omega \cdot 2$ (**ne** 2ω — više o razlozima kasnije). Primijetimo da je taj ordinal sličan skupu $\mathbb{N} \times 2$, preko očite sličnosti

$$(a, b) \mapsto \begin{cases} a & , b = 0 \\ \omega + a & , b = 1 \end{cases} ,$$

no, kao što smo već vidjeli kod zbrajanja, njegovi elementi općenito nisu uređeni parovi, tako da doslovni antileksikografski uređaj na njemu nema smisla. Ipak, to nam daje ideju: možemo prirodni broj n zapisati kao $0 + n = \omega \cdot 0 + n$, te $\omega + n$ kao $\omega \cdot 1 + n$, i onda antileksikografski uspoređivati parove ("slobodni koeficijent", "koeficijent uz ω").

Sljedeći ordinal je njegov sljedbenik, $(\omega\cdot2)^+ = \omega\cdot2+1 = \omega\cdot2\cup\{\omega\cdot2\} = \{0, 1, 2, \dots, \omega, \omega + 1, \dots, \omega \cdot 2\}$. Nakon njega dolaze $\omega \cdot 2 + 2$, $\omega \cdot 2 + 3$, i općenito svi ordinali oblika $\omega \cdot 2 + n$, gdje je n prirodan broj.

Sada bismo opet mogli gledati skup svih do-ovog-trena-definiranih ordinalâ, no možemo to i pojednostavniti. Primijetimo da je ω ne samo skup svih prirodnih brojeva, već i njihov *supremum*: najmanji ordinal veći od svih prirodnih brojeva. Pojednostavljenje dolazi kad shvatimo da za to ne moramo uzeti sve prirodne brojeve: na primjer, ω je supremum skupa svih prirodnih brojeva većih od 5, kao i supremum skupa svih parnih prirodnih brojeva, pa čak i skupa svih prostih brojeva. Svaki beskonačan podskup od ω ima supremum ω, odnosno kofinalan je u ω. Jednako tako, za supremum $\omega \cdot 2$ nam je dovoljno uzeti samo ordinale oblika $\omega+n$, jer su svi oni veći od svih prirodnih brojeva. Tako je i $\omega \cdot 3$, naš sljedeći ordinal, supremum svih ordinalâ oblika $\omega \cdot 2 + n$, no u sebi sadrži i ordinale oblika $\omega + n$, kao i sve prirodne brojeve.

Imajući dvije osnovne operacije, sljedbenik i supremum, dalje nastavljamo izgrađivati hijerarhiju. Operacijom sljedbenika od $\omega\cdot3$ dobivamo $\omega \cdot 3 + 1$, kao i sve ordinale oblika $\omega \cdot 3 + n$. Operacijom supremuma od svih njih dobivamo $\omega \cdot 3 + \omega = \omega \cdot 4$. Na njega također možemo primijeniti isti postupak, i dobiti $\omega \cdot 5$. I tako dalje. . .

Vidimo da na taj način možemo dobiti sve ordinale oblika $\omega \cdot i + j$, gdje su i i j prirodni brojevi. Oni se uspoređuju (dokažite!) baš kao što se antileksikografski uspoređuju parovi (j, i), elementi Kartezijevog kvadrata $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$. Zato je prirodno skup takvih ordinalâ, tako uređen, zvati $\omega^2 = \omega \cdot \omega$.

Treba li nam za njegovo dobivanje nova operacija? Ne — $\omega^2 = \omega \cdot \omega$ je jednostavno supremum svih ordinalâ oblika $\omega \cdot n$, za $n \in \omega$; baš kao što je $\omega \cdot 2 = \omega + \omega$ supremum svih ordinalâ oblika $\omega + n$, za $n \in \omega$. Vidimo da su, shvativši supremum po $n \in \omega$ kao neku vrstu limesa po n (što je i prirodno, jer se ordinali izgrađuju u beskonačnost samo na jednu stranu, prema gore), zbrajanje i množenje neprekidni u ω (komutiraju sa supremumom), kao i u ostalim ordinalima koji su dobiveni operacijom supremuma. Također, zbog analogije s limesima, takvi ordinali se još zovu *granični*.

Možemo nastaviti i dalje: sljedbenik od ω^2 je $\omega^2 + 1$, njegov sljedbenik je $\omega^2 + 2$, i tako možemo dobiti sve ordinale oblika $\omega^2 + n$, za prirodne n. Njihov supremum je $\omega^2 + \omega = \omega \cdot \omega + \omega \cdot 1 = \omega \cdot (\omega + 1)$, jer za ordinale vrijede svi zakoni kao i za ordinalne tipove, pa tako i distributivnost množenja slijeva prema zbrajanju.

Sljedbenik tog ordinala je $\omega^2 + \omega + 1$, te tako možemo dobiti sve ordinale oblika $\omega^2 + \omega + n$, čiji je supremum $\omega^2 + \omega \cdot 2 = \omega \cdot (\omega + 2)$. Jednako dobivamo i $\omega^2 + \omega \cdot 3$, i općenito $\omega^2 + \omega \cdot i + j$, za prirodne i i j, odnosno $\omega^2 + \alpha$, gdje je $\alpha \in \omega^2$.

Supremum svih takvih je, po neprekidnosti zbrajanja, $\omega^2 + \omega^2$, odnosno $\omega^2 \cdot 2$. Na njega također možemo dodavati elemente iz ω^2, i tako u supremumu dobiti $\omega^2 \cdot 3$. Analogno možemo i dalje, do $\omega^2 \cdot 4$, te $\omega^2 \cdot 5, \ldots$ Primijetimo još jednu zanimljivost vezanu uz ordinale koje smo do sada izgradili: na primjer, $\omega^2 \cdot 3 + \omega \cdot 5 + 7$ se može, analogno gornjoj reprezentaciji (i, j) za brojeve do ω^2, shvatiti kao uređena trojka $(7, 5, 3)$ (i takve uređene trojke se mogu uspoređivati antileksikografski baš jednako kao i sami ordinali) — ali se može shvatiti i kao "troznamenkasti ordinal" zapisan u bazi ω, sa znamenkom "stoticâ" jednakom 3, znamenkom "deseticâ" jednakom 5, i znamenkom "jedinicâ" jednakom 7. Općenito, znamenke u tom zapisu su proizvoljni prirodni brojevi. Takav pogled na ordinale zove se *Cantorova normalna forma*, i pomaže pri shvaćanju ponašanja ordinalâ s obzirom na razne operacije: na primjer, uspoređivanje i zbrajanje ordinalâ obavlja se jednako kao i za dekadske brojeve. Štoviše, zbrajanje je još jednostavnije, jer ne postoji mogućnost prijenosa u višu znamenku: zbroj dva prirodna broja ne može prijeći ω.

Supremum svih troznamenkastih ordinalâ je prvi četveroznamenkasti: ω^3. Pomoću njega se mogu dobiti i ostali četveroznamenkasti, iz njih operacijom supremuma peteroznamenkasti (počevši s ω^4), i tako dalje.

Kao i množenje i zbrajanje, i potenciranje je neprekidno, te tako supremum svih ω^n po $n \in \omega$ (odnosno supremum svih konačnoznamenkastih) iznosi ω^ω. To je prvi ordinal koji u Cantorovoj normalnoj formi ima beskonačno mnogo znamenaka, koje možemo zamišljati kao "jedinica, i nakon nje ω nulâ". No njime hijerarhija ordinalâ nipošto ne završava: na dobro poznate načine iz njega možemo dobiti ordinale oblika $\omega^\omega + n$, zatim $\omega^\omega + \omega \cdot n$, $\omega^\omega + \omega^n$, $\omega^\omega \cdot n$, te kao njihov supremum, $\omega^\omega \cdot \omega = \omega^{\omega+1}$.

Sad vidimo da nam se, kad neke posebne naše ordinale zapišemo u Cantorovoj normalnoj formi, u eksponentu od ω ponavlja hijerarhija ordinala od početka: $1 = \omega^0$, $\omega = \omega^1$, $\omega^2, \dots$, ω^ω, $\omega^{\omega+1}$. (Naravno, ti "posebni" više **nisu** sljedbenici jedan drugome, i između njih sada ima beskonačno mnogo ordinalâ.) Ako sada cijelu priču od 0 do ω^ω preselimo u eksponent (a moguće ju je preseliti zahvaljujući neprekidnosti potenciranja), kao rezultat dobivamo ordinal ω^{ω^ω} (kao i standardno potenciranje, shvaća se odozgo prema dolje: $\omega^{(\omega^\omega)}$). To možemo shvatiti kao novu operaciju, "hiperpotenciranje", i označiti taj broj s $\omega \uparrow 3$ — ω^ω je onda $\omega \uparrow 2$. Vidimo da, ako prirodno shvatimo ω kao $\omega \uparrow 1$ i 1 kao $\omega \uparrow 0$, možemo napraviti niz $\omega \uparrow n$, po $n \in \omega$, čiji supremum će biti novi ordinal, koji možemo označiti s $\omega \uparrow \omega$ (još se označava s ϵ_0).

Naravno, možemo i dalje (pokušajte za domaću zadaću zamisliti nastavak hijerarhije) — uvijek možemo i dalje, poštujući osnovni princip: relacija "$\in$" je osnovna relacija uređaja među ordinalima, odnosno svaki ordinal je upravo skup svih onih koji su prije njega. Također, treba biti svjestan da pričama poput gornje nikada nećemo prijeći neke granice: na primjer, svi ordinali koje smo izgradili gore (do ϵ_0) su najviše prebrojivi. Iako nam za dokazati postojanje neprebrojivih ordinalâ općenito treba aksiom izbora, čini se da je nerealno očekivati da na gornji način možemo dobiti sve ordinale. To će postati puno jasnije kada (na predavanjima) otkrijemo da su ordinali upravo indeksi razinâ kumulativne hijerarhije, koja bi trebala u sebi sadržavati sve skupove koje uopće možemo zamisliti i/ili trebati u matematici.

4. Zbrajanje ordinalâ

No ono što također treba imati na umu je da su nam gornje operacije, sljedbenik i supremum, dovoljne da od 0 dobijemo *sve* ordinale — iako broj, pa i struktura, korakâ potrebnih za takvo što nikako nisu ograničeni. Odnosno, preciznije, svaki ordinal je ili prazan (nula), ili sljedbenik nekog ordinala, ili supremum nekog skupa ordinalâ (gore smo rekli da se takvi ordinali zovu granični). Koristeći to, možemo definirati funkcije i operacije na ordinalimâ, definirajući ih posebno na nuli, na sljedbenicima, i na graničnim ordinalima. Evo jednog važnog primjera, koji smo neformalno već vidjeli gore:

Zbrajanje je (binarna) operacija, što znači da ima dva argumenta — no kao i sve operacije na ordinalima, definira se s obzirom na "drugi" (desni) argument. Odnosno, za svaki (fiksni) ordinal α, definiramo kako se on zbraja s nulom, sljedbenicima i graničnima. Ako je drugi pribrojnik 0, naravno, definirat ćemo zbroj da bude α (što je u skladu s definicijom zbrajanja za ordinalne tipove — "dodali" smo prazan skup na kraj nekog skupa ordinalnog tipa α):

$$\alpha + 0 := \alpha \ .$$

Ako je drugi pribrojnik sljedbenik, recimo β^+, trebamo definirati što znači $\alpha + \beta^+$. No to možemo (bar načelno) činiti kao što smo i izgrađivali hijerarhiju ordinalâ u prošloj točki: od manjih prema većima. To podrazumijeva da, u trenutku kada nas zanima koliko je $\alpha + \beta^+$, već znamo koliko je $\alpha + \gamma$ za sve $\gamma \in \beta^+ = \beta \cup \{\beta\}$, specijalno znamo koliko je $\alpha + \beta$. Pogledajmo sad $\alpha + \beta^+$ kao ordinalni tip: sastoji se od nekog skupa tipa α, nakon kojeg dolazi $\beta \cup \{\beta\}$, neki skup tipa β i na kraju još jedan (maksimalni) element, označimo ga s x. Ako sad pogledamo taj TUS bez elementa x, vidimo da se on sastoji od dva dijela jedan nakon drugog, jednog tipa α i drugog tipa β — odnosno upravo je tipa $\alpha + \beta$. Ako tu sličnost označimo s f, i dodefiniramo je u x sa $\tilde{f}(x) := \alpha + \beta$, imamo sličnost između našeg početnog TUSa, tipa $\alpha + \beta^+$, i sljedbenika od $\alpha + \beta$. Dakle, prirodno je definirati

$$\alpha + \beta^+ := (\alpha + \beta)^+ \ .$$

Vidimo da je operacija sljedbenika "prešla" s desnog pribrojnika na rezultat. Istaknimo još jednom: usprkos simetričnoj oznaci + za zbrajanje, operandi se tretiraju prilično drugačije: lijevi je parametar funkcije koja nas zanima, koja preslikava desni operand β u rezultat $\alpha + \beta$. Sva lijepa svojstva od te funkcije koja možemo zahtijevati, odnose se na vezu β s rezultatom, i često nemaju direktne veze s α. Na primjer, operacija sljedbenika ne "prelazi" tako lijepo s lijevog pribrojnika na rezultat, i zaista, u mnogim slučajevima će biti $\alpha^+ + \beta \neq (\alpha + \beta)^+$, kao što ćemo vidjeti na primjerima. Također, kao direktna posljedica toga, zbrajanje općenito neće biti komutativno.

Sličnim argumentom kao za operaciju sljedbenika (detaljnije kad budemo dokazivali punu neprekidnost zbrajanja), možemo vidjeti da operacija supremuma prirodno prelazi s desnog pribrojnika na zbroj, pomoću čega možemo definirati zbrajanje s graničnim ordinalima:

$$\alpha + \lambda := \sup_{\beta \in \lambda} (\alpha + \beta) \quad \text{ako je} \quad \lambda = \sup_{\beta \in \lambda} \beta \ ,$$

odnosno, ako je λ granični ordinal (kao što se u teoriji skupova grčka slova s početka alfabeta obično koriste za ordinale, slovo λ se obično koristi specijalno za granične ordinale).

Pomoću gornja tri pravila možemo zbrajati proizvoljne ordinale. Evo nekih primjerâ:

Izračunajmo $3+2$.

<u>*Rj.:*</u>
$$\begin{aligned} 3+2 &= && \text{(definicija od 2 kao sljedbenika od 1)}\\ &= 3+1^+ = && \text{(pravilo zbrajanja sa sljedbenikom)}\\ &= (3+1)^+ = && \text{(definicija 1 kao sljedbenika od 0)}\\ &= (3+0^+)^+ = && \text{(zbrajanje sa sljedbenikom, u zagradi)}\\ &= ((3+0)^+)^+ = && \text{(pravilo zbrajanja s nulom)}\\ &= (3^+)^+ = && \text{(definicija 4 kao sljedbenika od 3)}\\ &= 4^+ = 5 && \text{(definicija 5 kao sljedbenika od 4)} \end{aligned}.$$

Općenito, aritmetika prirodnih brojeva je podteorija aritmetike ordinalâ: svaka tvrdnja o zbrajanju (i množenju i potenciranju) konkretnih prirodnih brojeva vrijedi i promatrajući ih kao ordinale — na primjer, $52+65=117$. No to ne znači da *zakoni* — univerzalne tvrdnje o operacijama na prirodnim brojevima — vrijede i za ordinale. Na primjer, zbrajanje nije komutativno, kao što se vidi iz sljedećeg primjera:

Koliko je $1+\omega$?
<u>*Rj.:*</u> Budući da je desni pribrojnik, omega, granični, rezultat dobivamo pomoću pravila za zbrajanje s graničnim ordinalom: $1+\omega = 1+\sup_{n\in\omega} n = \sup_{n\in\omega}(1+n)$. Sada je još samo ostalo odrediti taj supremum, supremum skupa svih $1+n$, gdje je $n\in\omega$. To je skup $\{1,2,3,\ldots\}$, za koji se lako vidi da je kofinalan u ω, odnosno supremum mu je jednak ω (konkretno, svi članovi su mu manji od ω, pa je ω gornja međa, no nijedan broj manji od ω — dakle, prirodan broj n — nije gornja međa, jer u skupu postoji od njega veći $1+n$). Dakle, $1+\omega=\omega$, odnosno komutativnost zbrajanja ne vrijedi, jer $\omega+1\neq\omega$ (desna strana je element lijeve, pa ne mogu biti jednake po aksiomu utemeljenosti).

Da bismo gornja razmišljanja egzaktnije provodili, primijetimo da za supremume (hiper)nizova ordinalâ vrijedi "princip sendviča": ako β_ι smjestimo između γ_ι i δ_ι, za svaki $\iota\in\zeta$, tada će vrijediti i $\sup_{\iota\in\zeta}\gamma_\iota \le \sup_{\iota\in\zeta}\beta_\iota \le \sup_{\iota\in\zeta}\delta_\iota$.

Konkretno, u gornjem slučaju, $1+n=n+1$ (jer je to zbroj prirodnih brojeva) je očito veće od n, a manje od ω. Dakle, supremum takvih ordinala je veći (ili jednak) od $\sup_{n\in\omega} n=\omega$, a manji ili jednak od $\sup_{n\in\omega}\omega=\omega$. Odnosno, jednak je ω.

DZ: dokažite $3+\omega=\omega$.

Zapravo, to je početak principa apsorpcije, koji kaže (otprilike) da se "bitno manji" ordinal može apsorbirati u "bitno veći", ako se s njim zbraja tako da je manji slijeva, a veći zdesna. No za općenitije primjere, trebamo se malo bolje upoznati sa zakonima koji vrijede za operacije u svijetu ordinalâ.

5. Množenje i potenciranje ordinalâ

Slično kao što smo definirali zbrajanje s fiksnim ordinalom, možemo definirati i množenje:

$$\alpha \cdot 0 := 0$$
$$\alpha \cdot \beta^+ := \alpha \cdot \beta + \alpha$$
$$\alpha \cdot \lambda := \sup_{\beta \in \lambda} (\alpha \cdot \beta) \ .$$

Primijetimo da, kao i kod zbrajanja, rezultate izgrađujemo postepeno: u trenutku kada nas zanima koliko je $\alpha \cdot \lambda$, već znamo koliko je $\alpha \cdot \beta$ za sve β izgrađene prije λ. Također, obratimo pažnju na drugo pravilo: u trenutku kada izgrađujemo operaciju množenja, pretpostavljamo da već imamo potpuno izgrađenu operaciju zbrajanja (s proizvoljnim ordinalom: primijetimo da se lijevi pribrojnik mijenja).

Analogno možemo i za potenciranje, koristeći množenje — s jednim malim izuzetkom. Naime, sve operacije koje smo dosada definirali bile su prirodno rastuće. To nam je omogućavalo da željenu "neprekidnost" u graničnim ordinalima postignemo jednostavnom primjenom supremuma na sve prethodne vrijednosti. Jedini izuzetak je potenciranje s nulom kao bazom: $0^0 = 1$, dok je $0^n = 0$ za sve ostale prirodne n. Htjeli bismo da 0^ω bude 0, no za to moramo u supremumu "preskočiti" slučaj 0^0. Za ostale baze, potenciranje je rastuće, pa također smijemo preskočiti nulu u eksponentu. Zato je definicija:

$$\alpha^0 := 1$$
$$\alpha^{\beta^+} := \alpha^\beta \cdot \alpha$$
$$\alpha^\lambda := \sup_{0 \neq \beta \in \lambda} \alpha^\beta \ .$$

Naravno, ako smo sigurni da se u bazi ne može pojaviti nula, možemo slobodno koristiti jednostavnije pravilo $\alpha^\lambda = \sup_{\beta \in \lambda} \alpha^\beta$.

Primjer: izračunajmo $3 \cdot 2$.

<u>*Rj.:*</u>
$$\begin{aligned} 3 \cdot 2 &= && \text{(definicija 2 kao sljedbenika od 1)} \\ = 3 \cdot 1^+ &= && \text{(pravilo množenja sa sljedbenikom)} \\ = 3 \cdot 1 + 3 &= && \text{(definicija 1 kao sljedbenika od 0)} \\ = 3 \cdot 0^+ + 3 &= && \text{(pravilo množenja sa sljedbenikom)} \\ = (3 \cdot 0 + 3) + 3 &= && \text{(pravilo množenja s nulom)} \\ = (0 + 3) + 3 & \end{aligned} \ .$$

Dalje je samo zbrajanje:

$$(0+3)+3 = (0+2^+)+3 = (0+2)^+ + 3 = (0+1^+)^+ + 3 = ((0+1)^+)^+ + 3 =$$
$$= ((0+0^+)^+)^+ + 3 = (((0+0)^+)^+)^+ + 3 = ((0^+)^+)^+ + 3 = (1^+)^+ + 3 =$$
$$= 2^+ + 3 = 3 + 3 = 3 + 2^+ = (3+2)^+ = 5^+ = 6 \ .$$

DZ: izračunajte 2^2.

Naravno, ovakve stvari nećemo ubuduće računati: koristit ćemo svoje znanje aritmetike u $\mathbb{N}$. No dobro je na početku vidjeti kako se gornja pravila koriste u jednostavnim situacijama.

Koliko je $3 \cdot \omega$?
Rj.: Budući da je ω granični ordinal, bit će $3 \cdot \omega = \sup_{n\in\omega}(3 \cdot n)$. Taj supremum je očito supremum skupa kofinalnog u ω ($\{0, 3, 6, 9, \ldots\}$), pa iznosi ω. Mogli smo i metodom sendviča: $3 \cdot n$ je očito veće ili jednako n, a manje od ω. Dakle supremum mu je između $\sup_{n\in\omega} n = \omega$ i $\sup_{n\in\omega} \omega = \omega$, pa iznosi ω.

Često se javljaju supremumi gornjeg tipa, i sve za njih je zajedničko da su to supremumi *neograničenih nizova prirodnih brojeva* (skraćeno NNPB), te iznose ω. Dakle, da bismo opravdali da je supremum nekog niza (odnosno njegove slike) jednak ω, moramo vidjeti da su svi njegovi članovi prirodni brojevi, i da je on neograničen. Oba uvjeta su nužna. Evo još jednog primjera:

Koliko je n^ω, za prirodni n?
Rj.: Budući da je ω granični ordinal, tražimo

$$\sup_{0\neq k\in\omega} n^k = \sup\{n, n^2, n^3, \ldots\} .$$

Ako je $n \geq 2$, to je zaista NNPB ($n^k \geq 2^k > k$), pa je $n^\omega = \omega$. No za manje n, to nije neograničeno: za $n = 1$, niz je $1, 1, 1, \ldots$, sa supremumom 1, a za $n = 0$, niz je (zahvaljujući gore opisanom izuzetku) $0, 0, 0, \ldots$, sa supremumom 0. Dakle, možemo reći

$$n^\omega = \begin{cases} n\,, & n < 2 \\ \omega\,, & n \geq 2 \end{cases} .$$

Koliko je $2 \cdot (\omega + 1)$?
Rj.: $2 \cdot (\omega + 1) = 2 \cdot \omega^+ = 2 \cdot \omega + 2 = \sup_{n\in\omega}(2 \cdot n) + 2 = \omega + 2$, budući da je $0, 2, 4, 6, \ldots$ NNPB.

DZ: izračunajte $5^{\omega+1}$.