Teorija skupova

predavanja

Vedran Čačić

akademska godina 2023./24.

Sadržaj

0 Uvod, jezik i motivacija

0.1 Logistika kolegija

Polaganje:

- Kolokvij, 20 bodova, 120 minuta. Sadrži i teorijska pitanja. Neobavezan ali preporučen. Predstavlja pripremu za pismeni ispit. Bodovi se pribrajaju pismenom.
- Pisani ispit, 100 bodova, 120 minuta. Zadaci iz čitavog gradiva (s naglaskom na drugi dio). 45 bodova za prolaz.
- Usmeni ispit — samo za studente koji prođu pismeni. Na usmenom se određuje konačna ocjena, uzevši u obzir bodove s pisanog ispita (i kolokvija).

Nastava (svi kontaktni podaci su na Merlinu):

- predavanja: Maja Resman i Vedran Čačić
- vježbe: Matea Čelar i Lucija Validžić
- demonstrature: (demonstratori će biti objavljeni naknadno)

Web-stranica: https://web.math.hr/nastava/ts/index.php

O literaturi

Vuković, *Teorija skupova — predavanja* sadrži bilješke po kojima su se ranije držala predavanja iz ovog kolegija. Osnovne razlike su drugačiji redoslijed gradiva, dvostruki pristup (naivno i aksiomatski), i puno više tvrdnji ostavljenih za vježbu čitatelju.

Dobar dio ovih bilježaka nastao je prema Hrbáček i Jech, *Introduction to Set Theory*: ta knjiga puno dublje pokriva čitavo gradivo koje ćemo obraditi, i mnogo više od toga.

Također postoji i Čačić i dr., *Zbirka zadataka iz teorije skupova*, koja se trenutno osvježava i priprema za novo izdanje.

Nekoliko diplomskih radova koji mogu poslužiti za produbljivanje znanja o nekim temama vezanim uz teoriju skupova:

- Bašić, *Ordinalni kalkulator* — za definiciju i svojstva operacija na ordinalima te provjeru rezultata ordinalne aritmetike

- Gunja, *Zornova lema i srodne tvrdnje* — za tvrdnje ekvivalentne aksiomu izbora te „elementarni” dokaz Zornove leme
- Doko, *Kardinalna aritmetika* — za definiciju i svojstva operacija na kardinalima

Oni koje zanima daljnji razvoj teorije skupova mogu ponešto naći u magistarskom radu Čačić, *Nezavisnost i relativna konzistentnost aksioma izbora i hipoteze kontinuuma*.

0.2 Osnovno pitanje

Na prvi pogled, htjeli bismo strogo odgovoriti na pitanje „Što je skup?”. Na drugi pogled, matematičke grane često se ne bave individualnim objektima, već *strukturama* u kojima ti objekti prirodno „prebivaju”.

Na linearnoj algebri niste čuli općenit odgovor na pitanje „što je vektor?”, osim kroz neke geometrijske primjere. Čuli ste, odnosno naveli aksiome koji odgovaraju na pitanje, što je *vektorski prostor*, a vektor je onda bilo koji element vektorskog prostora — bio on zapravo n-torka, klasa ekvivalencije usmjerenih dužina, funkcija, ili nešto četvrto.

Na vjerojatnosti i statistici niste čuli općenit odgovor na pitanje „što je slučajni događaj?”, osim u obliku nekih fizikalnih interpretacija. Čuli ste, odnosno naveli aksiome koji odgovaraju na pitanje, što je *vjerojatnosni prostor*, a slučajni događaj je onda bilo koji izmjeriv podskup vjerojatnosnog prostora.

Slično je i u teoriji skupova: navest ćemo aksiome koji opisuju *kumulativnu hijerarhiju*, matematičku strukturu u kojoj se (na njenim *razinama*) nalaze skupovi. Jedan mali problem je u tom što je teorija skupova „osnovnija” od linearne algebre i vjerojatnosti: svaki vektorski i vjerojatnosni prostor je prije svega *skup*, s nekom dodatnom strukturom. Kumulativna hijerarhija *nije* skup (skupova), baš kao što ni vektorski prostor nije vektor (barem ne u samom tom prostoru).

0.3 Klase

Treba nam neki način da govorimo o proizvoljnim kolekcijama skupova. Tradicionalno se za to koristi pojam „klasa”. Kako možemo zadati klasu? Najjednostavniji način je tako da preciziramo neko *svojstvo* skupova. Recimo, možemo govoriti o klasi svih prebrojivih skupova, klasi svih skupova (to će biti unija svih razina kumulativne hijerarhije), klasi svih vektorskih prostora, klasi svih analitičkih funkcija, klasi svih praznih skupova, klasi svih skupova koji sadrže broj π kao element, ...

Uglavnom, elementi klasa su skupovi. Što su elementi skupova? Mogu biti brojevi, funkcije, razne matematičke strukture, ... ali velika snaga teorije skupova (i razlog zašto se smatra

temeljem matematike) je da se svi ti objekti mogu shvatiti kao skupovi specijalnog oblika (s vremenom ćemo vidjeti kako točno). Dakle, **elementi skupova su skupovi**.

Prva važna posljedica tog uvida: ne zanima nas „skup knjiga na polici u mom uredu", „skup studenata koji ove godine slušaju Teoriju skupova", pa čak niti „skup slova u riječi ‚skup'". Zanimaju nas skupovi matematičkih objekata, i to onih koji se na prirodan način mogu reprezentirati kao skupovi.

Druga posljedica: općenite klase ne mogu biti elementi skupova. Ne postoji „skup svih klasā". (Ne postoji ni „klasa svih klasā", jer smo se dogovorili da su klase kolekcije skupova.) Ne postoji čak niti jednočlan skup čiji je jedini element kumulativna hijerarhija. Drugim riječima, klase ne spadaju u „matematičke objekte koji se na prirodan način mogu reprezentirati kao skupovi".

Treća posljedica: iako klase nisu isto što i skupovi, *neke klase jesu skupovi*, ili su im barem jednake u smislu da predstavljaju kolekciju istih elemenata (skupova). Recimo, klasa svih praznih skupova jednaka je skupu svih praznih skupova, $\{\emptyset\}$ (pokazat ćemo da je to skup). Dobar dio početnog razvoja teorije skupova sastoji se u tome da za razne klase utvrdimo da su zapravo skupovi. Intuicija koju pritom treba imati je: jedini način na koji klasa može ne biti skup je da bude „prevelika", odnosno da ima previše elemenata. *Dovoljno male* klase su uvijek skupovi. Točno značenje pojma „dovoljno male" preciziraju **aksiomi** teorije skupova, koji za neke osnovne konstrukcije kažu da ako krenemo od skupova, ono što dobijemo su ponovo skupovi. Recimo, aksiom para kaže da je svaka dvočlana klasa skup, odnosno „dva elementa je uvijek dovoljno malo".

Zanimljivo je da obrat tvrdnje iz prethodnog odlomka vrijedi u potpunosti: *svaki skup je klasa*. Kao što smo rekli, za nas je svaki skup x kolekcija skupova, i zadana je svojstvom „biti element od x". Precizni opis što znači „svojstvo" dat ćemo kasnije, kad budemo govorili o jeziku teorije skupova.

0.4 Russellov paradoks

Da su klase „iznad" skupova, i općenito ne mogu biti reprezentirane skupovima, zaključili smo po analogiji. No to zapravo možemo i sasvim precizno dokazati.

Teorem 0.1 (Russell)**.** *Postoji klasa koja nije skup (tzv.* prava *klasa).*

Dokaz. Promotrimo klasu R svih skupova koji nisu elementi samih sebe. Dakle svojstvo skupa x koje karakterizira elemente klase R je $x \notin x$. To znači da za svaki skup x vrijedi: $x \in R$ ako i samo ako $x \notin x$. Kad bi R bio skup, tad bismo mogli tu ekvivalenciju primijeniti na $x := R$, i dobiti da je $R \in R$ ako i samo ako $R \notin R$, što je očito nemoguće. Jedini izlaz je da prihvatimo da je pretpostavka da je R skup pogrešna. (Tada paradoks nestaje, jer doista ne vrijedi $x \in x$ za $x = R$, ali iz toga ne možemo zaključiti $R \in R$ jer R nije skup. R sadrži *skupove* koji nisu elementi samih sebe.) □

Upravo dokazani teorem naziva se *paradoksom*, jer doista jest paradoks u tzv. *naivnoj* teoriji skupova, gdje ne pravimo razliku između skupova i klasa, i jednostavno sve kolekcije matematičkih objekata zovemo skupovima.

Teoriju skupova stvorio je njemački matematičar **Georg Ferdinand Ludwig Philipp Cantor**, jer mu je trebala za proučavanje konvergencije Fourierovih redova. Tek je kasnije primijetio da se na njoj može zasnovati gotovo čitava matematika. Iako je Cantor bio svjestan razlike između konzistentnih i inkonzistentnih mnoštava (ono što danas zovemo skupovima i pravim klasama), nije nigdje formalno precizirao razliku, već se rukovodio intuicijom. Friedrich Ludwig Gottlob Frege je pokušao tu njegovu teoriju formalizirati kroz aksiome, i u tako formaliziranoj teoriji Bertrand Arthur William Russell je pronašao upravo navedeni paradoks. No Cantor se nikada nije slagao s Fregeovom aksiomatizacijom, i nije smatrao da Russellov paradoks (kao ni mnogi drugi kasnije otkriveni paradoksi) bitno narušava njegovu teoriju.

Ipak, ako nemamo intuiciju kao Cantor, dobro bi bilo imati formalni opis konstrukcija odnosno svojstava koja generiraju skupove. Danas naivno/aksiomatsko nije binarna podjela: teorije su više ili manje naivne, ovisno o tome koliko precizno navode svoje aksiome i zaključuju. Mi ćemo aksiome vrlo precizno navesti, ali zaključivanja ćemo uglavnom provoditi neformalno.

0.5 Izgradnja kumulativne hijerarhije

Pojam *hijerarhija* ima mnogo definicija, ali sve u sebi sadrže neku ideju *stupnja*, ranga odnosno razine (nivoa). Tako i kumulativna hijerarhija ima razine, što smo već nagovijestili kada smo kazali da su elementi skupova ponovo skupovi. Kako smo u Russellovom paradoksu vidjeli da je problematična relacija „$x \in x$", jedan prirodni način da je izbjegnemo je da skupove gradimo po razinama: elementi skupa A jesu također skupovi, ali „niže razine" nego A. Primjerice, elementi skupa $\mathbb{R}$ su realni brojevi, odnosno Dedekindovi rezovi u $\mathbb{Q}$. Dakle, elementi realnog broja su racionalni brojevi. Svaki racionalni broj je klasa ekvivalencije parova cijelih brojeva, dakle elementi racionalnog broja su parovi $(x, y) = \{\{x\}, \{x, y\}\}$, gdje su x i y cijeli brojevi. Njihovi elementi su još jednostavniji od njih, i tako dalje — sve do praznog skupa, koji nema elemenata. „Svi njegovi elementi su na razini nižoj od najniže" tada također vrijedi, jer takvih elemenata nema. Dakle, kumulativna hijerarhija počinje praznim skupom, koji se (jedini) nalazi na prvoj razini V_1. Obično smatramo da ispod nje postoji još jedna razina V_0, koja je prazna (nema elemenata).

Pojam „kumulativna" znači da hijerarhija raste, odnosno akumulira sve dosad izgrađene skupove: $V_n \subseteq V_{n+1}$ za $n \in \mathbb{N}$, ili općenito $V_\alpha \subseteq V_\beta$ za $\alpha < \beta$. Zato, kad kažemo da pri izgradnji skupova na razini $n > 0$ možemo koristiti samo elemente na razinama manjima od n, zapravo je dovoljno tražiti da koristimo elemente razine V_{n-1} — svi ispod, recimo oni s razine V_{n-3} ako takva postoji, bit će također u V_{n-1}. Dakle, na taj način, svaki element razine V_{n+1} zapravo ima sve svoje elemente na razini V_n, odnosno *podskup* je od V_n. Štoviše,

svaki podskup od V_n je na razini V_{n+1}, odnosno V_{n+1} je upravo klasa svih podskupova klase V_n. Pokazat će se da su sve razine kumulativne hijerarhije skupovi, pa vrijedi $V_{\alpha+1} = \mathscr{P}(V_\alpha)$ (partitivni skup).

Iz toga već znamo izračunati V_n za sve $n \in \mathbb{N}$: recimo, $V_3 = \mathscr{P}\big(\mathscr{P}(\mathscr{P}(\emptyset))\big)$ (ima $2^{2^{2^0}} = 4$ elementa — napišite ih sve!). Ali to očito nisu sve razine. Naime, lako je vidjeti indukcijom po n da su svi V_n konačni, a tada su i svi njihovi podskupovi konačni, dakle taj dio kumulativne hijerarhije $(V_n, n \in \mathbb{N})$ pokriva samo konačne skupove. Da bismo dobili beskonačne skupove, morat ćemo napraviti novu razinu, koja sadrži sve dosad izgrađene skupove: $V_\omega := \bigcup_{n\in\mathbb{N}} V_n$; i onda skupiti sve podskupove toga: $V_{\omega+1} := \mathscr{P}(V_\omega)$.

Što je ω? Iz konstrukcije je jasno, to je redni broj razine koja dolazi iza V_0, V_1, V_2, … — odnosno, to je novi redni broj nakon svih prirodnih brojeva (**nulu smatramo prirodnim brojem**). Takve „generalizirane redne brojeve" obično označavamo malim grčkim slovima (kao što smo činili u prethodnoj točki) i zovemo *ordinali* (od engleskog *ordinal number*). Oni imaju mnoga svojstva kao prirodni brojevi (recimo, svaki α ima sljedbenika $\alpha + 1$, te takvu razinu gradimo pomoću partitivnog skupa), ali isto tako nemaju neka svojstva koja kod prirodnih brojeva vrijede. Konkretno, svaki prirodni broj je ili nula ili sljedbenik (svog prethodnika). Ordinali mogu biti i trećeg tipa: *granični* ordinali, koji nemaju prethodnika. Zaista, ω je takav: njegov prethodnik trebao bi biti najveći prirodni broj, što znamo da ne postoji. Zato smo, iako je hijerarhija kumulativna, morali u V_ω skupiti sve niže razine, a ne samo „zadnju" — jer takve nema.

Dakle, sva pravila za izgradnju kumulativne hijerarhije su:

$$V_0 := \emptyset, \qquad V_{\alpha+1} := \mathscr{P}(V_\alpha), \qquad V_\lambda := \bigcup_{\gamma<\lambda} V_\gamma \text{ za granični } \lambda. \tag{0.1}$$

0.6 Jezik teorije skupova

Već u dosadašnjoj vrlo neformalnoj izgradnji teorije koristili smo brojne pretpostavke — recimo, da su skupovi (i klase) jednaki ako se sastoje od istih elemenata. Za izgradnju prvih konačnih razina kumulativne hijerarhije (kao skupova) koristili smo činjenicu da je prazna klasa skup, te da je klasa svih podskupova nekog skupa ponovo skup. Za granične razine koristili smo pretpostavku da je familija $\{V_\gamma : \gamma < \lambda\}$ ponovo skup, te da je unija te familije opet skup. I to je samo što se razina tiče: za pojedine skupove na svakoj razini trebat ćemo još neke pretpostavke. Sve one se mogu zapisati u obliku aksioma, što ćemo i učiniti.

Ipak, neke od tih pretpostavki, kao i formalniji govor o klasama, trebat će formalizaciju „svojstva" skupova. Aksiome i svojstva predstavljamo pomoću *formula* određene logike — o čemu ćete više čuti na Matematičkoj logici, ali zasad napravimo samo ono što nam je potrebno za teoriju skupova. Mnoge od tih stvari već ste čuli na Elementarnoj matematici.

Kao varijable koristit ćemo obično mala slova s kraja latinične abecede (x, y, z, x_1, ...), ali ponekad ćemo radi jasnoće koristiti i neke druge simbole. Podrazumijevamo da ih ima beskonačno mnogo, odnosno preciznije, da za svaku formulu možemo naći „svježu" varijablu koja se u njoj ne pojavljuje. *Formule* su dobivene isključivo sljedećim pravilima:

- Ako su x i y varijable, tada su $x \in y$ i $x = y$ formule (tzv. *atomarne* formule).
- Ako su φ i ψ formule, tada su $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$ i $(\varphi \leftrightarrow \psi)$ formule.
- Ako je φ formula i x varijabla, tada su $\forall x\varphi$ i $\exists x\varphi$ formule.

Značenje tih formula („x je element od y", ..., „postoji skup x takav da vrijedi φ") je, nadamo se, jasno otprije. Za sve pojave varijable x u formulama $\forall x\varphi$ i $\exists x\varphi$ kažemo da su *vezane*. Važno je napomenuti da **vezane varijable označavaju isključivo skupove**: ako želimo reći da nešto vrijedi za svaku klasu X, to nikada nećemo formalizirati kao „$\forall X$".

Kažemo da je varijabla x *slobodna* u formuli ψ ako postoji njena pojava u ψ koja nije vezana. Slobodne varijable u formuli su one o kojima na neki način ovisi značenje te formule. Kad kažemo da je istinita neka formula ψ sa slobodnim varijablama $x_1, \ldots, x_k$, a da pritom ne preciziramo njihove vrijednosti, smatramo da zapravo vrijedi $\forall x_1 \cdots \forall x_k \psi$.

0.7 Pokrate i proširenja jezika

Već u tom jeziku može se formalizirati sve što želimo, ali bi formule bile dosta duge i nečitljive. Da bismo ih učinili čitljivijima, uvodimo razne pokrate. Prvo, zagrade često ne pišemo ako je bez njih značenje formule jasno — ponekad ih čak dodajemo ako čine formulu jasnijom. Drugo, $\neg(x \in y)$ skraćeno pišemo kao $x \notin y$, dok $\neg(x = y)$ skraćeno pišemo kao $x \neq y$; $\neg\exists x$ pišemo kao $\nexists x$. Treće, formulu oblika $\forall x(x \in y \to \varphi)$ pišemo skraćeno kao $(\forall x \in y)\varphi$ („za sve x iz y vrijedi φ"), i analogno $\exists x(x \in y \wedge \varphi)$ skraćujemo u $(\exists x \in y)\varphi$ („postoji x iz y takav da vrijedi φ"). Formulu $\exists y \forall x(x = y \leftrightarrow \varphi)$, gdje y nije slobodna u φ, skraćeno pišemo $\exists! x\varphi$ („postoji jedinstveni x takav da vrijedi φ").

Četvrto, za bilo kakvu formulu možemo uvesti skraćeni zapis, dok god u tom zapisu spomenemo sve slobodne varijable u toj formuli. Primjerice, „formula" $x \subseteq y$ nam je pokrata za $(\forall z \in x)(z \in y)$, što je pak pokrata za $\forall z(z \in x \to z \in y)$ (x i y su slobodne, z je vezana). Peto, za bilo kakvu formulu φ u kojoj je y slobodna, ako znamo da vrijedi $\exists! y\varphi$, možemo uvesti *funkcijsku oznaku* za taj y, u kojoj moramo spomenuti sve ostale slobodne varijable u φ. Primjerice, $\{x_1, x_2\}$ nam je oznaka za jedinstveni y takav da vrijedi $x_1 \in y \wedge x_2 \in y \wedge (\forall z \in y)(z = x_1 \vee z = x_2)$ (postojanje i jedinstvenost takvog y slijedit će iz aksioma). Specijalno, ako φ nema drugih slobodnih varijabli osim y, takav jedinstveni y je konstanta, pa za njega uvodimo oznaku koja ne spominje nikakve varijable. Primjerice, $\emptyset$ nam je oznaka za jedinstveni y takav da vrijedi $\forall x(x \notin y)$ (opet, postojanje i jedinstvenost tog objekta slijedit će iz aksioma).

0.8 Formalni govor o klasama

Neka je ψ formula s jednom slobodnom varijablom x. Klasu svih skupova za koje vrijedi ψ označavamo s $\{x : \psi\}$. To općenito neće biti skup — recimo za $\psi = (x \notin x)$ dobijemo Russellov paradoks — i zapravo bismo mogli reći da je važan zadatak moderne teorije skupova, karakterizirati sve „dobre" formule ψ takve da je $\{x : \psi\}$ skup. Mnogi aksiomi bit će upravo tog tipa, odnosno propisivat će neke specijalne oblike „dobrih" formula. Dva važna specijalna slučaja su:

(*separacija*) Ako je z skup, $\{x \in z : \psi\}$ nam označava *skup* $\{x : x \in z \wedge \psi\}$.

(*zamjena*) Ako je z skup te $f(x)$ funkcijska oznaka za jedinstveni y za koji vrijedi φ, tada je $\{f(x) : x \in z\}$ skraćena oznaka za *skup* $\{y : (\exists x \in z)\varphi\}$.

Ponekad ćemo uvoditi i konstantne oznake za prave klase, ali one će uvijek biti masno otisnute (recimo, $\mathbf{V}$ je oznaka za klasu svih skupova) i atomarne formule s njima bit će samo pokrate za formule koje ne koriste masno otisnuta slova. Konkretno, ako nam je $\mathbf{A}$ oznaka za klasu $\{x : \psi\}$, te $\mathbf{A}'$ oznaka za $\{x : \psi'\}$, tada $x \in \mathbf{A}$ zapravo znači ψ; $y = \mathbf{A}$ (i $\mathbf{A} = y$) zapravo znači $x \in y \leftrightarrow \psi$; te $\mathbf{A} = \mathbf{A}'$ znači $\psi \leftrightarrow \psi'$. S druge strane, $\mathbf{A} \in x$ i $\mathbf{A} \in \mathbf{A}'$ ne znače ništa (to su sintaksne greške) jer, kao što smo rekli, prave klase ne mogu biti elementi skupova niti klasa.

I za kraj, ponekad ćemo neku oznaku koju smo uveli za skupove koristiti i za klase: pritom treba razumjeti da se definicije tih oznaka zapišu u osnovnom jeziku (eliminirajući sve pokrate), te se tada atomarne formule s masnim slovima umjesto slobodnih varijabli interpretiraju kao u prethodnom odlomku. Recimo, $\mathbf{A} \subseteq \mathbf{A}'$ znači $\forall x\,(x \in \mathbf{A} \to x \in \mathbf{A}')$, dakle zapravo $\forall x(\psi \to \psi')$. S druge strane, $\{\mathbf{A}, \mathbf{A}'\}$ ne znači ništa, jer bi svojstvo jedinstvenog y označenog tom oznakom, u sebi uključivalo sintaksnu grešku $\mathbf{A} \in y$.

1 Osnovni aksiomi

1.1 Aksiom ekstenzionalnosti

Na nekoliko mjesta već smo se pozivali na intuiciju da skupovi „nemaju ništa drugo" osim svojih elemenata. Redoslijed nije bitan, i „broj pojavljivanja" nema smisla: za sve skupove y i x vrijedi $y \in x$ ili $y \notin x$, i time je njihov odnos u potpunosti opisan. Štoviše, sām skup x je već u potpunosti opisan odgovorima na pitanja $y \in^? x$ za sve y. Odnosno, ako dva skupa imaju iste elemente, onda su jednaki. To je jedan od najvažnijih aksioma teorije skupova, aksiom *ekstenzionalnosti*:

$$\forall z\,(z \in x \leftrightarrow z \in y) \rightarrow x = y. \tag{1.1}$$

Obrat tog aksioma vrijedi po logičkom značenju jednakosti: za svaku formulu φ s jednom slobodnom varijablom iz $\varphi(x)$ i $x = y$ slijedi $\varphi(y)$. Konkretno (za formulu $z \in x$) iz $x = y$ slijedi $z \in x \rightarrow z \in y$. Također iz $x = y$ slijedi $y = x$, pa vrijedi i $z \in y \rightarrow z \in x$. Formalizacija toga je kompliciranа, ali takvo zaključivanje, kao i oznake poput $\varphi(y)$ za uvrštavanje jedne varijable umjesto druge, smatramo intuitivno jasnim.

Drugim riječima, da nije specijalnog logičkog statusa jednakosti, atomarnu formulu $x = y$ mogli bismo smatrati skraćenim zapisom za lijevu stranu u (1.1), koju možemo zapisati i kao $x \subseteq y \wedge y \subseteq x$. U tom bi slučaju jedina „prava" atomarna formula bila oblika $x \in y$. Jednako tako, pomoću $\neg$ i $\rightarrow$ mogli bismo izraziti sve ostale veznike, a kvantifikator $\exists$ pomoću $\neg$ i $\forall$, čime bismo bitno smanjili broj osnovnih simbola u jeziku — ali to nam neće biti cilj. Primijetimo samo da su pravila za jednakost klasa, kao i jednakost skupa i klase, u skladu s tim shvaćanjem.

1.2 Aksiom praznog skupa

Ostali aksiomi teorije skupova uglavnom navode neke specijalne formule φ sa slobodnom varijablom z, za koje možemo zaključiti da je klasa $\{z : \varphi\}$ skup. Na jeziku teorije skupova to možemo reći u obliku $\exists y(y = \{z : \varphi\})$ gdje y nije slobodna u φ (jer kvantificiramo samo po skupovima), odnosno, uzevši u obzir pravilo za jednakost klase i skupa, $\exists y \forall z(z \in y \leftrightarrow \varphi)$.

Napomena 1.1. Čim smo dokazali (ili propisali kao aksiom) formulu $\exists y \forall z(z \in y \leftrightarrow \varphi)$, možemo uvesti funkcijsku oznaku za y, jer takav y uvijek mora biti jedinstven. $\triangleleft$

Dokaz. Pretpostavimo da su y_1 i y_2 takvi da vrijedi $\forall z(z \in y_1 \leftrightarrow \varphi)$ i $\forall z(z \in y_2 \leftrightarrow \varphi)$. Tada za svaki z imamo da su sve tri formule ($z \in y_1$, φ i $z \in y_2$) ekvivalentne, pa specijalno vrijedi $z \in y_1 \leftrightarrow z \in y_2$. Po aksiomu ekstenzionalnosti, iz toga slijedi $y_1 = y_2$. □

Recimo, da bismo uopće započeli izgrađivati kumulativnu hijerarhiju (čije su razine skupovi), moramo znati da je prazna klasa V_0 skup. To nam kaže aksiom *praznog skupa*:

$$\exists y \, \forall z \, (z \notin y). \tag{1.2}$$

Primijetimo da je ta formula oblika iz prvog odlomka, za neku formulu φ koja je uvijek lažna (recimo $z \neq z$). Time imamo osigurano postojanje praznog skupa, a po napomeni 1.1 i jedinstvenost — te možemo uvesti oznaku $\emptyset$ za njega. To je konstanta, jer formula $z \neq z$ nema drugih slobodnih varijabli osim z.

1.3 Aksiom partitivnog skupa

Da bismo nastavili izgrađivati kumulativnu hijerarhiju a da pritom razine ostanu skupovi, treba nam partitivni skup, odnosno aksiom da je klasa svih podskupova zadanog skupa x ponovo skup. Svojstvo φ je tada $z \subseteq x$, te aksiom *partitivnog skupa* glasi

$$\forall x \, \exists y \, \forall z \, (z \in y \leftrightarrow z \subseteq x). \tag{1.3}$$

Strogo govoreći, ovaj kvantifikator $\forall x$ na početku nam ne treba jer je u skladu s našim shvaćanjem istinitosti formula sa slobodnim varijablama, ali stavili smo ga radi jasnoće. Opet po napomeni 1.1, (za svaki x) postoji jedinstveni y čiji su elementi upravo podskupovi od x, te za njega možemo uvesti oznaku $\mathscr{P}(x)$. Ta oznaka mora spominjati x, jer formula $z \subseteq x$ pored z sadrži i x kao slobodnu varijablu.

Pomoću aksioma partitivnog skupa možemo za svaki $n \in \mathbb{N}$ dobiti da je V_n skup. Što je s V_ω? Pokazuje se da je potrebno dosta „sastojaka”: prvo moramo vidjeti da je uopće ω skup, zatim da iz toga slijedi da je familija $\{V_n : n \in \omega\}$ (po principu zamjene, to je skraćeni zapis za $\{y : (\exists n \in \omega)(y = V_n)\}$) skup, i napokon, da je unija te familije skup.

1.4 Aksiom unije

Prva dva koraka odgodit ćemo za kasnije, kad preciznije definiramo prirodne brojeve kao skupove. Zasad se pozabavimo trećim korakom. Na prvi pogled čini se da za to trebamo precizirati pojam *familije* skupova, ali to zapravo nije potrebno: svaki skup je familija, jer su njegovi elementi opet skupovi. (*Indeksirane* familije su kompliciranije, ali one će nam trebati tek mnogo kasnije.)

Dakle, neka je x proizvoljni skup, shvaćen kao familija $\{t : t \in x\}$. Unija te familije $\bigcup_{t\in x} t$ tada sadrži sve one z koji se nalaze bar u jednom $t \in x$. Dakle, svojstvo φ je $(\exists t \in x)(z \in t)$, pa aksiom unije glasi:

$$\forall x\, \exists y\, \forall z \left(z \in y \leftrightarrow (\exists t \in x)(z \in t)\right). \tag{1.4}$$

Po napomeni 1.1, (za svaki x) takav y je jedinstven, te možemo uvesti oznaku za njega koja spominje x. Službena oznaka je $\bigcup x$, iako često zbog jasnoće koristimo i oznaku $\bigcup_{t\in x} t$, podrazumijevajući da je t vezana varijabla.

Propozicija 1.2. *Za svaki skup x vrijedi $\bigcup \mathscr{P}(x) = x$.*

Dokaz. Zbog aksioma ekstenzionalnosti, dovoljno je dokazati dvije *inkluzije* $\bigcup \mathscr{P}(x) \subseteq x$ i $x \subseteq \bigcup \mathscr{P}(x)$. Prva je univerzalno kvantificirana po z, pa neka je $z \in \bigcup \mathscr{P}(x)$ proizvoljan. Po definiciji unije, to znači da postoji $t \in \mathscr{P}(x)$ takav da je $z \in t$. Po definiciji partitivnog pak skupa, $t \in \mathscr{P}(x)$ znači $t \subseteq x$. Sada po definiciji relacije $\subseteq$ iz $z \in t$ slijedi $z \in x$, što smo trebali doikazati.

Za drugu inkluziju, uzmimo proizvoljni $z \in x$. Pitamo se: postoji li $t \in \mathscr{P}(x)$ takav da je $z \in t$? Naravno: $t := x$ je sasvim u redu. (Mogli bismo poželjeti uzeti $t := \{z\}$, ali iz dosad navedenih aksioma ne slijedi da je to skup.) Očito je $x \subseteq x$, dakle $x \in \mathscr{P}(x)$. Sada iz $z \in x \in \mathscr{P}(x)$ (skraćeni zapis za $z \in x \wedge x \in \mathscr{P}(x)$) slijedi $z \in \bigcup \mathscr{P}(x)$, što smo trebali. □

1.5 Aksiom para

Dokazali smo $x = \bigcup \mathscr{P}(x)$. Vrijedi li i $x = \mathscr{P}(\bigcup x)$? Intuitivno, ne (iako jedna inkluzija vrijedi — dokažite!): partitivni skup uvijek ima broj elemenata koji je potencija od 2. Dakle, samo za kontraprimjer trebamo staviti neki skup koji ima 3, ili 5, ... elemenata. Postoji li takav? Prazan skup jest takav (0 nije potencija od 2), ali postoje li drugi? Začuđujuće, iz dosad navedenih aksioma to ne slijedi. Što se trenutno aksiomatizirane teorije tiče, sasvim je moguće da su jedini skupovi oblika V_n, $n \in \mathbb{N}$.

Još jedna tema za razmišljanje: uniju smo uveli u obliku koji nam je bio pogodan za V_ω (ili općenito V_λ gdje je λ granični ordinal), ali zapravo, unija se obično uvodi kao binarna operacija. Za skupove a i b, htjeli bismo reći da je $a \cup b$ skup. Na prvi pogled, to je specijalni slučaj aksioma unije, primijenjenog na familiju $\{a, b\}$ — ali tko nam kaže da je ta familija skup? Doista, za općenite skupove a i b, to će nam reći novi aksiom, aksiom *para*:

$$\forall a\, \forall b\, \exists y\, \forall z\, (z \in y \leftrightarrow z = a \vee z = b). \tag{1.5}$$

Vidimo da je svojstvo φ oblika $z = a \vee z = b$, sa slobodnim varijablama z, a i b — i opet, kao i ranije, zapravo nismo morali pisati „$\forall a\, \forall b$" na početku aksioma. Po napomeni 1.1, možemo uvesti oznaku za taj y, koja spominje a i b. Uvodimo oznaku $\{a, b\}$ — naravno, ako znamo da je $a = b$, to radije pišemo kao $\{a\}$ umjesto $\{a, a\}$. Sada za skupove a i b vrijedi $a \cup b := \{x : x \in a \vee x \in b\} = \bigcup\{a, b\}$, što je skup po aksiomu para i aksiomu unije. Drugim

riječima, klasa **V** je zatvorena na unije. Zatvorenost na druge skupovne operacije dokazat ćemo kasnije.

Vidjeli smo da iz aksioma para slijedi da su ne samo parovi (dvočlane klase) skupovi, već i singletoni (jednočlane klase), jednostavno tako da uzmemo $a = b$. No zapravo iz aksioma para i unije slijedit će puno više: sve konačne klase su skupovi.

Propozicija 1.3. *Neka je $k \in \mathbb{N}$ prirodan broj, te $x_1, x_2, \ldots, x_k$ skupovi.*
Tada je i klasa $\{x_1, \ldots, x_k\} := \{x : x = x_1 \vee x = x_2 \vee \cdots \vee x = x_k\}$ skup.

Dokaz. Matematičkom indukcijom po k. Za $k = 0$, ta klasa je prazna, te tvrdnja slijedi po aksiomu praznog skupa. Pretpostavimo da tvrdnja vrijedi za $k = l$, te neka su x_1, x_2, …, x_{l+1} skupovi. Po pretpostavci indukcije $\{x_1, x_2, \ldots, x_l\}$ je skup, a po aksiomu para singleton $\{x_{l+1}\}$ je također skup. Po aksiomu para i unije tada je i $\{x_1, \ldots, x_l\} \cup \{x_{l+1}\} = \{x_1, \ldots, x_{l+1}\}$ skup, pa tvrdnja vrijedi za $k = l + 1$. □

Napomena 1.4. Formalno, u našoj teoriji dokazali smo sve formule φ_n, gdje je $n \in \mathbb{N}$, zadane s

$$\varphi_n := \forall x_1 \forall x_2 \cdots \forall x_n \exists y \, \forall z \, (z \in y \leftrightarrow z = x_1 \vee z = x_2 \vee \cdots \vee z = x_n). \tag{1.6}$$

Konkretno, formula φ_2 je upravo aksiom para (s preimenovanim vezanim varijablama). φ_0 je aksiom praznog skupa, ako praznu disjunkciju shvatimo kao laž. Primijetimo da ne možemo na početak formule dopisati $(\forall n \in \mathbb{N})$ i time objediniti sve formule u jednu, iz dva razloga: prvo, $\mathbb{N}$ još nismo formalno uveli, i ne znamo je li to skup; a drugo, duljina formule φ_n ovisi o n, pa ne možemo nakon $(\forall n \in \mathbb{N})$ napisati formulu kao konačni niz znakova. Također, matematičku indukciju smo koristili „izvana", da bismo njome konstruirali dokaze: svaki pojedini dokaz formule φ_n (recimo, dokaz formule φ_5) ne koristi matematičku indukciju, već samo logičke aksiome i aksiome teorije skupova koje smo naveli. ◁

1.6 Uređeni par

Skupove možemo koristiti kao spremnike podataka, ali pritom bismo često htjeli sačuvati informaciju o njihovom redoslijedu. Za skupove a i b možemo napraviti par $\{a, b\}$, ali je on (po ekstenzionalnosti) jednak paru $\{b, a\}$, čak i za $a \neq b$. Treba nam *uređeni* par: par zajedno s informacijom koji element u paru je prvi, a koji je drugi element. Zanimljivo je da se uređeni parovi mogu implementirati u teoriji skupova, odnosno reprezentirati kao skupovi. Zasad ćemo samo navesti definiciju, a objašnjenje zašto tako izgleda dat ćemo kasnije (napomena 3.30).

Definicija 1.5. Neka su x i y skupovi. Oznakom (x, y) označavamo skup $\big\{\{x\}, \{x, y\}\big\}$. ◁

Primijetimo da je (x, y) doista skup, trostrukom primjenom aksioma para: jednom na x i x, drugi put na x i y, te treći put na tako dobivene skupove $\{x\}$ i $\{x, y\}$. Sada dokažimo da ima osnovno svojstvo koje bi uređeni par trebao imati.

Lema 1.6. *Za bilo koje skupove x, y i z, jednakost $\{x,y\} = \{x,z\}$ povlači $y = z$.*

Dokaz. Po aksiomu para je $y = x \vee y = z$, i također $z = x \vee z = y$. U tri od četiri tako dobivena slučaja je odmah $y = z$, a u četvrtom je $y = x$ i $z = x$, pa je opet $y = z$. □

Propozicija 1.7. *Neka su a, b, c i d skupovi. Ako je $(a,b) = (c,d)$, tada je $a = c$ i $b = d$.*

Dokaz. Po pretpostavci je $\big\{\{a\},\{a,b\}\big\} = \big\{\{c\},\{c,d\}\big\}$. Tada je po aksiomu para $\{a\}$ element tog skupa, pa je opet po aksiomu para $\{a\} = \{c\}$ ili $\{a\} = \{c,d\}$. Sada gledano s desne strane, u svakom slučaju je $c \in \{a\}$, pa po aksiomu para vrijedi $c = a \vee c = a$, dakle $c = a$.

Uvrštavajući to u pretpostavku dobijemo $\big\{\{a\},\{a,b\}\big\} = \big\{\{a\},\{a,d\}\big\}$. Primjenom leme 1.6 dobijemo $\{a,b\} = \{a,d\}$, i onda još jednom primjenom iste leme $b = d$. □

Lema 1.8. *Ako je $x \in a$ i $y \in b$, tada je $(x,y) \in \mathscr{P}\big(\mathscr{P}(a \cup b)\big)$.*

Dokaz. Iz $x \in a \in \{a,b\}$ slijedi $x \in \bigcup\{a,b\} = a \cup b$, iz čega je $\{x\} \subseteq a \cup b$, odnosno $\{x\} \in \mathscr{P}(a \cup b)$. Analogno je $y \in a \cup b$, te je $\{x,y\} \subseteq a \cup b$, dakle $\{x,y\} \in \mathscr{P}(a \cup b)$. Iz tog dvojeg slijedi $(x,y) = \big\{\{x\},\{x,y\}\big\} \subseteq \mathscr{P}(a \cup b)$, odnosno tvrdnja leme. □

Lema 1.9. *Ako je $(x,y) \in R$, tada su $x, y \in \bigcup\bigcup R$.*

Dokaz. Iz $\{x,y\} \in (x,y) \in R$ imamo $\{x,y\} \in \bigcup R$, pa onda iz $x \in \{x,y\} \in \bigcup R$ imamo $x \in \bigcup\bigcup R$, i analogno za y. □

1.7 Shema aksioma separacije

Već smo rekli da klase općenito nisu skupovi, ali pritom su jedini problem „prevelike" klase. Ako na bilo koji način možemo ograničiti veličinu klase, ona će zapravo biti skup. Jedan vrlo jednostavan ali efektan način da ograničimo klasu jest da kažemo da je potklasa nekog skupa: ako je $\{z : \varphi\} \subseteq x$, tada $\exists y(y = \{z : \varphi\})$. Ako je φ formula sa slobodnom varijablom z, pretpostavku možemo zapisati kao $\varphi \to z \in x$, iz čega slijedi $\varphi \Leftrightarrow z \in x \wedge \varphi$, pa radi jednostavnosti možemo smatrati da φ već jest takvog oblika.

Varijabla x je obična slobodna varijabla u iskazu aksioma, ali φ je proizvoljna formula (u kojoj y nije slobodna), pa zapravo nemamo jedan aksiom, već po jedan za svaku formulu φ. Napisati „$\forall\varphi$" na početku nema smisla iz barem dva razloga, sličnih kao u napomeni 1.4: formule nismo formalizirali kao skupove, a i nema nekog uniformnog oblika da u osnovnom jeziku referiramo na proizvoljnu formulu (nemamo formalizirane varijable za formule). Takvu kolekciju aksioma zovemo *shemom*. Sve u svemu, shema aksioma *separacije* glasi:

$$\exists y\, \forall z \big(z \in y \leftrightarrow (z \in x \wedge \varphi)\big), \tag{1.7}$$

gdje je φ proizvoljna formula koja ne sadrži (slobodnu) varijablu y.

Opet, na početak aksioma možemo dodati $\forall x$, ali isto tako i $\forall x_i$ za svaku slobodnu varijablu x_i u φ. Radi jednostavnosti, ovaj put nećemo napisati sve te univerzalne kvantifikatore, već ćemo se osloniti na naše shvaćanje istinitosti formula sa slobodnim varijablama.

Kao i obično (napomena 1.1), y je jedinstven, te za njega uvodimo oznaku $\{z \in x : \varphi\}$. Primijetimo da ona svakako spominje x, ali i sve slobodne varijable u φ, samim njenim navođenjem. Recimo, za svaka dva skupa a i b, njihov presjek $\{z : z \in a \wedge z \in b\}$ je skup po aksiomu separacije (preciznije, po instanci sheme aksioma separacije), jer se može zapisati kao $a \cap b = \{z \in a : z \in b\}$. Slično se može pokazati (učinite to!) da je klasa $\mathbf{V}$ zatvorena na skupovnu razliku, a onda pomoću unije i na simetričnu skupovnu razliku.

Napomena 1.10. Jednom kad imamo shemu aksioma separacije, ostale aksiome koji govore da su neke klase skupovi možemo iskazati u slabijem obliku, navodeći samo jedan smjer. Primjerice, aksiom partitivnog skupa bi onda glasio $\forall x \exists y \forall z (z \subseteq x \to z \in y)$. Za zadani x, separacijom iz takvog y pomoću svojstva $z \subseteq x$ dobili bismo $\mathscr{P}(x)$.

Posebno se aksiomi unije $\exists y(\forall t \in x)(t \subseteq y)$ i para $\exists y(a \in y \ni b)$ mogu puno konciznije zapisati koristeći tu tehniku. Kako nam je razumljivost aksiomā važnija od kratkoće njihovog zapisa, ostavit ćemo ih u već napisanom obliku — ali tehnika je korisna za kompliciranije aksiome, i dobro će nam doći kasnije, kod zapisa aksioma beskonačnosti. ◁

1.8 Kartezijev produkt

Individualni uređeni parovi su dobri za pamćenje dva podatka, no općenito bismo njima htjeli modelirati neke odnose među skupovima. Skup uređenih parova zovemo *relacijom*. Relacije najčešće zadajemo kao *binarne* relacije, tako da navedemo neke skupove a i b, te među parovima (x, y), gdje je $x \in a \wedge y \in b$, odaberemo one koji zadovoljavaju neku formulu s dvije slobodne varijable, x i y. To možemo formalizirati primjenom aksioma separacije, ali prethodno nam treba skup *svih* uređenih parova (x, y) takvih da je $x \in a$ i $y \in b$.
To doista jest skup, i zovemo ga *Kartezijevim produktom* skupova a i b. Iz sljedeće propozicije i napomene 1.1 slijedit će da možemo uvesti oznaku za njega, $a \times b$.

Propozicija 1.11. *Neka su a i b skupovi.*
Tada je klasa $\{(x, y) : x \in a, y \in b\}$ (što je pokrata za $\big\{p : (\exists x \in a)(\exists y \in b)\big(p = (x, y)\big)\big\}$) skup.

Dokaz. Taj skup možemo dobiti primjenom aksioma separacije. Formula piše u iskazu propozicije, ali iz kojeg skupa mora biti p? Ovdje nam može pomoći lema 1.8. Prema njoj, svaki uređeni par elemenata iz a i iz b, dakle svaki p koji zadovoljava tu formulu, mora biti u skupu $\mathscr{P}\big(\mathscr{P}(a \cup b)\big)$. Dakle,

$$a \times b = \big\{p \in \mathscr{P}\big(\mathscr{P}(a \cup b)\big) : (\exists x \in a)(\exists y \in b)\big(p = (x, y)\big)\big\} \tag{1.8}$$

je skup po aksiomu separacije. □

2 Relacije i funkcije

2.1 Relacije

Relacije i funkcije upoznali ste, i mnoga njihova svojstva dokazali, na Elementarnoj matematici. Ovdje uglavnom ponavljamo i naglašavamo svojstva koja će nam biti bitna.

Neka su a i b skupovi. *Relacija* između a i b je bilo koji podskup njihovog Kartezijevog produkta: $R \subseteq a \times b$. Umjesto $(x, y) \in R$ skraćeno pišemo $x\ R\ y$. Zbog leme 1.9 za svaku relaciju R postoji skup $c := \bigcup\bigcup R$ takav da je $R \subseteq c \times c$ (R je relacija između c i c, što kratko zovemo „relacija *na* c"). *Domena* relacije R je skup (po aksiomu separacije primijenjenom na c) $\operatorname{dom} R := \{x : \exists y(x\ R\ y)\}$. Analogno, *slika* relacije R je skup $\operatorname{rng} R := \{y : \exists x(x\ R\ y)\}$.

Zadatak 2.1. *Dokažite: svaka relacija R je između* $\operatorname{dom} R$ *i* $\operatorname{rng} R$.

Inverz relacije R je relacija R^{-1} između $\operatorname{rng} R$ i $\operatorname{dom} R$ zadana s $y\ R^{-1}\ x :\Leftrightarrow x\ R\ y$. Često ćemo tako (formulom) zadavati relacije između zadanih skupova. To je pokrata za $R^{-1} := \{(y, x) \in \operatorname{rng} R \times \operatorname{dom} R : x\ R\ y\} = \big\{p \in \operatorname{rng} R \times \operatorname{dom} R : \exists y \exists x\big(p = (y, x) \wedge x\ R\ y\big)\big\}$. *Kompozicija* dviju relacijā R i S je relacija $S \circ R$ između $\operatorname{dom} R$ i $\operatorname{rng} S$, zadana s $x\ (S \circ R)\ z :\Leftrightarrow \exists y(x\ R\ y \wedge y\ S\ z)$. Formulu pod kvantifikatorom skraćeno zapisujemo $x\ R\ y\ S\ z$.

Za relaciju R i skup c (obično je $c \subseteq \operatorname{dom} R$, ali ne mora biti), *restrikcija* R na c je relacija $R|_c := R \cap (c \times \operatorname{rng} R)$. Sliku te restrikcije zovemo još *slikom skupa c po relaciji R* i označavamo $R[c]$. Sliku skupa d po inverznoj relaciji R^{-1} zovemo još *praslikom skupa d po R*.

Relacija R je *simetrična* ako vrijedi $x\ R\ y \to y\ R\ x$. (Po konvenciji o istinitosti formula sa slobodnim varijablama, podrazumijevamo da ispred piše $\forall x\, \forall y$. Još kažemo da $x\ R\ y$ *povlači* $y\ R\ x$, i pišemo $x\ R\ y \Rightarrow y\ R\ x$.) *Antisimetrična* je ako $x\ R\ y\ R\ x \Rightarrow x = y$. *Tranzitivna* je ako vrijedi $x\ R\ y\ R\ z \Rightarrow x\ R\ z$. *Irefleksivna* je ako vrijedi $\nexists x(x\ R\ x)$.

Kažemo da je relacija R na skupu a *refleksivna na a* ako vrijedi $(\forall x \in a)(x\ R\ x)$.
Tada je $\operatorname{dom} R = \operatorname{rng} R = a$, pa se a može rekonstruirati iz R.

2.2 Parcijalni uređaji

Definicija 2.2. Neka je a skup, i R relacija na a. Kažemo da je R *refleksivni parcijalni uređaj na a* ako je R refleksivna na a, antisimetrična i tranzitivna.
Kažemo da je R *strogi parcijalni uređaj na a* ako je R irefleksivna i tranzitivna. ◁

Lema 2.3. *Ako je R refleksivni parcijalni uređaj na a,*
tada je $s\ x\ S\ y :\Leftrightarrow x\ R\ y \wedge x \neq y$ zadan strogi parcijalni uređaj na a.

Dokaz. Očito, S je dobivena separacijom iz R, pa vrijedi $S \subseteq R \subseteq a \times a$, odnosno S je također relacija na a. Kad bi bilo $x\ S\ x$, vrijedilo bi $x\ R\ x$ i $x \neq x$, što je očito nemoguće — dakle, S je irefleksivna.

Za tranzitivnost, neka je $x\ S\ y\ S\ z$. To znači $x\ R\ y\ R\ z$, te $x \neq y$ i $y \neq z$. Iz ovog prvog je $x\ R\ z$ jer je R tranzitivna, ali iz ovog drugog ne možemo zaključiti $x \neq z$. No kad bi bilo $x = z$, tada bismo imali $x\ R\ y\ R\ x$, pa bi po antisimetričnosti vrijedilo $x = y$, kontradikcija. Dakle doista vrijedi $x \neq z$, odnosno $x\ S\ z$. □

Lema 2.4. *Ako je S strogi parcijalni uređaj na a,*
tada je $s\ x\ R\ y :\Leftrightarrow x\ S\ y \vee x = y \in a$ zadan refleksivni parcijalni uređaj na a.

Dokaz. R je unija S i relacije $id_a := \{(x,x) : x \in a\} := \{p \in a \times a : \exists x(p = (x,x))\}$ (koja je skup po aksiomu separacije), pa je skup po aksiomu unije. Također, i S i id_a su podskupovi od $a \times a$, pa je i njihova unija takva — odnosno, R je relacija na a.

Refleksivnost na a je očita: za svaki $x \in a$ vrijedi $x\ S\ x \vee (x = x \in a)$. Za antisimetričnost, pretpostavimo $x\ R\ y\ R\ x$. Ako vrijedi $x = y$, gotovi smo. Inače bi vrijedilo $x\ S\ y\ S\ x$, te po tranzitivnosti $x\ S\ x$, što je nemoguće zbog irefleksivnosti od S. Za tranzitivnost, iz $x\ R\ y\ R\ z$ imamo četiri slučaja:

1. $x\ S\ y\ S\ z$, iz čega $x\ S\ z$ zbog tranzitivnosti od S;
2. $x\ S\ y = z \in a$, iz čega $x\ S\ z$ po logičkim svojstvima jednakosti;
3. $x = y\ S\ z$, iz čega opet $x\ S\ z$, analogno;
4. $x = y = z \in a$, iz čega slijedi $x = z \in a$.

Dakle, u svakom slučaju je $x\ S\ z$ ili $x = z \in a$, odnosno $x\ R\ z$. □

Definicija 2.5. Neka je a skup, i $\prec$ strogi parcijalni uređaj na njemu. Tada kažemo da je $(a, \prec)$ *parcijalno uređen skup*, ili da je a parcijalno uređen relacijom $\prec$.
Odgovarajući refleksivni parcijalni uređaj (u smislu leme 2.4) označavamo s $\preceq$. ◁

Upravo dokazane leme pokazuju da je svejedno je li nam na skupu zadan strogi ili refleksivni parcijalni uređaj. Zato ćemo često govoriti i da je $(a, \preceq)$ parcijalno uređen skup, gdje je $\preceq$ refleksivni parcijalni uređaj na a, pritom zapravo misleći na $(a, \prec)$ gdje je $\prec$ odgovarajući strogi parcijalni uređaj (u smislu leme 2.3).

Napomena 2.6. Često samo kažemo „a je parcijalno uređen skup", ako znamo na koji uređaj se misli. Takav govor — zamjena strukture $(S, \ldots)$ njenim *nosačem* S — je uobičajen u matematici, recimo kad kažemo „vektorski prostor V" umjesto „$(V, F, +, \cdot)$". ◁

Neka je $(a, \prec)$ parcijalno uređen skup, i $b \subseteq a$ (tada je i $\big(b, (\prec) \cap b \times b\big)$ parcijalno uređen skup — ponekad kažemo i da je $(b, \prec)$ parcijalno uređen skup). Za $x \in a$ kažemo da je *minimalan* (*maksimalan*) ako ne postoji $y \in a$ takav da je $y \prec x$ ($x \prec y$). Kažemo da je x *najmanji* (*najveći*) element skupa a ako za svaki $y \in a$ vrijedi $x \preceq y$ ($y \preceq x$). Kažemo da je x *donja* (*gornja*) *međa* za b ako za svaki $y \in b$ vrijedi $x \preceq y$ ($y \preceq x$). Kažemo da je x *supremum* (*infimum*) skupa b ako je x najmanja gornja (najveća donja) međa skupa b.

Primjer 2.7. Neka je a skup. Tada je $\big(\mathscr{P}(a), \subset\big)$ parcijalno uređen skup. U njemu, najmanji (i jedini minimalni) element je $\emptyset$, najveći (i jedini maksimalni) element je a, a supremum skupa $b \subseteq \mathscr{P}(a)$ je $\bigcup b$. Što je infimum proizvoljnog $b \subseteq \mathscr{P}(a)$? $\lhd$

2.3 Uređeni skupovi

Ako su x i y proizvoljni elementi parcijalno uređenog skupa a, mogu biti jednaki ($x = y$), a može i jedan od njih biti manji: $x \prec y$ ili $y \prec x$. Ta tri slučaja se međusobno isključuju zbog irefleksivnosti i tranzitivnosti uređaja (dokažite!), ali ne pokrivaju sve mogućnosti. Ako ne vrijedi nijedna od te tri tvrdnje, kažemo da su x i y *neusporedivi*.

Mnogo je lakše kad nemamo neusporedivih elemenata, jer u uobičajenoj matematičkoj praksi rijetko na njih nailazimo (iako ih ima ponekad: recimo, za $a \neq b$, skupovi $\{a\}$ i $\{b\}$ su neusporedivi s obzirom na $\subset$). Ako su svi elementi od a usporedivi, uređaj $\prec$ zovemo *totalnim*, odnosno kažemo da je $(a, \prec)$ *totalno uređen skup*.

Propozicija 2.8. *U svakom totalno uređenom skupu, pojmovi minimalnog i najmanjeg elementa su ekvivalentni, te su pojmovi maksimalnog i najvećeg elementa ekvivalentni.*

Dokaz. Dokažimo samo prvu tvrdnju, druga je sasvim analogna. Neka je $(a, \prec)$ totalno uređen skup i $x \in a$. Trebamo dokazati da je x minimalan ako i samo ako je najmanji.

Za smjer ($\Rightarrow$), neka je x minimalan i neka je $y \in a$ proizvoljan. Zbog totalnosti vrijedi $x = y$, $x \prec y$ ili $y \prec x$. No ovo treće je nemoguće jer je x minimalan. Dakle za sve $y \in a$ je $x \preceq y$, odnosno x je najmanji element u a.

Smjer ($\Leftarrow$) zapravo vrijedi u svakom parcijalno uređenom skupu: neka je x najmanji. Kad ne bi bio minimalan, postojao bi $y \in a$ takav da je $y \prec x$. No x je najmanji, pa vrijedi $x \preceq y$. Iz $x \preceq y \prec x$ po tranzitivnosti dobivamo $x \prec x$, što je u kontradikciji s irefleksivnošću. $\square$

Parcijalno uređen skup ne može imati više najmanjih (niti najvećih) elemenata: ako su x i y najmanji elementi u a, tada vrijedi $x \preceq y \preceq x$, odnosno $x = y$ po antisimetričnosti.
Dakle, u totalno uređenim skupovima je minimalni element jedinstven, što opravdava naziv *minimum* i oznaku $\min a$ (odnosno naziv *maksimum* i oznaku $\max a$ za maksimalni element), ako takav element postoji.

Zadatak 2.9. *Dokažite: u svakom parcijalno uređenom skupu,*
najmanji element (ako postoji) je jedinstveni minimalni element.
Je li minimalni element, ako je jedinstven, nužno najmanji? Dokažite ili opovrgnite.

Postojanje minimuma je važno svojstvo, koje može a i ne mora vrijediti: recimo, u $\mathbb{R}$, segment $[0,1]$ ima minimum, dok ga otvoreni interval $\langle 0,1\rangle$ nema. Naravno, da bi skup imao minimum, mora biti neprazan. Kasnije će nam biti važni skupovi čiji *svaki* neprazni podskup ima minimum.

Definicija 2.10. Za parcijalno uređen skup $(a,\prec)$ kažemo da je *dobro utemeljen* ako svaki njegov neprazni podskup ima minimalni element, a kažemo da je *dobro uređen* ako svaki njegov neprazni podskup ima najmanji element. $\lhd$

Teorem 2.11. *Parcijalno uređen skup je dobro uređen ako i samo ako je totalno uređen i dobro utemeljen.*

Dokaz. Smjer ($\Leftarrow$) slijedi iz propozicije 2.8. Za smjer ($\Rightarrow$), dobra uređenost očito povlači dobru utemeljenost zbog zadatka 2.9; još treba vidjeti da povlači i totalnu uređenost.

Neka je $(a,\prec)$ proizvoljni parcijalno uređen skup. Za svaka dva njegova elementa $x,y\in a$ je par $\{x,y\}$ neprazni podskup od a, pa mora imati najmanji element z. Po definiciji para, $z\in\{x,y\}$ znači $z=x$ ili $z=y$. Prvo povlači $x\preceq y$ a drugo $y\preceq x$, pa u svakom slučaju x i y moraju biti usporedivi. $\square$

Važan (zasad samo intuitivni) primjer dobro uređenog skupa je skup prirodnih brojeva $\mathbb{N}$. Mnogo više o dobro uređenim i dobro utemeljenim skupovima reći ćemo kasnije, kad budemo formalno uvodili ordinale. Zasad samo dokažimo da su konačni skupovi (u smislu propozicije 1.3) uvijek dobro utemeljeni.

Propozicija 2.12. *Neka je $k\in\mathbb{N}\setminus\{0\}$. Tada svaki parcijalno uređeni skup oblika $(\{x_1,x_2,\ldots,x_k\},\prec)$, ima minimalni (i ima maksimalni) element.*

Dokaz. Matematičkom indukcijom po k od 1 nadalje. Baza: za $k=1$, skup $\{x_1\}$ očito ima minimalni (čak najmanji) element x_1. Pretpostavimo da tvrdnja vrijedi za $k=l$, i pogledajmo skup oblika $\{x_1,\ldots,x_l,x_{l+1}\}$. Po pretpostavci indukcije, skup $\{x_1,\ldots,x_l\}$ ima minimalni element: uzmimo jedan od njih i označimo ga s m. Ako je m minimalni i u početnom skupu, gotovi smo. Inače, postoji x_i takav da je $x_i\prec m$. Ne može biti $i\leq l$, jer m jest minimalni među prvih l elemenata. Dakle, mora biti $i=l+1$, odnosno $x_{l+1}\prec m$. Kad bi postojao x_j takav da je $x_j\prec x_{l+1}$, moralo bi biti $j\leq l$ (zbog irefleksivnosti nije $x_{l+1}\prec x_{l+1}$) i $x_j\prec m$ po tranzitivnosti, što je kontradikcija s minimalnošću m među prvih l elemenata. Dakle, u slučaju da m nije minimalni i u većem skupu, x_{l+1} jest takav, pa u svakom slučaju imamo minimalni element. Po principu matematičke indukcije, tvrdnja vrijedi za sve $k\in\mathbb{N}\setminus\{0\}$. Egzistencija maksimalnog elementa dokazuje se sasvim analogno. $\square$

Korolar 2.13. *Svaki konačni parcijalno uređeni skup je dobro utemeljen.*
Svaki konačni totalno uređeni skup je dobro uređen.

Samo napomenimo da nam za dokaz tog korolara treba činjenica da je podskup konačnog skupa konačan. Za „nabrojene" skupove u smislu propozicije 1.3 to se lako dokaže indukcijom po k, ali jednom kad formalno definiramo konačne skupove, to ćemo morati preciznije dokazati.

2.4 Antileksikografski uređaj

Prikazat ćemo relativno standardni način na koji možemo urediti razne skupove parova, ako su prva i druga komponenta para već nekako uređene. Formalno to definiramo za Kartezijev produkt, ali zapravo je definicija primjenjiva i šire.

Definicija 2.14. Neka su $(a, \prec)$ i $(b, \lhd)$ parcijalno uređeni skupovi.
Antileksikografski uređaj je relacija $<$ na $a \times b$ zadana s

$$(s,t) < (u,v) :\Longleftrightarrow t \lhd v \vee (t = v \wedge s \prec u). \tag{2.1}$$

Propozicija 2.15. *Ako su $(a, \prec)$ i $(b, \lhd)$ (1) parcijalno uređeni, (2) totalno uređeni, (3) dobro utemeljeni, (4) dobro uređeni; tada je takav i $(a \times b, <)$ uređen antileksikografski.*

Dokaz. Za tvrdnju (1), kad bi bilo $(s,t) < (s,t)$ to bi značilo ili $t \lhd t$ (nemoguće zbog irefleksivnosti $\lhd$) ili $t = t \wedge s \prec s$ (nemoguće zbog irefleksivnosti $\prec$). Dakle, $(<)$ je irefleksivna.

Tranzitivnost: neka je $(s,t) < (u,v) < (x,y)$. Prema (2.1) imamo četiri mogućnosti.

$[t \lhd v \lhd y]$: Tada je $t \lhd y$ po tranzitivnosti $\lhd$, pa je $(s,t) < (x,y)$.

$[t \lhd v = y \wedge u \prec x]$ ili $[t = v \lhd y \wedge s \prec u]$: Opet je $t \lhd y$ pa i $(s,t) < (x,y)$.

$[t = v = y \wedge s \prec u \prec x]$: Tada je $t = y$ i $s \prec x$ po tranzitivnosti $=$ i $\prec$ redom, pa je $(s,t) < (x,y)$.

Za tvrdnju (2), neka su $(a, \prec)$ i $(b, \lhd)$ totalno uređeni, i neka su $(s,t), (u,v) \in a \times b$. Znamo da su $t, v \in b$ usporedivi. Ako je $t \lhd v$, tada je $(s,t) < (u,v)$, a ako je $v \lhd t$, tada je $(u,v) < (s,t)$. Ako je pak $t = v$, tada usporedimo $s, u \in a$. Ako je $s \prec u$, tada je $(s,t) < (u,t) = (u,v)$, a ako je $u \prec s$, tada je $(u,v) < (s,v) = (s,t)$. Ako je i $s = u$, tada je $(s,t) = (u,v)$. Dakle u svakom slučaju su usporedivi.

Za tvrdnju (3), neka su $(a, \prec)$ i $(b, \lhd)$ dobro utemeljeni, i neka je $R \subseteq a \times b$ neprazan skup (relacija). Tada je $\operatorname{rng} R$ neprazni podskup od b pa ima minimalni element: fiksirajmo jedan i označimo ga s n. Također je $R^{-1}[\{n\}]$ neprazni podskup od a (jer je $n \in \operatorname{rng} R$) pa ima minimalni element: fiksirajmo jedan i označimo ga s m. Tvrdimo da je (m,n) minimalni element u R: kad ne bi bio, postojao bi $(p,q) \in R$ takav da je $(p,q) < (m,n)$, što vodi na dvije mogućnosti. Prva je zbog $q \in \operatorname{rng} R$ u kontradikciji s minimalnošću n, a druga je zbog $p \in R^{-1}[\{q\}] = R^{-1}[\{n\}]$ u kontradikciji s minimalnošću m.

Tvrdnja (4) slijedi direktno iz tvrdnji (2) i (3). □

Vidimo da antileksikografski možemo urediti Kartezijev produkt, i to je prirodno smatrati općenitim „množenjem" uređenih skupova, koje čuva strukturu uređaja. No antileksikografski se uređaj može koristiti i za „zbrajanje": *konkatenacija* uređenih skupova $(a, \prec)$ i $(b, \lhd)$ je skup $a \times \{0\} \cup b \times \{1\} \subseteq (a \cup b) \times \{0,1\}$, uređen „antileksikografski". Pritom elemente prvog faktora $a \cup b$ uspoređujemo samo ako se druge komponente (0 ili 1) podudaraju, a onda su oni iz istog skupa (a ili b) pa ih znamo usporediti (relacijom $\prec$ odnosno $\lhd$).

Zadatak 2.16. *Dokažite da za konkatenaciju vrijedi analogon propoziciji 2.15.*

2.5 Relacije ekvivalencije

Kao što relacije uređaja predstavljaju generalizaciju pojma „manji”,
relacije ekvivalencije predstavljaju generalizaciju pojma „jednak”.

Definicija 2.17. Neka je a skup, i $\sim$ relacija na a. Kažemo da je $\sim$ *relacija ekvivalencije* na a ako je $\sim$ refleksivna na a, simetrična i tranzitivna. $\lhd$

Ako nemamo zadan skup nego samo relaciju, skup možemo rekonstruirati iz relacije, a onda je i refleksivnost na tom skupu posljedica preostalih svojstava.

Lema 2.18. *Neka je $\sim$ simetrična i tranzitivna relacija.*
Tada postoji jedinstveni skup a takav da je $\sim$ relacija ekvivalencije na a.

Dokaz. Za egzistenciju, tvrdimo da je $a := \mathrm{dom}(\sim)$ takav skup. Očito iz $x \sim y$ slijedi $x \in \mathrm{dom}(\sim) = a$ te po simetričnosti $y \sim x$ odnosno $y \in a$, pa je $(\sim) \subseteq a \times a$, odnosno $\sim$ jest relacija na a. Još je potrebno dokazati refleksivnost.

Neka je $x \in a$ proizvoljan. Po definiciji domene to znači da postoji y takav da je $x \sim y$. Po simetričnosti je tada i $y \sim x$, a onda po tranzitivnosti $x \sim y \sim x$ povlači $x \sim x$.

Za jedinstvenost, pretpostavimo da pored upravo definiranog $a = \mathrm{dom}(\sim)$ postoji još jedan skup b takav da je $\sim$ relacija ekvivalencije na b. Upravo smo vidjeli da $x \in a$ povlači $(x, x) \in (\sim) \subseteq b \times b$, dakle $x \in b$. S druge strane, $x \in b$ povlači $x \sim x$ po refleksivnosti, iz čega $x \in \mathrm{dom}(\sim) = a$. Po aksiomu ekstenzionalnosti, $b = a$. $\square$

Možemo li precizirati tvrdnju da relacija ekvivalencije generalizira jednakost? U jednom smjeru, jednakost na svakom skupu svakako jest relacija ekvivalencije. (Štoviše, čitava jednakost kao klasa $\{(x, x) : x \in \mathbf{V}\}$ zadovoljava svojstva relacije ekvivalencije do na činjenicu da nije skup. Takve klase zovemo *klasnim relacijama*.) No i u drugom smjeru, svaka relacija ekvivalencije može se prikazati kao jednakost na odgovarajući način „transformiranih” elemenata. Ta transformacija se zove *kvocijentnim preslikavanjem*, a njene vrijednosti se zovu *klasama ekvivalencije*.

Definicija 2.19. Neka je a skup, R relacija ekvivalencije na a, i $x \in a$. *Klasa ekvivalencije* elementa x s obzirom na R je $[x]_R := R[\{x\}]$ (slika skupa $\{x\}$ po relaciji R). Pišemo samo $[x]$ ako se R podrazumijeva. *Kvocijentni skup* skupa a po relaciji R je $a/_R := \{[x]_R : x \in a\}$. $\lhd$

Sada možemo formalizirati ideju „svaka ekvivalencija je jednakost”. (Dokaz je potpuno isti kao na Elementarnoj matematici, ali je dobra vježba vidjeti možete li ga reproducirati.)

Lema 2.20. *Neka je a skup, $\sim$ relacija ekvivalencije na a, te $x, y \in a$. Tada:*

1. *$x \sim y$ ako i samo ako je $[x] = [y]$ (klase ekvivalentnih elemenata su jednake).*
2. *$x \not\sim y$ ako i samo ako je $[x] \cap [y] = \emptyset$ (klase neekvivalentnih elemenata su disjunktne).*

Činjenica da je svaka relacija ekvivalencije svojevrsna jednakost ne znači nužno da se ponaša kao jednakost u formulama, u smislu da uvrštavanjem jednakih objekata u razne postupke ponovo dobivamo jednake objekte. Ako želimo provesti neki postupak na $[x]_\sim$, česta je strategija objasniti kako se provodi na x (rezultat tog postupka označimo s x'), ali tada moramo dokazati da $x \sim y$ povlači $x' \sim y'$, odnosno da je svejedno koji element (*reprezentant*) klase $[x]$ smo odabrali. Ta *neovisnost o reprezentantima* bit će prilično važna u daljnjem razvoju teorije.

2.6 Particije

Promatrajući svojstva kvocijentnog skupa, vidimo da nijedna klasa ekvivalencije nije prazna, različite klase su disjunktne, te je svaki element polaznog skupa u nekoj klasi. Bilo koju familiju skupova s tim svojstvima zovemo *particijom*.

Definicija 2.21. Neka su a i P skupovi. Kažemo da je P *particija* od a ako vrijede svojstva: $\emptyset \notin P$, $\bigcup P = a$ te $b = c \vee b \cap c = \emptyset$ za sve $b, c \in P$. ◁

Kao kod leme 2.18, ako nam a nije zadan, uvijek ga možemo jedinstveno rekonstruirati kao $a := \bigcup P$. No nas će zanimati particije konkretnog skupa, zbog njihove veze s relacijama ekvivalencije. Prvo samo ustanovimo da smo dobro formalizirali particije kao generalizacije kvocijentnih skupova.

Korolar 2.22. *Neka je a skup i $\sim$ relacija ekvivalencije na a. Tada je $a/_\sim$ particija od a.*

Dokaz. Prvo svojstvo slijedi iz činjenice da je svaki element od $a/_\sim$ oblika $[x]$ za neki $x \in a$, pa je neprazan jer sadrži x po refleksivnosti. Treće svojstvo slijedi direktno iz leme 2.20.

Drugo svojstvo dokazujemo pomoću dvije inkluzije:
($\subseteq$): Neka je $y \in [x] \in a/_\sim$. Tada je $x \sim y$ pa je $y \in a$ jer je $\sim$ relacija na a.
($\supseteq$): Za svaki $x \in a$ je $x \in [x] \in a/_\sim$, odnosno $x \in \bigcup(a/_\sim)$. □

Međutim, vrijedi i svojevrsni obrat: particije nisu u pravom smislu riječi generalizacije kvocijentnih skupova, jer je *svaka* particija zapravo kvocijentni skup s obzirom na neku relaciju ekvivalencije. Dokazi te i sličnih tvrdnji predstavljaju dobru vježbu.

Zadatak 2.23. *Neka je a skup. Za njegovu particiju P definiramo relaciju $\mathcal{E}q(P)$ pomoću $x \,\mathcal{E}q(P)\, y :\Longleftrightarrow (\exists b \in P)(\{x, y\} \subseteq b)$. Dokažite:*

1. *za svaku particiju P skupa a, $\mathcal{E}q(P)$ je relacija ekvivalencije na a.*
2. *za svaku particiju P skupa a vrijedi jednakost $P = a/_{\mathcal{E}q(P)}$.*
3. *za svaku relaciju ekvivalencije $\sim$ na a vrijedi jednakost $(\sim) = \mathcal{E}q(a/_\sim)$.*

2.7 Funkcije

Kao i relacije, funkcije ste upoznali na Elementarnoj matematici.
Međutim, teorija skupova modelira funkcije na nešto drugačiji način od onog koji ste tamo vidjeli, pa je dobro unekoliko raspisati detalje.

Definicija 2.24. Neka su a i b skupovi, i f relacija između njih. Kažemo da f *ima funkcijsko svojstvo* ako $x\ f\ y_1 \wedge x\ f\ y_2 \Rightarrow y_1 = y_2$. Ako uz to vrijedi $\operatorname{dom} f = a$, kažemo da je *funkcija sa a u b* i pišemo $f : a \to b$. Za funkciju f, ako inverzna relacija f^{-1} ima funkcijsko svojstvo, kažemo da je f *injekcija*, a ako je $\operatorname{rng} f = b$, kažemo da je f *surjekcija na b*. Ako za funkciju f vrijedi oboje, zovemo je *bijekcijom* između a i b. ◁

Primijetimo da uz takve definicije ne postoji jedinstvena „kodomena" funkcije: kad god je $f : a \to b \subset c$, tada je i $f : a \to c$ (u Elementarnoj matematici to su dvije različite funkcije). Posljedica toga je da ne postoji opći pojam „surjekcije": svaka funkcija je surjekcija na neki skup, konkretno na svoju sliku. (Jednako tako, svaka relacija s funkcijskim svojstvom je funkcija s nekog skupa: konkretno, sa svoje domene.) No injektivnost, kao i domena funkcije, pojmovi su koji ovise samo o funkciji kao takvoj.

Napomena 2.25. Dakle, čim imamo bijekciju f između a i b te $s \subseteq a$,
funkcija $f|_s$ je bijekcija između s i $f[s]$. ◁

Ono što ovdje zovemo funkcijom u Elementarnoj ste matematici zvali *grafom funkcije*.

Lema 2.26. *Za sve a, b i f, $f : a \to b$ je ekvivalentno s $f \subseteq a \times b \wedge (\forall x \in a)(\exists! y \in b)(x\ f\ y)$.*

Dokaz. ($\Rightarrow$) $f : a \to b$ svakako znači da je f relacija između a i b, dakle $f \subseteq a \times b$. Uzmimo proizvoljni $x \in a$. Zbog $a = \operatorname{dom} f$ postoji y takav da je $x\ f\ y$. Takav y mora biti iz b zbog $f \subseteq a \times b$, a mora biti jedinstven zbog funkcijskog svojstva od f.

($\Leftarrow$) Opet imamo da je f relacija između a i b, no sada trebamo dokazati da ima funkcijsko svojstvo i domenu a. Ovo drugo slijedi po aksiomu ekstenzionalnosti: ako je $x \in \operatorname{dom} f$, tada je $x\ f\ y$ za neki y, no $(x, y) \in f \subseteq a \times b$ povlači $x \in a$. Također, po pretpostavci za svaki $x \in a$ postoji y (iz b, jedinstven) takav da je $x\ f\ y$, pa je $x \in \operatorname{dom} f$.

Za funkcijsko svojstvo, neka je $x\ f\ y_1$ i $x\ f\ y_2$. Prema prethodno dokazanom je $x \in \operatorname{dom} f = a$ (i $y_1, y_2 \in b$), pa za njega postoji jedinstveni $y \in b$ takav da vrijedi $x\ f\ y$. To znači da je $y_1 = y$ i $y_2 = y$, pa i $y_1 = y_2$. □

Prema upravo dokazanoj lemi, za $f : a \to b$ i $x \in a$ postoji jedinstveni y takav da vrijedi $x\ f\ y$, pa možemo uvesti funkcijsku oznaku za njega koja spominje x i f. Naravno, oznaka koju uvodimo je $f(x)$. Takva oznaka ima smisla jedino za $x \in \operatorname{dom} f$, ali ponekad se radi određenosti definira i $f(x) := \emptyset$ za $x \notin \operatorname{dom} f$.

Primjer 2.27. Neka je a skup. Jednakost na a, relacija $id_a := \{(x, x) : x \in a\}$, očito ima funkcijsko svojstvo, i vrijedi $id_a : a \to a$. Štoviše, id_a je bijekcija između a i a. ◁

Mnoge operacije na relacijama *čuvaju* funkcije, u smislu da primijenjene na funkcijama ponovo daju funkcije. Ističemo tri najvažnije.

Propozicija 2.28. *Neka su a, b i c skupovi, i $f : a \to b$. Tada vrijede sljedeće tvrdnje:*

1. *ako je $c \subseteq a$, tada je $f|_c : c \to b$.*
2. *ako je $g : b \to c$, tada je $g \circ f : a \to c$.*
3. *ako je f bijekcija između a i b, tada je $f^{-1} : b \to a$.*

Dokaz. Za (1), iz $f \subseteq a \times b$ i $c \subseteq a$ slijedi $f|_c = f \cap (c \times \operatorname{rng} f) \subseteq (a \times b) \cap (c \times \operatorname{rng} f) \subseteq c \times b$. Također, za svaki $x \in c$ je $x \in a$ pa postoji $y \in b$ takav da je $x\ f\ y$. Tada je $y \in \operatorname{rng} f$, pa je $(x, y) \in c \times \operatorname{rng} f$, što zajedno s $x\ f\ y$ daje $x\ (f|_c)\ y$. Jedinstvenost takvog $y \in b$ slijedi iz funkcijskog svojstva od f, jer $x\ (f|_c)\ y$ povlači $x\ f\ y$.

Za (2), iz $x\ (g \circ f)\ z$ slijedi da postoji y takav da vrijedi $x\ f\ y\ g\ z$, pa iz $(x, y) \in f$ slijedi $x \in a$, a iz $(y, z) \in g$ slijedi $z \in c$. Tada je $(x, z) \in a \times c$, pa je $g \circ f$ relacija između a i c. Uzmimo sada $x \in a$. Za njega postoji $y \in b$ takav da je $x\ f\ y$, a za njega pak postoji $z \in c$ takav da je $y\ g\ z$. Sve u svemu, imamo $x\ (g \circ f)\ z$ za $z \in c$, još samo trebamo dokazati jedinstvenost. Neka je $x\ (g \circ f)\ z_1$ i $x\ (g \circ f)\ z_2$. Tada postoje y_1 i y_2 takvi da je $x\ f\ y_1\ g\ z_1$ i $x\ f\ y_2\ g\ z_2$. Iz funkcijskog svojstva od f slijedi $y_1 = y_2$, a onda iz funkcijskog svojstva od g slijedi $z_1 = z_2$.

Dokazati (3) lakše je po definiciji: inverzna relacija f^{-1} je između b i a, njeno funkcijsko svojstvo je upravo injektivnost od f, a $\operatorname{dom}(f^{-1}) = \operatorname{rng} f = b$ zbog surjektivnosti. □

Neke od tih operacija čuvaju i dodatna svojstva.

Propozicija 2.29. *Kompozicija relacija s funkcijskim svojstvom je ponovo relacija s funkcijskim svojstvom. Kompozicija injekcijā je ponovo injekcija.*

Dokaz. Prva tvrdnja dokazuje se slično kao jedinstvenost u tvrdnji (2) propozicije 2.28.

Neka su f i g injekcije. Lako se vidi da je $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ — naime, $x\ (g \circ f)^{-1}\ y$ znači $y\ (g \circ f)\ x$, odnosno postoji z takav da vrijedi $y\ f\ z\ g\ x$. To pak možemo zapisati kao $x\ g^{-1}\ z\ f^{-1}\ y$, odnosno $x\ (f^{-1} \circ g^{-1})\ y$. Sada druga tvrdnja slijedi iz prve i iz upravo dokazane jednakosti: ako f^{-1} i g^{-1} imaju funkcijsko svojstvo, onda ga ima i njihova kompozicija. □

Propozicija 2.30. *Ako su a, b i c skupovi te f bijekcija između a i b, i g bijekcija između b i c, tada je:*

1. *$g \circ f$ bijekcija između a i c;*
2. *f^{-1} bijekcija između b i a.*

Dokaz. Za tvrdnju (1), već smo dokazali da je $g \circ f$ funkcija između a i c, te da je injekcija. Još trebamo dokazati surjektivnost, i to samo inkluziju $c \subseteq \operatorname{rng}(g \circ f)$. Neka je $z \in c$ proizvoljan. Jer je g surjekcija na c, postoji $y \in b$ takav da je $z = g(y)$, a jer je f surjekcija na b postoji i $x \in a$ takav da je $y = f(x)$. Sada $x\ f\ y\ g\ z$ znači da je $z = (g \circ f)(x) \in \operatorname{rng}(g \circ f)$.

Za tvrdnju (2), već smo dokazali da je f^{-1} funkcija između b i a, čija injektivnost slijedi iz funkcionalnosti od $(f^{-1})^{-1} = f$. Surjektivnost na a slijedi iz $\operatorname{rng}(f^{-1}) = \operatorname{dom} f = a$. □

Vrijedi i svojevrsni obrat propozicije 2.30(2), koji ponekad koristimo kad želimo dokazati da je neka funkcija bijekcija.

Lema 2.31. *Neka su a i b skupovi te $f : a \to b$. Tada je f bijekcija između a i b ako i samo ako postoji funkcija $g : b \to a$ takva da je $g \circ f = id_a$ i $f \circ g = id_b$.*

Dokaz (Skica; raspišite!). Za smjer ($\Rightarrow$), uzmimo $g := f^{-1}$. Lako je vidjeti da je $f^{-1} \circ f = id_a$ i $f \circ f^{-1} = id_b$ ako je f bijekcija. Za smjer ($\Leftarrow$), injektivnost slijedi iz postojanja funkcije g sa svojstvom $g \circ f = id_a$ (*lijevog inverza*), a surjektivnost iz postojanja funkcije g sa svojstvom $f \circ g = id_b$ (*desnog inverza*). □

Zadatak 2.32. *Što mislite, može li se samo iz injektivnosti funkcije zaključiti da ona ima lijevi inverz? Može li se samo iz surjektivnosti zaključiti da ima desni inverz?*

2.8 Shema aksioma zamjene

Često funkciju f definiramo tako da specificiramo domenu a (i kodomenu, ali ona je zapravo nebitna u prije opisanom smislu) te pravilo pridruživanja $f(x) := \tau$, gdje je τ neki izraz (logički *term*) koji najčešće ima slobodnu varijablu x (primjeri: $x \times \{\emptyset\}$, $x \cap \mathscr{P}(x)$, $\bigcup x$). To zapravo znači da definiramo $f := \{(x, \tau) : x \in a\}$ — ali kako znamo da je to skup?

Kad bismo znali da je *slika* te funkcije, odnosno klasa $\{\tau : x \in a\}$, skup, dalje bi bilo lako. Ako je označimo s b, tada je f dobivena separacijom iz $a \times b$ pomoću formule sa slobodnom varijablom p, koja glasi $(\exists x \in a)(\exists y \in b)\big(p = (x, y) \wedge y = \tau\big)$. Logičko opravdanje terma τ je (u našoj teoriji) jednostavno: svaki term možemo zapisati u obliku $\tau = \{z : \psi\}$ gdje je ψ „dobra" formula sa slobodnim varijablama z i x. Dakle, dio $y = \tau$ je zapravo pokrata za formulu $\varphi := \forall z(z \in y \leftrightarrow \psi)$. Puno je zanimljivije pitanje: kako znamo da je b skup?

Rekli smo da su „male" klase uvijek skupovi. Ako već imamo skup a, i za svaki $x \in a$ imamo jedinstveni objekt τ, očito takvih objekata ne može biti više nego elemenata od a; pa ako je a „dovoljno malen", mora i b biti takav. To ćemo formalizirati u sljedećoj točki — *ekvipotentnošću* skupova, ali da bismo uopće znali da govorimo o skupovima, treba nam novi aksiom *zamjene* (tako nazvan jer u skupu a svaki x „zamjenjujemo" odgovarajućim τ). Zapravo, radi se o shemi aksioma, jer za svaku formulu φ (određenu, kako smo napisali, „dobrom" formulom ψ) imamo zasebnu instancu.

Da bismo opisali sve moguće instance, mogli bismo odgovarajuće formule φ karakterizirati sintaksno, slično kao što smo to učinili kod sheme aksioma separacije; ali ovdje je to kompliciranije, jer ne znamo sintaksno karakterizirati „dobre" formule ψ. Mnoge familije takvih formula znamo karakterizirati, ali u tim slučajevima nam ne treba novi aksiom. Konstrukcija situacije u kojoj se baš ne možemo izvući bez korištenja aksioma zamjene dosta je kompliciranа, ali intuitivno, zamislimo nastavak kumulativne hijerarhije nakon V_ω:

$$V_{\omega+1} := \mathscr{P}(V_\omega), \quad V_{\omega+2} := \mathscr{P}(V_{\omega+1}), \quad \ldots, \quad V_{\omega\cdot 2} = \bigcup_{i<\omega} V_{\omega+i}. \tag{2.2}$$

Da bismo konstruirali $V_{\omega\cdot 2}$ moramo primijeniti aksiom unije na familiju $\{V_{\omega+i} : i < \omega\}$, no da bismo to mogli, moramo prvo znati da je ta familija skup — a to će slijediti iz aksioma zamjene (jednom kad znamo da je ω skup, za što će nam trebati još jedan aksiom).

Zato ćemo pri zapisivanju aksioma zamjene koristiti drugi, „semantički" pristup: formule φ koje nas zanimaju bit će opisane kao one koje zadovoljavaju uvjet $(\forall x \in a)\exists! y\, \varphi$. Tako nas ne zanima koje su formule dobre, dok god imamo jedinstveni skup y za sve $x \in a$. Primijetimo da prije navedeni oblik formule $\varphi := \forall z(z \in y \leftrightarrow \psi)$ zadovoljava taj uvjet: egzistenciju jer je ψ „dobra" formula (rekli smo da vezane varijable uvijek označuju skupove!), a jedinstvenost po napomeni 1.1.

Shema će biti iskazana u obliku implikacije s tim uvjetom, tako da će one instance čije formule φ ne zadovoljavaju taj uvjet biti trivijalno istinite. Slični trik smo koristili kod iskazivanja univerzalne kvantifikacije po skupu a, gdje je iskaz $\forall x(x \in a \to \cdots)$ služio da restringira ostatak formule samo na elemente od a. Sve u svemu, shema aksioma zamjene glasi:

$$(\forall x \in a)\exists! y\, \varphi \to \exists b\, \forall y\big(y \in b \leftrightarrow (\exists x \in a)\varphi\big), \tag{2.3}$$

gdje je φ proizvoljna formula u kojoj varijabla b nije slobodna. Kao što smo već nekoliko puta rekli, možemo ispred napisati $\forall a$, ali isto tako i $\forall x_i$ za sve slobodne varijable formule φ — ali ne trebamo, u skladu s dogovorenim shvaćanjem istinitosti formula sa slobodnim varijablama.

Aksiom zamjene nam omogućuje da funkciju f zadamo samo navodeći domenu a i pravilo pridruživanja (term τ), i budemo sigurni da smo dobili skup, odnosno objekt u našoj teoriji. To ćemo ubuduće često koristiti. U većini slučajeva (recimo, kad već imamo kodomenu — neki skup b takav da je $\tau \in b$ za svaki $x \in a$) se možemo izvući i lakše, ali za sasvim općenitu definiciju funkcije tog oblika aksiom zamjene je nužan.

Zamjenjujući a klasom u takvoj formuli dobivamo i pojam *klasne funkcije*: klase uređenih parova s funkcijskim svojstvom. Važni primjeri su klasni hipernizovi (definirani na klasi svih ordinala), i skupovne operacije (recimo, presjek je klasna funkcija $(\cap) : \mathbf{V} \times \mathbf{V} \to \mathbf{V}$).

3 Kardinalnost

3.1 Ekvipotentnost

Formalizacija pojma funkcije (a posebno pojmova injekcije i bijekcije) omogućuje nam preciziranje intuicije koja stoji iza određivanja broja elemenata nekog skupa. Iako je brojenje elemenata konačnih skupova vrlo jednostavna operacija, formalnije zaključivanje nam je potrebno za beskonačne skupove — prvo, jer nam prirodni brojevi više nisu dovoljni, a drugo, jer neke zakonitosti koje smo naučili za konačne skupove (recimo, da skup ima strogo više elemenata od svog pravog podskupa) ne vrijede općenito.

Što smo zapravo učinili kad smo utvrdili da neki skup A ima 3 elementa? Operativno, uzeli smo (ili pokazali na) neki element skupa A i pritom rekli „jedan". Tako uspostavljamo funkciju f između nekog skupa hrvatskih imena za prirodne brojeve, i skupa A. Zatim smo uzeli neki element skupa A različit od upravo uzetog i pritom rekli „dva". Uzimanje uvijek različitih (još neodabranih) elemenata znači da je f injekcija. Onda smo ponovo uzeli neki još neupotrijebljeni element od A i pritom rekli „tri". Tada smo shvatili da smo iscrpili sve elemente od A, odnosno da je f surjekcija na A, i time bijekcija između skupova {„jedan", „dva", „tri"} i A. Posljednji upotrijebljeni element domene („tri") zovemo *brojem elemenata* od A.

Ako taj postupak želimo provesti za beskonačni skup A, prvi problem koji upada u oči je nezgrapnost imena za brojeve — ovisno o tome kojeg jezikoslovca pitate, hrvatski jezik ili nema imena za sve prirodne brojeve, ili ih ima, ali su vrlo nespretna za formaliziranje. No fundamentalniji je problem u tome što ne postoji uvijek „posljednji upotrijebljeni element domene" (recimo, ako prebrajamo skup $\mathbb{N}$ standardnim redoslijedom). Oba problema ćemo riješiti, formalnim uvođenjem prirodnih brojeva (kao skupova) u poglavlju 4 te njihovom generalizacijom na *ordinale* u poglavlju 6. Zasad se usredotočimo na drugi dio postupka prebrajanja: uspostavljanje bijekcije između skupova.

Definicija 3.1. Za skupove a i b kažemo da su *ekvipotentni*, i pišemo $a \sim b$, ako postoji bijekcija između njih. ◁

Teorem 3.2. *Ekvipotentnost je klasna relacija ekvivalencije (na klasi* **V** *svih skupova).*

Dokaz. Refleksivnost je posljedica primjera 2.27: id_a pokazuje $a \sim a$.

Simetričnost slijedi iz propozicije 2.30(2): ako f pokazuje $a \sim b$, tada f^{-1} pokazuje $b \sim a$.

Tranzitivnost je posljedica propozicije 2.30(1): ako f pokazuje $a \sim b$, a g pokazuje $b \sim c$, tada $g \circ f$ pokazuje $a \sim c$. □

Klase ekvivalencije ekvipotentnosti zovemo *kardinalnostima*, i označavamo $\mathfrak{K}(a) := [a]_\sim$. To su prave klase (osim $\mathfrak{K}(\emptyset) = \{\emptyset\}$, koja je jednočlana), pa ćemo trebati razviti posebne metode da bismo ih reprezentirali pomoću skupova (*kardinalnih brojeva* ili *kardinala*). Ako ih budemo trebali stavljati u skupove (sjetimo se da prave klase ne mogu biti elementi skupova), pretvarat ćemo se da već imamo neke fiksirane reprezentante koje ćemo zapravo stavljati u skupove. Kasnije (teorem 7.13) ćemo objasniti kako fiksirati te reprezentante.

Zasad samo opišimo što s kardinalnostima možemo raditi. To ćemo opisati preko reprezentanata, ali se nećemo baviti specifičnim reprezentantima, nego ćemo dokazati da provedeni postupci *ne ovise o reprezentantima*. Tako ćemo, jednom kad uvedemo kardinale kao konkretne reprezentante, znati da sva dokazana svojstva tih operacija i dalje vrijede.

3.2 Operacije na kardinalnostima

Najjednostavnija operacija na kardinalnostima vjerojatno je množenje.
Princip produkta iz Diskretne matematike kaže nam da je broj elemenata u Kartezijevom produktu dva konačna skupa jednak umnošku brojeva elemenata pojedinih skupova.
To možemo generalizirati na beskonačne skupove kao *definiciju* umnoška.

Propozicija 3.3. *Za bilo koje skupove a, b, c i d, $a \sim c$ i $b \sim d$ povlače $a \times b \sim c \times d$.*

Dokaz. Neka je f bijekcija između a i c te g bijekcija između b i d. Definiramo funkciju $h : a \times b \to c \times d$ kao $h(x,y) := \big(f(x), g(y)\big)$, i tvrdimo da je to bijekcija između $a \times b$ i $c \times d$.

Za sve $(x,y) \in a \times b$ je po definiciji Kartezijevog produkta $x \in a$ i $y \in b$, pa je $f(x) \in c$ i $g(y) \in d$, odnosno $h(x,y) \in c \times d$, pa imamo funkciju između ta dva skupa. Za injektivnost, iz $h(x,y) = h(x',y')$ slijedi (po propoziciji 1.7) $f(x) = f(x')$ i $g(y) = g(y')$. Po injektivnosti funkcijā f i g imamo $x = x'$ i $y = y'$, odnosno $(x,y) = (x',y')$. Za surjektivnost, lako se vidi da je $\operatorname{rng} h = \operatorname{rng} f \times \operatorname{rng} g$, što je jednako $c \times d$ zbog surjektivnosti funkcijā f i g. □

Definicija 3.4. Za proizvoljne kardinalnosti $\mathfrak{K}(a)$ i $\mathfrak{K}(b)$ (dakle za proizvoljne skupove a i b, ali neovisno o reprezentantima), definiramo *umnožak* $\mathfrak{K}(a) \cdot \mathfrak{K}(b) := \mathfrak{K}(a \times b)$. ◁

Neovisnost o reprezentantima definicije 3.4 izrečena je u propoziciji 3.3. Tako ćemo i za ostale operacije, prije definicije pomoću reprezentanata dokazati propoziciju koja kaže da definicija ne ovisi o reprezentantima.

Zbrajanje je također jednostavna operacija, i odgovara uniji, ali moramo osigurati da su skupovi disjunktni. Srećom, to nije teško.

Zadatak 3.5. *Dokažite da za svaka dva skupa postoje disjunktni ekvipotentni skupovi. Precizno, za proizvoljne skupove a i b postoje skupovi $a' \sim a$ i $b' \sim b$ takvi da je $a' \cap b' = \emptyset$. Uputa: promotrite skupove $a \times \{\emptyset\}$ i $b \times \big\{\{\emptyset\}\big\}$.*

Propozicija 3.6. *Za bilo koje skupove a, b, c i d takve da je $a \cap b = c \cap d = \emptyset$, $a \sim c$ i $b \sim d$ povlače $a \cup b \sim c \cup d$.*

Dokaz. Neka je f bijekcija između a i c te g bijekcija između b i d. Definiramo funkciju $h : a \cup b \to c \cup d$ pomoću $h(x) := \begin{cases} f(x), & x \in a \\ g(x), & x \in b \end{cases}$. Zbog $a \cap b = \emptyset$ je definicija po slučajevima dobra (pokušajte precizirati odgovarajući term τ!), a zbog $f(x) \in c$ za $x \in a$ te $g(x) \in d$ za $x \in b$ je $h(x) \in c \cup d$.

Za injektivnost, neka je $h(x) = h(x')$, za $x, x' \in a \cup b$. Kad bi x i x' bili u različitim skupovima, recimo $x \in a \wedge x' \in b$, tada $h(x) \in c$ i $h(x') \in d$ ne bi nikako mogli biti jednaki zbog disjunktnosti c i d. Dakle, x i x' su u istom skupu. Ako je to skup a tada je $f(x) = h(x) = h(x') = f(x')$ pa je $x = x'$ zbog injektivnosti od f; analogno, ako su oba u b tada su jednaki zbog injektivnosti od g. Za surjektivnost, opet, lako se vidi $\operatorname{rng} h = \operatorname{rng} f \cup \operatorname{rng} g$, što je jednako $c \cup d$ zbog surjektivnosti funkcijā f i g. □

Definicija 3.7. Za proizvoljne kardinalnosti $\mathfrak{K}(a)$ i $\mathfrak{K}(b)$ skupova takvih da je $a \cap b = \emptyset$, definiramo *zbroj* kao $\mathfrak{K}(a) + \mathfrak{K}(b) := \mathfrak{K}(a \cup b)$. ◁

Pri definiranju zbrajanja i množenja kardinalnosti poslužili su nam kombinatorni principi sume i produkta redom. Možemo reći i da nam je za definiciju jednakosti kardinalnosti (ekvipotentnosti) poslužio princip bijekcije. Za potenciranje trebamo malo razmisliti. Što brojimo kad kažemo da je $3^4 = 81$? „Permutacije s ponavljanjem", odnosno uređene četvorke čije su komponente elementi nekog tročlanog skupa. Već znamo da uređene četvorke možemo shvatiti kao funkcije s četveročlanom domenom, i eto nam odgovora: pri računanju $\mathfrak{K}(b)^{\mathfrak{K}(a)}$ brojimo sve funkcije s a u b. Precizno, za skupove a i b definiramo

$$^a b := \{f : (f : a \to b)\}. \tag{3.1}$$

To jest skup jer je svaka f podskup od $a \times b$, pa je $^a b$ dobiven separacijom iz $\mathscr{P}(a \times b)$, što je skup po aksiomu partitivnog skupa i propoziciji 1.11.

Propozicija 3.8. *Za bilo koje skupove a, b, c i d, $a \sim c$ i $b \sim d$ povlače $^a b \sim {}^c d$.*

Dokaz. Neka je f bijekcija između a i c te g bijekcija između b i d. Za svaku funkciju $u \in {}^a b$ definiramo $h(u) := g \circ u \circ f^{-1}$. Iz propozicije 2.28 slijedi da je $h(u) \in {}^c d$. Želimo dokazati da je h bijekcija između $^a b$ i $^c d$.

To možemo elegantno po lemi 2.31: tvrdimo da je s $k(v) := g^{-1} \circ v \circ f$ zadan inverz funkcije h. Doista, za sve $u \in {}^a b$ i za sve $v \in {}^c d$ vrijedi

$$k\big(h(u)\big) = g^{-1} \circ (g \circ u \circ f^{-1}) \circ f = (g^{-1} \circ g) \circ u \circ (f^{-1} \circ f) = id_b \circ u \circ id_a = u, \text{ i} \tag{3.2}$$

$$h\big(k(v)\big) = g \circ (g^{-1} \circ v \circ f) \circ f^{-1} = (g \circ g^{-1}) \circ u \circ (f \circ f^{-1}) = id_d \circ v \circ id_c = v, \tag{3.3}$$

koristeći asocijativnost operacije komponiranja i činjenicu da su identitete svojevrsni „neutralni elementi" za tu operaciju. □

Definicija 3.9. Za proizvoljne kardinalnosti $\mathfrak{K}(a)$ i $\mathfrak{K}(b)$ definiramo $\mathfrak{K}(b)^{\mathfrak{K}(a)} := \mathfrak{K}(^a b)$. ◁

3.3 Uređaj na kardinalnostima

Vidjeli smo kako kardinalnosti možemo preko njihovih reprezentanata uspoređivati s obzirom na jednakost, zbrajati, množiti i potencirati. Sada ćemo vidjeti i kako ih možemo uspoređivati „po veličini". Precizno, definirat ćemo refleksivni parcijalni uređaj na klasi svih kardinalnosti, tako da definiramo refleksivnu i tranzitivnu relaciju na reprezentantima, takvu da odgovarajuća relacija na klasama ne ovisi o tome koje smo reprezentante uzeli. Antisimetričnost te relacije (na klasama) je nešto kompliciranija, i dokazat ćemo je kasnije. Zasad ćemo dokazati da su operacije iz prethodne točke (uz neka ograničenja) *monotone* (rastuće) s obzirom na tu relaciju.

Valjda je najprirodniji uređaj na skupovima, koji smo već vidjeli, inkluzija. Želimo je iskoristiti za definiciju uređaja: podskup ima manju kardinalnost od nadskupa. S tim pristupom postoje dva problema. (Za njihovu ilustraciju koristimo neformalne prirodne brojeve.)

Prvi je da takav uređaj ne može biti strog: za beskonačne skupove, sasvim je moguće da je (pravi) podskup ekvipotentan nadskupu. Recimo (sjetite se, $0 \in \mathbb{N}$!), $\mathbb{N} \sim \mathbb{N} \setminus \{0\}$: sljedbenik je bijekcija između ta dva skupa. Zato ćemo morati definirati refleksivni uređaj, a strogi uređaj ćemo definirati iz njega pomoću leme 2.3.

Drugi problem je da inkluzija sama po sebi ovisi o reprezentantima: recimo, $\{1\} \subset \{1,2\}$, ali $\{1\} \sim \{3\} \not\subset \{1,2\}$. Zato ćemo morati „zatvoriti" inkluziju s obzirom na ekvipotentnost. Precizno, želimo relaciju $\subsetneq$ koja zadovoljava sljedeća dva svojstva:

inkluzivnost: ako je $a \subseteq b$, tada je $a \subsetneq b$;

neovisnost o reprezentantima: ako je $a \subsetneq b$, $a \sim c$ i $b \sim d$, tada je i $c \subsetneq d$.

Propozicija 3.10. *Najmanja klasna relacija koja zadovoljava inkluzivnost i neovisnost o reprezentantima je*

$$a \subsetneq b :\Longleftrightarrow \textit{postoji injekcija s } a \textit{ u } b. \tag{3.4}$$

Dokaz. Prvo dokažimo da tako definirana relacija ima tražena svojstva. Za inkluzivnost, znamo da je $id_a : a \to a$ injektivna, a iz $a \subseteq b$ slijedi i $id_a : a \to b$. Kako je injektivnost svojstvo funkcije same (koje ne ovisi o kodomeni), našli smo injekciju s a u b.

Za neovisnost o reprezentantima, neka je $f : a \to b$ injekcija te $g : a \to c$ bijekcija između a i c, i $h : b \to d$ bijekcija između b i d. Iz toga vidimo da je $g^{-1} : c \to a$ bijekcija između c i a, te je $h \circ f : a \to d$ injekcija kao kompozicija dvije injekcije. Na kraju je onda i $h \circ f \circ g^{-1} : c \to d$ injekcija kao kompozicija dvije injekcije, što smo trebali dokazati.

Trebamo još dokazati da je to *najmanja* relacija s tim svojstvima, odnosno da čim klasna relacija $\mathbf{R}$ ima ista svojstva, vrijedi $(\subsetneq) \subseteq \mathbf{R}$. Ova ideja „najmanje relacije s nekim svojstvima", u smislu „ima ta svojstva i potklasa je svake druge relacije koja ima ista svojstva" sasvim je analogna definiciji najmanjeg elementa u parcijalno uređenom skupu, osim što formalno klase (pa tako ni klasne relacije) ne mogu biti elementi skupova.

U svakom slučaju, neka klasna relacija $\mathbf{R}$ ima zahtijevana svojstva, i neka je $a \subsetneq b$. Trebamo dokazati $a\ \mathbf{R}\ b$. Po pretpostavci, postoji injekcija $f : a \to b$. Tada je i (po zadatku 2.1) $f : a \to c := \operatorname{rng} f \subseteq b$. Kako je f injekcija, vidimo da je i bijekcija između a i c (surjekcija je po definiciji skupa c), pa vrijedi $a \sim c$. Jer je $\mathbf{R}$ inkluzivna, iz $c \subseteq b$ slijedi $c\ \mathbf{R}\ b$, a jer je neovisna o reprezentantima, iz $a \sim c\ \mathbf{R}\ b \sim b$ napokon dobivamo $a\ \mathbf{R}\ b$, što smo htjeli. □

Zadatak 3.11. *Neka je a skup i R relacija na a.*
Dokažite da je $R \cup R^{-1}$ najmanja simetrična relacija koja sadrži R.

Definicija 3.12. Za proizvoljne skupove a i b definiramo $\mathfrak{K}(a) \leq \mathfrak{K}(b) :\Leftrightarrow a \subsetneq b$. ◁

Propozicija 3.10 kaže da ta definicija ne ovisi o reprezentantima. Primijetimo da uređaj na kardinalnostima nije nužno skup, jer sve kardinalnosti ne čine skup. Jednom kad definiramo kardinalne brojeve kao reprezentante kardinalnosti, vidjet ćemo da se zapravo radi o klasnoj relaciji (točnije, o pravoj klasi uređenih parova kardinalnih brojeva). Zasad samo dokažimo neka njena svojstva (za koja uopće nije bitno radi li se o skupu).

Korolar 3.13. *Klasna relacija $\leq$ na kardinalnostima je refleksivna i tranzitivna.*

Dokaz. Za refleksivnost, id_a je injekcija s a u a, za bilo koji skup a. Za tranzitivnost, samo treba primijetiti da je kompozicija injekcije s a u b i injekcije s b u c, injekcija s a u c. □

Antisimetričnost, koja će nam pokazati da se radi o parcijalnom uređaju, je mnogo kompliciranija: ako imamo injekciju s a u b i neku drugu injekciju s b u a, možemo li konstruirati bijekciju između a i b? Pokazat će se da možemo, i to će biti prvi „ozbiljniji" teorem teorije skupova koji ćemo dokazati. Zapravo, puno kasnije ćemo čak dokazati da se radi o totalnom, pa i o dobrom uređaju na kardinalnim brojevima.

3.4 Svojstva operacija na kardinalnostima

S obzirom na jednakost i uređaj, već sad možemo dokazati mnoga svojstva uvedenih operacija na kardinalnostima: zbrajanja, množenja i potenciranja. Svi ti dokazi su vrlo slični: konstruiramo injekcije ili bijekcije među skupovima određenog oblika, eventualno koristeći već zadane injekcije.

Teorem 3.14. *Neka su α, β i γ proizvoljne kardinalnosti, $0 = \mathfrak{K}(\emptyset)$ i $1 = \mathfrak{K}(\{\emptyset\})$. Tada vrijedi:*

$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma \qquad \alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$$
$$\alpha + \beta = \beta + \alpha \qquad \alpha \cdot \beta = \beta \cdot \alpha$$
$$\alpha + 0 = \alpha \cdot 1 = \alpha^1 = \alpha \qquad \alpha \cdot 0 = 0 \wedge 1^\alpha = \alpha^0 = 1$$
$$\alpha \neq 0 \wedge \beta \leq \gamma \Rightarrow \alpha^\beta \leq \alpha^\gamma \qquad \alpha \neq 0 \Rightarrow 0^\alpha = 0$$
$$(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma \qquad (\alpha \cdot \beta)^\gamma = \alpha^\gamma \cdot \beta^\gamma$$
$$\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma \qquad \alpha^{\beta \cdot \gamma} = \left(\alpha^\beta\right)^\gamma$$
$$\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma \wedge \alpha \cdot \gamma \leq \beta \cdot \gamma \wedge \alpha^\gamma \leq \beta^\gamma$$

Dokaz. Neka su a, b i c reprezentanti takvi da je $\alpha = \mathfrak{K}(a)$, $\beta = \mathfrak{K}(b)$ i $\gamma = \mathfrak{K}(c)$. Dokazali smo da nije bitno koje reprezentante odaberemo. Dokazat ćemo neka svojstva za primjer, svakako je korisno raspisati i ostala.

[asocijativnost zbrajanja]: Pogledajmo skupove $a' := a \times \{\emptyset\}$, $b' := b \times \big\{\{\emptyset\}\big\}$ i $c' := c \times \big\{\{\{\emptyset\}\}\big\}$. Lako se vidi da su svi ti skupovi u parovima disjunktni: recimo, $z \in b' \cap c'$ bi morao biti oblika $z = \big(x, \{\{\emptyset\}\}\big) = \big(y, \{\{\{\emptyset\}\}\}\big)$, što bi povlačilo $\{\emptyset\} \in \big\{\{\emptyset\}\big\} = \big\{\{\{\emptyset\}\}\big\}$, odnosno po aksiomu para $\{\emptyset\} = \big\{\{\emptyset\}\big\}$, i opet istim razmišljanjem $\emptyset = \{\emptyset\}$, odnosno $\emptyset \in \emptyset$, što je nemoguće po aksiomu praznog skupa.

Kako su a' i b' disjunktni s c', takva je i njihova unija, zbog distributivnosti unije prema presjeku: $(a' \cup b') \cap c' = (a' \cap c') \cup (b' \cap c') = \emptyset \cup \emptyset = \emptyset$. Jednako tako, a' je disjunktan s $b' \cup c'$. To znači da na lijevoj strani stoji kardinalnost skupa $a' \cup (b' \cup c')$, a na desnoj kardinalnost skupa $(a' \cup b') \cup c'$, no to je jedan te isti skup zbog asocijativnosti unije.

[$\alpha^0 = 1$]: Trebamo konstruirati bijekciju između skupova ${}^{\emptyset}a$ i $\{\emptyset\}$. Štoviše, dokazat ćemo da su ta dva skupa jednaka po aksiomu ekstenzionalnosti. Elementi skupa ${}^{\emptyset}a$ su funkcije $f : \emptyset \to a$; svaka takva mora biti relacija između $\emptyset$ i a, dakle $f \subseteq \emptyset \times a = \emptyset$, iz čega slijedi da je $f = \emptyset \in \{\emptyset\}$. S druge strane, $\emptyset$ je svakako relacija između $\emptyset$ i a, i ima funkcijsko svojstvo: za sve parove iz $\emptyset$ vrijedi što god želimo. Dakle, ${}^{\emptyset}a = \{\emptyset\}$, pa i ${}^{\emptyset}a \sim \{\emptyset\}$ po refleksivnosti.

[$\alpha \neq 0 \wedge \beta \leq \gamma \Rightarrow \alpha^\beta \leq \alpha^\gamma$]: Prva pretpostavka po kontrapoziciji kaže da je a neprazan, dakle ima element. Uzmimo jedan njegov element i označimo ga s t. Druga pretpostavka kaže da imamo injekciju $f : b \to c$. Želimo konstruirati injekciju h sa skupa ${}^{b}a$ u skup ${}^{c}a$, odnosno svakoj funkciji $g : b \to a$ pridružiti funkciju $h(g) : c \to a$, i to tako da različitim funkcijama pridružimo različite funkcije. Kako to učiniti?

Neka je $z \in c$ proizvoljan. Kad bismo imali neki $y \in b$, mogli bismo z jednostavno preslikati u $g(y)$. Imamo li ga? Ako je $z \in \operatorname{rng} f$, zbog injektivnosti od f postoji jedinstveni $y := f^{-1}(z) \in b$ koji se u njega preslika. Tada definiramo $\big(h(g)\big)(z) := g\big(f^{-1}(z)\big)$. No što ako $z \notin \operatorname{rng} f$? Sve što trebamo je neki element od a, a njega smo fiksirali na početku. Dakle, za $z \notin \operatorname{rng} f$ definiramo $\big(h(g)\big)(z) := t$. Time je $h(g) : c \to a$ u potpunosti definirana, a kako je $g \in {}^{b}a$ bila proizvoljna, na taj način smo definirali i funkciju h.

Dokažimo da je h injekcija: u tu svrhu, neka su $g \neq g'$ dvije funkcije s b u a. Nije teško vidjeti da su funkcije s istom domenom, koje se razlikuju kao skupovi, različite i u smislu kolegija Elementarna matematika: postoji element domene na kojem poprimaju različite vrijednosti. Dakle, uzmimo jedan $y \in b$ takav da je $g(y) \neq g'(y)$. Označimo $z := f(y) \in c$. Tada je $\big(h(g)\big)(z) = g\big(f^{-1}(f(y))\big) = g(y) \neq g'(y) = \big(h(g')\big)(z)$, pa mora biti $h(g) \neq h(g')$.

[$\alpha^{\beta \cdot \gamma} = \big(\alpha^\beta\big)^\gamma$]: Trebamo uspostaviti bijekciju h između skupova funkcija ${}^{b \times c}a$ i ${}^{c}\big({}^{b}a\big)$, odnosno svakoj funkciji $f : b \times c \to a$ pridružiti bijektivno neku funkciju $h(f) : c \to {}^{b}a$. Da bismo definirali $h(f)$, moramo je definirati u svakom elementu od c, pa neka je $z \in c$. Tada $\big(h(f)\big)(z)$ mora biti funkcija s b u a, odnosno svakom elementu $y \in b$ mora pridružiti neki element iz a. Koji? Prirodno se nameće da primijenimo f na uređeni par (y, z). Dakle, definicijom $\big((h(f))(z)\big)(y) := f\big((y, z)\big)$ je definirana funkcija $h : {}^{b \times c}a \to {}^{c}\big({}^{b}a\big)$, samo još treba vidjeti da je bijekcija.

Za injektivnost, ako su $f \neq f'$ dvije različite funkcije s $b \times c$ u a, postoji konkretni uređeni par (svi elementi Kartezijevog produkta su uređeni parovi) $(y', z') \in b \times c$ takav da je $f\big((y', z')\big) \neq f'\big((y', z')\big)$. To možemo zapisati kao $\big((h(f))(z')\big)(y') \neq \big((h(f')(z')\big)(y')$, iz čega dvaput primijenjenom kontrapozicijom dobijemo $h(f) \neq h(f')$.

Za surjektivnost, neka je $g : c \to {}^b a$ proizvoljna. Želimo definirati $f : b \times c \to a$ takvu da je $h(f) = g$. Gledajući definiciju funkcije h, nemamo baš izbora: za proizvoljni $(y, z) \in b \times c$, definiramo $f\big((y, z)\big) := \big(g(z)\big)(y)$. [Ova tehnika, gdje se funkcija više argumenata definira tako da se primijeni na jedan argument, pa rezultat na drugi argument, zove se *currying* i česta je u računarstvu.] Sada $h(f)$ i g jednako djeluju na svakom $z \in c$ (jer njihove vrijednosti jednako preslikavaju svaki y iz njihove zajedničke domene b), pa su jednake. □

Zadatak 3.15. *Za kardinalnosti definiramo svojstva N i J kao „jednaka* 0" *i „jednaka* 1". *Karakterizirajte N i J na zbroju, umnošku i potenciji pomoću N i J na njihovim operandima. Recimo,* $N(\alpha \cdot \beta) \Leftrightarrow N(\alpha) \vee N(\beta)$, *jer je* $\alpha \cdot \beta = 0$ *ako i samo ako je* $\alpha = 0$ *ili* $\beta = 0$.

3.5 Cantorov osnovni teorem

Za konačne skupove kardinalnost, praktički po definiciji, odgovara uobičajenom broju elemenata kakav se proučava u kombinatornoj i diskretnoj matematici. No iz te perspektive, beskonačni skupovi se ne promatraju posebno detaljno, a jednostavne bijekcije koje svi znamo iskonstruirati, koje pokazuju $\mathbb{N} \sim \mathbb{N} \setminus \{0\}$ ili $\mathbb{N} \sim \mathbb{Z}$, mogu nas navesti da pomislimo da su svi beskonačni skupovi međusobno ekvipotentni, odnosno da su sve moguće kardinalnosti upravo $0, 1, 2, 3, \ldots, \infty$.

Najvažniji Cantorov uvid je da to ne može biti dalje od istine: kardinalnosti beskonačnih skupova čine jednu od najkompliciranijih struktura ikad proučavanih u matematici, o kojoj se i danas pišu visoko rangirani radovi i postoje brojni neriješeni problemi. Neki od njih, iako vrlo jednostavni za iskazati (kao što je *hipoteza kontinuuma*: postoji li kardinalnost između $\aleph(\mathbb{N})$ i $\aleph(\mathbb{R})$?), dokazano se ne mogu riješiti (ni pozitivno ni negativno) koristeći samo općeprihvaćene aksiome teorije skupova.

Ovdje ćemo dokazati jedan od prvih Cantorovih rezultata: da ne postoji maksimalna kardinalnost, odnosno da od svake kardinalnosti postoji strogo veća. Prema lemi 2.3, $\aleph(b) > \aleph(a)$ znači $a \subsetneq b \wedge a \not\sim b$. Prvo kaže da postoji injekcija $f : a \to b$, a drugo da *ne postoji bijekcija* između a i b, **ne samo da** f **nije bijekcija**. Dakle, tu trebamo dokazati negaciju egzistencije: nije dovoljno naći jednu injekciju koja nije surjekcija na b.

Teorem 3.16 (Cantorov osnovni teorem)**.** *Za svaki skup a je* $\aleph\big(\mathscr{P}(a)\big) > \aleph(a)$.

Dokaz. Preslikavanje $g : a \to \mathscr{P}(a)$ zadano s $g(x) := \{x\}$ je injekcija: po aksiomu para, $\{x\} = \{y\}$ povlači $x = y$. Dakle, $a \subsetneq \mathscr{P}(a)$. Još je potrebno dokazati $a \not\sim \mathscr{P}(a)$.

Pretpostavimo suprotno, da je f neka bijekcija između a i $\mathscr{P}(a)$. Po aksiomu separacije, $b := \{x \in a : x \notin f(x)\}$ je skup, podskup od a. Kako je f surjekcija na $\mathscr{P}(a)$, postoji $r \in a$ takav

da je $b = f(r)$. Ta jednakost znači da $\forall z\big(z \in b \leftrightarrow z \in f(r)\big)$, pa posebno $r \in b \Leftrightarrow r \in f(r)$. No definicija od b kaže da je $r \in b \Leftrightarrow r \in a \wedge r \notin f(r) \Leftrightarrow r \notin f(r)$ (jer je $r \in a$). Sve zajedno daje $r \in f(r) \Leftrightarrow r \notin f(r)$, što je očito nemoguće. □

Uočimo sličnost provedenog dokaza (za $f = id$) s Russellovim paradoksom. Još neke primjere tog *dijagonalnog postupka* vidjet ćete u nastavku matematičkog obrazovanja.

Intuitivno, to znači da je kumulativna hijerarhija ne samo rastuća, već je strogo rastuća po kardinalnosti: svaka sljedeća razina $V_{\alpha+1} = \mathscr{P}(V_\alpha)$ je strogo „brojnija" od prethodne, a onda je jasno i da je V_λ za granični λ strogo brojnija od svih prethodnih (raspišite!).

Primijetimo da iz toga odmah slijedi i da **V** nije skup: kad bi bio, svaki podskup od **V** bi bio u **V**, odnosno imali bismo $\mathscr{P}(\mathbf{V}) \subseteq \mathbf{V}$, po inkluzivnosti $\aleph\big(\mathscr{P}(\mathbf{V})\big) \leq \aleph(\mathbf{V})$, što je u kontradikciji s Cantorovim osnovnim teoremom (jednom kad dokažemo antisimetričnost).

Zadatak 3.17. *Dokažite: za svaki skup a je $\mathscr{P}(a) \sim {}^a\{0,1\}$. [Zbog $\aleph(\{0,1\}) = 2$, Cantorov osnovni teorem možemo iskazati u obliku: za svaku kardinalnost α je $2^\alpha > \alpha$.]*

3.6 Knaster–Tarskijev teorem o fiksnoj točki

Vrijeme je da se pozabavimo antisimetričnošću relacije $\leq$ na kardinalnostima.
Ipak, prethodno trebamo jedan tehnički rezultat za parcijalno uređene skupove.

Definicija 3.18. Neka su $(a, \prec)$ i $(b, \lhd)$ parcijalno uređeni skupovi, i $f : a \to b$.
Kažemo da f *čuva strogi uređaj* ako za sve $x, y \in a$, $x \prec y$ povlači $f(x) \lhd f(y)$.
Kažemo da f *čuva refleksivni uređaj* ako za sve $x, y \in a$, $x \preceq y$ povlači $f(x) \trianglelefteq f(y)$.
Kažemo da je f *sličnost* ako je bijekcija između a i b, te f i f^{-1} obje čuvaju uređaj.
Kažemo da su a i b *slični*, i pišemo $(a, \prec) \simeq (b, \lhd)$, ako postoji sličnost između njih. ◁

Napomena 3.19. Ako f čuva strogi uređaj, onda i čuva refleksivni uređaj — jer $x = y$ uvijek povlači $f(x) = f(y)$. Iz istog razloga, obrat vrijedi ako je f injekcija.
Zato u definiciji sličnosti ne treba specificirati *kakav* uređaj čuvaju f i f^{-1}. ◁

Sličnostima, posebno onima na totalno i dobro uređenim skupovima,
bavit ćemo se kasnije. Zasad nas zanimaju funkcije koje čuvaju uređaj.

Teorem 3.20 (Knaster–Tarski)**.** *Neka je a parcijalno uređen skup, i $f : a \to a$ funkcija koja čuva refleksivni uređaj. Ako svaki podskup od a ima supremum, tada f ima najveću fiksnu točku. Ako svaki podskup od a ima infimum, tada f ima najmanju fiksnu točku.*

Dokaz. Dokažimo samo prvu tvrdnju; druga se dokazuje sasvim analogno. Označimo s $\preceq$ refleksivni parcijalni uređaj na a. Po aksiomu separacije, $b := \{x \in a : x \preceq f(x)\}$ je skup. Kao podskup od a, on ima supremum, i taj supremum je jedinstven (kao najmanji element u skupu c svih gornjih međa od b), pa ga označimo s $t := \sup b = \min c \in c$. Tvrdimo da je t tražena najveća fiksna točka od f.

Za svaki $x \in b$ vrijedi $x \preceq t$ zbog $t \in c$. Jer f čuva refleksivni uređaj, vrijedi i $f(x) \preceq f(t)$. S druge strane, za $x \in b$ je $x \preceq f(x)$ po definiciji od b. Spojivši to dvoje po tranzitivnosti, dobivamo da za sve $x \in b$ vrijedi $x \preceq f(t)$. To znači da je $f(t) \in c$, odnosno $t = \min c \preceq f(t)$.

Na to još jednom primijenimo to da f čuva uređaj: dobijemo $f(t) \preceq f\big(f(t)\big)$. No to znači da je $f(t) \in b$ (opet po definiciji od b), pa je $f(t) \preceq t$. To dvoje po antisimetričnosti povlači $f(t) = t$, odnosno t je fiksna točka od f.

Još moramo dokazati da je najveća, odnosno da je veća od svake fiksne točke od f. Neka je u proizvoljna fiksna točka od f. Iz $u = f(u) \in a$ po refleksivnosti uređaja slijedi $u \preceq f(u)$, pa je $u \in b$. No to znači da je $u \preceq t$, jer je $t \in c$. □

Napomena 3.21. Uvjet „svaki podskup ima supremum" često se promatra posebno za prazan podskup. Očito, svaki element od a je gornja međa od $\emptyset$ ($c = a$), pa je $\sup \emptyset$ upravo najmanji element od a. Dakle, uvjet Knaster–Tarskijevog teorema možemo iskazati u obliku „a ima najmanji element, i svaki *neprazni* podskup od a ima supremum".
Slično izdvajanje praznog skupa vidjet ćemo kad budemo proučavali Zornovu lemu. ◁

Korolar 3.22. *Neka je A skup i neka je $F : \mathscr{P}(A) \to \mathscr{P}(A)$ funkcija takva da $X \subseteq Y \subseteq A$ povlači $F(X) \subseteq F(Y)$. Tada postoji $S \subseteq A$ takav da je $F(S) = S$.*

Dokaz. Primijenimo teorem o fiksnoj točki na $\big(\mathscr{P}(A), \subseteq\big)$. Otprije znamo (primjer 2.7) da je to refleksivno parcijalno uređen skup, u kojem svaki $B \subseteq \mathscr{P}(A)$ ima supremum $\bigcup B$. □

3.7 Cantor–Schröder–Bernsteinov teorem

Propozicija 3.23. *Neka je a skup i $f : a \to a$. Tada $b \subseteq c \subseteq a$ povlači $f[b] \subseteq f[c]$ i $a \setminus c \subseteq a \setminus b$.*

Dokaz. Za prvu inkluziju, $y \in f[b]$ znači da postoji $x \in b$ takav da je $y = f(x)$.
Zbog $b \subseteq c$ je i $x \in c$, odnosno $y \in f[c]$.

Za drugu inkluziju, $x \in a \setminus c$ znači $x \in a$ i $x \notin c$. Pretpostavka $x \in b$ bi vodila (zbog $b \subseteq c$) na kontradikciju s $x \notin c$, dakle $x \notin b$, što zajedno s $x \in a$ daje $x \in a \setminus b$. □

Lema 3.24 (Banach)**.** *Neka su a i b skupovi te $f : a \to b$ i $g : b \to a$.*
Tada postoji $s \subseteq a$ takav da je $g\big[b \setminus f[s]\big] = a \setminus s$.

Dokaz. Definiramo $F : \mathscr{P}(a) \to \mathscr{P}(a)$ formulom $F(x) := a \setminus g\big[b \setminus f[x]\big]$.
Četverostrukom primjenom propozicije 3.23 imamo (za $x, y \subseteq a$):

$$\begin{aligned} x \subseteq y &\Longrightarrow f[x] \subseteq f[y] \Longrightarrow b \setminus f[y] \subseteq b \setminus f[x] \Longrightarrow \\ &\Longrightarrow g\big[b \setminus f[y]\big] \subseteq g\big[b \setminus f[x]\big] \Longrightarrow a \setminus g\big[b \setminus f[x]\big] \subseteq a \setminus g\big[b \setminus f[y]\big] \Longleftrightarrow F(x) \subseteq F(y), \end{aligned} \tag{3.5}$$

dakle F čuva skupovnu inkluziju. Po korolaru 3.22 postoji $s \subseteq a$ takav da je $s = F(s) = a \setminus t$, gdje je $t := g\big[b \setminus f[s]\big]$. Sada $s = a \setminus t$ znači (s i t su disjunktni i unija im je a) isto što i $t = a \setminus s$, što smo trebali. □

Teorem 3.25 (Cantor–Schröder–Bernstein)**.** *Za skupove a i b, $a \subsetneq b \subsetneq a$ povlači $a \sim b$.*

Dokaz. Pretpostavka znači da imamo injekcije $f : a \to b$ i $g : b \to a$. Po Banachovoj lemi, postoji $s \subseteq a$ takav da je $g\big[b \setminus f[s]\big] = a \setminus s$. Prema napomeni 2.25, vrijedi $s \sim f[s]$ i $b \setminus f[s] \sim g\big[b \setminus f[s]\big] = a \setminus s$. Kako je očito s disjunktan s $a \setminus s$ i $f[s]$ disjunktan s $b \setminus f[s]$, prema propoziciji 3.6 slijedi $s \cup (a \setminus s) \sim f[s] \cup (b \setminus f[s])$, odnosno $a \sim b$. □

Korolar 3.26. *Klasna relacija $\leq$ na kardinalnostima je refleksivni parcijalni uređaj.*

Dokaz. U korolaru 3.13 smo dokazali da je refleksivna i tranzitivna, a sada smo dokazali da je i antisimetrična. Doista, $\mathfrak{K}(a) \leq \mathfrak{K}(b) \leq \mathfrak{K}(a)$ znači $a \subsetneq b \subsetneq a$, što po Cantor–Schröder–Bernsteinovom teoremu (CSB) povlači $a \sim b$, odnosno $\mathfrak{K}(a) = \mathfrak{K}(b)$. □

Kao što smo nagovijestili, radi se o totalnom (za svaka dva skupa postoji injekcija s jednoga od njih u drugi), pa čak i o dobrom uređaju, ali za dokaze tih svojstava trebat ćemo dodatne aksiome, kao i preciznu formulaciju pojma kardinalnog broja.

3.8 Reprezentacija parcijalno uređenih skupova

Definicija 3.27. Neka je $(a, \prec)$ parcijalno uređen skup i $x \in a$.
Tada *(otvoreni) početni komad* elementa x u a definiramo kao $p_a(x) := \{y \in a : y \prec x\}$.
Zatvoreni početni komad elementa x je $\bar{p}_a(x) := \{y \in a : y \preceq x\}$. ◁

Sljedeći rezultat je u određenom smislu pojačanje napomene 2.25.

Propozicija 3.28. *Neka su $(a, \prec)$ i $(b, \lhd)$ parcijalno uređeni skupovi, f sličnost između njih, i $x \in a$. Tada je restrikcija funkcije f sličnost između $p_a(x)$ i $p_b\big(f(x)\big)$.*

Dokaz. Restrikcija $f|_{p_a(x)}$ čuva uređaj, kao i njen inverz, jer su f i f^{-1} takve. Slika joj je podskup od $p_b\big(f(x)\big)$ jer $z \prec x$ povlači $f(z) \lhd f(x)$. No vrijedi i druga inkluzija, jer $w \lhd f(x)$ povlači $f^{-1}(w) \prec x$, i zato je $w = f\big(f^{-1}(w)\big) \in f[p_a(x)]$. □

Baš kao strogi i refleksivni parcijalni uređaj, otvoreni i zatvoreni početni komad su međusobno definabilni: $p_a(x) = \bar{p}_a(x) \setminus \{x\}$, odnosno $\bar{p}_a(x) = p_a(x) \cup \{x\}$. Ubuduće ćemo se puno više baviti otvorenim početnim komadima, ali zatvoreni su bitni za sljedeći teorem, koji pokazuje kako se bilo koji parcijalni uređaj može reprezentirati skupovnom inkluzijom.

Teorem 3.29. *Za svaki parcijalno uređeni skup $(a, \prec)$*
postoji skup $A \subset \mathscr{P}(a)$ takav da vrijedi $(a, \prec) \simeq (A, \subset)$.

Dokaz. Promotrimo funkciju $\bar{p}_a : a \to \mathscr{P}(a)$ koja svaki $x \in a$ preslikava u $\bar{p}_a(x)$.
Ona ne može biti surjekcija na čitav $\mathscr{P}(a)$ jer očito ne poprima $\emptyset$, pa je $A := \operatorname{rng} \bar{p}_a \subset \mathscr{P}(a)$.

Tada je $\bar{p}_a$ surjekcija na A po definiciji. Za injektivnost, pretpostavimo da je $\bar{p}_a(x) = \bar{p}_a(y)$. Tada $x \in \bar{p}_a(x) = \bar{p}_a(y)$ povlači $x \preceq y$, i analogno $y \preceq x$, pa je po antisimetričnosti $x = y$.

Dokažimo da $\bar{p}_a$ čuva refleksivni uređaj (tada zbog injektivnosti čuva i strogi uređaj). Neka je $(x, y) \in (\preceq)$. Tada $z \preceq x \preceq y$ povlači $z \preceq y$, pa je $\bar{p}_a(x) \subseteq \bar{p}_a(y)$.

Dokažimo da i $\bar{p}_a^{-1} : A \to a$ također čuva refleksivni uređaj (ona je sigurno injekcija jer joj je inverz funkcija $\bar{p}_a$): neka su $X, Y \in A$ takvi da je $X \subseteq Y$. Po definiciji skupa A, postoje $x, y \in a$ takvi da je $X = \bar{p}_a(x)$ i $Y = \bar{p}_a(y)$. Zbog injektivnosti $\bar{p}_a$, upravo je $x = \bar{p}_a^{-1}(X)$ i $y = \bar{p}_a^{-1}(Y)$. Tada $x \in X \subseteq Y$ povlači $x \in Y$, odnosno $x \preceq y$. □

Napomena 3.30. Sada napokon možemo opravdati „čudnu" definiciju 1.5. Naime, ako uređeni par različitih skupova x i y shvatimo doslovno kao (totalno) uređeni dvočlani skup $t := (\{x, y\}, \prec)$ uređajem u kojem je $x \prec y$, njegova reprezentacija u smislu teorema 3.29 je

$$\operatorname{rng} \bar{p}_t = \bar{p}_t[\{x, y\}] = \{\bar{p}_t(x), \bar{p}_t(y)\} = \{\{x\}, \{x, y\}\}. \tag{3.6}$$

To ne može biti formalna definicija (jer nam za definiciju uređaja $\prec$ i uređenog skupa t treba pojam uređenog para), ali dobro pokazuje zašto je definicija baš takva, odnosno da uopće nije tako „proizvoljna" kako se u prvi mah čini. ◁

Zadatak 3.31. *Zašto dokaz teorema 3.29 ne bi prošao s otvorenim početnim komadima?*

4 Skup prirodnih brojeva

4.1 Motivacija

Na nekoliko mjesta su nam već dosad (uglavnom za ilustracije) zatrebali prirodni brojevi, i oslanjali smo se na to da već imamo intuitivnu predodžbu o njima. Mogli bismo ih pokušati formalizirati kao kardinalnosti konačnih skupova (kao što smo činili za $0 = \mathfrak{K}(\emptyset)$, $1 = \mathfrak{K}(\{\emptyset\})$ i $2 = \mathfrak{K}(\{0,1\})$), ali nismo precizno definirali ni kardinalnosti (kao skupove) ni konačnost.

Također, za dokaze smo koristili princip matematičke indukcije, opet „na vjeru". Obično se prirodni brojevi uvode aksiomatski, Peanovim aksiomima, i onda je matematička indukcija jedan od aksioma na tom popisu. Ako teorija skupova želi biti temelj matematike, trebalo bi u njoj moći: • definirati prirodne brojeve kao skupove, • formalizirati svojstvo „biti prirodan broj" kao neku formulu koju zadovoljavaju točno oni skupovi koji označavaju prirodne brojeve, i • *dokazati* Peanove aksiome, među kojima i aksiom matematičke indukcije, pomoću aksiomā teorije skupova. To ćemo učiniti ovdje.

Peanovi aksiomi zapravo ne definiraju svaki prirodni broj pojedinačno — niti to mogu, jer ih ima beskonačno mnogo. Ono što se zapravo definira je *početak* (nula ili jedan, ovisno o preferencijama — u teoriji skupova počinjemo od nule) i *sljedbenik*, za koji se postuliraju svojstva koja osiguravaju da je prirodnih brojeva beskonačno mnogo, odnosno da operacijom sljedbenika uvijek dobivamo nove brojeve.

Što uzeti kao nulu? Vrlo prirodnim odabirom čini se prazan skup. Sljedbenik je kompliciraniji: radi se o klasnoj funkciji koja uvijek mora davati nove elemente. Jedan jednostavni način da osiguramo, barem intuitivno, da sve prirodne brojeve reprezentiraju različiti skupovi, je da zahtijevamo da skup n ima n elemenata. Zasad je to ispunjeno: $0 := \emptyset$ ima nula elemenata, a primijetimo da i ostali „kanonski reprezentanti" kardinalnosti koje smo uveli imaju to svojstvo: $1 := \{\emptyset\} = \{0\}$ ima jedan element, a $2 := \{0,1\}$ ima dva elementa (različiti su upravo jer je svaki novi prirodni broj doista novi skup). To možemo nastaviti i dalje: $3 := \{0,1,2\}$, $4 := \{0,1,2,3\}$ i tako u beskonačnost.

Kao što rekosmo, sigurno nećemo sve prirodne brojeve pojedinačno tako definirati, već ćemo postupak dobivanja uvijek novog broja generalizirati kroz funkciju sljedbenika. Pogledajmo: kojom skupovnom operacijom iz 3 dobijemo 4? Dokaz propozicije 1.3 daje ideju: $\{0,1,2,3\} = \{0,1,2\} \cup \{3\}$, odnosno $4 = 3 \cup \{3\}$. Isti postupak možemo provesti za bilo koji skup.

Definicija 4.1. Za skup a definiramo *sljedbenik* od a kao skup $a^+ := a \cup \{a\}$. ◁

Lako se vidi, koristeći aksiome para i unije, da je a^+ doista skup za svaki skup a. Zašto smo dobili novi element? Intuitivno, zato što dodani element a nije bio među već navedenima (elementima od a). Začudo, ta činjenica ($a \notin a$ za svaki skup a) nije posljedica dosad navedenih aksioma — iako slijedi iz našeg intuitivnog poimanja izgradnje kumulativne hijerarhije, da skupove gradimo tek nakon što su svi njihovi elementi već izgrađeni. Morat ćemo dodati novi aksiom, koji ukratko kaže da je klasna relacija $\in$ dobro utemeljena.

4.2 Aksiom dobre utemeljenosti *

Kako iskazati dobru utemeljenost relacije „biti element" formulom? Doslovno, to znači da svaki neprazni skup x, kad ga „uredimo" relacijom $\in$, ima minimalni element y. Navodnici su tu jer $\in$ ne mora doista biti relacija parcijalnog uređaja na x: konkretno, nema razloga očekivati da bude tranzitivna — i doista nije, recimo na skupu $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$ (raspišite!).

Ali svejedno možemo raspisati svojstvo: y je minimalni element od x ako ne postoji $z \in x$ koji bi bio manji od y. No relacija „manji" je upravo $\in$, pa to zapravo kaže da ne postoji $z \in x$ takav da je $z \in y$ — drugim riječima, da su x i y disjunktni. Dakle, *aksiom dobre utemeljenosti* glasi:

$$(x \neq \emptyset) \to (\exists y \in x)(x \cap y = \emptyset) \tag{4.1}$$

— pritom smo koristili već uvedene oznake $\neq$, $\emptyset$ i $\cap$. Također smo ispustili kvantifikator $\forall x$ na početku formule, kao što smo već mnogo puta radili.

Intuitivno, ako x ima elemente, oni se nalaze na nekim razinama kumulativne hijerarhije. Od svih tih razinā postoji najniža V_α, i bilo koji element od x s te razine (označimo jedan takav s y) mora biti disjunktan s x — jer svi elementi od y nalaze se ispod razine V_α, a svi elementi od x su iznad ili na razini V_α. Drugim riječima, aksiom dobre utemeljenosti opravdan je intuitivnom idejom da su razine kumulativne hijerarhije dobro uređene.

Pogledajmo sada formalne posljedice tog aksioma.

Lema 4.2. *(1) Ne postoji skup a takav da je $a \in a$. (2) Ne postoje skupovi a i b takvi da vrijedi $a \in b \in a$. (3) Ne postoje skupovi a, b i c takvi da vrijedi $a \in b \in c \in a$.*

Slično kao kod propozicije 1.3, mogli bismo iskazati niz formula oblika „ne postoje skupovi $x_1, x_2, \ldots, x_k$ takvi da vrijedi $x_1 \in x_2 \in \cdots \in x_k \in x_1$", pa bi navedene tri tvrdnje bile samo specijalni slučajevi, ali zapravo će nam trebati te tvrdnje samo za do tri skupa. Dokazi su više-manje isti (provedite ih sva tri!); pokazat ćemo kako dokaz izgleda za dva skupa.

Dokaz. Pretpostavimo suprotno, da postoje takvi skupovi a i b. Po aksiomu para postoji $x := \{a, b\}$. On je neprazan zbog $a \in x$, pa po aksiomu dobre utemeljenosti postoji $y \in x$ takav da su y i x disjunktni. No po aksiomu para, $y \in x$ znači $y = a$ ili $y = b$, a nijedan od njih nije disjunktan s x: a i x imaju (barem) zajednički element b, a b i x imaju zajednički element a. To je kontradikcija, pa takvi skupovi a i b ne mogu postojati. □

Propozicija 4.3. *Sljedbenik je injekcija bez fiksne točke. Nula nije u slici sljedbenika.*

Dokaz. Za prvu tvrdnju, pretpostavimo suprotno da je $a^+ = b^+$ za neke različite skupove a i b. Iz $b \in b^+ = a^+$ slijedi $b \in a \vee b = a$, odnosno $b \in a$ jer smo pretpostavili da nije $b = a$. Potpuno analogno dobijemo $a \in b$. To je u kontradikciji s lemom 4.2(2).

Za drugu tvrdnju, pretpostavimo suprotno da je $a = a^+$ fiksna točka sljedbenika.
Tada je $a \in a^+ = a$ u kontradikciji s lemom 4.2(1).

Za treću tvrdnju, pretpostavimo da je $\emptyset = a^+$ za neki skup a.
Tada je $a \in a^+ = \emptyset$, što je u kontradikciji s aksiomom praznog skupa. □

Zadatak 4.4. *Nađite skupovnu operaciju koja odgovara prethodniku!*

Što se aksioma tiče, još je preostalo formalizirati i dokazati matematičku indukciju — ali to nije sve. Naime, aritmetičke operacije se u Peanovoj aritmetici uvode aksiomatski, ali u teoriji skupova bolje bi bilo dokazati da doista postoje (kao skupovi) funkcije s $\mathbb{N} \times \mathbb{N}$ u $\mathbb{N}$, koje odgovaraju operacijama zbrajanja i množenja (a vrlo slično i potenciranja). To se može, ali nije baš jednostavno: ključni teorem je *Dedekindov teorem rekurzije*, koji ćemo dokazati.

4.3 Karakterizacija prirodnih brojeva

U svakom slučaju, matematička indukcija trebala bi biti neka shema teoremā, po jedan za svako svojstvo P koje se odnosi na prirodne brojeve, koji kaže da ako vrijedi $P(0)$ i ako $P(n)$ povlači $P(n^+)$ za svaki prirodni broj n, tada vrijedi $P(n)$ za svaki prirodni broj n. Ako svojstvo P iskažemo u obliku formule s jednom slobodnom varijablom, vidimo da moramo pronaći način da kvantificiramo tu varijablu samo po prirodnim brojevima.

Najjednostavnije bi bilo da imamo formulu ν, s jednom slobodnom varijablom n, koja kazuje da je n prirodan broj, i onda „za svaki prirodni broj vrijedi φ" formaliziramo kao $\forall n(\nu \to \varphi)$. Možemo li pronaći takvu formulu ν?

Na prvi pogled, čini se neuhvatljivim: trebali bismo reći „n je ili 0 ili 0^+ ili $(0^+)^+$ ili ...", no to je beskonačna disjunkcija. Možemo pokušati s „n je 0 ili postoji prirodni broj m takav da je $n = m^+$", no da bismo iskazali da je m prirodni broj trebamo upravo formulu koju pokušavamo konstruirati. Možemo pokušati s „n je dobiven konačnim brojem primjena sljedbenika na nuli", no ovo „konačnim brojem" zapravo znači „prirodnim brojem" pa se opet vrtimo u krug. Mogli bismo, kao što smo već činili, napraviti shemu formula „n je prirodni broj manji od m", po jednu za svaki m, i onda napraviti egzistencijalnu kvantifikaciju po m, ali te formule su različite duljine i ne možemo ih upotrebljivo generalizirati. Pokušajte sami smisliti još neke načine prije nego što pogledate rješenje.

A rješenje se sastoji u tome da prijeđemo na višu razinu. Snaga teorije skupova je u tome što nam je jednako lako govoriti o objektima i o skupovima koji ih sadrže, jer su svi oni istog „tipa". U većini matematičkih grana nije tako: recimo, bitno je teže formulirati tvrdnje o vektorskim potprostorima nego o vektorima. U geometriji imamo točke, pravce i ravnine

na istoj razini, ali to seže samo „do dubine 1” (ravnine nisu skupovi pravaca, već točaka): snopovi pravaca ili svežnjevi ravnina su opet kompliciraniji objekti.

To znači da trebamo pokušati karakterizirati *skup* prirodnih brojeva. Na prvi pogled nismo puno profitirali jer nam je zadati skup više-manje isto što i zadati formulu; ali ovdje idemo na višu razinu, odnosno ne opisujemo „moguće prirodne brojeve n” kao elemente fiksnog skupa $\mathbb{N}$, već opisujemo *moguće skupove prirodnih brojeva* w formulom s jednom slobodnom varijablom w. Jasno je što ta formula treba reći: w sadrži nulu i zatvoren je na operaciju sljedbenik.

$$\iota := \big(0 \in w \wedge (\forall m \in w)(m^+ \in w)\big) \tag{4.2}$$

Skupovi koji zadovoljavaju ι zovu se *induktivni* skupovi, zbog očite asocijacije na princip matematičke indukcije: efektivno, uobičajeni oblik matematičke indukcije glasi „ako je S induktivni podskup od $\mathbb{N}$, tada je $S = \mathbb{N}$”. No ako već imamo jednu inkluziju kao pretpostavku pa dobijemo jednakost kao zaključak, ono što nam induktivnost daje je druga inkluzija: „ako je S induktivni skup, tada je $\mathbb{N} \subseteq S$”. To na već dobro poznati način možemo iskazati kao „$\mathbb{N}$ je najmanji induktivni skup”.

Ovo zadnje nije teško iskazati formulom: elementi od $\mathbb{N}$ (*prirodni brojevi*) su upravo oni skupovi koji su elementi svih induktivnih skupova.

$$\nu := \forall w(\iota \to n \in w) \tag{4.3}$$

4.4 Aksiom beskonačnosti *

Tako smo napokon dobili formulu koja kazuje da je n prirodan broj, i možemo konstruirati klasu $\omega := \{n : \nu\}$ koja bi trebala predstavljati formalizaciju skupa $\mathbb{N}$. No dosad uvedeni aksiomi ne omogućavaju nam da zaključimo da je ν „dobra” formula, odnosno da je ω skup. Zapravo, sa svim dosadašnjim aksiomima je sasvim konzistentno da su svi skupovi *konačni*, dok bi ω, barem intuitivno, trebao biti beskonačan. Zato se aksiom koji osigurava postojanje ω zove *aksiom beskonačnosti*.

Taj aksiom bismo mogli napisati u obliku $\exists w(\omega = w)$, koristeći činjenicu da kvantificirane varijable uvijek označavaju skupove; odnosno, koristeći pokratu za jednakost klase i skupa, $\exists w \forall n(\nu \leftrightarrow n \in w)$. No možemo tražiti i manje, ako se sjetimo napomene 1.10: dovoljno je zahtijevati da postoji jedan induktivni skup, koji sigurno po definiciji sadrži sve prirodne brojeve. Tada se ω može dobiti iz tog skupa separacijom s formulom ν. Dakle, aksiom beskonačnosti glasi $\exists w\, \iota$, ili raspisanije,

$$\exists w\big(\varnothing \in w \wedge (\forall n \in w)(n \cup \{n\} \in w)\big). \tag{4.4}$$

Propozicija 4.5. *Klasa $\omega := \{n : \nu\}$ je skup. Štoviše, to je najmanji induktivni skup.*

Dokaz. Po aksiomu beskonačnosti postoji induktivni skup: fiksirajmo jedan i označimo ga s w. Tvrdimo da je $\omega = \{n \in w : \nu\}$, iz čega će odmah slijediti da se radi o skupu po aksiomu separacije. U skladu s konvencijom o jednakosti klase i skupa, zapravo trebamo dokazati $\forall n\big(\nu \leftrightarrow (n \in w \wedge \nu)\big)$: smjer $\Leftarrow$ je očit, a za $\Rightarrow$ je dovoljno pokazati da ν povlači $n \in w$. No ν kaže da se n nalazi u svakom induktivnom skupu, a w je takav prema aksiomu beskonačnosti.

Za dokaz da je ω induktivan, trebamo dokazati da je 0 prirodni broj, te da je sljedbenik svakog prirodnog broja prirodni broj. Za prvo, neka je u proizvoljni induktivni skup. Po definiciji induktivnosti vrijedi $0 \in u$, pa je 0 prirodni broj. Za drugo, neka je n prirodni broj, i u proizvoljni induktivni skup. Želimo dokazati da je $n^+ \in u$. No očito je $n \in u$ (jer je svaki prirodni broj u svakom induktivnom skupu), a onda je i $n^+ \in u$ jer je u kao induktivni skup zatvoren na operaciju sljedbenik.

Dokažimo još da se radi o najmanjem induktivnom skupu. Neka je u proizvoljni induktivni skup; želimo dokazati $\omega \subseteq u$. U tu svrhu, neka je $n \in \omega$ proizvoljan. To znači da je n prirodan broj — element svakog induktivnog skupa, pa tako i u. □

Primijetimo (dokažite!) da je presjek bilo koje neprazne familije (pa čak i klase) induktivnih skupova ponovo induktivan. Skup ω je presjek klase *svih* induktivnih skupova, i kao takav je podskup bilo kojeg od njih. Jedino što je bilo potrebno za dokaz da se doista radi o skupu jest da je ta klasa *neprazna*, odnosno da postoji barem jedan induktivni skup.

Korolar 4.6. *Ne postoji induktivni prirodni broj.*

Dokaz. Pretpostavimo da je skup a takav. Tada bi a (kao prirodni broj) morao biti element svakog induktivnog skupa, pa tako i samog sebe, što je nemoguće po lemi 4.2(1). □

Kad generaliziramo prirodne brojeve na općenite ordinale, vidjet ćemo da postoje induktivni ordinali: zvat ćemo ih *graničnim ordinalima*. No o tome kada dođe vrijeme.

4.5 Matematička indukcija

Kao što smo već spomenuli, sada imamo i formalno opravdanje dokazivanja svojstava prirodnih brojeva matematičkom indukcijom.

Teorem 4.7. *Neka je P svojstvo prirodnih brojeva iskazivo formulom, takvo da (baza) vrijedi $P(0)$ te (korak) $P(n)$ za $n \in \omega$ povlači $P(n^+)$. Tada svi prirodni brojevi imaju svojstvo P.*

Dokaz. Označimo s φ formulu sa slobodnom varijablom n koja formalizira svojstvo P. Za term τ, označimo s φ_τ formulu dobivenu od φ zamjenom svih pojava varijable n s τ (ako term τ označava prirodni broj m, ta formula iskazuje da m ima svojstvo P). Po aksiomu separacije, postoji skup $s := \{n \in \omega : \varphi\}$, i tvrdimo da je taj skup induktivan. Zbog baze vrijedi φ_0 odnosno $0 \in s$; još je preostalo dokazati da je s zatvoren na operaciju sljedbenik.

Neka je $n \in s$ proizvoljan. To znači da vrijedi $n \in \omega$ i φ. Iz toga zbog koraka slijedi φ_{n^+}, ali i $n^+ \in \omega$ jer je ω induktivan (propozicija 4.5). Dakle je $n^+ \in s$, što smo trebali.

Iz induktivnosti s slijedi (opet po propoziciji 4.5) $\omega \subseteq s$, odnosno $\forall n(\nu \to \varphi)$, što točno znači da svi prirodni brojevi imaju svojstvo P. □

Primijetimo suptilnost: ako samo kažemo: „u teoriji skupova možemo dokazati $P(0)$" i za svaki prirodni n, „u teoriji skupova možemo dokazati $P(n) \to P(n^+)$" (konkretno, možemo dokazati sve formule $P(0) \to P(1)$, $P(1) \to P(2)$, $P(2) \to P(3)$, ... — možda bitno različitim dokazima) tada možemo zaključiti da za svaki prirodni broj n „u teoriji skupova možemo dokazati $P(n)$" (konkretno, možemo dokazati sve formule $P(0)$, $P(1)$, ... — uvrštavajući gornje dokaze jedne u druge), ali to je nezanimljiva primjena matematičke indukcije, **na** dokaze u teoriji skupova (što smo već imali dosad; pogledajte napomenu 1.4). Teorem 4.7 kaže nešto drugo: ako u teoriji skupova možemo dokazati $0 \in s$ i *jednu formulu* $(\forall n \in \omega)(n \in s \to n^+ \in s)$, tada očito možemo dokazati i njihovu konjunkciju, koja kaže da je s induktivan, pa zaključiti $(\forall n \in \omega)(n \in s)$. To je primjena matematičke indukcije **u** dokazima u teoriji skupova (što dosad nismo imali).

Tako matematička indukcija za nas više nije aksiom, nego teorem — precizno, shema teorema, po jedan za svaku formulu s jednom slobodnom varijablom, koja iskazuje neko svojstvo prirodnih brojeva. A zapravo, to samo znači da možemo nastaviti dokazivati (formulama iskaziva) svojstva, sada formalno definiranih, prirodnih brojeva matematičkom indukcijom kao i prije. Evo jednog jednostavnog primjera takvog dokaza; malo kompliciranije primjere vidjet ćemo u idućim točkama.

Propozicija 4.8. *Svaki element prirodnog broja je prirodni broj.*

Dokaz. Matematičkom indukcijom po m dokazujemo da $n \in m$ povlači ν, odnosno $n \in \omega$. Baza je očita: $n \in 0$ povlači što god želimo, jer je 0 prazan skup. Pretpostavimo da za prirodni broj m vrijedi $n \in m \to \nu$, i neka je $n \in m^+ = m \cup \{m\}$. To znači da imamo dva slučaja. U prvom je $n \in m$, pa je prirodan po pretpostavci indukcije. U drugom je $n \in \{m\}$, odnosno $n = m$ — pa je prirodan jer smo pretpostavili da je m prirodni broj (to formalno nije „pretpostavka indukcije", već pretpostavka *konteksta* indukcije, jer se matematička indukcija odnosi samo na prirodne brojeve). □

Korolar 4.9. *Vrijedi* $\bigcup\omega = \omega$.

Dokaz. Po aksiomu ekstenzionalnosti. Jedna inkluzija je direktna posljedica upravo dokazane propozicije: $n \in \bigcup\omega$ znači $n \in m$ za neki $m \in \omega$, odnosno $n \in \omega$. Za drugu inkluziju, $n \in \omega$ povlači (jer je ω induktivan) i $n^+ \in \omega$, a očito je $n \in n^+$. □

4.6 Uređaj na prirodnim brojevima

Na početku poglavlja rekli smo da nam je ideja vodilja pri definiciji pojedinačnih prirodnih brojeva, da svaki broj bude upravo skup svih brojeva manjih od njega. Sad kada imamo formalne prirodne brojeve, tu intuiciju možemo formalizirati kao *definiciju* pojma „manji".

Definicija 4.10. Za $n, m \in \omega$ kažemo da je *n manji od m*, i pišemo $n < m$, ako je $n \in m$. $\triangleleft$

Propozicija 4.11. *S upravo definiranim uređajem, $(\omega, <)$ je parcijalno uređen skup.*

Dokaz. Irefleksivnost vrijedi direktno po lemi 4.2(1).
Za tranzitivnost, dokazujemo da $a < b < c$ povlači $a < c$ matematičkom indukcijom po c. Baza vrijedi trivijalno, jer $a < b < 0$ nije moguće. Pretpostavimo da $a < b < c$ povlači $a < c$, i neka je $a < b < c^+$. Druga nejednakost znači $b \in c \cup \{c\}$, odnosno $b < c \vee b = c$, pa imamo dva slučaja. U prvome vrijedi $a < c$ po pretpostavci indukcije, a u drugome jer b i c kao jednaki skupovi imaju jednake elemente. $\square$

Po lemi 2.4 imamo $n \leq m \Leftrightarrow n < m \vee n = m \Leftrightarrow n \in m \vee n \in \{m\} \Leftrightarrow n \in m \cup \{m\} \Leftrightarrow n < m^+$. Relacija $\leq$ je tranzitivna, štoviše $a \leq b < c$ (kao i $a < b \leq c$) povlači $a < c$ (dokažite!).

Lema 4.12. *1. Za svaki prirodni broj x vrijedi $0 \leq x$.*

2. Sljedbenik čuva strogi uređaj: $x < y$ povlači $x^+ < y^+$ (za prirodne brojeve x i y).

Dokaz. (1) Matematičkom indukcijom po x: $0 = 0$, a $0 \leq x$ povlači $0 < x^+$, pa i $0 \leq x^+$.

(2) Matematičkom indukcijom po y. Baza: $x < 0$ kao laž povlači bilo što. Pretpostavimo $x < y \Rightarrow x^+ < y^+$ (tada svakako $x \leq y \Rightarrow x^+ \leq y^+$, jer je sljedbenik funkcija na ω), i neka je sada $x < y^+$. To znači $x \leq y$ pa po pretpostavci indukcije $x^+ \leq y^+$, odnosno $x^+ < (y^+)^+$. $\square$

Propozicija 4.13. *$(\omega, <)$ je totalno uređen skup.*

Dokaz. Dokazujemo $a < b \vee a = b \vee b < a$ (što se ekvivalentno može zapisati $a \leq b \vee b < a$ ili $a < b \vee b \leq a$) matematičkom indukcijom po b. Baza: po lemi 4.12(1) je $0 \leq a$.

Pretpostavimo da je (za neki b) $a \leq b \vee b < a$ za sve a, i dokažimo tu tvrdnju za b^+. Iz $a \leq b$ sigurno slijedi $a < b^+$; a iz $b < a$ po lemi 4.12(2) slijedi $b^+ < a^+$, odnosno $b^+ \leq a$. $\square$

Napomena 4.14. Pomoću principa matematičke indukcije možemo dokazati i princip *jake* ili *totalne* indukcije, koji kaže: ako pretpostavka „svi prirodni brojevi manji od n imaju svojstvo Q" povlači „n ima svojstvo Q", tada svi prirodni brojevi imaju svojstvo Q.
Doista, potrebno je samo primijeniti obični princip matematičke indukcije na svojstvo

$$P(n) :\Longleftrightarrow \text{„svi elementi od } n \text{ imaju svojstvo } Q\text{"}. \tag{4.5}$$

Baza je trivijalna: svi elementi od 0 imaju koje god svojstvo želimo, jer ih nema. Pretpostavimo da vrijedi $P(n)$. Gornja pretpostavka kaže da $P(n)$ povlači $Q(n)$, pa povlači i njihovu konjunkciju $\big(Q(n) \wedge P(n)\big)$, koja je upravo ekvivalentna s $P(n^+)$. („Svi elementi od n^+" su upravo „svi elementi od n", i sām n). Po principu (obične) matematičke indukcije, za sve n vrijedi $P(n)$, a kako $P(n)$ povlači $Q(n)$, vrijedi i $Q(n)$ za sve n. $\triangleleft$

Zadatak 4.15. *Dokažite razne druge varijante principa matematičke indukcije (s početkom 1, s korakom 2, itd.) koristeći obični princip matematičke indukcije.*

Sada pomoću totalne indukcije možemo dokazati da je ω dobro uređen. Pokušajte: za proizvoljni $a \subseteq \omega$, jakom indukcijom po n dokažite da $n \in a$ povlači da a ima najmanji element. Ipak, možemo i puno jednostavnije.

Propozicija 4.16. $(\omega, <)$ *je dobro utemeljen, pa onda i dobro uređen, skup.*

Dokaz. Dovoljno je dokazati dobru utemeljenost; dobra uređenost će onda slijediti iz propozicije 4.13. Neka je $\emptyset \neq a \subseteq \omega$ proizvoljan. Po aksiomu dobre utemeljenosti, postoji $m \in a$ takav da je $m \cap a = \emptyset$. Tvrdimo da je m minimalni (pa onda i najmanji po propoziciji 2.8) element od a. Pretpostavimo suprotno, da postoji $n \in a$ takav da je $n < m$. No tada je $n \in a \cap m = \emptyset$, kontradikcija. □

Ovaj fenomen, koji smo vidjeli kod dobre uređenosti od ω, odražava općenitu situaciju vezanu uz aksiom dobre utemeljenosti. I induktivni i aksiomatski dokaz imaju prednosti i mane. Dokaz pomoću aksioma dobre utemeljenosti obično je puno kraći, ali zahtijeva novi aksiom i često zahtijeva dodatna svojstva poput totalnosti uređaja (koja se moraju dokazati induktivno). Induktivno se mogu dokazati sve važne tvrdnje za prirodne brojeve, ali ne i za općenite skupove, gdje nam dobra utemeljenost nije induktivno zadana.

Zadatak 4.17. *U dokazu propozicije 4.11, aksiomom dobre utemeljenosti smo vrlo jednostavno dokazali irefleksivnost, dok smo tranzitivnost dokazali induktivno. Pokušajte obrnuto: dokažite tranzitivnost aksiomom dobre utemeljenosti, a irefleksivnost induktivno.*

4.7 Konačnost i beskonačnost

Sad kada imamo izgrađen prvi (neformalno) beskonačni skup, vrijeme je da pogledamo kako ga tretira naša teorija kardinalnosti (koju smo razvili upravo jer kombinatorni principi prebrajanja sami po sebi nisu dovoljno jaki za beskonačne skupove). Za početak iskoristimo formalno definirane prirodne brojeve za formalizaciju konačnosti.

Definicija 4.18. Za skup a kažemo da je *konačan* ako postoji $n \in \omega$ takav da je $a \sim n$.
Inače kažemo da je *a beskonačan.* ◁

Lema 4.19. *Za svaki $n \in \omega$, svaka injekcija $f : n \to n$ je i surjekcija na n.*

Dokaz. Tvrdnju dokazujemo matematičkom indukcijom po n. Baza: svaka funkcija koja ide u $0 = \emptyset$ je surjekcija na 0, jer $\operatorname{rng} f \subseteq \emptyset$ povlači $\operatorname{rng} f = \emptyset$. Pretpostavimo da je svaka injekcija s n u n surjekcija, i neka je $f : n^+ \to n^+$ injekcija. Ako je $f(n) = n$, tada je $f|_n$ injekcija kao restrikcija injekcije, i ide s n u n, jer za svaki $i < n$ vrijedi $i \neq n$ pa i $f(i) \neq f(n) = n$.
Po pretpostavci indukcije $f|_n$ je surjekcija na n, pa je

$$\operatorname{rng} f = f[n^+] = f[n \cup \{n\}] = f[n] \cup f[\{n\}] = \operatorname{rng}(f|_n) \cup \{f(n)\} = n \cup \{n\} = n^+. \tag{4.6}$$

Inače je $u := f(n) < n$. No funkcija f mora poprimati i vrijednost n, jer inače bi opet $f|_n$ bila injekcija s n u n, po pretpostavci indukcije bila bi surjekcija na n, pa bi specijalno

poprimala i $u \in n$: postojao bi $i \in n$ takav da je $f|_n(i) = f(i) = u$. No $i \in n$ znači $i \neq n$ po lemi 4.2(1), pa bi $f(i) = u = f(n)$ bila kontradikcija s injektivnošću od f.

Dakle, postoji $v \in n^+$ takav da je $f(v) = n$. Slučaj $v = n$ smo već razriješili, pa preostaje slučaj $v < n$.

U tom slučaju „preusmjerimo strelice" (pogledajte sliku): definiramo funkciju $g : n \to n$ pomoću $g(x) := \begin{cases} f(x), & x \neq v \\ u, & x = v \end{cases}$, i tvrdimo da je to injekcija. Doista, neka su $x, x' \in n$ različiti: tada najviše jedan od njih može biti jednak v.

Ako su x i x' oba različiti od v, tada je $g(x) = f(x) \neq f(x') = g(x')$ jer je f injekcija. Ako je jedan od njih (bez smanjenja općenitosti x') jednak v, tada je $g(x) = f(x) \neq u$ (jer je $f(n) = u$ te $x < n$, a f je injekcija), dok je $g(x') = g(v) = u$ pa su različiti.

Po pretpostavci indukcije, g je surjekcija na n. Tvrdimo da iz toga slijedi da je i f surjekcija na n^+. Doista, neka je $y \in n^+$ proizvoljan. Ako je $y = n$, tada je $y = f(v)$. Inače je $y \in n = \operatorname{rng} g$ pa postoji $x \in n$ takav da je $g(x) = y$. Ako je $x \neq v$, tada je i $f(x) = g(x) = y$, a ako je $x = v$, tada mora biti $y = g(v) = u = f(n)$. U svakom slučaju našli smo element iz n^+ koji f preslikava u y. □

Teorem 4.20. *1. Ni za jedan $n \in \omega$ ne vrijedi $n^+ \subsetneq n$.*

2. Svi prirodni brojevi su međusobno neekvipotentni.

3. Skup ω je beskonačan.

Dokaz. Za prvu tvrdnju, pretpostavimo suprotno, da je $n \in \omega$ i $f : n^+ \to n$ injekcija. Tada je $f|_n : n \to n$ injekcija kao restrikcija injekcije, pa je prema lemi 4.19 surjekcija na n: specijalno, poprima vrijednost $f(n) \in n$, pa postoji $i \in n$ takav da je $f|_n(i) = f(i) = f(n)$. No to je nemoguće jer je f injekcija.

Za drugu tvrdnju, neka su m i n različiti prirodni brojevi. Po propoziciji 4.13 je ili $n < m$ ili $m < n$; bez smanjenja općenitosti pretpostavimo ovo prvo. Tada je prema lemi 4.12(2) $n^+ < m^+$ odnosno $n^+ \leq m$, drugim riječima $n^+ \subseteq m$, pa kad bi postojala bijekcija f između m i n, njena restrikcija $f|_{n^+}$ bila injekcija s n^+ u n, koja ne postoji prema prvoj tvrdnji.

Treća tvrdnja se dokazuje isto kao i druga: pretpostavimo suprotno da postoji $n \in \omega$ i bijekcija f između ω i n. Iz $n \in \omega$ slijedi $n^+ \subseteq \omega$ (dokažite!), pa je $f|_{n^+}$ injekcija s n^+ u n, što je nemoguće prema prvoj tvrdnji. □

Zadatak 4.21. *Dokažite (indukcijom): za svaki $n \in \omega$, za svaki $a \subset n$, postoji $m \in n$ takav da je $a \sim m$.* **Posljedica:** *Svaki podskup konačnog skupa je konačan.*

4.8 Dedekindov teorem rekurzije

Kao što smo rekli, sada bismo htjeli definirati osnovne operacije na prirodnim brojevima. Uzmimo zbrajanje; množenje je sasvim analogno (jednom kad imamo zbrajanje).
Zbrajanje u Peanovoj aritmetici se obično definira rekurzivnim jednakostima

$$m+0 := m, \qquad m+n^+ := (m+n)^+, \qquad \text{za sve } m,n \in \omega \tag{4.7}$$

— no kako opravdati tu definiciju u teoriji skupova? Želimo funkciju $g : \omega \times \omega \to \omega$ takvu da je $g\big((m,n)\big) = m+n$ za sve $m,n \in \omega$. Iako je ona nesumnjivo dobro definirana pravilima (4.7), nije *a priori* jasno da se ta pravila mogu zapisati u obliku formule, tako da tom formulom možemo iz $(\omega \times \omega) \times \omega$ separirati odgovarajuće „uređene trojke" $(x,y,z) := \big((x,y),z\big)$ za koje vrijedi $z = x+y$. Naravno, formula ne može koristiti funkcijsku oznaku $+$, jer to tek želimo definirati. Ipak, pokazat će se da je teorija skupova dovoljno jaka da dokaže postojanje i jedinstvenost takvih funkcija.

Ideja je graditi funkciju g „korak po korak", odnosno aproksimirati je odozdo tako da izgrađujemo njene restrikcije $g|_n$ na prirodne brojeve. Još jedna korist od takvog pristupa je da u rekurzivnoj definiciji pri zadavanju $g(n)$ možemo koristiti sve prethodno izračunane vrijednosti (funkciju $g|_n$), a ne samo onu neposredno prethodnu. Iz istog razloga ne moramo ni odvajati bazu: slučaj $n = 0$ jednostavno prepoznamo tako što je tada $g|_n = \emptyset$. Jedan nedostatak je što je malo kompliciranije opisati domenu rekurzivne definicije, ali nije strašno.

Definicija 4.22. Za skup t, označimo $t^* := \bigcup_{n\in\omega} {}^n t$ (skup svih *konačnih nizova* u t). ◁

Teorem 4.23 (Dedekind)**.** *Neka je t neprazni skup i neka je $F : t^* \to t$ funkcija.*
Za funkciju f kažemo da je F-rekurzivna ako $n\ f\ m$ povlači $f|_n\ F\ m$.
Tada postoji jedinstvena F-rekurzivna funkcija $g : \omega \to t$.

Dokaz. Prvo, $B := \{{}^n t : n \in \omega\}$ je skup po aksiomu zamjene primijenjenom na skup ω (posljedica aksioma beskonačnosti) i formulu $\varphi := (y = {}^x t)$. Sada je $t^* = \bigcup B$ skup po aksiomu unije, pa je $G := \{f \in t^* : f \text{ je } F\text{-rekurzivna}\}$ također skup po aksiomu separacije, primijenjenom na skup t^* i formulu $(\forall n \in \operatorname{dom} x)\big(x(n) = F(x|_n)\big)$.

Elementi skupa G predstavljaju dobre aproksimacije tražene funkcije g: svaka od njih ima vrijednost koju treba imati do neke (konačne) granice, a onda „posustane". To znači da je svaka $f \in G$ *podskup* od g, odnosno prirodno je definirati $g := \bigcup G$. Ona postoji po aksiomu unije; samo još trebamo strogo dokazati da ima sva tražena svojstva, i da je jedina takva.

[g je relacija između ω i t]: Svaki element $p \in g = \bigcup G$ mora biti element neke $f \in G$. Svaka $f \in G$ je element od $t^* = \bigcup B$ jer je $G \subseteq t^*$, pa to zapravo znači da postoji $n \in \omega$ takav da je $f : n \to t$. Sada $p \in f$ znači da je $p = (x,y)$ za neke $x \in n$ i $y \in t$, a iz $x \in n$ slijedi da je x prirodni broj po propoziciji 4.8. Sve u svemu, vrijedi $p \in \omega \times t$, pa je $g \subseteq \omega \times t$.

[g ima funkcijsko svojstvo]: Upravo smo vidjeli da su svi elementi od g uređeni parovi. Neka su $(x,y),(x,y') \in g$ s istom prvom koordinatom $x \in \omega$. Dokazujemo $y = y'$. Iz $(x,y) \in g$

slijedi da postoji $f \in G$ takva da je $y = f(x)$, a $f \in G \subseteq t^*$ znači da postoji $n \in \omega$ takav da je $f : n \to t$. Sasvim jednako, postoje $n' \in \omega$ i $f' : n' \to t$ takvi da je $y' = f'(x)$.

Dakle, x mora biti iz obje domene: $x \in n \cap n'$. Po propoziciji 4.8 je x prirodni broj, pa tvrdnju $f(x) = f'(x)$ možemo dokazati jakom indukcijom po x. U tu svrhu, pretpostavimo da je $f(z) = f'(z)$ za sve $z \in x$. No to upravo znači da je $f|_x = f'|_x$, pa (jer su f i f' obje F-rekurzivne) vrijedi $f(x) = F(f|_x) = F(f'|_x) = f'(x)$.

Jednom kad smo dokazali da je g funkcija, vidimo da se sve funkcije iz G moraju „slagati" na presjeku svojih domena, jer se slažu s g.

[g je F-rekurzivna]: Neka je $(n, m) \in g$. Tada postoji $f \in G$ takva da je $g(n) = m = f(n) = F(f|_n) = F(g|_n)$ (jer je f F-rekurzivna, a f i g se slažu na n i svim njegovim elementima).

[$\operatorname{dom} g = \omega$]: Iz $g \subseteq \omega \times t$ odmah slijedi $\operatorname{dom} g \subseteq \omega$, trebamo dokazati drugu inkluziju: za svaki $n \in \omega$ indukcijom dokazujemo da postoji $f \in G$ takva da je $f : n \to t$. (Iz toga će slijediti tvrdnja, jer je $\operatorname{dom} g = \bigcup_{f \in G} \operatorname{dom} f \supseteq \bigcup_{n \in \omega} n = \omega$ po korolaru 4.9.) Za $n = 0$ uzmimo $\emptyset : 0 \to t$ koja je trivijalno F-rekurzivna. Ako je $f : n \to t$ F-rekurzivna, tada za $h := f \cup \{(n, F(f))\}$ vrijedi $h : n^+ \to t$, i h je F-rekurzivna: za svaki $m \in n^+$ je ili $m < n$ pa je $h(m) = f(m) = F(f|_m) = F(h|_m)$, ili je $m = n$ pa je $h(m) = h(n) = F(f) = F(h|_n)$.

[g je jedinstvena takva funkcija]: Pretpostavimo da je $g' : \omega \to t$ još jedna takva, i jakom indukcijom po n dokažimo $g(n) = g'(n)$. Ako vrijedi $g(m) = g'(m)$ za sve $m \in n$, tada je $g|_n = g'|_n$ pa je $g(n) = F(g|_n) = F(g'|_n) = g'(n)$. □

Najjednostavniji slučaj rekurzije, tzv. *primitivnu* rekurziju, dobijemo po analogiji s principom matematičke indukcije: zadamo $f(n^+)$ pomoću $f(n)$, a $f(0)$ zadamo posebno.

Korolar 4.24. *Neka je t skup, $s \in t$ i $G : t \to t$. Tada postoji jedinstvena funkcija $g : \omega \to t$ takva da je $g(0) = s$ i $g(n^+) = G\big(g(n)\big)$ za sve n.*

Dokaz. Primijenimo teorem rekurzije na funkciju zadanu s $F(f) := \begin{cases} s, & f = \emptyset \\ G(f(\bigcup \operatorname{dom} f)), & \text{inače} \end{cases}$.
Tada će biti $g(0) = F(g|_0) = F(\emptyset) = s$, i $g(n^+) = F\big(g|_{n^+}\big) = G\big((g|_{n^+})(\bigcup n^+)\big) = G\big(g(n)\big)$. □

4.9 Operacije na prirodnim brojevima

Sada napokon možemo pomoću primitivne rekurzije uvesti zbrajanje, a onda i množenje i potenciranje, prirodnih brojeva.

Primjer 4.25. Neka je $m \in \omega$ proizvoljan. Primijenimo korolar 4.24 na $t := \omega$, $s := m$ i $G(x) := x^+$.
Dobijemo jedinstvenu funkciju $z_m : \omega \to \omega$ za koju je $z_m(0) = m$ i $z_m(n^+) = \big(z_m(n)\big)^+$.
Sada je $z : \omega \to {}^{\omega}\omega$ zadana s $z(m) := z_m$ funkcija, pa tehnikom *currying* možemo definirati jednu funkciju $+ : \omega \times \omega \to \omega$, čije vrijednosti $+\big((m, n)\big) := z_m(n)$ označavamo s $m + n$.

Primijenimo korolar 4.24 na $t := \omega$, $s := 0$ i $G := z_m$. Dobijemo funkciju $u_m : \omega \to \omega$ za koju je $u_m(0) = 0$ i $u_m(n^+) = m + u_m(n)$. *Currying* daje $\cdot : \omega \times \omega \to \omega$, i $u_m(n)$ označavamo s $m \cdot n$.

I još jednom, primjenjujući korolar 4.24 na $t := \omega$, $s := 1$ i $G := u_m$, dobijemo funkciju (čiju vrijednost u n označavamo s m^n) takvu da je $m^0 = 1$ i $m^{n^+} = m \cdot m^n$. ◁

Iz toga možemo rekonstruirati čitavu aritmetiku prirodnih brojeva.

Zadatak 4.26. *Uz oznake* $5 := 4^+$ *i* $6 := 5^+$, *dokažite* $2 + 3 = 5$ *i* $2 \cdot 3 = 6$. *Koliko je* 2^3*?*

Teorem 4.27. *Neka su* $a, b, c \in \omega$, *te* $0 = \emptyset$ *i* $1 = \{\emptyset\}$. *Tada vrijedi:*

$$\begin{aligned}
a + (b + c) &= (a + b) + c & a \cdot (b \cdot c) &= (a \cdot b) \cdot c \\
a + b &= b + a & a \cdot b &= b \cdot a \\
0 + a = 1 \cdot a = a^1 &= a & 0 \cdot a = 0 \wedge 1^a = a^0 &= 1 \\
a > 1 \wedge b < c &\Rightarrow a^b < a^c & a > 0 &\Rightarrow 0^a = 0 \\
a \cdot (b + c) &= a \cdot b + a \cdot c & (a \cdot b)^c &= a^c \cdot b^c \\
a^{b+c} &= a^b \cdot a^c & a^{b \cdot c} &= \left(a^b\right)^c \\
a < b \wedge c > 0 &\Rightarrow a + c < b + c \wedge a \cdot c < b \cdot c \wedge a^c < b^c
\end{aligned}$$

Dokaz. Primijetimo da su tvrdnje vrlo slične tvrdnjama teorema 3.14 o aritmetici s kardinalnostima (do na činjenicu da operacije čuvaju strogi uređaj), no dokazi su bitno drugačiji (induktivni) jer su definicije rekurzivne. Napomenimo još da, za razliku od teorema 3.14 gdje su se tvrdnje mogle nezavisno dokazivati, ovdje je prilično bitan redoslijed kojim se dokazuju, jer mnoge tvrdnje koriste neke druge u svojm dokazima. Ipak, uobičajena „pohlepna tehnika" (pokušamo nešto dokazati, a ako vidimo da nam pritom treba neka druga tvrdnja, prvo nju dokažemo i onda nastavimo dokaz prethodne) funkcionira. Opet, dobra je vježba raspisati svaki od tih dokaza; ovdje ćemo pokazati samo neke.

[komutativnost zbrajanja]: Indukcijom po b. Baza: trebamo dokazati $a + 0 = 0 + a$. Lijeva strana je a po definiciji, a desna po već dokazanom svojstvu. Korak: pretpostavimo da je $a + b = b + a$. Tada je $a + b^+ = (a + b)^+ = (b + a)^+$, i želimo dokazati da je to jednako $b^+ + a$. Taj dokaz provodimo (ugniježđenom) indukcijom po a: $(b+0)^+ = b^+ = b^+ + 0$, a $(b+a)^+ = b^+ + a$ povlači $(b + a^+)^+ = \left((b + a)^+\right)^+ = (b^+ + a)^+ = b^+ + a^+$.

[distributivnost potenciranja prema množenju]: Indukcijom po c. Baza: $a^0 \cdot b^0 = 1 \cdot 1 = 1 \cdot 0^+ = 1 + 1 \cdot 0 = 1 + 0 = 1 = (a \cdot b)^0$. Korak: pretpostavimo da je $(a \cdot b)^c = a^c \cdot b^c$. Tada je $(a \cdot b)^{c^+} = (a \cdot b) \cdot (a^c \cdot b^c) = (a \cdot a^c) \cdot (b \cdot b^c) = a^{c^+} \cdot b^{c^+}$ zbog (već dokazanih) komutativnosti i asocijativnosti množenja.

[zbrajanje čuva strogi uređaj]: Neka je $a < b$ (pretpostavka $c > 0$ ovdje nije potrebna). Indukcijom po c dokažimo $a + c < b + c$. Baza: $a + 0 = a < b = b + 0$. Korak: $a + c < b + c$ povlači $(a + c)^+ < (b + c)^+$ po lemi 4.12(2), a to znači $a + c^+ < b + c^+$.

Posljedica upravo dokazanog i komutativnosti zbrajanja je $a < b \wedge c < d \Rightarrow a + c < b + d$. Pomoću toga se lako dokaže da množenje (brojem većim od nule) čuva strogi uređaj. □

Posljedica monotonosti (čuvanja strogog uređaja) je da, iako nemamo operaciju oduzimanja na prirodnim brojevima, ipak možemo „poništiti" iste pribrojnike u jednakostima.

Korolar 4.28. *Za sve $a, b, c \in \omega$ vrijedi $a + c = b + c \Rightarrow a = b$.*

Dokaz. Kad ne bi bilo $a = b$, zbog totalnosti uređaja bilo bi $a < b$ (pa onda i $a + c < b + c$) ili $a > b$ (pa onda i $b + c < a + c$). U svakom slučaju dobijemo kontradikciju s $a + c = b + c$. □

Za kraj dokažimo postojanje „ograničenog oduzimanja".

Propozicija 4.29. *Za sve $a, b \in \omega$, ako je $a \leq b$, tada postoji $c \in \omega$ takav da je $a + c = b$.*

Dokaz. Indukcijom po b. Ako je $a \leq 0$, po lemi 4.12(1) i antisimetričnosti je $a = 0$, pa za $c := 0$ vrijedi $0 + 0 = 0$.

Pretpostavimo da $a \leq b$ povlači postojanje c takvog da je $a + c = b$, i neka je $a \leq b^+$.
Po lemi 2.4 to znači $a < b^+$ ili $a = b^+$. U prvom slučaju je $a \leq b$ pa po pretpostavci indukcije postoji c takav da je $a + c = b$ — no tada za c^+ vrijedi $a + c^+ = (a + c)^+ = b^+$. U drugom slučaju za $c = 0$ vrijedi $b^+ + 0 = b^+$. □

Zadatak 4.30. *Dokažite: ako je $a \in b \in \omega$, tada postoji $c \in \omega$ takav da je $a + c^+ = b$.*

5 Skupovi brojeva $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$

5.1 Skup cijelih brojeva

Sada je cilj, pomoću skupa ω, operacija na njemu i njihovih svojstava, definirati veće skupove brojeva, operacije na njima, i dokazati njihova svojstva. Gotovo sve to ste već napravili na Elementarnoj matematici.

Prvi na redu je skup cijelih brojeva. Cijele brojeve dobivamo kao razlike prirodnih, s tim da moramo poistovjetiti npr. razlike $1-5$ i $3-7$. Pri tome svojstvo da su razlike $a-b$ i $c-d$ jednake treba izraziti koristeći samo operacije na prirodnim brojevima.

Propozicija 5.1. *Na $\omega\times\omega$, $s\,(a,b)\overset{+}{\sim}(c,d) :\Leftrightarrow a+d=c+b$ je zadana relacija ekvivalencije.*

Dokaz. Refleksivnost i simetričnost slijede iz istih svojstava relacije jednakosti.
Za tranzitivnost, neka je $(a,b)\overset{+}{\sim}(c,d)\overset{+}{\sim}(e,f)$. To znači $a+d=c+b$ i $c+f=e+d$, iz čega zbrajanjem dobijemo $(a+d)+(c+f)=(c+b)+(e+d)$. Rearanžiranjem pribrojnika (asocijativnost i komutativnost zbrajanja, teorem 4.27) dobijemo $(a+f)+(c+d)=(e+b)+(c+d)$. Poništavanjem (korolar 4.28) dobijemo $a+f=e+b$, odnosno $(a,b)\overset{+}{\sim}(e,f)$. □

Klasu ekvivalencije $[(a,b)]_{\overset{+}{\sim}}$ označavamo s $a-b$ i zovemo *razlikom* a i b.
Specijalno, razliku $0-x$ pišemo skraćeno kao $-x$, a $x-0$ kao $+x$.
Kvocijentni skup $\omega\times\omega/_{\overset{+}{\sim}}$ zovemo *skupom cijelih brojeva* i označavamo ga sa $\mathbb{Z}$.

Teorem 5.2. *Na razlikama definiramo operacije i uređaj pomoću:*

$$(a-b)+(c-d) := (a+c)-(b+d) \tag{5.1}$$
$$(a-b)\cdot(c-d) := (a\cdot c+b\cdot d)-(a\cdot d+b\cdot c) \tag{5.2}$$
$$a-b<c-d :\Leftrightarrow a+d<c+b \tag{5.3}$$

(na desnoj strani se radi o operacijama i uređaju na prirodnim brojevima).

1. *Te definicije ne ovise o reprezentantima razlikā.*
2. *Uz tako definirane operacije, $(\mathbb{Z},+,\cdot)$ je integralna domena.*
3. *$(\mathbb{Z},<)$ je totalno uređen, zbrajanje čuva uređaj, a množenje čuva pozitivnost.*
4. *Preslikavanje $x\mapsto +x$ je ulaganje ω u $\mathbb{Z}$ (injekcija koja čuva operacije i uređaj).*

Dokaz. Opet, nećemo dokazati svih $3+8+5+4=20$ svojstava, ali mnoga su vrlo jednostavna ili jednostavno slijede iz svojstava prirodnih brojeva. Evo nekih dokaza koji pokazuju korištene tehnike. (Oznaku za množenje obično ispuštamo.)

[neovisnost definicije množenja o reprezentantima]: Neka su $(a,b) \overset{+}{\sim} (e,f)$ i $(c,d) \overset{+}{\sim} (g,h)$. Želimo dokazati da je $(ac+bd, ad+bc) \overset{+}{\sim} (eg+fh, eh+fg)$. Koristeći tranzitivnost, dovoljno je dokazati da su oba para u relaciji s $(ce+df, de+cf)$, koji se dobije tako da se samo prvi faktor (a,b) zamijeni ekvivalentnim (e,f), dok drugi faktor (c,d) ostane isti. Dokažimo samo prvu ekvivalenciju, druga je sasvim analogna. Dakle, imamo pretpostavku $a+f=e+b$, i raspisujemo:

$$ac+bd+de+cf = c(a+f)+d(b+e) = c(e+b)+d(a+f) = ce+bc+ad+df, \tag{5.4}$$

iz čega slijedi $(ac+bd, ad+bc) \overset{+}{\sim} (ce+df, de+cf)$.

[neutralni elementi]: Očito je $0-0=+0=-0$. To je neutralni element za zbrajanje, jer je $(a-b)+(0-0)=(a+0)-(b+0)=a-b$. Također, $+1$ je neutralni element za množenje, jer je $(1-0)\cdot(a-b)=(1a+0b)-(1b+0a)=(a+0)-(b+0)=a-b$.

Za element $x \in \mathbb{Z}$ kažemo da je *pozitivan* ako je $x > +0$. Lako je vidjeti da je $b-a$ aditivni inverz za $a-b$, jer je $(a-b)+(b-a)=(a+b)-(b+a)=0-0$ zbog $a+b+0=0+b+a$. Također (dokažite sami!), za svaki $x \in \mathbb{Z} \setminus \{+0\}$ je ili x pozitivan ili je njegov aditivni inverz $-x$ pozitivan (tada kažemo da je x *negativan*).

[umnožak pozitivnih je pozitivan]: Neka je $a-b>+0$ i $c-d>+0$. To znači $b<a$ i $d<c$, pa po zadatku 4.30 vrijedi $a=b+u^+$ i $c=d+v^+$ za neke u i v. Trebamo $(a-b)(c-d)>+0$, odnosno $ac+bd>ad+bc$. No lijeva strana je $(b+u^+)(d+v^+)+bd = bd+bd+bv^++du^++u^+v^+ = b(d+v^+)+d(b+u^+)+u^+v^+ = bc+ad+u^+v^+$, pa je dovoljno dokazati $u^+v^+>0$, što lako slijedi iz $u^+v^+=(uv+u+v)^+$.

Sada se lako pomoću distributivnosti dobije $(-x)\cdot y=-(x\cdot y)$, pa je umnožak pozitivnog i negativnog negativan, a umnožak negativnih pozitivan. Iz toga i totalnosti uređaja odmah dobivamo da nema djelitelja nule. (Vjerojatno ste to dokazali na Algebarskim strukturama.)

[$x \mapsto +x$ čuva strogi uređaj]: Neka je $x<y$ u ω. To možemo zapisati kao $x+0<y+0$, odnosno $x-0<y-0$, dakle $+x<+y$ u $\mathbb{Z}$. Iz toga odmah slijedi i da se radi o injekciji. □

Slika unarnog plusa je upravo skup nenegativnih brojeva (dokažite!), koji označavamo sa $\mathbb{Z}_{+0}$. Zbog posljednje stavke, poistovjećujemo $n \in \omega$ s $+n \in \mathbb{Z}_{+0}$, i više uglavnom ne pišemo unarni plus. Primjerice, kad kažemo $6 \in \mathbb{Z}$, zapravo mislimo $+6 \in \mathbb{Z}$. U tom smislu kažemo da je $\omega \subseteq \mathbb{Z}$. To možemo i doslovno napraviti tako da stavimo $\mathbb{Z} := (\omega\times\omega)/_{\overset{+}{\sim}} \setminus \mathbb{Z}_{+0} \cup \omega$ (iz kvocijentnog skupa izvadimo sliku ulaganja i umjesto nje ubacimo prave prirodne brojeve) uz odgovarajuću redefiniciju operacija po slučajevima — ali ne trebamo biti toliko precizni.

Zadatak 5.3. *Dokažite: svaki cijeli broj je oblika $+x$ ili oblika $-x$, za neki $x \in \omega$.*

5.2 Skup racionalnih brojeva

Prilično analogno, kao što smo cijele brojeve uveli kao razlike prirodnih, racionalne uvodimo kao količnike cijelih. Ipak, treba paziti da djelitelj nije nula, i zapravo smijemo pretpostaviti da je pozitivan. Skup pozitivnih cijelih brojeva označavamo sa $\mathbb{Z}_+$.

Propozicija 5.4. *Na $\mathbb{Z}\times\mathbb{Z}_+$, $s\,(a,b)\sim(c,d) :\Leftrightarrow ad=cb$ je zadana relacija ekvivalencije.*

Dokaz. Refleksivnost i simetričnost slijede iz istih svojstava relacije jednakosti (kao za $\overset{+}{\sim}$). Za tranzitivnost, neka je $(a,b)\sim(c,d)\sim(e,f)$. To znači $ad=cb$ i $cf=ed$, dakle množenjem $adcf=cbed$, odnosno $0=acdf-bcde=cd(af-eb)$. U $\mathbb{Z}$ nema djelitelja nule, pa imamo tri mogućnosti:

1. $af-eb=0$: to znači $(a,b)\sim(e,f)$, što smo trebali.
2. $d=0$: ovo je zapravo nemoguće, jer je $(c,d)\in\mathbb{Z}\times\mathbb{Z}_+$, a $0\notin\mathbb{Z}_+$ zbog irefleksivnosti.
3. $c=0$: tada je $ad=cb=0b=0$, dakle $a=0$ (jer d nije) i analogno $e=0$, pa svakako i $0f=0b=0$, odnosno $(0,b)\sim(0,f)$, što je tražena tvrdnja zbog $a=e=0$. □

Klasu ekvivalencije $[(a,b)]_\sim$ označavamo s $\frac{a}{b}$ i zovemo *razlomkom* s brojnikom a i nazivnikom b. Kvocijentni skup $\mathbb{Z}\times\mathbb{Z}_+/_\sim$ zovemo *skupom racionalnih brojeva* $\mathbb{Q}$.

Teorem 5.5. *Na razlomcima definiramo operacije i uređaj pomoću:*

$$\frac{a}{b}+\frac{c}{d}:=\frac{ad+cb}{bd}\,,\qquad \frac{a}{b}\cdot\frac{c}{d}:=\frac{ac}{bd}\,,\qquad \frac{a}{b}<\frac{c}{d}:\Leftrightarrow ad<cb\,. \tag{5.5}$$

(na desnoj strani se radi o operacijama i uređaju na cijelim brojevima).

1. *Te definicije ne ovise o reprezentantima razlomaka.*
2. *Uz tako definirane operacije, $(\mathbb{Q},+,\cdot,<)$ je uređeno polje (karakteristike 0).*
3. *Preslikavanje $x\mapsto\frac{x}{1}$ je ulaganje $\mathbb{Z}$ u $\mathbb{Q}$.*

Dokaz. Prvo primijetimo da je nazivnik bd novodefiniranih razlomaka pozitivan kao umnožak pozitivnih cijelih brojeva. Opet, dokazat ćemo samo neke reprezentativne tvrdnje.

[neovisnost definicije zbrajanja o reprezentantima]: Neka su $(a,b)\sim(e,f)$ i $(c,d)\sim(g,h)$. Tada je $af=eb$ i $ch=gd$, pa je

$$(ad+cb)fh=afdh+chbf=ebdh+gdbf=(eh+gf)bd, \tag{5.6}$$

odnosno $(ad+cb,bd)\sim(eh+gf,fh)$, što smo i trebali.

[inverz s obzirom na množenje]: Lako je vidjeti da je $\frac{0}{1}$ neutralni element za zbrajanje, a $\frac{1}{1}$ neutralni za množenje. Neka je sad $\frac{a}{b}\neq\frac{0}{1}$; tražimo razlomak $\frac{c}{d}$ takav da je $\frac{a}{b}\cdot\frac{c}{d}=\frac{1}{1}$, odnosno $(ac,bd)\sim(1,1)$. Pretpostavka kaže $1a\neq 0b$, odnosno $a\neq 0$, pa a ili $-a$ mora biti pozitivan. Ako je a pozitivan, $\frac{b}{a}$ je traženi inverz: $(ab,ba)\sim(1,1)$ zbog komutativnosti množenja. Ako

je pak $-a$ pozitivan, $\frac{-b}{-a}$ je traženi inverz: $\big(a\cdot(-b), b\cdot(-a)\big) \dot{\sim} (1,1)$ kao posljedica distributivnosti.

[karakteristika 0]: Trebamo dokazati da suma $\frac{1}{1}+\frac{1}{1}+\frac{1}{1}+\cdots+\frac{1}{1}$ nikad nije $\frac{0}{1}$; indukcijom po broju pribrojnika (barem 1) dokazat ćemo da je uvijek veća od $\frac{0}{1}$. Baza: $\frac{1}{1} > \frac{0}{1}$ jer je $1\cdot 1 > 0\cdot 1$ u $\mathbb{Z}$ (a to vrijedi jer se radi o prirodnim brojevima, uz ulaganje ω u $\mathbb{Z}$). Korak slijedi iz baze, pretpostavke i činjenice da zbrajanje čuva strogi uređaj (što vrijedi u svakom uređenom polju). □

Slično kao za $\omega \subseteq \mathbb{Z}$, možemo shvatiti da je $\mathbb{Z} \subseteq \mathbb{Q}$ poistovjećujući $x \in \mathbb{Z}$ s $\frac{x}{1} \in \mathbb{Q}$. Opet, to možemo napraviti sasvim formalno, redefinirajući $\mathbb{Q}$ tako da iz kvocijentnog skupa $(\mathbb{Z}\times\mathbb{Z}_+)/\dot{\sim}$ izvadimo sliku ulaganja i umjesto nje ubacimo pravi $\mathbb{Z}$ (koji prema prethodnom sadrži kao podskup pravi ω); ili neformalno, shvaćajući npr. $4 \in \mathbb{Q}$ kao pokratu za $\frac{4}{1} \in \mathbb{Q}$ odnosno $\frac{+4}{+1} \in \mathbb{Q}$. O tome više nećemo eksplicitno govoriti, ali potpuno isti fenomen imat ćemo i s $\mathbb{Q} \subseteq \mathbb{R}$ i s $\mathbb{R} \subseteq \mathbb{C}$ (a i s većim skupovima brojeva ako ih budemo trebali izgraditi).

5.3 Prebrojivost

Zbog teorema 4.20(2) sve su kardinalnosti $\mathfrak{K}(n), n \in \omega$ različite i prirodno je svaku od njih reprezentirati *kardinalnim brojem n*. No zbog teorema 4.20(3) kardinalnost $\mathfrak{K}(\omega)$ mora biti neki novi broj. Mogli bismo koristiti sām ω, ali s time postoji jedan problem.

Uređaj i rekurzivno definirane operacije na induktivno definiranim prirodnim brojevima podudaraju se s uređajem i operacijama na kardinalnostima *konačnih skupova* uvedenima u poglavlju 3. No prirodno proširenje indukcije na beskonačne skupove — *transfinitna* indukcija — daje operacije koje se više ne podudaraju s operacijama na kardinalnostima. Recimo, vidjet ćemo da je u induktivnom smislu $2^\omega = \omega$, što je u direktnoj kontradikciji s Cantorovim osnovnim teoremom ako ω shvatimo kao kardinalni broj.

Taj problem teorija skupova rješava na pomalo nekonvencionalni način: kardinalni brojevi definiraju se kao (neki) ordinalni brojevi, ali se za njih (na beskonačnim skupovima) koriste **druge oznake**. Tako ćemo $\mathfrak{K}(\omega)$ označavati s $\aleph_0$, i bit će $2^{\aleph_0} > \aleph_0$ u skladu s Cantorovim osnovnim teoremom. To treba shvatiti tako da se radi o dvije različite *operacije* potenciranja (koje se podudaraju na prirodnim brojevima) ali se iz tradicionalnih razloga za obje koristi ista oznaka, evocirajući različitost operacijā različitim oznakama za *operande*.

Definicija 5.6. Za skup a kažemo da je *prebrojiv* ako je $a \sim \omega$. Definiramo $\aleph_0 := \mathfrak{K}(\omega)$. Kažemo da je a *neprebrojiv* ako je $\mathfrak{K}(a) > \aleph_0$. ◁

Napomenimo da se u nekim granama matematike (recimo, u teoriji mjere) konačni skupovi također smatraju prebrojivima — u teoriji skupova to **ne** činimo. Nezgodna posljedica toga je da *neprebrojiv* ne znači negaciju od „prebrojiv”: konačni skupovi nisu ni jedno ni drugo.

Lema 5.7. *Neka je $a \subseteq \omega$ neprazan.*
Ako a ima maksimum, tada je a konačan. Ako a nema maksimum, tada je a prebrojiv.

Dokaz. Pretpostavimo da a ima maksimum i označimo ga s n.
Tada za svaki $x \in a$ vrijedi $x \leq n$, odnosno $a \subseteq n^+$ pa je a konačan po zadatku 4.21.

Inače, za svaki $x \in a$ postoji veći element, pa je skup $\{y \in a : y > x\}$ neprazni podskup od $a \subseteq \omega$, i kao takav ima jedinstveni minimum (zbog dobre uređenosti od ω). Aksiom zamjene nam daje funkciju $s : a \to a$ koja preslikava svaki $x \in a$ u najmanji $y \in a$ veći od x. Također, čitav a kao neprazni podskup od ω ima minimum, označimo ga s m. Sada korolar 4.24 daje funkciju $f : \omega \to a$ takvu da je $f(0) = m$ i $f(n^+) = s\big(f(n)\big)$. Očito je $s(x) > x$, pa se lako indukcijom dobije da f čuva strogi uređaj, i zato je injekcija. Iz toga slijedi $\omega \subsetneq a$, što zajedno s $a \subseteq \omega$ (po CSB) daje $a \sim \omega$. □

Korolar 5.8. *Svaki podskup prebrojivog skupa je ili konačan ili prebrojiv.*

Dokaz. Neka je b prebrojiv skup: to znači da postoji bijekcija između b i ω. Uzmimo jednu i označimo je s f. Neka je $c \subseteq b$ proizvoljan. Označimo $a := f[c] \subseteq \omega$: tada je $f|_c$ bijekcija između c i a. Ako je a prazan, tada je i c prazan pa je konačan ($c \sim 0 = a \in \omega$). Ako a ima maksimum, tada je a konačan pa je i c konačan ($c \sim a \sim n \in \omega$). Inače je a prebrojiv pa je takav i c ($c \sim a \sim \omega$). □

Zadatak 5.9. *Dokažite (slično kao korolar 5.8): svaki skup $a \subsetneq \omega$ je konačan ili prebrojiv.*

Zadatak 5.10. *[Minimum teorije parnih i neparnih brojeva za iduću lemu.] Dokažite (indukcijom) da za svaki $b \in \omega$ postoji $u \in \omega$ takav da je $3^b = 2 \cdot u + 1$. Također dokažite da ne postoje $u, v \in \omega$ takvi da je $2u + 1 = 2v$ (uputa: dokažite da nije moguće ni $u < v$ ni $u \geq v$).*

Lema 5.11. *Kartezijev produkt prebrojivih skupova je prebrojiv.*
Kvocijentni skup prebrojivog skupa je konačan ili prebrojiv.

Dokaz. Za prvu tvrdnju, zapravo trebamo dokazati $\aleph_0 \cdot \aleph_0 = \aleph_0$, a za to je dovoljno dokazati $\omega \times \omega \sim \omega$ (jer množenje kardinalnosti ne ovisi o reprezentantima). Očito je $\omega \subsetneq \omega \times \omega$ jer je $x \mapsto (x, 0)$ injekcija; za drugi smjer, tvrdimo da je s $g(x, y) := 2^x \cdot 3^y$ zadana injekcija s $\omega \times \omega$ u ω. Doista, pretpostavimo da je $2^a \cdot 3^b = 2^c \cdot 3^d$. Ako je $a = c$, tada je (zbog monotonosti množenja) $2^a = 0$ ili $3^b = 3^d$: po svojstvima potenciranja prirodnih brojeva prvo je nemoguće (dokažite!), a drugo daje $b = d$, odnosno $(a, b) = (c, d)$.

Ako je pak $a \neq c$, jedan je veći: bez smanjenja općenitosti $c > a$, odnosno (po zadatku 4.30) $c = a + e^+$ za neki $e \in \omega$. Sada je $2^a \cdot 3^b = 2^a \cdot 2^{e^+} \cdot 3^d$, odnosno (slično prethodnom) $3^b = 2 \cdot (2^e \cdot 3^d)$ — no to je nemoguće po zadatku 5.10. Dakle, $g(a, b) = g(c, d)$ povlači $(a, b) = (c, d)$, odnosno g je injekcija. Po CSB to znači $\omega \times \omega \sim \omega$.

Za drugu tvrdnju, neka je a prebrojiv skup, f bijekcija između ω i a, i R relacija ekvivalencije na a. Lako je vidjeti da je $P := \{(m, n) \in \omega \times \omega : f(m)\ R\ f(n)\}$ relacija ekvivalencije na ω, te je $\omega/_P \sim a/_R$: konkretno, $K \mapsto f[K]$ je bijekcija. No $\omega/_P$ je konačan ili prebrojiv po zadatku 5.9, jer je preslikavanje $K \mapsto \min K$ injekcija s $\omega/_P$ u ω: dobro je definirano jer su sve klase neprazni podskupovi dobro uređenog skupa ω, a injekcija je jer su one u parovima disjunktne. □

Teorem 5.12. *Skupovi $\omega = \mathbb{N}$, $\mathbb{Z}$ i $\mathbb{Q}$ su prebrojivi.*

Dokaz. Prvo, ω je prebrojiv jer je očito $\omega \sim \omega$, a $\mathbb{Z}_+$ jer je kompozicija unarnog plusa i sljedbenika $x \mapsto +x^+$ bijekcija između ω i $\mathbb{Z}_+$. Također, $\omega \times \omega$ je prebrojiv pa je $\mathbb{Z}$ konačan ili prebrojiv (kao njegov kvocijentni skup), no zbog $\mathbb{Z}_+ \subseteq \mathbb{Z}$ znamo da mora biti prebrojiv.

Sada je $\mathbb{Z} \times \mathbb{Z}_+$ prebrojiv kao Kartezijev produkt dva prebrojiva skupa, te je $\mathbb{Q}$ konačan ili prebrojiv kao njegov kvocijentni skup, no zbog $\mathbb{Z} \subseteq \mathbb{Q}$ (ili $\mathbb{Z} \subsetneq \mathbb{Q}$ ako želimo razlikovati x i $\frac{x}{1}$) mora biti prebrojiv. □

Zadatak 5.13. *Dokažite: ako je A neprazan konačan ili prebrojiv skup, tada je A^* prebrojiv. (Uputa: smislite injekciju s ω^* u ω, i dokažite da je to dovoljno).*

5.4 Skup realnih brojeva

Dobro poznata konstrukcija *Dedekindovih rezova* (vidjeli ste je već na Elementarnoj matematici, a možda i na Matematičkoj analizi) daje nam realne brojeve i operacije s njima.

Definicija 5.14. Za $a \subseteq \mathbb{Q}$ kažemo da je *realan broj* ako je a:

- netrivijalan: $\emptyset \subset a \subset \mathbb{Q}$;
- zatvoren nadolje: $x < y \in a$ povlači $x \in a$; i
- nema maksimum: $(\forall x \in a)(\exists y \in a)(x < y)$.

Separacijom iz $\mathscr{P}(\mathbb{Q})$ dobijemo *skup realnih brojeva*, koji označavamo s $\mathbb{R}$. ◁

Na ovako definiranim realnim brojevima je lako definirati zbrajanje i uređaj:

$$a + b := \{x + y : x \in a \wedge y \in b\}, \qquad a < b :\Leftrightarrow a \subset b. \tag{5.7}$$

Također je lako definirati ulaganje $x \mapsto p_{\mathbb{Q}}(x) := \{y \in \mathbb{Q} : y < x\}$ iz $\mathbb{Q}$ u $\mathbb{R}$. Malo je teže dokazati da je zbroj realnih brojeva doista realan broj, a zapetljano je i definirati množenje: „očita" definicija $a \cdot b := \{xy : x \in a \wedge y \in b\}$ prolazi samo ako se ograničimo na *pozitivne* (realne i racionalne) brojeve. U općem slučaju moramo dodati $\mathbb{Q} \setminus \mathbb{Q}_+$ na desnu stranu, a za negativni a ili b moramo koristiti definicije poput $a \cdot b := -\big((-a) \cdot b\big)$, uz prikladno definiran suprotni realni broj. Naravno, umnožak s nulom definiramo da je nula.

Sve te tehnikalije ovdje nam nisu bitne — realni brojevi se dovoljno detaljno obrađuju u matematičkoj analizi i ovdje nas neće previše zanimati svojstva realnih operacija i funkcija. Zanimat će nas kardinalnost i svojstva uređaja. Ovdje samo navedimo (bez dokaza; koga zanima, može pogledati Mardešić, *Matematička analiza u n-dimenzionalnom realnom prostoru*) teorem koji karakterizira skup $\mathbb{R}$.

Teorem 5.15. *Struktura $(\mathbb{R}, +, \cdot, <)$ je potpuno uređeno polje.*
Štoviše, svako potpuno uređeno polje je izomorfno s $\mathbb{R}$.

Teorem govori, među ostalim, o potpunosti.
Kako se radi o svojstvu uređaja, precizno definirajmo i dokažimo to svojstvo.

Propozicija 5.16. *Skup* $\mathbb{R}$ *je* potpun*:*
svaki neprazni podskup od $\mathbb{R}$ *koji ima gornju među u* $\mathbb{R}$*, ima i supremum u* $\mathbb{R}$*.*

Dokaz. Osnovna ideja je vrlo jednostavna: kako je uređaj na realnim brojevima definiran inkluzijom, prirodno je očekivati da supremum bude unija. Dakle, neka je $X \subseteq \mathbb{R}$ neprazan i s gornjom međom g: sve što treba dokazati je da je $\bigcup X$ realni broj. Očito to jest skup po aksiomu unije, i očito je podskup od $\mathbb{Q}$ jer je $\mathbb{Q}$ jedna gornja međa za X (iako $\mathbb{Q} \notin \mathbb{R}$).

[netrivijalan]: Neprazan je jer je $X \neq \emptyset$ i svi elementi od X su neprazni.
Također, $g \in \mathbb{R}$ je pravi podskup od $\mathbb{Q}$, pa je i $\bigcup X \subseteq g \subset \mathbb{Q}$.

[zatvoren nadolje]: Neka je $x \in \bigcup X$ i $y < x$. Prvo znači da postoji $t \in X$ takav da je $x \in t$.
No t je realan broj zbog $X \subseteq \mathbb{R}$, pa je zatvoren nadolje, iz čega slijedi $y \in t$, odnosno $y \in \bigcup X$.

[nema maksimum]: Pretpostavimo da je $m \in \bigcup X$ najveći. Tada po definiciji unije postoji $v \in X$ takav da je $m \in v$, no v je realan broj pa m sigurno nije maksimum od v: postoji $s \in v$ takav da je $s > m$. No tada je i $s \in \bigcup X$, što je kontradikcija s pretpostavkom da je m maksimum tog skupa. □

Zadatak 5.17. *Dokažite:* $(\mathbb{R}, \subset)$ *je totalno uređen skup.*

Prvi veliki uspjeh Cantorove teorije skupova bio je dokaz neprebrojivosti skupa $\mathbb{R}$, čime je prvi put utvrđeno da „ne postoji samo jedna beskonačnost", odnosno postoje beskonačni skupovi različitih veličina. Nama to u ovom trenutku nije iznenađenje jer znamo za Cantorov osnovni teorem (po kojem je npr. $\mathscr{P}(\omega)$ neprebrojiv), ali zanimljivo je vidjeti da postoji i dublja veza. Označimo $\mathfrak{c} := \aleph(\mathbb{R})$.

Propozicija 5.18. $\mathbb{R} \sim \mathscr{P}(\omega)$*, odnosno* $\mathfrak{c} = 2^{\aleph_0}$.

Dokaz. Prvo, ekvivalentnost te dvije tvrdnje slijedi odmah iz zadatka 3.17. Dokazat ćemo ih pomoću Cantor–Schröder–Bernsteinovog teorema. Prvo, zbog $\mathbb{R} \subseteq \mathscr{P}(\mathbb{Q})$ je $\mathfrak{c} \leq 2^{\aleph(\mathbb{Q})} = 2^{\aleph_0}$.

U drugom smjeru, promotrimo funkciju $f : {}^{\omega}\{0,1\} \to \mathbb{R}$ koja svakom nizu nulā i jedinicā pridružuje realni broj s tim nizom decimala: $f\big((a_n)_n\big) := \overline{a_0.a_1a_2\cdots}$. Preciznije, $f(a) := \bigcup_{m\in\omega} p_{\mathbb{Q}}\big(g(m)\big)$, gdje je g definirana pomoću teorema 4.23 ($t := \mathbb{Q}$; $F(f) := f(\bigcup n) + \frac{a(n)}{10^n}$ za $n := \operatorname{dom} f > 0$; $F(\emptyset) := a(0)$). Neka rudimentarna realna analiza sada daje injektivnost funkcije f. Recimo, za različite $a, b : \omega \to \{0,1\}$ postoji najmanji n takav da je $a_n \neq b_n$;
bez smanjenja općenitosti je $a_n = 0$ i $b_n = 1$ (te $a_i = b_i$ za sve $i < n$), pa je

$$f(a) = \overline{a_0.a_1\cdots a_{n-1}0a_{n+1}\cdots} = \overline{b_0.b_1\cdots b_{n-1}0a_{n+1}\cdots} \leq \overline{b_0.b_1\cdots b_{n-1}0111\cdots} <$$
$$< \overline{b_0.b_1\cdots b_{n-1}1000\cdots} \leq \overline{b_0.b_1\cdots b_{n-1}1b_{n+1}\cdots} = f(b), \quad (5.8)$$

dakle $f(a) \neq f(b)$. Iz te injektivnosti zaključujemo preostalu nejednakost $2^{\aleph_0} \leq \mathfrak{c}$. □

Napomena 5.19. Za bazu brojevnog sustava u dokazu propozicije 5.18 možemo koristiti standardnu $10 := 2 \cdot 5$, ali možemo i bilo koju drugu osim baze 2 (zašto?). ◁

Korolar 5.20. $\mathfrak{c} > \aleph_0$*, odnosno* $\mathbb{R}$ *je neprebrojiv.*

5.5 Skup kompleksnih brojeva

Skup *kompleksnih brojeva* $\mathbb{C} := \mathbb{R} \times \mathbb{R}$ je, uz operacije

$$(a,b) + (c,d) := (a+c, b+d), \qquad (a,b) \cdot (c,d) := (ac - bd, ad + bc), \tag{5.9}$$

algebarski zatvoreno polje karakteristike 0. Algebarsku zatvorenost je vrlo teško dokazati [možete pogledati Gogić i Tomašević, *Gelfand–Mazurov teorem i osnovni teorem algebre*], a ostala su svojstva jednostavna, jednom kad ih imamo za skup $\mathbb{R}$ (teorem 5.15).

Preslikavanje $x \mapsto (x,0)$ je ulaganje $\mathbb{R}$ u $\mathbb{C}$ i omogućuje nam identifikaciju $\mathbb{R}$ s $\mathbb{R} \times \{0\} \subseteq \mathbb{C}$. Uz oznaku $i := (0,1) \in \mathbb{C}$, svaki kompleksni broj je oblika $(x,y) = (x,0) + (y,0) \cdot i = x + yi$.

Propozicija 5.21. *Ne postoji uređaj $<$ na $\mathbb{C}$ takav da je $(\mathbb{C}, +, \cdot, <)$ uređeno polje.*

Dokaz. Pretpostavimo da takav uređaj postoji: tada mora biti totalan, pa $1 \neq 0$ znači $1 > 0$ ili $1 < 0$. Lako se vidi da suprotni brojevi (inverzi s obzirom na zbrajanje) moraju imati suprotne predznake: $x > 0$ i $-x > 0$ zbrajanjem daju $0 > 0$, a $x < 0$ i $-x < 0$ daju $0 < 0$.

Dakle, $1 < 0$ bi povlačilo da je $-1 > 0$. Kako u uređenom polju umnožak pozitivnih mora biti pozitivan, $(-1) \cdot (-1) = 1$ je kontradikcija. Zaključujemo da je nužno $1 > 0$, a onda $-1 < 0$.

Sada promotrimo i i $-i$. Prema gornjem, barem jedan od njih je pozitivan, no obje mogućnosti vode na kontradikciju: $i \cdot i = (-i) \cdot (-i) = -1$, što smo vidjeli da je negativan broj. □

Propozicija 5.22. $\mathbb{C} \sim \mathbb{R}$, *odnosno* $\mathfrak{c}^2 = \mathfrak{c}$ *($\mathbb{C}$ je neprebrojiv).*

Dokaz. Prvo, iz $1 \subseteq 2 \subseteq \omega$ slijedi $1 \leq 2 \leq \aleph_0$, pa je po monotonosti množenja kardinalnosti

$$\aleph_0 = \aleph_0 \cdot 1 \leq \aleph_0 \cdot 2 \leq \aleph_0 \cdot \aleph_0 = \aleph_0, \tag{5.10}$$

odnosno po CSB, $\aleph_0 \cdot 2 = \aleph_0$. Sada je

$$\mathfrak{K}(\mathbb{C}) = \mathfrak{K}(\mathbb{R} \times \mathbb{R}) = \mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}^1 \cdot \mathfrak{c}^1 = \mathfrak{c}^{1+1} = \mathfrak{c}^2 = \left(2^{\aleph_0}\right)^2 = 2^{\aleph_0 \cdot 2} = 2^{\aleph_0} = \mathfrak{c}. \quad \square \tag{5.11}$$

Dokaz propozicije 5.22 dobro pokazuje snagu kardinalne aritmetike: jednom kad usvojimo zakone računanja s kardinalnostima, počevši od jednakosti kao što su ${\aleph_0}^2 = \aleph_0$ i $2^{\aleph_0} = \mathfrak{c}$, možemo mnoge jednakosti dokazati „aritmetički", bez mukotrpne potrage za injekcijama.

Zadatak 5.23. *Dokažite* $\mathbb{R} \sim {}^{\mathbb{N}}\mathbb{R} \sim {}^{\mathbb{Z}}\mathbb{C} \sim M_{5,3}(\mathbb{C}) \sim SL_2(\mathbb{R}) \nsim {}^{\mathbb{C}}2 \sim {}^{\mathbb{R}}\mathbb{R} \sim \mathscr{P}(\mathbb{R})$.

5.6 Invarijante sličnosti

Vrijeme je da se detaljnije pozabavimo uređajima na standardnim skupovima brojeva (osim $\mathbb{C}$, zbog propozicije 5.21). Svi su oni totalni, pa je prirodno ograničiti razmatranja na totalne uređaje. Prisjetimo se, sličnost je bijekcija (injekcija i surjekcija) između dva parcijalno uređena skupa, takva da i ona i njen inverz čuvaju uređaj. No u slučaju *totalno* uređenih skupova, dovoljno je dokazati dvostruko manje: dva svojstva umjesto četiri.

Lema 5.24. *Neka su $(a,\prec)$ i $(b,<)$ totalno uređeni skupovi te $f : a \to b$ surjekcija na b koja čuva strogi uređaj. Tada je f sličnost.*

Dokaz. Trebamo dokazati injektivnost, i da f^{-1} čuva uređaj. Za prvo, neka su $s,t \in a$ različiti. Po totalnoj uređenosti, vrijedi $s \prec t$ ili $t \prec s$. U prvom slučaju je $f(s) < f(t)$, a u drugom je $f(t) < f(s)$ (jer f čuva strogi uređaj), dakle u svakom slučaju $f(s) \neq f(t)$ po irefleksivnosti.

Za drugo, neka su $u,v \in b$ takvi da je $u < v$. U ovom trenutku znamo da je f bijekcija, pa označimo $s := f^{-1}(u)$ i $t := f^{-1}(v)$; Tada je $s \prec t$, jer inače bi bilo $s = t$ (nemoguće jer je $u \neq v$ a f je funkcija) ili $t \prec s$ (što bi povlačilo $v = f(t) < f(s) = u < v$, kontradikcija). □

Ipak, glavnina ove točke bit će rezultati u suprotnom smjeru, pomoću kojih možemo zaključiti *izostanak* sličnosti. Samo napomenimo, totalno uređeni skupovi uvijek će dolaziti s nekim podrazumijevanim uređajima (za skupove brojeva to će biti već definirani uređaji koji čuvaju operacije), pa ćemo često koristiti napomenu 2.6.

Definicija 5.25. Za svojstvo P totalno uređenih skupova kažemo da je *invarijanta sličnosti* ako $P(a)$ i $a \simeq b$ povlače $P(b)$. ◁

Ekvivalentno, to se može zapisati kao $P(a) \wedge \neg P(b) \Rightarrow a \not\simeq b$. Odnosno, učinkovit način da se dokaže da totalno uređeni skupovi a i b nisu slični sastoji se u tome da se nađe neka invarijanta sličnosti koju jedan od njih ima a drugi nema.

Definicija 5.26. Neka je $(a,<)$ totalno uređen skup i $b \subseteq a$. Kažemo da je *b gust u a* ako za sve $(x,y) \in (<)$ postoji $z \in b$ takav da je $x < z < y$. „a je gust" znači „a je gust u a". ◁

Teorem 5.27. *Sva sljedeća svojstva (totalno uređenog skupa a) su invarijante sličnosti:*

- *„$\aleph(a) = \alpha$" (za bilo koji fiksni α), konačnost, beskonačnost, prebrojivost, neprebrojivost*
- *„a ima minimum" (i analogno „a ima maksimum"), „a je dobro uređen"*
- *„svaki početni komad $p_a(x)$ je konačan", „svaki segment $[x,y]_a$ je konačan"*
- *gustoća (u samom sebi), separabilnost („postoji prebrojiv podskup od a gust u a")*
- *potpunost („svaki neprazan odozgo ograničen podskup ima supremum")*

Zadatak 5.28. *Za standardne skupove brojeva sa standardnim (definiranim) uređajima ustanovite (i dokažite) koja od svojstava navedenih u teoremu 5.27 imaju a koja nemaju. Izradite tablicu! Zaključite da su svi standardni skupovi brojeva međusobno neslični.*

Dokaz (ideja dokaza teorema 5.27). Svi dokazi da je nešto invarijanta sličnosti su „na isti kalup": sličnosti čuvaju kardinalnost (jer su bijekcije) i uređaj, pa je svako svojstvo koje se može opisati samo koristeći kardinalnost i uređaj, invarijanta sličnosti.

Ako je $f : a \to b$ sličnost i a ima neko svojstvo koje počinje egzistencijalnim kvantifikatorom, uzmemo neki „svjedok" za to $x \in a$ i dokazujemo da je $f(x)$ svjedok iste tvrdnje u b. Ako svojstvo počinje univerzalnim kvantifikatorom, uzmemo proizvoljni $y \in b$ i za njega

dokažemo što već treba koristeći analognu tvrdnju za $f^{-1}(y)$ u a. Isti postupak se može umjesto na elemente primijeniti na podskupove $c \subseteq a$ (prelaskom na $f[c]$) i $d \subseteq b$ (prelaskom na $f^{-1}[d]$).

Primjera radi, dokažimo da je separabilnost invarijanta sličnosti. Neka su $(a, \prec)$ i $(b, <)$ slični totalno uređeni skupovi, $f : a \to b$ sličnost, i postoji $c \subseteq a$ koji je prebrojiv i gust u a. Tvrdimo da je $d := f[c] \subseteq b$ prebrojiv i gust u b. Prebrojivost odmah slijedi iz činjenice da je $d \sim c \sim \omega$, jer je $f|_c$ bijekcija između c i d (injekcija je kao restrikcija injekcije, a surjekcija jer je $d := f[c] = \operatorname{rng}(f|_c)$).

Za gustoću, uzmimo proizvoljne $(u, v) \in (<)$. Tada je $s := f^{-1}(u) \prec t := f^{-1}(v)$ jer f^{-1} čuva uređaj, pa jer je c gust u a postoji $r \in c$ takav da je $s \prec r \prec t$. Iz toga djelujući s f (koja čuva uređaj) odmah dobijemo da za $w := f(r) \in f[c] = d$ vrijedi $u < w < v$. □

5.7 Uređajne karakterizacije

Lako je vidjeti da je svaka konjunkcija invarijanata sličnosti ponovo invarijanta sličnosti. No neke specijalne konjunkcije su i bolje, u smislu da omogućuju zaključak da dva skupa *jesu* slični (a ne samo da nisu).

Definicija 5.29. Za svojstvo P totalno uređenih skupova kažemo da je *uređajna karakterizacija* ako $P(a)$ i $P(b)$ povlače $a \simeq b$. ◁

Obično se skup a (s nekim standardnim uređajem) fiksira pa se govori o *uređajnoj karakterizaciji skupa a*. Navest ćemo uređajne karakterizacije konačnih skupova i standardnih skupova brojeva. Sve će one biti u obliku konjunkcijā („popisā") invarijanti sličnosti koje uvjetuju sličnost s odgovarajućim standardnim skupom — pa ćemo zapravo uvijek u teoremima imati oba smjera, iako ćemo dokazati samo onaj zanimljiviji.

Propozicija 5.30. *Neka je $(a, \prec)$ totalno uređen skup i $n \in \omega$. Ako je $a \sim n$ tada je $a \simeq n$.*

Dokaz. Indukcijom po n. Baza: $a \sim 0$ znači $a = \emptyset$ (inače ne možemo imati ni funkciju u 0, a kamoli bijekciju). Korak: pretpostavimo da $b \sim n$ povlači $b \simeq n$ (za sve totalno uređene skupove b), i neka je $a \sim n^+$. Zbog induktivnosti ω je $n^+ \in \omega$, pa je a konačan. Označimo s f jednu bijekciju između a i n^+.

Zbog $n^+ \neq 0$ je $a \neq \emptyset$, pa a ima maksimum (dokažite formalni ekvivalent propozicije 2.12). Označimo $m := \max a$ i $b := p_a(m) = a \setminus \{m\}$ — tada je b konačan kao podskup konačnog skupa, označimo $t := \mathfrak{K}(b) \in \omega$. Sada su b i $\{m\}$ disjunktni i unija im je a, pa je $n^+ = \mathfrak{K}(a) = \mathfrak{K}(b) + \mathfrak{K}(\{m\}) = t + 1 = t^+$, te zbog injektivnosti sljedbenika imamo $n = t$. Dakle je $b \sim n$, pa je po pretpostavci indukcije $b \simeq n$; označimo s g jednu sličnost, i definirajmo $h : a \to n^+$ pomoću $h(x) := \begin{cases} g(x), & x \in b \\ n, & x = m \end{cases}$. Tvrdimo da je to sličnost: po lemi 5.24 je dovoljno dokazati surjektivnost i čuvanje strogog uređaja. Prvo slijedi zbog $\operatorname{rng} h = h[b \cup \{m\}] = h[b] \cup \{h(m)\} = g[b] \cup \{n\} = n \cup \{n\} = n^+$.

Za drugo, neka je $x \prec x'$. U svakom slučaju x ne može biti m (jer od njega postoji veći x'), ali x' može, pa imamo dva slučaja. Ako $x' \neq m$, tada je $h(x) = g(x) < g(x') = h(x')$ jer g čuva strogi uređaj. Ako je pak $x' = m$, tada je $h(x) = g(x) \in n = h(m) = h(x')$. □

Teorem 5.31. *Neka je $(a, \prec)$ totalno uređen skup. Ako je a beskonačan, a svaki početni komad mu je konačan, tada je $a \simeq \omega$.*

Dokaz. Konačnost svih početnih komada daje ideju: definiramo $h(x) := \mathfrak{K}\big(p_a(x)\big) \in \omega$, i opet koristimo lemu 5.24 da dokažemo da je to sličnost.

Da h čuva uređaj vidimo ovako: ako je $x \prec x'$ tada je $p_a(x) \subset p_a(x')$ (jer $t \prec x \Rightarrow t \prec x'$ po tranzitivnosti, a $x \in p_a(x') \setminus p_a(x)$). Sad po zadatku 4.21 slijedi $\mathfrak{K}\big(p_a(x)\big) \in \mathfrak{K}\big(p_a(x')\big)$.

Za surjektivnost, neka je $n \in \omega$ proizvoljan. Iz upravo dokazanog (h čuva strogi uređaj) slijedi da je h injekcija, pa je $\operatorname{rng} h \sim a$ beskonačan. Zato je $\operatorname{rng} h \not\subseteq n^+$ (podskup konačnog skupa je konačan), pa postoji $m > n$ takav da je $m = h(u)$ za neki $u \in a$. Po definiciji h je $m \sim p_a(u)$; označimo s f jednu bijekciju između tih skupova. Sada je $h \circ f : m \to m$ injekcija kao kompozicija dvije injekcije (ide u m jer h čuva uređaj: $v \prec u \Rightarrow h(v) \in m$), pa je surjekcija po lemi 4.19. Posebno to znači da je $n \in m = \operatorname{rng}(h \circ f) = h[\operatorname{rng} f] \subseteq \operatorname{rng} h$. □

Teorem 5.32. *Neka je $(a, \prec)$ totalno uređen skup. Ako je a neprazan, nema ni minimum ni maksimum, i svaki segment mu je konačan, tada je $a \simeq \mathbb{Z}$.*

Dokaz. Pretpostavka je da je a neprazan: fiksirajmo jedan njegov element i nazovimo ga z. Kad bi skup $p := a \setminus p_a(z) = \{x \in a : z \preceq x\}$ bio konačan, imao bi maksimum (neprazan je zbog $z \in p$), koji bi onda bio i najveći u čitavom a, što je kontradikcija. Dakle, p je beskonačan, no svaki početni komad mu je konačan, jer je $p_p(x) \subseteq [z, x]_p$ podskup konačnog skupa. Po teoremu 5.31 postoji sličnost f između p i ω.

Lako je vidjeti da totalno uređen skup $\big(p_a(z), \succ\big)$ ima ista svojstva, pa po teoremu 5.31 postoji sličnost g između $\big(p_a(z), \succ\big)$ i $(\omega, <)$, a time i između $\big(p_a(z), \prec\big)$ i $(\omega, >)$.
S $t(x) := -x - 1$ je zadana sličnost između $(\omega, >)$ i $\mathbb{Z}_- := \mathbb{Z} \setminus \mathbb{Z}_{+0}$.

Definiramo $h : a \to \mathbb{Z}$ pomoću $h(x) := \begin{cases} +f(x), & x \in p \\ t\big(g(x)\big), & x \prec z \end{cases}$. Očito je

$$\operatorname{rng} h = \operatorname{rng}((+) \circ f) \cup \operatorname{rng}(t \circ g) = +[\operatorname{rng} f] \cup t[\operatorname{rng} g] = +[\omega] \cup t[\omega] = \mathbb{Z}_{+0} \cup \mathbb{Z}_- = \mathbb{Z} \tag{5.12}$$

jer su sve sličnosti (t, f, g) surjekcije, pa je i h surjekcija. Po lemi 5.24, još samo trebamo dokazati da h čuva strogi uređaj. Neka je $x \prec x'$. Ovisno o tome gdje x i x' „padnu" u odnosu na z, imamo tri slučaja.

Ako je $z \preceq x \prec x'$, tada su x i x' oba iz p, pa tvrdnja slijedi iz činjenice da f (i unarni plus) čuva uređaj. Ako je $x \prec z \preceq x'$, tada je $h(x) \in \mathbb{Z}_-$ a $h(x') \in \mathbb{Z}_{+0}$, pa je $h(x) < 0 \leq h(x')$.
A ako je $x \prec x' \prec z$, tada je $g(x) > g(x')$, pa je $h(x) = t\big(g(x)\big) < t\big(g(x')\big) = h(x')$. □

Važnost upravo dokazanog teorema nije toliko u samom rezultatu, koliko u tehnici dokazivanja: kao što je $\mathbb{Z}$ „proširenje" od ω, sličnost a sa $\mathbb{Z}$ se dobije tako da se nađe podskup $p \subset a$ sličan s ω, i onda se sličnost „proširi" na čitav a. Uskoro ćemo vidjeti važniji primjer upotrebe te tehnike, pri proširenju s $\mathbb{Q}$ na $\mathbb{R}$.

5.8 Karakterizacija uređaja racionalnih brojeva

Teorem 5.33. *Neka je $(A, \prec)$ totalno uređen skup.*
Ako je A prebrojiv, gust i nema ni minimum ni maksimum, tada je $A \simeq \mathbb{Q}$.

Dokaz. Po pretpostavci je $\omega \sim A$: fiksirajmo jednu bijekciju $a : \omega \to A$. Po teoremu 5.12, $\mathbb{Q}$ je prebrojiv: fiksirajmo jednu bijekciju $q : \omega \to \mathbb{Q}$. Nemamo razloga očekivati da $q \circ a^{-1}$ bude sličnost, jer a i q „ne mare" za uređaje na A odnosno $\mathbb{Q}$. No ono što nam a daje je *dobar uređaj* na A (neovisan o $\prec$), u smislu da kad god postoji element iz A s nekim svojstvom P, postoji i *prvi* takav element na popisu $a_0, a_1, a_2, \ldots$ — precizno, $a_{\min\{i \in \omega : P(a_i)\}}$. Sasvim analogno za $\mathbb{Q}$ i q.

Također, bijekcije s ω (tzv. *enumeracije*) omogućavaju primjenu Dedekindovog teorema rekurzije: sličnost $h : A \to \mathbb{Q}$ ćemo konstruirati kao skup uređenih parova $f(n) = \big(d(n), e(n)\big)$, gdje je $n \in \omega$. Precizno, $h := \operatorname{rng} f$, gdje je $f : \omega \to t := A \times \mathbb{Q}$ definirana teoremom 4.23. Za to moramo precizirati $d(n)$ i $e(n)$ pod pretpostavkom da već imamo $d(i)$ i $e(i)$ za sve $i < n$. Pritom moramo osigurati da d bude surjekcija na A, i e surjekcija na $\mathbb{Q}$.

Zapravo je moguće, kako je Cantor to originalno napravio, $d(n)$ uvijek definirati tako da bude prvi još neupotrijebljeni element u A (dakle $d := a$), a $e(n)$ kao prvi još neupotrijebljeni element u enumeraciji q što zadovoljava uvjete koje već treba da bi h čuvala uređaj — ali je tako bitno teže dokazati da je h (odnosno e) surjekcija.

Mi ćemo slijediti moderniju varijantu dokaza, koja *alternira* uloge elemenata od A i racionalnih brojeva: za parne n ćemo napraviti doslovno kako piše u prethodnom odlomku, a za neparne ćemo obrnuto: definirati $e(n)$ kao prvi još neupotrijebljeni racionalni broj, a onda definirati $d(n)$ kao prvi još neupotrijebljeni element od A koji prema prijašnjim elementima $d(i)$ stoji u istom odnosu kao $e(n)$ prema odgovarajućim $e(i), i < n$.

Dakle, neka je n paran, i pretpostavimo da imamo $f(i) = \big(d(i), e(i)\big)$ za sve $i \in n$, tako da $f[n]$ čuva strogi uređaj. Želimo definirati $u =: d(n)$ i $v =: e(n)$ tako da $f[n^+] = f[n] \cup \{(u, v)\}$ i dalje čuva uređaj. [Tehnički, da bismo primijenili teorem 4.23, moramo F definirati i na funkcijama $f : n \to t$ čija slika ne čuva uređaj, ali zapravo je svejedno kako tamo djeluje: radi određenosti recimo da je tada $F(f) := (a_0, q_0)$.]

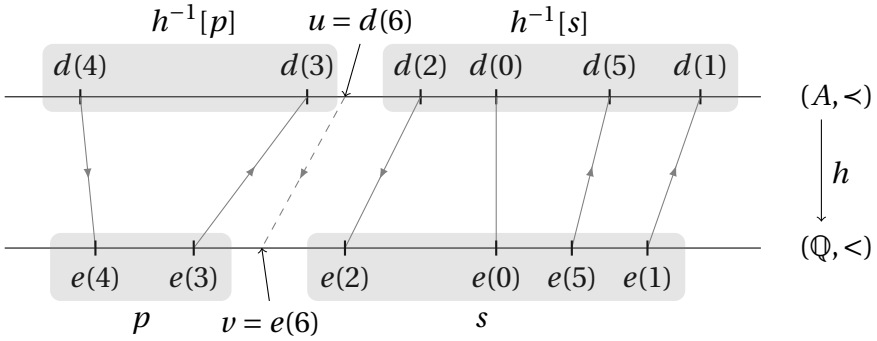
Skup $\operatorname{rng} d \sim n$ je konačan, pa je pravi podskup od A: prvi element u $A \setminus \operatorname{rng} d$ nazovimo $u =: d(n)$. To je bio lakši dio, sada treba definirati $v =: e(n)$. U tu svrhu primijetimo da za sve $i \in n$ treba vrijediti $d(i) \prec u \Rightarrow e(i) < v$ i $d(i) \succ u \Rightarrow e(i) > v$ (ne može biti $d(i) = u$ jer je $u \notin d[n]$). Zato podijelimo $e[n]$ u dva dijela, $p := \{e(i) : d(i) \prec u\}$ i $s := \{e(j) : d(j) \succ u\}$. To su konačni totalno uređeni skupovi, pa je svaki od njih ili prazan, ili ima minimum i maksimum. Dakle, imamo četiri slučaja.

$p = \emptyset = s$ Ovo znači da je $e[n] = \emptyset \cup \emptyset = \emptyset$, što je jedino moguće za $n = 0$, pa nemamo nikakvih uvjeta na v. Definiramo $v := q_0$ (prvi racionalni broj koji zadovoljava „sve" uvjete).

$p = \emptyset \neq s$ Ovo znači da je $e[n] = s$. Označimo s v prvi racionalni broj takav da je $v < \min s$ (takav postoji jer $\mathbb{Q}$ nema minimum). Tada je $v < x$ za sve $x \in s = e[n]$, odnosno $v \notin \operatorname{rng} e$ i svi uvjeti čuvanja uređaja ostaju zadovoljeni.

$p \neq \emptyset = s$ Sasvim analogno, definiramo v kao prvi racionalni broj za koji je $v > \max p$.

$p \neq \emptyset \neq s$ Za sve $e(i) \in p$ i $e(j) \in s$ vrijedi $d(i) \prec u \prec d(j)$, po tranzitivnosti $d(i) \prec d(j)$, pa onda i $e(i) < e(j)$ jer $f[n]$ čuva strogi uređaj. Zato je $\max p < \min s$, pa zbog gustoće skupa $\mathbb{Q}$ postoje racionalni brojevi između njih: označimo s v prvi takav.
Opet, $e(i) \in p$ i $e(j) \in s$ povlače $e(i) < v < e(j)$, pa vrijedi $v \notin p \cup s = e[n]$ i svi uvjeti čuvanja uređaja ostaju zadovoljeni.



Primijetimo da smo od svojstava skupa $\mathbb{Q}$ koristili samo to da nema minimum ni maksimum, i da je gust. Kako A ima ta ista svojstva, možemo za neparne n provesti isti postupak, samo za zamijenjenim ulogama A i $\mathbb{Q}$ (zapravo će biti tri slučaja tada: prvi je nemoguć jer $n = 0$ nije neparan broj). Time smo za bilo koju $f|_n \in t^*$ definirali $F(f|_n) := (u, v) \in t$, i to tako da ako $h|_{d[n]} = f[n]$ čuva strogi uređaj, to čini i $f[n^+] = f[n] \cup \{(u, v)\}$. Kako $f[0] = \emptyset$ trivijalno čuva strogi uređaj, indukcijom slijedi da će ga čuvati sve funkcije $h|_{d[n]} = f[n]$, pa tako i njihova unija h. Iz toga odmah slijedi injektivnost, kao i da h^{-1} čuva uređaj.

Još treba dokazati $\operatorname{dom} h = A$ i $\operatorname{rng} h = \mathbb{Q}$, no to je opet prilično simetrično; pokažimo prvu jednakost. Zapravo želimo pokazati da je $d : \omega \to A$ surjekcija. Indukcijom ćemo dokazati da je $a[n] \subseteq d[2n]$ za sve n; tada tvrdnja slijedi iz činjenice da je a surjekcija. Baza je trivijalna: $\emptyset \subseteq \emptyset$. Ako je $a[n] \subseteq d[2n]$, tada ćemo u $(2n)$. koraku imati već definirane $d(j)$ za $j < 2n$; specijalno, za svaki $i < n$ će biti $a_i \in a[n] \subseteq d[2n]$. Ako je i $a_n \in d[2n]$, tada je $a[n^+] = a[n] \cup \{a_n\} \subseteq d[2n] \cup d[2n] = d[2n] \subset d[(2n)^+]$. Ako nije, tada će u $(2n)$. koraku prvi neupotrijebljeni element skupa A biti upravo a_n, pa će biti $a_n = d(2n) \in d[(2n)^+]$, i opet $a[n^+] \subseteq d[(2n)^+] \subset d[2n+2] = d[2n^+]$. □

5.9 Karakterizacija uređaja realnih brojeva

Teorem 5.34. *Neka je $(A, \prec)$ totalno uređen skup.*
Ako je A separabilan, potpun i nema ni minimum ni maksimum, tada je $A \simeq \mathbb{R}$.

Dokaz. Kao što smo već nagovijestili, koristit ćemo tehniku proširenja već postojeće sličnosti. Zbog separabilnosti, postoji $B \subseteq A$ koji je prebrojiv i gust u A. Tada je očito i gust u sebi (ako između svaka dva elementa iz A postoji element skupa B, tada to specijalno vrijedi za svaka dva elementa iz B). Pretpostavimo da B ima minimum m — tada m ne može biti minimum od A, pa postoji $a \in A$ takav da je $a < m$. No B je gust u A, pa postoji $b \in B$ takav da je $a < b < m$, što je u kontradikciji s $m = \min B$. Dakle, B nema minimum, a sasvim jednako nema ni maksimum. Po teoremu 5.33 postoji sličnost $f : \mathbb{Q} \to B$. Definiramo $F : \mathbb{R} \to A$ s $F(x) := \sup f[x]$ i tvrdimo da je to sličnost.

Prvo se uvjerimo da je definicija dobra, odnosno da $f[x]$ ima supremum. Svaki $x \in \mathbb{R}$ je neprazan skup racionalnih brojeva, pa je $f[x]$ neprazni podskup od $B \subseteq A$. Također je $x \subset \mathbb{Q}$ pa postoji $q \in \mathbb{Q} \setminus x$. Kad bi postojao $u \in x$ takav da je $u > q$, bilo bi i $q \in x$ jer je x zatvoren nadolje, kontradikcija — dakle q je gornja međa za x, odnosno $f(q)$ je gornja međa za $f[x]$. Sada supremum postoji zbog potpunosti skupa A.

Drugo, pokažimo da je $F|_{\mathbb{Q}} = f$ (uz uobičajeno poistovjećivanje q s $p_{\mathbb{Q}}(q)$), odnosno da za svaki $q \in \mathbb{Q}$ vrijedi $s := \sup f[p_{\mathbb{Q}}(q)] = f(q)$. Nejednakost ($\leq$) vrijedi jer je $f(q)$ gornja međa za $f[p_{\mathbb{Q}}(q)]$, što pak vrijedi jer je po definiciji q gornja međa za $p_{\mathbb{Q}}(q)$.
A kad bi bilo $s < f(q)$, tada bi između njih postojao element skupa B; označimo jedan takav s b. Jer f^{-1} čuva uređaj, $b < f(q)$ povlači $f^{-1}(b) \in p_{\mathbb{Q}}(q)$, odnosno $b \in f[p_{\mathbb{Q}}(q)]$, što je kontradikcija s $b > s$.

Treće, dokažimo da F čuva strogi uređaj. Neka su x i y realni brojevi takvi da je $x < y$. Tada postoje $q, r \in \mathbb{Q}$ takvi da je $x < q < r < y$ (zašto?), pa su $f(q), f(r) \in f[y] \setminus f[x]$ jer je f injekcija. Tvrdimo da vrijedi

$$F(x) = \sup f[x] \preceq f(q) \prec f(r) \preceq \sup f[y] = F(y), \tag{5.13}$$

iz čega odmah slijedi $F(x) \prec F(y)$. Druga (stroga) nejednakost u (5.13) slijedi iz $q < r$ jer f čuva uređaj. Treća slijedi jer je $f(r) \in f[y]$. Prva slijedi jer je q gornja međa od x, pa je $f(q)$ gornja međa od $f[x]$.

I četvrto, dokažimo da je F surjekcija. Za $a \in A$, označimo $S := \{b \in B : b \prec a\}$, i tvrdimo da je $x := f^{-1}[S] \subseteq \mathbb{Q}$ realan broj, čija je slika po F jednaka a.

Netrivijalnost: A nema ni minimum ni maksimum, pa u A postoje i manji i veći element od a: $m' \prec a \prec M'$. B je gust u A, pa postoje $m, M \in B$ takvi da je $m' \prec m \prec a \prec M \prec M'$. Sada je $f^{-1}(m) \in x$ i $f^{-1}(M) \notin x$, dakle $\emptyset \neq x \neq \mathbb{Q}$.

Zatvorenost nadolje: $S \subseteq B$ je očito zatvoren nadolje (tranzitivnost), a to svojstvo f^{-1} čuva.

Pretpostavimo da $f^{-1}[S]$ ima maksimum: tada bi ga imao i S (invarijanta sličnosti). No tada između $\max S$ i a ne bi mogao biti nijedan element iz B (pogledajte i sljedeći odlomak), što je kontradikcija s gustoćom B u A.

Sada je $F(x) = \sup f[x] = \sup f\left[f^{-1}[S]\right] = \sup S$, i tvrdimo da je to jednako a. Po definiciji je a gornja međa od S, pa je $\sup S \preceq a$. A kad bi bilo $\sup S \prec a$, između njih bi postojao neki $b \in B$. Tada bi $b \prec a$ značilo $b \in S$, što je kontradikcija s $b \succ \sup S$. □

6 Ordinali

6.1 Motivacija

U ovom poglavlju cilj nam je generalizirati prirodne brojeve na skupove koji mogu poslužiti kao indeksi razina kumulativne hijerarhije. Vidjeli smo da na razinama indeksiranim prirodnim brojevima dobivamo samo konačne skupove, i natuknuli kako bi otprilike išlo dalje: $V_0, V_1, V_2, \ldots, V_\omega, V_{\omega+1}, V_{\omega+2}, \ldots$ — zasad sve te indekse možemo formalizirati (operacijom sljedbenika), ali što nakon njih? Po analogiji, trebalo bi ići $\omega + \omega$, ali kakav je to skup?

Zapravo imamo sličan problem kao kod izgradnje prirodnih brojeva: individualne ordinale koji nas zanimaju uvijek možemo izgraditi „ručno"; problem nastaje kad ih pokušamo karakterizirati općenito. Doslovno isti pristup ne prolazi jer svi ordinali ne čine skup, ali morat ćemo naći neka svojstva skupova koja karakteriziraju ordinale, a ne „napikavati" ih jedan po jedan.

Kod prirodnih brojeva osnovni su bili nula i sljedbenik. Ovdje znamo da nam to nije dovoljno: granični ordinal moramo shvatiti kao *skup svih manjih* ordinala. Jednom kad osvijestimo tu intuiciju, možemo je primijeniti na *sve* ordinale, čak i one konačne: doista, nula je također skup svih manjih od nje (dakle prazan skup, jer takvih nema), a sljedbenik od n je skup svih manjih od n i još n, dakle upravo skup svih manjih od n^+.

Ta osnovna intuicija: ordinal α je skup svih β takvih da je $\beta < \alpha$ (općenite ordinale označavamo grčkim slovima s početka alfabeta), može se iz druge perspektive reći „$\beta \in \alpha$ ako i samo ako je $\beta < \alpha$", pa nam (slično kao kod kombinatorike prebrajanja) to može poslužiti kao *definicija* uređaja: ordinali su **skupovi uređeni relacijom** $\in$. Za prirodne brojeve to je bio dobar uređaj, no kako je dobra utemeljenost aksiom, dovoljno je bilo dokazati totalnost. Za prirodne brojeve to je išlo indukcijom; ovdje će totalnost biti ugrađena u definiciju.

6.2 Svojstva dobro uređenih skupova

Kao pripremu dokažimo neka korisna svojstva dobro uređenih skupova.

Lema 6.1. *Ako je $(a, \prec)$ dobro uređen skup i $f : a \to a$ funkcija koja čuva strogi uređaj, tada za svaki $x \in a$ vrijedi $f(x) \succeq x$.*

U dokazu ove leme uvodimo tehniku *najmanjeg protuprimjera*, koju ćemo često koristiti. Ako želimo dokazati da neko svojstvo imaju svi elementi dobro uređenog skupa, pretpostavka suprotnog znači da postoji *najmanji* element bez tog svojstva.

Dokaz. Kad tako ne bi bilo, skup $p := \{x \in a : f(x) \prec x\}$ bi bio neprazni podskup od a, pa bi imao najmanji element $m := \min p$. Svakako je $m \in p$, pa je $f(m) \prec m$, i zbog toga $f(m) \notin p$ (jer je $m = \min p$). S druge strane, f čuva uređaj, što znači da iz $f(m) \prec m$ slijedi $f\big(f(m)\big) \prec f(m)$, pa po definiciji skupa p imamo $f(m) \in p$, kontradikcija. □

Primijetite sličnost upravo provedenog dokaza s dokazom Knaster–Tarskijevog teorema.

Propozicija 6.2. *1. Neka je $(a, \prec)$ dobro uređen skup, $t \in a$ i funkcija $f : a \to p_a(t)$. Tada f ne može čuvati strogi uređaj.*

2. Dobro uređen skup ne može biti sličan podskupu svog početnog komada.

3. Različitim elementima dobro uređenog skupa odgovaraju neslični početni komadi.

4. Između dva dobro uređena skupa postoji najviše jedna sličnost.

5. Identiteta je jedina sličnost dobro uređenog skupa sa samim sobom.

Dokaz. [1]: Po lemi 6.1, kad bi f čuvala strogi uređaj, bilo bi $f(t) \succeq t$, što bi značilo da f ne ide u $p_a(t)$.

[2]: Svaka sličnost između dobro uređenog skupa a i (podskupa) njegova početnog komada $p_a(t)$ bila bi funkcija s a u $p_a(t)$ koja čuva strogi uređaj — kakva ne postoji po (1).

[3]: Ako su $x, y \in a$ različiti, bez smanjenja općenitosti je $x \prec y$. Tada je $p_a(x) = p_{p_a(y)}(x)$ (raspišite!), pa bi $p_a(x) \simeq p_a(y)$ bilo u kontradikciji s (2).

[4]: Pretpostavimo da su $(a, \prec)$ i $(b, \lhd)$ dobro uređeni te f i g sličnosti između njih. Tada prema propoziciji 3.28 za svaki $x \in a$ vrijedi $p_a(x) \simeq p_b\big(f(x)\big)$ i $p_a(x) \simeq p_b\big(g(x)\big)$, pa je $p_b\big(f(x)\big) \simeq p_b\big(g(x)\big)$, iz čega po (3) slijedi $f(x) = g(x)$. Zbog proizvoljnosti x je $f = g$.

[5]: Očito je id_a sličnost između a i a, a jedinstvena je po (4). □

Teorem 6.3. *Za svaki totalno uređen skup $(a, \prec)$ vrijedi: a je dobro uređen skup ako i samo ako za svaki $b \subseteq a$, svojstvo $(\forall x \in a)\big(p_a(x) \subseteq b \to x \in b\big)$ povlači $b = a$.*

Dokaz. [⇒] Neka je a dobro uređen, i pretpostavimo suprotno da postoji $b \subset a$ takav da $p_a(x) \subseteq b$ povlači $x \in b$. Označimo $t := \min(a \setminus b)$ (*najmanji protuprimjer* — postoji jer je $a \setminus b \neq \emptyset$). Tada za svaki $y \in p_a(t)$ vrijedi $y \in a$ i $y \notin a \setminus b$, pa je $y \in b$. Dakle je $p_a(t) \subseteq b$, što po pretpostavci povlači $t \in b$, a to je kontradikcija s $t \in a \setminus b$.

[⇐]: Pretpostavimo da $(\forall x \in a)\big(p_a(x) \subseteq b \to x \in b\big)$ povlači $b = a$, i neka $c \subseteq a$ nema najmanji element. Označimo s $b := \{d \in a : (\forall y \in c)(d \prec y)\}$ skup svih strogih donjih međa skupa c (zbog irefleksivnosti su b i c disjunktni), i tvrdimo da $p_a(x) \subseteq b$ povlači $x \in b$. Kontrapozicijom, kada x ne bi bio u b, postojao bi $z \in c$ takav da je $z \preceq x$. No z nije najmanji u c, pa postoji $w \in c$ takav da je $w \prec z \preceq x$, odnosno $w \in p_a(x)$. Zbog disjunktnosti b i c je $w \notin b$, pa smo dobili $p_a(x) \not\subseteq b$.

Po pretpostavci bi moralo biti $b = a$, što (opet zbog disjunktnosti) povlači $c = \emptyset$. Dokazali smo da je svaki podskup od a bez najmanjeg elementa prazan, odnosno (kontrapozicijom) da je a dobro uređen skup. □

Teorem 6.4. *Za sve dobro uređene skupove a i b vrijedi točno jedno od sljedećeg:*

- *a i b su slični,*
- *a je sličan nekom (jedinstvenom) početnom komadu od b, ili*
- *b je sličan nekom (jedinstvenom) početnom komadu od a.*

Dokaz. Definirajmo relaciju $S \subseteq a \times b$ kao $x \mathrel{S} y :\Leftrightarrow p_a(x) \simeq p_b(y)$. S ima funkcijsko svojstvo prema propoziciji 6.2(3), i čuva uređaj zbog propozicije 3.28 (raspišite!). Zbog simetrije isto vrijedi za S^{-1}. Dakle, S je sličnost između $c := \operatorname{dom} S \subseteq a$ i $d := \operatorname{rng} S \subseteq b$. Prema tome jesu li inkluzije prave, imamo četiri slučaja.

$c = a \wedge d = b$ Tada je $a = c \simeq d = b$, što odgovara prvoj tvrdnji u teoremu.

$c \subset a \wedge d = b$ Označimo $u := \min(a \setminus c)$ i tvrdimo $c = p_a(u)$ (to odgovara trećoj tvrdnji u teoremu). Inkluzija ($\supseteq$) je očita: $x \lhd u$ znači $x \notin a \setminus c$, dakle $x \in c$. Za inkluziju ($\subseteq$), neka je $x \in c$; želimo $x \lhd u$. Suprotno bi značilo $u \in p_a(x)$ (uređaj je totalan, a $x = u$ je nemoguće jer su u disjunktnim skupovima). No $x \in c$ znači da postoji $y \in b$ takav da je $x \mathrel{S} y$, odnosno $p_a(x) \simeq p_b(y)$ — označimo s f (jedinstvenu) sličnost između njih. Sada prema propoziciji 3.28 imamo $p_a(u) \simeq p_b\big(f(u)\big)$, odnosno $u \mathrel{S} f(u)$, što je u kontradikciji s $u \notin c$. Dakle, $p_a(u) = c \simeq b$. Jedinstvenost u slijedi iz propozicije 6.2(3).

$c = a \wedge d \subset b$ Sasvim analogno, ovo odgovara drugoj tvrdnji u teoremu.

$c \subset a \wedge d \subset b$ Ovaj slučaj je zapravo nemoguć: označimo $u := \min(a \setminus c)$ i $v := \min(b \setminus d)$. Prema prethodna dva slučaja, vrijedi $c = p_a(u)$ i $d = p_b(v)$. Sada je S sličnost između ta dva skupa, pa bi ispalo $u \mathrel{S} v$, odnosno $u \in c \wedge v \in d$, kontradikcija.

Dakle, sigurno vrijedi jedna od tri navedene tvrdnje. Još treba vidjeti da ne može vrijediti više njih istodobno. Prva i treća ne mogu vrijediti jer bi $a \simeq b \simeq p_a(u)$ bilo u kontradikciji s propozicijom 6.2(2). Analogno ne mogu vrijediti prva i druga. Druga i treća tvrdnja ne mogu istovremeno vrijediti jer bi $a \simeq p_b(v)$ i $b \simeq p_a(u)$ prema propoziciji 3.28 povlačilo (označimo li s f sličnost između a i $p_b(v)$) $b \simeq p_a(u) \simeq p_{p_b(v)}\big(f(u)\big) = p_b\big(f(u)\big)$, što je opet u kontradikciji s propozicijom 6.2(2). □

6.3 Tranzitivni skupovi

Definicija 6.5. Za skup a kažemo da je *tranzitivan* ako $x \in y \in a$ povlači $x \in a$.
Kažemo da je *a ordinal* ako je a tranzitivan i svi elementi su mu usporedivi relacijom $\in$. ◁

Tranzitivnost možemo shvatiti kao implikaciju $y \in a \Rightarrow y \subset a$ (raspišite!).

Lema 6.6. *Svaki ordinal je dobro uređen (relacijom $\in$).*

Dokaz. Moramo dokazati da je $\in$ irefleksivna, tranzitivna (tada će zbog usporedivosti biti totalni uređaj) i dobro utemeljena (dobra uređenost tada će slijediti po teoremu 2.11). Treće i prvo svojstvo su direktne posljedice aksioma dobre utemeljenosti, odnosno leme 4.2. Drugo svojstvo također, iako je malo kompliciranije.

Neka su $x, y, z \in \alpha$, gdje je α ordinal, takvi da je $x \in y \in z$. Zbog usporedivosti je $x \in z$ ili $x = z$ ili $z \in x$, no drugi slučaj bi vodio na $x \in y \in x$, a treći na $x \in y \in z \in x$, što je (oboje) nemoguće po lemi 4.2. Dakle, mora biti $x \in z$. □

Intuicija „ordinal je skup svih manjih ordinala" formalizira se i preko početnih komada.

Lema 6.7. *Neka je α ordinal i $b \in \alpha$. Tada je b ordinal, i $p_\alpha(b) = b$ (skraćeno, $p_\alpha = id_\alpha$).*

Dokaz. Neka je $x \in y \in b$. Tada (zbog tranzitivnosti α) iz $y \in b \in \alpha$ slijedi $y \in \alpha$, pa opet iz $x \in y \in \alpha$ slijedi $x \in \alpha$. No relacija $\in$ je tranzitivna na α (ne brkati tranzitivnost skupa s tranzitivnošću uređaja na njemu!) po prethodnoj lemi pa (sad kada znamo da su x, y i b elementi od α) $x \in y \in b$ povlači $x \in b$. Dakle, b je tranzitivan. Također, tranzitivnost od α daje $b \subset \alpha$, pa su svi elementi od b ujedno elementi od α, i kao takvi usporedivi relacijom $\in$. Dakle, b je ordinal.

Sada $x \in p_\alpha(b)$ znači $x \in \alpha$ i $x \in b$, drugim riječima $x \in \alpha \cap b$, što je jednako b zbog $b \subset \alpha$. Dakle, jednakost $p_\alpha(b) = b$ vrijedi po aksiomu ekstenzionalnosti. □

Po upravo dokazanom, svi elementi ordinala su ordinali,
pa ćemo ih ubuduće implicitno uvijek označavati grčkim slovima.

Lema 6.8. *Neka su α i β ordinali, $f : \alpha \to \beta$ sličnost, i $\gamma \in \alpha$. Tada je $f[\gamma] = f(\gamma)$.*

Dokaz. Direktno korištenjem leme 6.7, propozicije 3.28 i ponovo leme 6.7:

$$f[\gamma] = f[p_\alpha(\gamma)] = \operatorname{rng}\big(f|_{p_\alpha(\gamma)}\big) = p_\beta\big(f(\gamma)\big) = f(\gamma). \quad \square \tag{6.1}$$

Propozicija 6.9. *Ako su α i β ordinali, tada $\alpha \simeq \beta$ povlači $\alpha = \beta$.*

Dokaz. Neka je $f : \alpha \to \beta$ sličnost; tehnikom najmanjeg protuprimjera pokazujemo da je $f = id_\alpha$. Kad ne bi tako bilo, postojao bi najmanji $\gamma \in \alpha$ takav da je $f(\gamma) \neq \gamma$. No tada su svi elementi od γ fiksne točke od f, pa imamo

$$f(\gamma) = f[\gamma] = \{f(\vartheta) : \vartheta \in \gamma\} = \{\vartheta : \vartheta \in \gamma\} = \gamma, \tag{6.2}$$

kontradikcija. Sada je zbog surjektivnosti $\beta = \operatorname{rng} f = \operatorname{rng} id_\alpha = \alpha$. □

Primijetite da propoziciju 6.9 ne bismo mogli dokazati (na ovaj način) kada bismo kodomenu smatrali sastavnim dijelom funkcije — jer bismo za jednakost funkcijā $f = id_\alpha$ prvo trebali vidjeti da im se kodomene podudaraju, a je to upravo tvrdnja koju pokušavamo dokazati!
U „pravoj" teoriji skupova nema tih problema: i f i id_α su jednostavno neki skupovi uređenih parova, i želimo vidjeti da su jednaki.

6.4 Teorem enumeracije

Propozicija 6.10. *Za svaka dva ordinala α i β vrijedi točno jedno od: $\alpha \in \beta$, $\alpha = \beta$ ili $\beta \in \alpha$.*

Dokaz. Prema lemi 6.6, $(\alpha, \in)$ i $(\beta, \in)$ su dobro uređeni skupovi,
pa prema teoremu 6.4 vrijedi jedna od sljedeće tri mogućnosti:

[$\alpha \simeq \beta$] Tada je po propoziciji 6.9 $\alpha = \beta$.

[$\alpha \simeq p_\beta(\delta)$ za neki $\delta \in \beta$] Tada je po propoziciji 6.9 i lemi 6.7 $\alpha = p_\beta(\delta) = \delta \in \beta$.

[$\beta \simeq p_\alpha(\gamma)$ za neki $\gamma \in \alpha$] Sasvim analogno, tada je $\beta \in \alpha$.

Da ne može vrijediti više od jedne tvrdnje u propoziciji, slijedi direktno iz leme 4.2. □

Korolar 6.11. *Svaki tranzitivni skup ordinala je ordinal.*

Teorem 6.12. *Klasa* **On** *svih ordinala je prava klasa, dobro uređena klasnom relacijom* $\in$.

Dokaz. Za početak, primijetimo da imamo formulu

$$v := (\forall x \in \alpha)(\forall y \in x)(y \in \alpha) \wedge (\forall x \in \alpha)(\forall y \in \alpha)(x \in y \vee x = y \vee y \in x) \tag{6.3}$$

s jednom slobodnom varijablom α, koja kazuje da je α ordinal. Dakle, $\mathbf{On} := \{\alpha : v\}$ jest klasa. Pretpostavimo da je skup. Tada bi taj skup bio tranzitivan po lemi 6.7 ($b \in \alpha \in \mathbf{On}$ povlači $b \in \mathbf{On}$) pa bi bio ordinal prema korolaru 6.11 — odnosno vrijedilo bi $\mathbf{On} \in \mathbf{On}$, što je nemoguće prema lemi 4.2(1). [Ovaj paradoks je prvi opazio Cesare Burali-Forti.]

Irefleksivnost relacije $\in$ na **On** je očita posljedica leme 4.2(1). Za tranzitivnost, neka je $\alpha \in \beta \in \gamma \in \mathbf{On}$. Tada je po propoziciji 6.10 ili $\alpha \in \gamma$ ili $\alpha = \gamma$ ili $\gamma \in \alpha$, no drugi i treći slučaj su nemogući baš kao u dokazu leme 6.6. Dakle, $\in$ je klasni parcijalni uređaj na **On**. Totalnost slijedi iz propozicije 6.10; još treba vidjeti dobru utemeljenost.

[Pazite! Ovdje se ne možemo samo pozvati na aksiom dobre utemeljenosti, jer on tvrdi da svaki neprazni *skup* ima $\in$-minimalni element. Mi želimo dokazati više: da svaka neprazna pot*klasa* od **On** ima takav element. Trebamo biti svjesni razlike tih dviju tvrdnji.]

Neka je **A** neprazna klasa ordinalā, zadana formulom ψ s jednom slobodnom varijablom x. Nepraznost znači $\exists x \psi$, pa fiksirajmo jedan element za koji vrijedi ψ i označimo ga s α. [Slova s kraja grčkog alfabeta označavaju formule, a slova s početka ordinale.]
Promotrimo $t := \{x \in \alpha : \psi\}$ — to je skup po aksiomu separacije. Ako je t prazan, po definiciji je $\alpha = \min \mathbf{A}$ pa smo gotovi. Inače je $t \neq \emptyset$, pa po aksiomu dobre utemeljenosti postoji $\beta \in t$ takav da je $\beta \cap t = \emptyset$. (Zbog $t \subseteq \alpha$ je $\beta \in \alpha$, pa smo ga označili grčkim slovom.) Tvrdimo da je $\beta = \min \mathbf{A}$ (s obzirom na relaciju $\in$).

Pretpostavimo suprotno, da postoji $\gamma \in \mathbf{A}$ takav da je $\gamma \in \beta$. Iz $\gamma \in \mathbf{A}$ slijedi da γ zadovoljava ψ (uvršten umjesto x), a iz $\gamma \in \beta \in \alpha$ slijedi $\gamma \in \alpha$, pa je $\gamma \in t$. No to je u kontradikciji s disjunktnošću β i t (našli smo im γ u presjeku). □

Upravo dokazani teorem opravdava definiciju: za ordinale α i β, pišemo $\alpha < \beta$ za $\alpha \in \beta$. Svaki ordinal, kao i klasu svih ordinala **On**, standardno smatramo uređenim relacijom $\in$. Važni teorem *enumeracije* je analogon teorema 3.29: baš kao što se svaki parcijalni uređaj može shvatiti kao $\subset$, svaki se dobar uređaj može shvatiti kao $\in$.

Zadatak 6.13. *Za dobro uređen skup $(a, \prec)$ uredimo sljedbenik a^+ relacijom $(\prec) \cup a \times \{a\}$. Dokažite da je to dobro uređen skup, i da je $p_{a^+}(a) = a$, te je $p_{a^+}(x) = p_a(x)$ za sve $x \in a$.*

Teorem 6.14. *Za svaki dobro uređen skup a postoji jedinstveni ordinal α takav da je $a \simeq \alpha$.*

Dokaz. Prvo, dovoljno je dokazati egzistenciju; jedinstvenost lako slijedi iz propozicije 6.9.

Neka je $(a, \prec)$ dobro uređen skup. Prema zadatku 6.13, a^+ je također dobro uređen. Do kraja ovog dokaza podrazumijevamo da su svi početni komadi u a^+, što radi preglednosti ne pišemo: umjesto $p_{a^+}(x)$ pišemo samo $p(x)$. Označimo $b := \{x \in a^+ : p(x) \text{ je sličan ordinalu}\}$. Dovoljno je dokazati $p(t) \subseteq b \Rightarrow t \in b$: tada prema teoremu 6.3 slijedi $b = a^+$, pa je $a \in b$ i zato je $p(a) = a$ sličan ordinalu.

Pa neka je $p(t)$ podskup od b: to znači da za svaki $x \in p(t)$ postoji ordinal η takav da je $p(x) \simeq \eta$. Opet po propoziciji 6.9, taj η je jedinstven — doista, $p(x) \simeq \eta \wedge p(x) \simeq \eta'$ povlači $\eta \simeq \eta'$ i zato $\eta = \eta'$ po propoziciji 6.9. To znači da za formulu $\varphi := \big(y \in \mathbf{On} \wedge p(x) \simeq y\big)$ vrijedi $\big(\forall x \in p(t)\big)\exists! y\, \varphi$, pa po aksiomu zamjene postoji skup s u kojem se nalaze svi takvi η, a onda (standardno, separacijom iz $p(t) \times s$) i funkcija $f : p(t) \to s$ koja svakom $x \in p(t)$ pridružuje odgovarajući η. Tvrdimo da je $\bullet s$ ordinal i $\bullet f$ sličnost, iz čega će slijediti $t \in b$.

Za prvu tvrdnju, po definiciji je s skup ordinala, pa je po korolaru 6.11 dovoljno dokazati da je tranzitivan. Neka je $\beta \in \eta \in s$: to znači da postoji $x \in p(t)$ takav da je $p(x) \simeq \eta = f(x)$. Ako s $g : \eta \to p(x)$ označimo (jedinstvenu) sličnost između njih, po propoziciji 3.28 je $p_\eta(\beta) \simeq p_{p(x)}\big(g(\beta)\big)$, odnosno po lemi 6.7, $\beta \simeq p\big(g(\beta)\big)$, pa je i $\beta \in s$.

Za drugu tvrdnju, po definiciji je $s = \operatorname{rng} f$, pa je po lemi 5.24 dovoljno dokazati da f čuva strogi uređaj. Neka je $u \prec v$ (u uređaju proširenom na skup a^+). Tada je ili $f(u) \in f(v)$ ili $f(u) = f(v)$ ili $f(v) \in f(u)$ po propoziciji 6.10. Drugi slučaj je nemoguć jer bismo imali $p_{p(v)}\big(p(u)\big) = p(u) \simeq f(u) = f(v) \simeq p(v)$, što bi bilo u kontradikciji s propozicijom 6.2(2). U trećem slučaju, ako s h označimo jednu sličnost između $f(u)$ i $p(u)$, prema propoziciji 3.28 imali bismo $p_{f(u)}\big(f(v)\big) \simeq p_{p(u)}\big(h(f(v))\big)$, odnosno $p(v) \simeq f(v) \simeq p\big(h(f(v))\big)$ po lemi 6.7. Zbog propozicije 6.2(3), moralo bi biti $v = h\big(f(v)\big) \in \operatorname{rng} h = p(u)$, kontradikcija. Dakle, doista mora vrijediti $f(u) \in f(v)$.

U prethodna dva odlomka dokazali smo $p(t) \simeq s \in \mathbf{On}$, dakle $t \in b$. Kako je već opisano, iz toga slijedi $b = a^+ \ni a$, odnosno a je sličan ordinalu — što smo htjeli. □

6.5 Transfinitna indukcija

Korolar 6.15. *Sljedbenik ordinala je ordinal. Unija bilo kojeg skupa ordinala je ordinal.*

Dokaz. To su jednostavne posljedice definicije ordinala, korolara 6.11 i leme 6.7. Zbog njih je dovoljno dokazati sljedeće dvije tvrdnje.

[sljedbenik tranzitivnog skupa je tranzitivan]: Neka je a tranzitivan i $x \in y \in a^+$. Tada je $y \in a$ (pa je $x \in a$ zbog tranzitivnosti skupa a), ili je $y = a$ (pa je $x \in a$ zbog $x \in y$). U svakom slučaju je $x \in a \subset a^+$.

[unija bilo kojeg skupa tranzitivnih skupova je tranzitivni skup]: Neka je s skup tranzitivnih skupova i $x \in y \in \bigcup s$. Tada po aksiomu unije postoji $z \in s$ takav da je $x \in y \in z$. No z je tranzitivan kao element od s, pa $x \in y \in z$ povlači $x \in z$. Sada $x \in z \in s$ znači da je $x \in \bigcup s$. □

Za ordinale smo definirali uređaj kao relaciju $\in$, ali zbog tranzitivnosti ordinala to je ekvivalentno s relacijom $\subset$. To zapravo znači da je klasa **On** dobro uređena relacijom $\subset$, pa su supremum i infimum zadani upravo kao unija i presjek familije ordinala. Štoviše, infimum (koji mora biti minimum, zbog teorema 6.12) se može definirati za bilo koju nepraznu **klasu** ordinala — dok se supremum mora definirati za *skup* (koji može biti i prazan) ordinala.

$$\sup s = \bigcup s \ = \{x : (\exists\, t \in s)(x \in t)\}, \text{ za svaki skup } s \subset \mathbf{On} \tag{6.4}$$

$$\min \mathbf{s} = \inf \mathbf{s} = \bigcap \mathbf{s} := \{x : (\forall\, t \in \mathbf{s})(x \in t)\}, \text{ za svaku klasu } \emptyset \subset \mathbf{s} \subseteq \mathbf{On} \tag{6.5}$$

Definicija 6.16. Za ordinal α kažemo da je *sljedbenik* ako postoji d takav da je $\alpha = d^+$. Ordinal je *granični* ako nije ni 0 ni sljedbenik. ◁

Zadatak 6.17. *Dokažite: ordinal je granični ako i samo ako je induktivan.*

Lema 6.18. 1. *Ordinal α je granični ili 0 ako i samo ako je $\alpha = \sup \alpha$.*

2. *Ordinal α je sljedbenik ako i samo ako je $\alpha = (\sup \alpha)^+$.*

Dokaz. Kako sljedbenik nema fiksnu točku (propozicija 4.3), nikada nije $\sup \alpha = (\sup \alpha)^+$, pa je dovoljno dokazati smjerove ($\Rightarrow$) obiju tvrdnji (obrazložite!).

Za prvu tvrdnju, ako je α granični ili 0, nije sljedbenik (za granične po definiciji, a za 0 po propoziciji 4.3). Očito je α gornja međa od α po relaciji $\in$, treba još vidjeti da je najmanja (odnosno minimalna, zbog propozicije 2.8). Uzmimo proizvoljni $\beta \in \alpha$. Po propoziciji 6.10 je $\beta^+ \in \alpha$ ili $\beta^+ = \alpha$ ili $\alpha \in \beta$ ili $\alpha = \beta$. No treći i četvrti slučaj ($\alpha \in \beta^+$) nisu mogući zbog leme 4.2(2), a drugi nije moguć jer α nije sljedbenik. To znači da je $\beta^+ \in \alpha$, pa β ne može nikako biti gornja međa od α: postoji element u α strogo veći od β (konkretno, β^+).

Za drugu tvrdnju, ako je $\alpha = d^+$ za neki d, tada je d ordinal zbog $d \in d^+ = \alpha$, pa ga označimo s δ. To je gornja međa od α: za svaki $\vartheta \in \alpha = \delta^+$ je $\vartheta \leq \delta$. Označimo $\gamma := \sup \alpha$ i $\beta := \gamma^+$ (to su ordinali po korolaru 6.15). Po propoziciji 6.10 je ili $\beta \in \alpha$ ili $\alpha = \beta$ ili $\alpha \in \beta$: ovo zadnje opet znači $\alpha \in \gamma$ ili $\alpha = \gamma$. Prvo je nemoguće kao u prethodnom odlomku: $\gamma \in \gamma^+ \in \alpha$ znači da γ ne može biti supremum od α. Treće je nemoguće jer bi značilo da α nije gornja međa za α. Četvrto bi značilo $\alpha = \delta^+ = \gamma = \sup \alpha$, što je nemoguće jer je δ gornja međa od α manja od δ^+. Preostaje druga mogućnost, odnosno $\alpha = \beta = \gamma^+ = (\sup \alpha)^+$. □

Zadatak 6.19. *Dokažite: za svaki ordinal α vrijedi $\alpha = \sup\{\beta^+ : \beta \in \alpha\}$.*

Tehnikom najmanjeg protuprimjera dokazali smo teorem 6.3[⇒], no u njemu zapravo nije bilo važno da je a skup. Važno je bilo da postoji najmanji protuprimjer, a on postoji i u dobro uređenim klasama poput klase **On**.

Lema 6.20 (Stroga transfinitna indukcija)**.** *Neka je* $\mathbf{B} \subseteq \mathbf{On}$ *proizvoljna klasa ordinala takva da* $\alpha \subseteq \mathbf{B}$ *povlači* $\alpha \in \mathbf{B}$ *(za sve ordinale* α*). Tada je* $\mathbf{B} = \mathbf{On}$.

Dokaz. Pretpostavimo suprotno, da **B** ne sadrži sve ordinale. Tada po teoremu 6.12 postoji najmanji ordinal koji nije u **B**: označimo ga s α. Tada su svi $\beta \in \alpha$ u **B** (jer je α najmanji koji nije), pa vrijedi $\alpha \subseteq \mathbf{B}$. No to prema pretpostavci povlači $\alpha \in \mathbf{B}$, kontradikcija. □

Upravo dokazana lema podsjeća na princip jake indukcije za prirodne brojeve (ako je $b \subseteq \omega$ takav da $n \subseteq b \Rightarrow n \in b$ za sve prirodne brojeve n, tada je $b = \omega$). Najčešći oblik indukcije kojom dokazujemo tvrdnje o ordinalima je *transfinitna indukcija*, koja izgleda kao obična indukcija za nulu i sljedbenike, a kao jaka indukcija za granične ordinale.

Teorem 6.21 (Transfinitna indukcija)**.** *Neka je* $\mathbf{B} \subseteq \mathbf{On}$. *Ako* **B** *ima sljedeća tri svojstva:*

- $0 \in \mathbf{B}$,
- $\alpha \in \mathbf{B} \Rightarrow \alpha^+ \in \mathbf{B}$ *za sve ordinale* α*, te*
- $\lambda \subseteq \mathbf{B} \Rightarrow \lambda \in \mathbf{B}$ *za sve granične ordinale* λ*,*

tada je $\mathbf{B} = \mathbf{On}$.

Dokaz. Kao i prije, pretpostavimo suprotno i neka je β najmanji kontraprimjer (po teoremu 6.12): dakle vrijedi $\beta \subseteq \mathbf{B} \wedge \beta \notin \mathbf{B}$. Tada β ne može biti 0 zbog prvog svojstva, i ne može biti granični zbog trećeg svojstva. Preostaje mogućnost da je β sljedbenik, recimo $\beta = \alpha^+$. No tada je $\alpha \in \alpha^+ = \beta \subseteq \mathbf{B}$, pa bi po drugom svojstvu bilo $\alpha^+ = \beta \in \mathbf{B}$, kontradikcija. □

6.6 Opći teorem rekurzije

Vidimo da se mnogi rezultati za prirodne brojeve jednostavno generaliziraju na ordinale; praktički jedine razlike su postojanje graničnih ordinala (fenomen koji nemamo u prirodnim brojevima) i Burali-Fortijev paradoks: svi ordinali ne čine skup. Zato je neke rezultate teže dokazati (jer se moramo baviti klasama i formulama umjesto skupovima), ali intuitivni osjećaj zašto vrijede za prirodne brojeve prenosi se i na ordinale. Važni primjer je Dedekindov teorem rekurzije, koji kaže da funkcije s domenom ω (*nizove*) možemo definirati rekurzivno, definirajući $g(n)$ pomoću $g|_n$. Sada ćemo vidjeti da i klasne funkcije s domenom **On** (*klasne hipernizove*) možemo definirati na isti način. Označimo klasu svih hipernizova s $\mathbf{H} := \{f : (\exists \alpha \in \mathbf{On})(f : \alpha \to \mathbf{V})\}$.

Teorem 6.22 (Opći teorem rekurzije)**.** *Neka je* $\mathbf{F} : \mathbf{H} \to \mathbf{V}$ *klasna funkcija.*
Za hiperniz f *kažemo da je* **F**-rekurzivan *ako* $\beta\ f\ y$ *povlači* $f|_\beta\ \mathbf{F}\ y$.
Tada postoji jedinstveni **F***-rekurzivni klasni hiperniz* $\mathbf{g} : \mathbf{On} \to \mathbf{V}$.

Dokaz (Skica). Kao što rekosmo, pratimo dokaz Dedekindovog teorema rekurzije, uzimajući u obzir da na mnogim mjestima sada ne govorimo o skupovima, već o klasama, odnosno o formulama koje ih karakteriziraju.
Konkretno, neka je $\mathbf{F} = \{y : \phi\}$ zadana formulom ϕ sa slobodnom varijablom y.

Neke stvari su i lakše: ne moramo fiksirati skup t, jer možemo jednostavno za kodomenu naših klasnih funkcija uzeti $\mathbf{V}$. Također, ne moramo dokazivati da je $\mathbf{H}$ (analogon skupa t^*) skup, jer nije niti mora biti. Sve što trebamo je vidjeti da je ta klasa zadana formulom

$$\chi := \exists\alpha\big(v \wedge (\forall p \in f)(\exists\beta \in \alpha)\exists z\big(p = (\beta, z)\big) \wedge (\forall\beta \in \alpha)\,\exists! z\,(\beta\ f\ z)\big) \tag{6.6}$$

sa slobodnom varijablom f. Dakle, odmah definiramo $\mathbf{G} := \{f \in \mathbf{H} : f \text{ je } \mathbf{F}\text{-rekurzivan}\}$ — što zapravo znači da je $\mathbf{G}$ zadana formulom $(\chi \wedge \rho)$, gdje formula

$$\rho := (\forall p \in f)\forall\beta\forall z\big(p = (\beta, z) \to \exists y\big(y = (f|_\beta, z) \wedge \phi\big)\big) \tag{6.7}$$

kazuje da je hiperniz f $\mathbf{F}$-rekurzivan. Sada $\mathbf{g} := \bigcup\mathbf{G}$ zadamo formulom $\gamma := \exists f\,(\chi \wedge \rho \wedge y \in f)$ sa slobodnom varijablom y, i tvrdimo da ima sva tražena svojstva, i da je jedinstvena takva. Dokazi su sasvim analogni onima iz Dedekindovog teorema rekurzije, dok god imamo na umu da zapravo govorimo o formulama.

Recimo, prvo moramo dokazati $\mathbf{g} \subseteq \mathbf{On} \times \mathbf{V}$, što zapravo znači $\forall y\big(\gamma \to \exists\alpha\exists z\big(v \wedge y = (\alpha, z)\big)\big)$, i dokaz je praktički isti: iz γ slijedi da je y element nekog f koji zadovoljava χ, pa je oblika (β, z) gdje je β ordinal. Ostatak ide analogno, samo je izuzetno komplicirano držati sve detalje pod kontrolom. Umjesto jake indukcije ovdje koristimo lemu 6.20, koja predstavlja analogon jake indukcije za ordinale.

Na jednom mjestu moramo biti naročito oprezni: kod dokazivanja da $\mathbf{g}$ zadovoljava ρ (uvršten umjesto f), moramo paziti da $\mathbf{g}|_\beta$ ne tretiramo kao klasu (jer je inače uređen par $(\mathbf{g}|_\beta, z)$ sintaksna greška, kako smo opisali na kraju prvog poglavlja) već kao skup.
To možemo, jer $\mathbf{g}|_\beta$ doista jest skup za svaki β, po aksiomu zamjene (pogledajte napomenu 6.24). Štoviše, tada se lako vidi da je $\mathbf{g}|_\beta \in \mathbf{H}$ (što ne bismo imali samo iz činjenice da formalno zadovoljava χ), pa dokaz i tu prolazi. □

Kao i za prirodne brojeve (korolar 4.24), zadavanje funkcije $\mathbf{F}$ je najčešće preopćenito. Obično je dovoljno zadati početnu vrijednost i korak, a za granične ordinale uzeti uniju.

Korolar 6.23. *Neka je s skup i $\mathbf{G} : \mathbf{V} \to \mathbf{V}$ klasna funkcija („unarna skupovna operacija"). Tada postoji jedinstveni klasni hiperniz $\mathbf{g} : \mathbf{On} \to \mathbf{V}$ takav da vrijedi:*

- $\mathbf{g}(0) = s$;
- $\mathbf{g}(\alpha^+) = \mathbf{G}\big(\mathbf{g}(\alpha)\big)$ *za svaki ordinal α; i*
- $\mathbf{g}(\lambda) = \bigcup\mathbf{g}[\lambda]$ *za svaki granični ordinal λ.*

Dokaz. Samo treba primijeniti opći teorem rekurzije na klasnu funkciju zadanu s

$$\mathbf{F}(f) := \begin{cases} s, & f = \emptyset \\ \mathbf{G}\big(f(\bigcup \operatorname{dom} f)\big), & \operatorname{dom} f \text{ je sljedbenik} . \\ \bigcup \operatorname{rng} f, & \text{inače} \end{cases} \tag{6.8}$$

□

Napomena 6.24. Kao i ostali teoremi koji govore o općenitim klasama, opći teorem rekurzije je zapravo *shema* teorema, koja ima po jednu instancu za svaku formulu ϕ s odgovarajućim svojstvima. No ovdje je i *izlaz* teorema (**g**) klasa, što znači da teorem zapravo opisuje kako iz formule ϕ dobiti formulu γ. Ipak, često se možemo zaustaviti na nekom konkretnom ordinalu α, pa onda zapravo možemo dobiti običnu funkciju $g : \alpha \to \mathbf{V}$ (po aksiomu zamjene primijenjenom na α i formulu $\gamma \wedge \exists z\big(y = (x,z)\big)$).

Važni specijalni slučaj dobije se za $\alpha := \omega$, što je **jače** od Dedekindovog teorema jer ne zahtijeva specifikaciju skupa t. Štoviše, često se zapravo napravi još jedan korak ($\alpha := \omega^+$), u kojem se formira unija slike tog niza. Jedan primjer smo već vidjeli u dokazu teorema 5.33. Drugi ćemo vidjeti u sljedećoj točki. ◁

Korolar 6.25. *Neka je s skup i $\mathbf{G} : \mathbf{V} \to \mathbf{V}$ skupovna operacija.*
Tada postoji jedinstveni niz skupova g takav da je $g(0) = s$ i $g(n^+) = \mathbf{G}\big(g(n)\big)$ za sve $n \in \omega$.

6.7 Kumulativna hijerarhija formalno

Primjer 6.26. Primjenjujući korolar 6.23 na $s := \emptyset$ i $\mathbf{G}(x) := \mathscr{P}(x)$ (prazan skup i operaciju partitivnog skupa), dobijemo klasnu funkciju $\alpha \mapsto V_\alpha$, koju zovemo *kumulativna hijerarhija*. Označavamo $\mathbf{W} := \bigcup_{\alpha \in \mathbf{On}} V_\alpha$. ◁

Zadatak 6.27. *Dokažite transfinitnom indukcijom da za svaki α vrijedi:*
(1) V_α je tranzitivan skup. (2) Za sve $\beta \in \alpha$ je $V_\beta \subset V_\alpha$.

Želimo dokazati $\mathbf{W} = \mathbf{V}$: jedna inkluzija je trivijalna, a za drugu zapravo treba dokazati $\forall x\, \exists \alpha\, (v \wedge x \in V_\alpha)$. Ubuduće ćemo pretpostavljati da i vezane varijable nazvane grčkim slovima označavaju ordinale, dakle $\exists \alpha$ nam je pokrata za $(\exists \alpha \in \mathbf{On})$ (i analogno za univerzalni kvantifikator). Prvo dokažimo jedan tehnički rezultat.

Propozicija 6.28. *Za svaki skup a postoji tranzitivni skup t takav da je $a \in t$.*

Dokaz. Primijenimo korolar 6.25 na $s := \{a\}$ i $\mathbf{G}(x) := \bigcup x$. Dobijemo niz u s članovima $u_0 = \{a\}$, $u_1 = a$, $u_2 = \bigcup a$, $u_3 = \bigcup\bigcup a$ itd. Sada definiramo $t := u_\omega = \bigcup_{n \in \omega} u_n$.

Očito je $a \in u_0 \subseteq t$, još treba dokazati tranzitivnost. Neka je $x \in y \in t$. Po definiciji skupa t postoji $n \in \omega$ takav da je $y \in u_n$. Sada $x \in y \in u_n$ znači $x \in \bigcup u_n = \mathbf{G}(u_n) = u_{n^+} \subseteq t$. □

Zadatak 6.29. *Dokažite da je tako definirani skup (u_ω iz dokaza propozicije 6.28)* najmanji *tranzitivni skup koji sadrži a kao element.*

Lema 6.30. *Za svaki skup m, $m \subseteq \mathbf{W}$ povlači $m \in \mathbf{W}$.*

Dokaz. Za svaki $x \in m$ po pretpostavci je $x \in \mathbf{W}$, pa postoji $\alpha \in \mathbf{On}$ takav da je $x \in V_\alpha$.
Po teoremu 6.12, postoji (jedinstveni) najmanji ordinal s tim svojstvom; označimo ga s y.
Tada formula $x \in V_y \wedge (\forall \alpha \in y)(x \notin V_\alpha)$ i skup m po aksiomu zamjene daju
skup ordinala b takav da za svaki $x \in m$ postoji $y \in b$ takav da je $x \in V_y$.

Sada $\delta := \sup b := \bigcup b$ ima svojstvo da su svi V_y podskupovi od V_δ (po zadatku 6.27(2)),
pa je svaki $x \in m$ element od V_δ. To znači da je $m \subseteq V_\delta$, odnosno $m \in \mathscr{P}(V_\delta) = V_{\delta^+} \subseteq \mathbf{W}$. □

Teorem 6.31. $\mathbf{V} = \mathbf{W}$.

Dokaz. Neka je $a \in \mathbf{V}$ proizvoljan. Po propoziciji 6.28 postoji tranzitivni t takav da je $a \in t$.
Kad t ne bi bio podskup od $\mathbf{W}$, skup $u := t \setminus \mathbf{W}$ (skup po aksiomu separacije) bi bio neprazan,
pa bi po aksiomu dobre utemeljenosti postojao $m \in u$ takav da je $m \cap u = \emptyset$.

Sada $m \in u \subseteq t$ znači $m \in t$, zbog tranzitivnosti $m \subset t$, no disjunktnost m i $u = t \setminus \mathbf{W}$ znači
da je $m \subseteq \mathbf{W}$ (raspišite!) pa je i $m \in \mathbf{W}$ po lemi 6.30. No to je kontradikcija s $m \in u = t \setminus \mathbf{W}$.

Zaključujemo da u ipak mora biti prazan, dakle $t \subseteq \mathbf{W}$. No tada $a \in t$ znači $a \in \mathbf{W}$.
Time smo dokazali $\mathbf{V} \subseteq \mathbf{W}$, a druga implikacija je naravno trivijalna. □

6.8 Hartogsov ordinal

Teorem enumeracije kaže da za svaki dobro uređeni skup postoji *dovoljno velik* ordinal.
Ako skup nije dobro uređen, možda ga ne možemo „dostići” ordinalima,
ali ga sigurno možemo „prestići”: za svaki skup postoji *prevelik* ordinal.

Lema 6.32. *Ako je α ordinal, a skup i $f : a \to \alpha$ injekcija,*
tada je a moguće dobro urediti tako da bude sličan s $(\operatorname{rng} f, \in)$.

Dokaz. Za $x, y \in a$ definiramo $x \lhd y :\Leftrightarrow f(x) \in f(y)$ (lako se dokaže da je to totalni uređaj).
Po definiciji je f sličnost između $(a, \lhd)$ i $(\operatorname{rng} f, \in)$, pa tvrdnja slijedi iz leme 6.6 primijenjene
na α, činjenice da je podskup dobro uređenog skupa dobro uređen (restrikcijom uređaja) i
činjenice da je dobra uređenost invarijanta sličnosti. □

Teorem 6.33 (Hartogs)**.** *Za svaki skup a postoji najmanji ordinal α takav da $\alpha \not\leq a$.*

Dokaz. Dovoljno je dokazati da postoji *neki* ordinal b sa svojstvom $b \not\leq a$:
tada će postojanje *najmanjeg* takvog ordinala slijediti iz teorema 6.12.

Promotrimo klasu svih dobro uređenih skupova $(s, \lhd)$ pri čemu je $s \subseteq a$. Tada očito mora
biti $(\lhd) \subseteq s \times s \subseteq a \times a$, pa je svaki $(s, \lhd)$ element Kartezijevog produkta $\mathscr{P}(a)$ s $\mathscr{P}(a \times a)$.
Po aksiomu partitivnog skupa i propoziciji 1.11, to je skup, iz kojeg se separacijom može
dobiti da je i početna klasa (svih dobro uređenih podskupova od a) skup: označimo ga s D.

Teorem enumeracije kaže da za svaki $(s, \lhd) \in D$ postoji jedinstveni ordinal η takav da je $(s, \lhd) \simeq (\eta, \in)$. Po aksiomu zamjene primijenjenom na skup D i formulu $x \simeq (y, \in)$, postoji skup b svih takvih η.

Ako je $\beta \in \eta \in b$, postoji $(s, \lhd) \in D$ i sličnost $g : \eta \to s$. No tada je $t := g[\beta] \subset s \subseteq a$ s restringiranim uređajem $(\lhd) \cap t \times t$ također u D, i po propoziciji 3.28 sličan s $p_\eta(\beta) = \beta$ (lema 6.7) pa je $\beta \in b$. To znači da je b tranzitivan skup ordinala, pa je ordinal po korolaru 6.11.

Kad bi postojala injekcija $h : b \to a$, njen inverz h^{-1} bi bio injekcija sa $s := \operatorname{rng} h \subseteq a$ u b, pa bi po lemi 6.32 postojao dobar uređaj $<$ na s te bismo imali $(s, <) \in D$. Također, po istoj lemi bi taj dobro uređeni skup bio sličan s $\operatorname{rng}(h^{-1}) = \operatorname{dom} h = b$ (dakle, b bi bio među spomenutim ordinalima η), pa bismo imali $b \in b$, što je nemoguće po lemi 4.2(1). □

Primijetite sličnost provedenog dokaza s dokazom teorema enumeracije.

Kao što je Cantorov osnovni teorem dobiven preciznom formulacijom Russellovog paradoksa i pažljivim promatranjem do kakve kontradikcije zapravo dolazimo, Hartogsov teorem je rezultat tog istog postupka primijenjenog na Burali-Fortijev paradoks.

$$\text{Russell} : \text{Cantor} \quad :: \quad \text{Burali-Forti} : \text{Hartogs} \tag{6.9}$$

7 Aksiom izbora

7.1 Motivacija

Na mnogo mjesta smo dosad bili u situaciji da smo dokazali formulu oblika $\exists! y\varphi$ (eventualno pod nekim uvjetima na ostale slobodne varijable u φ), i često smo to koristili da definiramo funkcijsku oznaku ($y = g(x)$) koju smo koristili dalje. Specijalno, po aksiomu zamjene, mogli smo za zadani skup a konstruirati skup $\{g(x) : x \in a\} =: b$, a onda i funkciju g kao skup $\{(x, y) \in a \times b : \varphi\} = \{p \in a \times b : \exists x \exists y (p = (x, y) \wedge \varphi)\}$ separacijom iz $a \times b$.

Je li jedinstvenost tu nužna? Što bi se dogodilo da za svaki pojedini x imamo dva objekta, y_1 i y_2, koja zadovoljavaju φ? Ili općenito, neprazni skup A_x takvih objekata? Dakle, na višoj razini imamo situaciju iz prethodnog odlomka: ako su svi x koji nas zanimaju elementi nekog skupa I (tada ih obično zovemo *indeksima* i označavamo slovom i), istim postupkom dobijemo funkciju

$$f = \{(i, A_i) : i \in I\} =: (A_i : i \in I),$$

koju zovemo *indeksiranom familijom*.
Primijetimo da su nizovi specijalni slučaj indeksiranih familija (za $I := \omega$).

Nas zanima možemo li ipak „uvesti funkcijsku oznaku", ili (ekvivalentno po aksiomu zamjene, jer je I skup) definirati funkciju c s domenom I, takvu da je $c(i) \in A_i$ za sve $i \in I$. Budući da c „izabire" po jedan element iz svakog skupa A_i, zovemo je *funkcijom izbora*.

Zanimljivo je da postojanje funkcije izbora za svaku indeksiranu familiju nepraznih skupova, općenito **ne slijedi** iz dosad uvedenih aksioma. Ako želimo uvijek biti sigurni da imamo funkciju izbora, moramo uvesti novi *aksiom izbora*:

$$\big(\forall A \in {}^{I}\big(\mathscr{P}(T) \setminus \{\emptyset\}\big)\big)\big(\exists c \in {}^{I}T\big)\big(\forall i \in I\big)\big(c(i) \in A(i)\big). \tag{7.1}$$

Kao i za ostale „napredne" aksiome (zamjene, dobre utemeljenosti), u mnogim specijalnim slučajevima možemo izbjeći njegovo korištenje, ali ne u svima.

Slikovito, svaki skup parova cipelā sigurno ima funkciju izbora koja svakom indeksu pridružuje lijevu cipelu odgovarajućeg para, dok je za postojanje funkcije izbora beskonačnog skupa parova čarapā nužno koristiti aksiom izbora. (Za više detalja pogledajte Vuković, *O aksiomu izbora, cipelama i čarapama*.) Pritom ne mislimo da smo sad najednom počeli u klasu **V** ubacivati doslovne cipele i čarape, već nam „par cipela" metaforički predstavlja *uređen* par matematičkih objekata, a „par čarapa" neuređen. [Ti parovi ne moraju doista biti uređeni; bitno je samo da se nekom formulom (poput „x je lijeva cipela") može jednoznačno odrediti jedan element para.]

7.2 Jednostavne ekvivalentne formulacije

Primijetimo da je bilo nužno reći da se u indeksiranoj familiji ne nalazi prazan skup (jer njemu funkcija izbora nema što pridružiti).
Skup T, odnosno činjenica da je kodomena baš $\mathscr{P}(T)\setminus\{\emptyset\}$, nije nužna: T uvijek možemo rekonstruirati kao $\bigcup \operatorname{rng} A$. (Usporedite sa zadatkom na početku točke 1.5.)

Za konačan („nabrojen") skup $I=\{i_1,\dots,i_k\}$, aksiom izbora nikada nije nužan, jer za svaki i_j pojedinačno možemo „ručno" odabrati element: kako je A_{i_j} neprazan, postoji njegov element, pa odaberimo jedan takav i dajmo mu neko ime. To je logički korak u dokazu (eliminacija egzistencijalnog kvantifikatora) i kao takav ne zahtijeva opravdanje nelogičkim aksiomima, ali je ključno da je dokaz (u logici prvog reda koju mi koristimo) *konačan* niz koraka. Dakle, tu strategiju ne možemo upotrijebiti za beskonačne indeksne skupove.

Recimo, za $I:=2=\{0,1\}$ i skupove A_0 i A_1, funkcija izbora $c:I\to A_0\cup A_1$ je zadana svojim vrijednostima $x:=c(0)\in A_0$ i $y:=c(1)\in A_1$, pa je možemo poistovjetiti s uređenim parom $(x,y)\in A_0\times A_1$. Očito je Kartezijev produkt dvaju nepraznih skupova neprazan, i u dokazu ne koristimo aksiom izbora: jednostavno, A_0 je neprazan pa postoji $x\in A_0$, A_1 je neprazan pa postoji $y\in A_1$, i onda je $(x,y)\in A_0\times A_1$. Analogno bismo dobili za $n\in\mathbb{N}$ skupova, ali za beskonačno mnogo skupova, nepraznost *Kartezijevog produkta indeksirane familije*

$$\prod_{i\in I}A_i:=\Big\{c\in{}^{I}\Big(\bigcup_{i\in I}A_i\Big):(\forall\, i\in I)\big(c(i)\in A_i\big)\Big\}\neq\emptyset \tag{7.2}$$

(pod pretpostavkom nepraznosti „faktorā" A_i) je samo drugačiji zapis aksioma izbora.

Još jedna ekvivalentna formulacija dobije se tako da se ne promatra indeksirana familija, već običan skup B nepraznih skupova. Tada umjesto funkcije izbora možemo tražiti *izborni skup* koji ima jednočlan presjek sa svakim elementom od B.
Ipak, tada je potrebno zahtijevati dodatni uvjet da su elementi od B u parovima disjunktni: primijetite da skup nepraznih skupova $\big\{\{1\},\{2\},\{1,2\}\big\}$ nema izborni skup.

Važni specijalni slučaj skupa nepraznih u parovima disjunktnih podskupova nekog skupa T je particija od T, odnosno (zadatak 2.23(2)) kvocijentni skup $T/_\sim$ po nekoj relaciji ekvivalencije na T.
I obrnuto, svaki takav skup P je particija od $\bigcup P$, pa se aksiom izbora ekvivalentno može izreći u obliku „svaka particija ima izborni skup". Primjer korištenja takve formulacije vidjet ćete na kolegiju Mjera i integral (Vitalijev neizmjeriv podskup od $\mathbb{R}$).

Kako je za nas svaki skup zapravo skup skupova, jedna vrlo elegantna formulacija aksioma izbora glasi

$$\emptyset\notin x\to\Big(\exists\, c\in{}^{x}\bigcup x\Big)(\forall\, a\in x)\big(c(a)\in a\big). \tag{7.3}$$

Zadatak 7.1. *Formulirajte precizno sve te varijante aksioma izbora, i dokažite da su ekvivalentne pod pretpostavkom ostalih aksioma.*
[Rješenja možete pogledati u Gunja, *Zornova lema i srodne tvrdnje*.]

7.3 Zornova lema

Zornova lema je vjerojatno rezultat teorije skupova koji je najkorisniji u drugim granama matematike. Posljedica je aksioma izbora, i ovdje ćemo to dokazati.

Definicija 7.2. Neka je $(X, \prec)$ parcijalno uređen skup i $L \subseteq X$ takav da su mu svaka dva elementa usporediva relacijom $\prec$. Tada kažemo da je L *lanac* u X. $\triangleleft$

Lema 7.3 (Zorn)**.** *Neka je $(A, \prec)$ parcijalno uređen skup u kojem svaki lanac ima gornju među. Tada u $(A, \prec)$ postoji barem jedan maksimalni element.*

Dat ćemo dva dokaza: jedan jednostavan i lako pratljiv, ali uz korištenje općeg teorema rekurzije; i drugi, tehnički zahtjevan ali sasvim elementaran.

Dokaz (opća rekurzija). Označimo s C skup svih lanaca u A (dobiven separacijom iz $\mathscr{P}(A)$). Pretpostavka leme kaže da je za svaki $L \in C$ skup $M_L := \{y \in A : (\forall x \in L)(x \preceq y)\}$ neprazan. Primjenom aksioma izbora na indeksiranu familiju $(M_L : L \in C)$ dobivamo funkciju $g : C \to A$ takvu da je za svaki $L \in C$, $g(L)$ gornja međa lanca L.

Pretpostavimo suprotno, da A nema maksimalni element.
Tada je za svaki $x \in A$, skup $S_x := \{y \in A : x \prec y\}$ neprazan. Primjenom aksioma izbora na $(S_x : x \in A)$ dobivamo funkciju $v : A \to A$ takvu da za sve $x \in A$ vrijedi $v(x) \succ x$.

Sada za bilo koji rastući (precizno, onaj koji čuva strogi uređaj) hiperniz $f : \eta \to A$ definiramo $\mathbf{F}(f) := v\big(g(\operatorname{rng} f)\big)$ (za ostale, nerastuće hipernizove definiramo npr. $\mathbf{F}(f) := \emptyset$) — tada prema općem teoremu rekurzije postoji jedinstveni $\mathbf{F}$-rekurzivni klasni hiperniz $\mathbf{h}$.

Dokažimo da vrijedi $(\forall \beta \in \alpha)\big(\mathbf{h}(\beta) \prec \mathbf{h}(\alpha)\big)$ za sve ordinale α, strogom transfinitnom indukcijom. Pretpostavka je $(\forall \beta \in \delta)\big(\mathbf{h}(\beta) \prec \mathbf{h}(\delta)\big)$ za sve $\delta \in \alpha$ — drugim riječima $\mathbf{h}|_\alpha$ čuva strogi uređaj, pa je $\operatorname{rng}(\mathbf{h}|_\alpha) = \mathbf{h}[\alpha] \in C$, odnosno $\mathbf{h}(\alpha) = \mathbf{F}(\mathbf{h}|_\alpha) = v\big(g(\mathbf{h}[\alpha])\big)$ je dobro definirani element od A. Za svaki $\beta \in \alpha$ je $\mathbf{h}(\beta) \in \mathbf{h}[\alpha]$, odnosno $\mathbf{h}(\beta) \preceq g(\mathbf{h}[\alpha]) \prec v\big(g(\mathbf{h}[\alpha])\big) = \mathbf{h}(\alpha)$ po svojstvima funkcija g i v, čime je korak indukcije proveden.

Označimo $h := \mathbf{h}|_\gamma$, gdje je γ Hartogsov ordinal od A (teorem 6.33). Iz prethodnog odlomka slijedi da h čuva strogi uređaj, odnosno injekcija je, što je nemoguće po definiciji od γ. $\square$

Dokaz (elementarni). Označimo s $\mathscr{L}$ skup svih lanaca u A te za svaki $C \in \mathscr{L}$ definiramo $G_C := \{x \in A : (\forall y \in C)(y \prec x)\} \subseteq A \setminus C$. Pretpostavimo suprotno, što znači da su svi $G_C \neq \emptyset$ (gornja međa od C nije maksimalna u A). Po aksiomu izbora postoji funkcija f takva da je $f(G_C) \in G_C$ za svaki $C \in \mathscr{L}$. Označimo

$$\left.\begin{aligned} \mathscr{E} &:= \{C \in \mathscr{L} : D \subseteq C \wedge G_D \not\subseteq G_C \Rightarrow f(G_D) \in C\} \\ \mathscr{F} &:= \{B \in \mathscr{P}(A) : C \in \mathscr{E} \Rightarrow B \setminus C \subseteq G_C\} \end{aligned}\right\} \mathscr{H} := \mathscr{E} \cap \mathscr{F},$$

i neka je $H := \bigcup \mathscr{H}$. Tvrdimo da je $H \in \mathscr{H}$, što znači $H \in \mathscr{F}$ i $H \in \mathscr{E}$.

$H \in \mathscr{F}$: Očito je $H \subseteq A$. Neka je $C \in \mathscr{E}$ proizvoljan i $x \in H \setminus C$. Tada zbog $x \in H$ postoji $B \in \mathscr{H}$ takav da je $x \in B$, no zbog $B \in \mathscr{H} \subseteq \mathscr{F}$ i $C \in \mathscr{E}$ imamo $G_C \supseteq B \setminus C \ni x$.

$H \in \mathscr{L}$: Neka su $x, y \in H$ proizvoljni. Tada je $y \in C$ za neki $C \in \mathscr{H} \subseteq \mathscr{E}$.
- Ako je i $x \in C$, usporediv je s y jer je C lanac.
- Inače je $x \in H \setminus C \subseteq G_C$ (zbog $H \in \mathscr{F}$ i $C \in \mathscr{E}$) pa je $y \prec x$ zbog $y \in C$.

$H \in \mathscr{E}$: Neka je $D \subseteq H$ proizvoljan takav da $G_D \not\subseteq G_H$. Tada postoji $x \in G_D$ takav da $x \notin G_H$, što znači $y \not\prec x$ za neki $y \in H$. Ovo zadnje pak znači da postoji $S \in \mathscr{H}$ takav da je $y \in S$. Pretpostavimo da postoji $z \in D \setminus S \subseteq H \setminus S \subseteq G_S$ (ovo zadnje zbog $H \in \mathscr{F}$ i $S \in \mathscr{H} \subseteq \mathscr{E}$). Tada $x \in G_D$ i $z \in D$ povlače $z \prec x$, te $z \in G_S$ i $y \in S$ povlače $y \prec z$, što po tranzitivnosti daje $y \prec x$, kontradikcija. Dakle z ne postoji, odnosno $D \subseteq S$, pa $f(G_D) \in D \subseteq S \subseteq H$.

Označimo $u := f(G_H) \in G_H$: dakle u je veći od svih elemenata iz H, pa je $K := H \cup \{u\} \in \mathscr{L}$ i $u = \max K$. Dokažimo $K \in \mathscr{H}$, odnosno (još) $K \in \mathscr{E}$ i $K \in \mathscr{F}$.

$K \in \mathscr{E}$: Neka je $D \subseteq K$ takav da $G_D \not\subseteq G_K$. Tada $u = \max K \notin D$ (jer inače svaki element veći od svih iz D mora biti veći i od u, pa tako i od svih iz K). Dakle $D \subseteq H$, iz čega $G_H \subseteq G_D$. Ako vrijedi i druga inkluzija, imamo jednakost $G_H = G_D$, a f je funkcija pa je $f(G_D) = f(G_H) = u \in K$; a inače ($G_D \not\subseteq G_H$) je $f(G_D) \in H \subseteq K$ zbog $H \in \mathscr{E}$.

$K \in \mathscr{F}$: Neka je $C \in \mathscr{E}$ proizvoljan. Očito je $R := K \setminus C = (H \cup \{u\}) \setminus C \subseteq H \setminus C \cup \{u\}$.

- Ako postoji $x \in H \setminus C$, tada je svaki takav $x \in G_C$ zbog $H \in \mathscr{F}$, pa i $u \in G_C$ zbog $x \prec u$.
- U protivnom je $H \subseteq C$ (odakle $G_C \subseteq G_H$) i $R \subseteq \emptyset \cup \{u\} = \{u\}$.
  - Ako je usto $G_H \subseteq G_C$, tad je i $u \in G_C$ pa opet imamo $R \subseteq G_C$.
  - Inače je $u = f(G_H) \in C$ zbog $C \in \mathscr{E}$, pa je čitav $K \subseteq C$ te je trivijalno $R = \emptyset \subseteq G_C$.

Sada iz $u \in K \in \mathscr{H}$ slijedi $u \in \bigcup \mathscr{H} = H$, što je kontradikcija s $u \in G_H$. □

Kao i aksiom izbora, Zornova lema pojavljuje se u mnogim varijantama.
Za početak, slično napomeni 3.21, prazan lanac se promatra odvojeno:
njegova gornja međa je bilo koji element od A, pa je dovoljno tražiti da
je A *neprazni* skup u kojem svaki *neprazni* lanac ima gornju među.

To je posebno korisno kad je uređaj $\prec$ baš inkluzija: tada je za gornju među lanca $L \subseteq A$ prirodno uzeti $\bigcup L$, ali $\bigcup \emptyset = \emptyset$ ne mora biti u A pa moramo naći neki drugi element — srećom, možemo uzeti bilo koji, jer je svaki element gornja međa praznog skupa.

Također, ponekad nam treba ne bilo kakav maksimalni element,
već onaj koji je „iznad" nekog unaprijed zadanog elementa. To se isto lako dokaže.
Evo jedne formulacije koja uključuje mnoge navedene aspekte.

Korolar 7.4. *Neka je t skup i $F \subseteq \mathscr{P}(t)$ takav da za svaki neprazni lanac $L \subseteq F$ vrijedi $\bigcup L \in F$. Tada za svaki $x \in F$ postoji $m \in F$ takav da je $x \subseteq m$ i da $m \subset n \subseteq t$ povlači $n \notin F$.*

Dokaz. Neka je $x \in F$ proizvoljan. Promotrimo $A := \{y \in F : x \subseteq y\}$ i uredimo ga inkluzijom. Svaki lanac L u A je ujedno i lanac u F jer je $A \subseteq F$. Ako je prazan, ima gornju među $x \in A$. Ako je neprazan, ima gornju među $\bigcup L \in F$, i trebamo još samo vidjeti da je $\bigcup L \in A$. No $L \neq \emptyset$ znači da postoji $y \in L$, pa je po definiciji unije $y \subseteq \bigcup L$ — a $y \in L \subseteq A$ znači $y \in A$ odnosno $x \subseteq y$. Po tranzitivnosti imamo $x \subseteq \bigcup L$, pa je $\bigcup L \in A$.

Po Zornovoj lemi postoji maksimalni element u F, odaberimo jedan i označimo ga s m. Kad bi bilo $m \subset n \subseteq t$ i $n \in F$, tada bi n bio pravi nadskup od m u F, što bi bila kontradikcija s maksimalnošću od m. □

Neke tvrdnje ekvivalentne Zornovoj lemi (Teichmüller–Tukeyeva lema, Hausdorffov princip) i njene primjene u algebri mogu se pronaći u Gunja, *Zornova lema i srodne tvrdnje*.

7.4 Primjene unutar teorije skupova

Propozicija 7.5. *Neka su a i b skupovi i $f : a \to b$ surjekcija na b. Tada postoji injekcija s b u a. [Tu tvrdnju možemo koncizno izreći kao:* $\operatorname{rng} f \subsetneq \operatorname{dom} f$ *za svaku funkciju f.]*

Dokaz. Za indeksni skup uzmimo $I := b$, i svakom $i \in b$ pridružimo $A_i := f^{-1}[\{i\}]$. Zbog surjektivnosti, svaki A_i je neprazan, i podskup je od a, pa imamo familiju nepraznih podskupova od a. Izborna funkcija c te familije je upravo tražena injekcija: ide s b u a, a $c(i) = c(j)$ bi značilo da je $i = f\big(c(i)\big) = f\big(c(j)\big) = j$. Naime, $c(i) \in f^{-1}[\{i\}]$ znači da mu je funkcijska vrijednost po f element od $\{i\}$, odnosno po aksiomu para jednaka i (i analogno za j). □

Korolar 7.6. *Ako između dva skupa postoje injekcija i surjekcija, tada postoji i bijekcija.*

Dokaz. Direktno iz propozicije 7.5 i teorema 3.25 (CSB). □

Propozicija 7.7. *Unija prebrojive indeksirane familije prebrojivih skupova je prebrojiva.*

Dokaz. Neka je $(A_i : i \in I)$ proizvoljna takva familija. Dakle, I je prebrojiv skup — odaberimo jednu bijekciju između ω i I te je označimo s f. Također, za svaki $i \in I$, označimo s B_i skup svih bijekcija između ω i A_i: dobiven je separacijom iz $\mathscr{P}(\omega \times A_i)$, a neprazan je zbog prebrojivosti A_i. Po aksiomu zamjene (na standardni način), $(B_i : i \in I)$ je indeksirana familija nepraznih skupova, pa postoji funkcija c s domenom I takva da je za svaki $i \in I$, $c(i) : \omega \to A_i$ bijekcija.

Definiramo $g : \omega \times \omega \to \bigcup_{i\in I} A_i$ formulom $g\big((m,n)\big) := c\big(f(m)\big)(n)$ (*currying* na $c \circ f$) — dobro je definirana jer je $f(m) \in I$ za $m \in \omega$ — i tvrdimo da je to surjekcija na uniju. Neka je $x \in \bigcup_{i\in I} A_i$: tada postoji (odaberimo jedan; recimo, onaj s najmanjom vrijednošću funkcije f) $i \in I$ takav da je $x \in A_i$. Označimo $m := f^{-1}(i) \in \omega$. Kako je $c(i)$ bijekcija na A_i, postoji $n := \big(c(i)\big)^{-1}(x) \in \omega$. Sada je $(m,n) \in \omega \times \omega$, i

$$g\big((m,n)\big) = c\big(f(m)\big)(n) = c\big(f\big(f^{-1}(i)\big)\big)(n) = c(i)(n) = c(i)\big((c(i))^{-1}(x)\big) = x. \tag{7.4}$$

Po propoziciji 7.5, $\mathfrak{K}(\bigcup_{i\in I} A_i) \leq \mathfrak{K}(\omega \times \omega) = \aleph_0{}^2 = \aleph_0$. S druge strane, $A_{f(0)} \subseteq \bigcup_{i\in I} A_i$ povlači $\aleph_0 = \mathfrak{K}(A_{f(0)}) \leq \mathfrak{K}(\bigcup_{i\in I} A_i)$, pa tvrdnja slijedi po CSB. □

Zadatak 7.8. *Označimo s N_X, K_X i P_X redom svojstva skupa X „biti neprazan", „biti konačan" i „biti prebrojiv". Povežite ta svojstva N_U, K_U i P_U na uniji indeksirane familije sa svojstvima N_I, K_I i P_I na indeksnom skupu te svojstvima N_A, K_A i P_A na pojedinim (svim) skupovima u familiji. Recimo, propozicija 7.7 kaže da $P_I \wedge P_A \Rightarrow P_U$.*

Napokon možemo ispuniti staro obećanje i dokazati da su kardinalnosti totalno uređene.

Teorem 7.9. *Za svaka dva skupa a i b postoji injekcija s a u b ili injekcija s b u a.*

Dokaz. Promotrimo skup F svih relacijā r između a i b takvih da r i r^{-1} imaju funkcijsko svojstvo (F je skup jer je dobiven separacijom iz $\mathscr{P}(a \times b)$), i uredimo ga inkluzijom. Ako je $L \subseteq F$ lanac, svaki element $p \in \bigcup L$ je u nekom elementu iz F, dakle u nekoj relaciji između a i b, odnosno p je uređeni par iz $a \times b$. Drugim riječima, $\bigcup L$ je relacija između a i b.

Ako su $(x, y_1), (x, y_2) \in \bigcup L$, postoje $r_1, r_2 \in L$ takve da je $x\ r_1\ y_1$ i $x\ r_2\ y_2$. L je lanac, pa je ili $r_1 \subseteq r_2$ ili $r_2 \subseteq r_1$ — bez smanjenja općenitosti ovo prvo. Sada imamo $(x, y_1) \in r_1 \subseteq r_2$ i $(x, y_2) \in r_2$. No $r_2 \in L \subseteq F$ znači da r_2 ima funkcijsko svojstvo, pa je $y_1 = y_2$.

Zaključujemo da $\bigcup L$ ima funkcijsko svojstvo, a sasvim analogno (raspišite!) bismo dobili da ga ima i njen inverz. Sve u svemu, $\bigcup L \in F$ je gornja međa lanca L. Po Zornovoj lemi, u F postoji maksimalni element — odaberimo jedan i označimo ga s f. Kako je $f \subseteq a \times b$, vrijedi $\operatorname{dom} f \subseteq a$ i $\operatorname{rng} f = \operatorname{dom}(f^{-1}) \subseteq b$.

Ako je $\operatorname{dom} f = a$, tada je očito $f : a \to b$ tražena injekcija. Analogno, ako je $\operatorname{dom}(f^{-1}) = b$, tada je $f^{-1} : b \to a$ tražena injekcija. Kad ne bi bilo nijedno od toga, postojali bi elementi $x \in a \setminus \operatorname{dom} f$ i $y \in b \setminus \operatorname{rng} f$, pa bi $g := f \cup \{(x, y)\} \supset f$ i g^{-1} imale funkcijsko svojstvo (pogledajte sljedeći odlomak), što je u kontradikciji s maksimalnošću od f.

Dokažimo funkcijsko svojstvo od g (za g^{-1} je sasvim analogno). Neka su $(x_0, y_1), (x_0, y_2) \in g$. Ako je $x_0 = x$, tada oni ne mogu biti u f, pa moraju biti u drugom članu unije, što znači $(x_0, y_1) = (x, y) = (x_0, y_2)$, iz čega $y_1 = y_2$. Ako pak $x_0 \neq x$, analogno oba para moraju biti u f, pa $y_1 = y_2$ slijedi iz funkcijskog svojstva od f. □

Primijetite sličnost provedenog dokaza s dokazom teorema 6.4.

Teorem 7.10 (Zermelo)**.** *Svaki skup se može dobro urediti.*

Dokaz. Neka je a skup. Po Hartogsovom teoremu, postoji ordinal α takav da ne postoji injekcija s α u a. No prema teoremu 7.9 tada mora postojati injekcija (fiksirajmo jednu) $f : a \to \alpha$. Sada tvrdnja slijedi iz leme 6.32. □

7.5 Kardinalni brojevi

Definicija 7.11. Za ordinal α kažemo da je *kardinalni broj* ako je α najmanji ordinal u svojoj klasi ekvipotentnosti; odnosno preciznije, ako vrijedi $(\forall \beta \in \alpha)(\beta \not\sim \alpha)$. ◁

Zadatak 7.12. *Dokažite da su svi prirodni brojevi, kao i ω, kardinalni brojevi, dok svi ostali ordinali do uključivo $\epsilon_0 := \sup\{1, \omega, \omega^\omega, \omega^{\omega^\omega}, \ldots\}$ nisu kardinalni brojevi.* [Za preciznu definiciju i važnost ordinala ϵ_0 pogledajte Bašić, *Ordinalni kalkulator*.]

Teorem 7.13. *Za svaki skup a postoji jedinstveni kardinalni broj α ekvipotentan s njim. Zovemo ga* kardinalnim brojem skupa *a i označavamo s* $\operatorname{card} a$.

Dokaz. Postojanje: Po Zermelovom teoremu, skup a se može dobro urediti. Po teoremu enumeracije, takav dobro uređen skup a je sličan jedinstvenom ordinalu, označimo ga s β. Svaka sličnost je bijekcija, pa je specijalno $a \sim \beta$. Označimo s $\mathbf{A} := \{\delta \in \mathbf{On} : \delta \sim a\}$ klasu svih ordinala ekvipotentnih s a. (Pitanje: je li to prava klasa?) Upravo smo vidjeli $\beta \in \mathbf{A}$, pa je $\mathbf{A} \neq \emptyset$. Po teoremu 6.12 postoji $\alpha := \min \mathbf{A}$.

Očito je $\alpha \sim a$ (zbog $\alpha \in \mathbf{A}$); trebamo još dokazati da je α kardinalni broj. Neka je $\gamma \in \alpha$ proizvoljan. Kad bi vrijedilo $\gamma \sim \alpha$, po tranzitivnosti ekvipotentnosti bismo imali i $\gamma \sim a$, odnosno $\gamma \in \mathbf{A}$, što je kontradikcija s $\gamma < \alpha = \min \mathbf{A}$.

Jedinstvenost: Pretpostavimo suprotno, da su različiti kardinalni brojevi α i β ekvipotentni s a. Po propoziciji 6.10, oni su usporedivi kao ordinali: bez smanjenja općenitosti je $\alpha \in \beta$. Po teoremu 3.2, iz $\alpha \sim a$ i $\beta \sim a$ imali bismo $\alpha \sim \beta$, što je zbog $\alpha \in \beta$ u kontradikciji s time da je β kardinalni broj. □

7.6 Operacije na kardinalnim brojevima

Klasu svih kardinalnih brojeva označavamo s **Cn**. To je prava klasa (što će postati jasno kasnije). Kardinalne brojeve obično označavamo grčkim slovima κ, λ, μ. Time smo napokon našli reprezentante kardinalnosti, i možemo formalno govoriti o operacijama na kardinalnim brojevima, i o njihovom uspoređivanju. Svi rezultati iz poglavlja 3 i dalje vrijede, jer su neovisni o reprezentantima — no treba dokazati da su ono što smo prije zvali „definicijama" uređaja, jednakosti, zbrajanja i množenja na kardinalnostima, sada specijalni slučajevi istih klasnih relacija odnosno operacija na kardinalnim brojevima kao specijalnim ordinalima.

Propozicija 7.14. *Za svaka dva skupa a i b vrijedi:*

1. $a \sim b \iff \operatorname{card} a = \operatorname{card} b$;
2. $a \precneqq b \iff \operatorname{card} a \leq \operatorname{card} b$;
3. $\operatorname{card}(a \times b) = \operatorname{card}(\operatorname{card} a \cdot \operatorname{card} b)$;
4. $a \cap b = \emptyset \implies \operatorname{card}(a \cup b) = \operatorname{card}(\operatorname{card} a + \operatorname{card} b)$.

Dokaz. Označimo $\alpha := \operatorname{card} a$ i $\beta := \operatorname{card} b$.

[1.⇒] Iz $\alpha \sim a \sim b \sim \beta$ imamo $\alpha \sim \beta$. Kad bi ti ordinali bili različiti, po propoziciji 6.10 jedan bi bio veći: bez smanjenja općenitosti možemo pretpostaviti $\alpha \in \beta$. No to je kontradikcija s činjenicom da je β kardinalni broj.

[1.⇐] Odmah imamo $a \sim \alpha = \beta \sim b$, iz čega je $a \sim b$.

[2.⇒] Kako relacija $\precneqq$ ne ovisi o reprezentantima, imamo i $\alpha \precneqq \beta$. Kad ne bi bilo $\alpha \leq \beta$, po propoziciji 6.10 bismo imali $\beta \in \alpha$, iz toga $\beta \subset \alpha$ jer je α tranzitivan, zatim $\beta \precneqq \alpha$ jer je $\precneqq$ inkluzivna, i napokon $\alpha \sim \beta$ po CSB, što je kontradikcija s time da je α kardinalni broj.

[2.⇐] Iz $\alpha \leq \beta$ imamo dva slučaja: ili je $\alpha \in \beta$ pa je $\alpha \subset \beta$ zbog tranzitivnosti β, ili je $\alpha = \beta$. U svakom slučaju je $\alpha \subseteq \beta$, pa i $\alpha \lesssim \beta$ zbog inkluzivnosti, a onda i $a \lesssim b$ zbog neovisnosti o reprezentantima.

[3.] Zbog (1.), dovoljno je dokazati $a \times b \sim \alpha \cdot \beta$, odnosno zbog neovisnosti definicije množenja o reprezentantima (propozicija 3.3), dovoljno je dokazati $\alpha \times \beta \sim \alpha \cdot \beta$. No koristeći teorem o dijeljenju s ostatkom (Bašić, *Ordinalni kalkulator*, teorem 2.2.14) lako je dokazati (učinite to!) jaču tvrdnju: da je $(\alpha \times \beta, <_{\mathsf{al}}) \simeq (\alpha \cdot \beta, \in)$, gdje je $<_{\mathsf{al}}$ antileksikografski uređaj (sličnost je zadana s $f(\xi, \eta) := \alpha \cdot \eta + \xi$).

[4.] Sasvim analogno kao (3.), jednom kad uočimo da se ordinali α i β mogu disjunktificirati kao $\alpha \times \{0\}$ i $\beta \times \{1\}$. Treba dokazati da je konkatenacija $t := \alpha \times \{0\} \cup \beta \times \{1\}$ ekvipotentna s $\alpha + \beta$, no opet, lako je dokazati (korištenjem teorema o oduzimanju — Bašić, *Ordinalni kalkulator*, teorem 2.1.12) da je $(t, <_{\mathsf{al}}) \simeq (\alpha + \beta, \in)$, iz čega to dakako slijedi. □

Napomena 7.15. Za potenciranje je situacija mnogo kompliciranija (neke rezultate možete vidjeti u Doko, *Kardinalna aritmetika*) — već smo rekli da se ono *ne podudara* s ordinalnim potenciranjem, i da se zato za kardinalne brojeve koriste druge oznake nego za ordinale koji su im jednaki. Recimo, $2^{\aleph_0} = \mathfrak{c}$ je neprebrojiv, dok je $2^{\omega} = \omega$ (Bašić, *Ordinalni kalkulator*) prebrojiv.

Ipak, za prirodne brojeve nam **ne trebaju** druge oznake, jer se potencija m^n kao kardinalni broj skupa funkcija s n u m podudara s rekurzivno definiranim potenciranjem prirodnih brojeva kao konačnih ordinala. Kako to vidimo? Tako što dokažemo (indukcijom) da zadovoljava rekurziju $m^0 = 1 \wedge m^{n^+} = m^n \cdot m$, i iskoristimo jedinstvenost iz Dedekindovog teorema rekurzije. Lijevi konjunkt se dobije tako da se dokaže da je $\emptyset$ jedina funkcija s 0 u m, a desni dokazom da je s $h(f) := \big(f|_n, f(n)\big)$ zadana bijekcija između ${}^{n^+}m$ i ${}^n m \times m$.

Štoviše, za dokaz u prethodnom odlomku nigdje nismo koristili konačnost baze m, dakle κ^n za $n \in \omega$ ima isto značenje u smislu kardinalnog i ordinalnog potenciranja, za bilo koji kardinalni broj κ. Specijalno, $\kappa \times \kappa \sim \kappa^2$, i $\kappa \times \kappa \times \kappa \sim \kappa^3$. To ćemo koristiti u dokazu teorema o kvadratu. ◁

7.7 Hijerarhija alefa i hipoteza kontinuuma

Propozicija 7.16. *Za svaki kardinalni broj κ postoji neposredni kardinalni sljedbenik κ^+.*

Dokaz. Prema Cantorovom osnovnom teoremu je $\operatorname{card}\mathscr{P}(\kappa) > \kappa$. Dakle, klasa svih kardinalnih brojeva većih od κ je neprazna. Kao klasa ordinala, ona ima najmanji element. Taj ordinal je element opisane klase, pa je kardinalni broj, po definiciji je veći od κ te između κ i njega nema drugih kardinalnih brojeva. Dakle, to je upravo κ^+. □

Zadatak 7.17. *Dokažite: Za svaki $\kappa \in \mathbf{Cn}$, κ^+ je upravo njegov Hartogsov ordinal.*

Zadatak 7.18. *Neka je S skup kardinalnih brojeva. Tada je $\bigcup S$ kardinalni broj.*
Ako S ima maksimum, to je upravo $\bigcup S$.
Inače, $\bigcup S$ je najmanji kardinalni broj veći od svih elemenata skupa S.
Dokažite sve to, i dokažite da iz tih tvrdnji slijedi da je **Cn** *prava klasa.*

Koristeći korolar 6.23 (uz $s := \omega$, $\mathbf{G}(\kappa) := \kappa^+$) definiramo klasni hiperniz $\aleph : \mathbf{On} \to \mathbf{Cn}$ s

$$\aleph_0 := \omega, \qquad \aleph_{\beta^+} := \aleph_\beta{}^+, \qquad \aleph_\gamma := \textstyle\bigcup_{\xi\in\gamma} \aleph_\xi \text{ za granični } \gamma, \tag{7.5}$$

i može se dokazati da je $\aleph$ klasna bijekcija (čak i klasna sličnost) između **On** i $\mathbf{Cn} \setminus \omega$.

Primijetimo da smo sada napokon opravdali $\aleph_0$ (i općenito $\aleph_\alpha$) kao skup. Štoviše, zbog surjektivnosti $\aleph$, svaku kardinalnost možemo shvatiti kao njenog reprezentanta na $\aleph$-skali.

Zadatak 7.19. *Neka je a neprazni skup, i $\mathfrak{K}(a)$ njegova neformalna kardinalnost — prava klasa ekvivalencije skupa a s obzirom na ekvipotentnost.*
Dokažite da postoji najniža razina kumulativne hijerarhije koju $\mathfrak{K}(a)$ siječe, i da je njen presjek s **On** *jednočlan skup: jedini element presjeka je upravo* $\operatorname{card} a$.

Mnoge prave klase **T** *imaju slično svojstvo: skup (dokažite da je to uvijek skup — iako ne mora biti jednočlan) svih elemenata od* **T** *koji se nalaze na najnižoj razini kumulativne hijerarhije koju* **T** *siječe, često može poslužiti kao vjerni reprezentant klase* **T** *u kumulativnoj hijerarhiji. Tu tehniku je uveo* ***Dana Stewart Scott****.*

Pored $\aleph_0$ i prirodnih brojeva, uveli smo i kardinalnost $\mathfrak{c}$ skupa realnih brojeva. Sada vidimo da $\mathfrak{c}$ mora biti neki $\aleph_\alpha$ — ali koji? Kako je po Cantorovom osnovnom teoremu $\mathfrak{c} = 2^{\aleph_0} > \aleph_0$, a $\aleph_1 = \aleph_0{}^+$ je najmanji takav, očito je $\mathfrak{c} \geq \aleph_1$. Prirodno je zapitati se (što je već Cantor učinio) vrijedi li jednakost. To pitanje, odnosno pretpostavka da jednakost vrijedi, zove se *hipoteza kontinuuma*. Ne znamo ni za jedan skup čiji bi kardinalni broj bio strogo između $\aleph_0$ i $\mathfrak{c}$, ali naravno da to ne znači ništa: možda nismo tražili dovoljno revno, a možda je i dokaz egzistencije nekonstruktivan (kao što je, recimo, primjena aksioma izbora na $\mathscr{P}(\mathbb{R}) \setminus \{\emptyset\}$). Potpuno isto se može reći za injekciju s $\mathfrak{c}$ u $\aleph_1$.

Istina je, pokazalo se, mnogo čudnija — **Paul Cohen** je 1963. tehnikom *forcinga* dokazao da je hipoteza kontinuuma *nezavisna* od ZFC: ako su aksiomi koje smo dosad naveli konzistentni, ona se iz njih ne može dokazati. Već je **Kurt Gödel** 1940. izgradnjom *konstruktibilne hijerarhije* pokazao da je hipoteza kontinuuma *relativno konzistentna* sa ZFC, pa imamo primjer tvrdnje **neodlučive** u ZFC: ili su aksiomi koje smo dosad naveli inkonzistentni pa dokazuju sve i nisu zanimljivi, ili su konzistentni (što imamo razloga vjerovati) i tada ne dokazuju niti hipotezu kontinuuma niti njenu negaciju.

Analogno razmišljanje može se provesti za svaki beskonačni kardinalni broj κ: pretpostavka da je $2^\kappa = \kappa^+$ za svaki takav, zove se *generalizirana hipoteza kontinuuma*. Istim sredstvima se može dokazati da je i ona neodlučiva u ZFC. Štoviše, pokazalo se da se *forcingom* može dokazati neodlučivost raznih tvrdnji o kardinalnim brojevima.

Još jedan veliki uspjeh te metode bio je dokaz da je aksiom izbora neodlučiv u ZF, dakle niti on niti njegova (univerzalno zatvorena) negacija ne slijede iz preostalih aksioma teorije skupova koje smo naveli. To znači da bilo da vjerujemo da aksiom izbora vrijedi u kumulativnoj hijerarhiji ili da vjerujemo da ne vrijedi, to svoje vjerovanje nećemo moći opravdati koristeći isključivo ostale aksiome teorije ZF. Ta situacija je prilično analogna situaciji s petim postulatom (tzv. „aksiom o paralelama") u Euklidovoj formalizaciji geometrije. Više o *forcingu*, konstruktibilnoj hijerarhiji i o još ponekim metodama dokazivanja neodlučivosti možete naći u Čačić, *Nezavisnost i relativna konzistentnost aksioma izbora i hipoteze kontinuuma*.

7.8 Teorem o kvadratu

Za kraj ćemo dokazati veliki rezultat kardinalne aritmetike, da kvadriranje ne mijenja beskonačne kardinalne brojeve. Taj rezultat nije toliko zanimljiv sam po sebi, ali ima važnu posljedicu da su zbrajanje i množenje beskonačnih kardinalnih brojeva u određenom smislu trivijalne operacije i svode se na uspoređivanje.

Propozicija 7.20. *1. Svaki beskonačni skup ima prebrojiv podskup.*

2. Za svaki beskonačni skup a je $a \sim a^+$.

3. Svaki beskonačni kardinalni broj je induktivni skup.

Dokaz. [1]: Neka je a beskonačan. Po teoremu 7.9 postoji injekcija s ω u a ili s a u ω.
U prvom slučaju smo gotovi: slika te injekcije je prebrojiv podskup od a.
U drugom slučaju, po zadatku 5.9, a je prebrojiv, pa je sām svoj prebrojiv podskup.

[2]: Prema (1), a ima prebrojiv podskup; označimo jedan takav s b,
i označimo s f neku bijekciju između ω i b. Nije teško vidjeti da je s

$$g(x) := \begin{cases} f(0), & x = a \\ f\big(f^{-1}(x)+1\big), & x \in b \\ x, & \text{inače} \end{cases} \tag{7.6}$$

zadana bijekcija između a^+ i a. Slikovito, sve elemente od b smo „pomaknuli udesno" i stavili a u tako stvorenu „rupu" — pogledajte priču o Hilbertovom hotelu u Doko, *Teorija skupova (vježbe)*, točka 2.1.1.

[3]: Neka je κ beskonačni kardinalni broj (tada očito nije 0). Zbog zadatka 6.17 je dovoljno dokazati da κ nije sljedbenik. Pretpostavimo suprotno da je $\kappa = \beta^+$ za neki ordinal β.
Prema (2) je tada $\kappa \sim \beta$, a kako je očito $\beta \in \beta^+ = \kappa$, to je u kontradikciji
s pretpostavkom da je κ kardinalni broj. □

Teorem 7.21. *Za svaki beskonačni kardinalni broj κ vrijedi $\kappa^2 = \kappa$.*

Dokaz. Očito je $\kappa \geq \omega > 1$, pa je (monotonost množenja) $\kappa^2 \geq \kappa$, odnosno dovoljno je dokazati $\kappa^2 \leq \kappa$. Pretpostavimo suprotno, i neka je κ baš najmanji protuprimjer (minimum neprazne klase $\{\eta : \eta \geq \omega \wedge \eta \times \eta \not\subseteq \eta\}$ — lako se vidi da to doista jest kardinalni broj). Promotrimo „graf binarne operacije maksimum na κ" (to je skup po aksiomu separacije),

$$M := \{(\alpha, \beta, \gamma) \in \kappa \times \kappa \times \kappa : \alpha < \beta = \gamma \vee \beta \leq \alpha = \gamma\}, \text{ uređen antileksikografski.} \tag{7.7}$$

Očito je $\kappa \times \kappa \sim M$: funkcija zadana s $f(\alpha, \beta) := (\alpha, \beta, \max\{\alpha, \beta\})$ je bijekcija između njih. M je dobro uređen, kao podskup dobro (propozicija 2.15(4)) uređenog skupa $\kappa \times \kappa \times \kappa$. Po teoremu 6.4, ili je $M \simeq \kappa$, ili $M \simeq \delta$ za neki $\delta \in \kappa$, ili $\kappa \simeq p_M(u)$ za neki (jedinstveni) $u = (\alpha, \beta, \gamma) \in M$. Prve dvije mogućnosti možemo zapisati kao $M \simeq \delta \leq \kappa$, što bi značilo $\kappa \times \kappa \sim M \sim \delta \subseteq \kappa$, kontradikcija.

Preostaje treća mogućnost. Zbog $u \in M$ je $\gamma \in \kappa$, dakle po propoziciji 7.20(3) i $\kappa > \gamma^+ \geq \operatorname{card} \gamma^+ =: \lambda$. Antileksikografski je $u = (\alpha, \beta, \gamma) < (\gamma^+, \gamma^+, \gamma^+) =: v \in M$, pa je $\kappa \sim p_M(u) \subseteq p_M(v) =: T$, dakle $\kappa \subseteq T$, pa $\kappa = \operatorname{card} \kappa \leq \operatorname{card} T$. Za svaki $(\alpha', \beta', \gamma') \in T$ vrijedi $\alpha', \beta' \leq \gamma' \leq \gamma^+$, pa je $T \subseteq (\gamma^+)^3$, dakle $\operatorname{card} T \leq \lambda^3$. Sveukupno, imamo $\lambda < \kappa \leq \operatorname{card} T \leq \lambda^3$.

Međutim, κ je najmanji beskonačni kardinalni broj manji od svojeg kvadrata, pa kardinalni broj $\lambda < \kappa$ mora biti ili konačan, ili (veći ili) jednak svom kvadratu. Prvo je očito nemoguće: λ^3 bi tada bio konačan, što je kontradikcija s $\kappa \leq \lambda^3$. No i drugo je nemoguće, jer $\lambda \geq \lambda^2$ bi povlačilo $\lambda \geq \lambda \cdot \lambda \geq \lambda^2 \cdot \lambda = \lambda^3 \geq \kappa > \lambda$. □

Korolar 7.22. *Za svaki beskonačni skup a je $a \times a \sim a$.*

Još davno smo to vidjeli za $\mathbb{N}$ (lema 5.11) i $\mathbb{R}$ (propozicija 5.22), a sada vidimo da je korištenjem aksioma izbora moguće (iako mnogo teže) to dokazati za sve beskonačne skupove.

Propozicija 7.23. *Za svaka dva kardinalna broja κ i λ od kojih je barem jedan beskonačan, njihov zbroj je jednak većem od njih.*
Ako usto nijedan od njih nije nula, njihov umnožak je također jednak većem od njih.

Dokaz. Neka su zadani takvi κ i λ. Prema teoremu 7.9 i propoziciji 7.14(2), oni su usporedivi: bez smanjenja općenitosti neka je $\lambda \leq \kappa$. Kad bi κ bio konačan, postojao bi $n \in \omega$ takav da je $\kappa \sim n$ — no κ je najmanji ordinal u svojoj klasi ekvipotentnosti, pa bismo imali $\lambda \leq \kappa \leq n$, iz čega bi slijedilo da su i λ i κ prirodni brojevi, dakle oba su konačni što znači da ne zadovoljavaju uvjete.

Dakle, κ je beskonačan. Sada koristeći teorem 3.14 (svojstva operacija definiranih na kardinalnostima neovisno o reprezentantima, pa vrijede za kardinalne brojeve) dokažimo niz nejednakosti. Prvo, po usporedivosti, vrijedi $\kappa \geq 2$ (jer bi $\kappa < 2$ značilo da je κ konačan, pa bismo dobili kontradikciju kao u prethodnom odlomku). Također, lako dobijemo $\kappa \cdot \kappa = \kappa^1 \cdot \kappa^1 = \kappa^{1+1} = \kappa^2$, i sasvim analogno $\kappa + \kappa = \kappa \cdot 2$. Sada imamo

$$\kappa = \kappa + 0 \leq \kappa + \lambda \leq \kappa + \kappa = \kappa \cdot 2 \leq \kappa \cdot \kappa = \kappa^2 = \kappa, \tag{7.8}$$

iz čega (CSB) slijedi $\kappa + \lambda = \kappa$. Za umnožak, ako λ nije 0, tada je (opet po usporedivosti) $\lambda \geq 1$. Sada imamo

$$\kappa = \kappa \cdot 1 \leq \kappa \cdot \lambda \leq \kappa \cdot \kappa = \kappa^2 = \kappa, \tag{7.9}$$

iz čega (CSB) slijedi $\kappa \cdot \lambda = \kappa$. □

Zadatak 7.24 (Poopćenje zadatka 5.13)**.** *Dokažite: za svaki beskonačni skup A je $A^* \sim A$.*

Zadatak 7.25. *Dokažite da* $\operatorname{card} A > \operatorname{card} B$ *povlači* $A \cup B \sim A \setminus B \sim A$.

Zadatak 7.26. *Dokažite: za bilo koju konačnu familiju beskonačnih međusobno ekvipotentnih skupova, njihova unija je ekvipotentna sa svakim od njih.*

Bibliografija

Čačić, Vedran. *Nezavisnost i relativna konzistentnost aksioma izbora i hipoteze kontinuuma*. Mag. rad. 2007.

Čačić, Vedran i dr. *Zbirka zadataka iz teorije skupova*. 2023.

Bašić, Bjanka. *Ordinalni kalkulator*. Mag. rad. PMF–MO, rujan 2020.

Doko, Marko. *Kardinalna aritmetika*. Mag. rad. PMF–MO, listopad 2006.

– *Teorija skupova (vježbe)*. Veljača 2010. URL: https://web.math.hr/~mdoko/nastava/teorija_skupova/TS-vjezbe.pdf.

Gogić, Ilja i Mateo Tomašević. *Gelfand–Mazurov teorem i osnovni teorem algebre*. *math.e* 37.3 ().

Gunja, Marin. *Zornova lema i srodne tvrdnje*. Mag. rad. PMF–MO, srpanj 2020.

Hrbáček, K. i T. Jech. *Introduction to Set Theory*. Chapman & Hall/CRC Pure and Applied Mathematics. Taylor & Francis, 1999. ISBN: 9780824779153.

Mardešić, Sibe. *Matematička analiza u n-dimenzionalnom realnom prostoru*. Ur. Krešimir Delinić. 2. izdanje. Manualia Universitatis studiorum Zagrabiensis. Školska knjiga, 1979.

Vuković, Mladen. *O aksiomu izbora, cipelama i čarapama*. *Poučak* 39 (2009).

– *Teorija skupova — predavanja*. PMF–MO, Zagreb, 2015.