

Teorija skupova

Marko Živković

23. siječnja 2026.

Sadržaj

1	Uvod	5
1.1	Teorija skupova u matematici	5
1.2	Jezik teorije skupova - osnove matematičke logike	6
2	Osnovni aksiomi	9
2.1	Aksiom ekstenzionalnosti	9
2.2	Aksiom praznog skupa	9
2.3	Aksiom partitivnog skupa	10
2.4	Aksiom para	10
2.5	Aksiom unije	10
2.6	Shema aksioma separacije	11
2.7	Uređeni par	13
2.8	Kartezijev produkt	13
3	Relacije i funkcije	15
3.1	Relacije	15
3.2	Parcijalni uređaj	16
3.3	Totalni uređaj	17
3.4	Relacije ekvivalencije	18
3.5	Particije	18
3.6	Funkcije	19
4	Prirodni brojevi	21
4.1	Definicija	21
4.2	Uređaj na prirodnim brojevima	23
4.3	Dedekindov teorem rekurzije	24
4.4	Operacije na prirodnim brojevima	27
4.5	Rekurzija s logičkim funkcijama, shema aksioma zamjene	27
5	Odnosi među skupovima	31
5.1	Ekvipotentnost	31
5.2	Konačni skupovi	31
5.3	Cantorov osnovni teorem	33
5.4	Cantor-Schröder-Bernsteinov teorem	34
5.5	Sličnost parcijalno uređenih skupova	35
6	Redni brojevi (ordinali)	37
6.1	Dobro uređeni skupovi	37

6.2	Definicija i uvodna svojstva rednih brojeva	38
6.3	Uređaj na rednim brojevima	39
6.4	Skupovi ordinala	41
6.5	Sljedbenik rednog broja	42
6.6	Teorem enumeracije	43
6.7	Transfinitna indukcija	44
6.8	Transfinitna rekurzija	45
6.9	Operacije na ordinalima	49
7	Aksiom izbora	51
7.1	Iskaz	51
7.2	Funkcija izbora	52
7.3	Zornova lema	52
7.4	Zermelov teorem	54
8	Kardinalni brojevi (kardinali)	57
8.1	Definicija	57
8.2	Operacije na kardinalima	58
8.3	Hijerarhija alefa	59
8.4	Teorem o kvadratu	60
9	Skupovi brojeva	63
9.1	Skup cijelih brojeva	63
9.2	Skup racionalnih brojeva	64
9.3	Skup realnih brojeva	64
9.4	Invarijante sličnosti	65
9.5	Uređajne karakterizacije	66
10	Dobra utemeljenost skupova	71
10.1	Aksiom dobre utemeljenosti	71
10.2	Kumulativna hijerarhija skupova	72

1 Uvod

1.1 Teorija skupova u matematici

Teorija skupova grana je matematike koja se bavi skupovima. Kao što znamo, skupovi se koriste i u svim drugim granama matematike. Intuitivno skup zamišljamo kao apstraktan pojam koji ima elemente i mislimo da je jednostavan za pojmiti.

Ipak, naivno poimanje skupova dovodi do paradoksa, kao što je *Rusellov paradoks* koji slijedi

Paradoks. *Neka je R skup svih skupova koji nisu elementi samih sebe. Formalno to možemo zapisati kao*

$$R := \{x \mid x \notin x\}.$$

Pitamo se je li $R \in R$? Pretpostavimo da je $R \in R$. Budući da je po definiciji R skup svih onih skupova koji nisu u samom sebi, mora biti $R \notin R$. Slično, ako $R \notin R$, onda R , budući da nije element samog sebe, mora biti $\in R$. Dakle, niti jedno nije moguće.

Zbog ovakvih logičkih paradoksa moramo biti oprezniji pri poimanju skupova, tj. ne možemo svaku kolekciju elemenata koju nekako opišemo nazivati skupom. Zato je potrebna teorija skupova, disciplina koja jasno određuje što možemo smatrati skupom, osiguravajući da ne dođe do paradoksa, a opet da skupovi budu dovoljni za potrebe matematike. Utemeljio ju je njemački matematičar Georg Cantor u drugoj polovici 19. stoljeća.

Da se strogo logički definira teorija, nasuprot naivnoj teoriji skupova uvodimo aksiomatsku teoriju skupova. Ubrzo se pokazalo da je teorija skupova vrlo moćna i da se gotovo cijela matematika može utemeljiti na njoj. Zato ova disciplina pripada u temelje matematike. Iako je u principu moguće da elementi skupova budu matematički objekti koji sami nisu skupovi, pokazalo se da to nije potrebno te će svi objekti u ovoj teoriji biti skupovi.

Najpoznatija aksiomska teorija je tzv. *Zermelo–Fraenkel* teorija skupova (sa ili bez aksioma izbora) koju su složili matematičari Ernst Zermelo i Abraham Fraenkel početkom 20. stoljeća. Ovdje ćemo proučavati tu teoriju s uključenim aksiomom izbora.

Iako su skupovi dovoljni za većinu matematike, postoji i šira teorija, tzv. *teorija klasa*. Klasama se smatraju neke kolekcije skupova koje ne mogu biti skupovi. Takve teorije nužne su primjerice za teoriju kategorija. Ipak, ovdje se nećemo baviti klasama.

1.2 Jezik teorije skupova - osnove matematičke logike

Za formalno zapisivanje izraza u teoriji skupova koriste se logički simboli tzv. *logike prvog reda*. To su logičke operacije ($\wedge, \vee, \dots$), varijable, kvantifikatori ($\forall, \exists$), itd. Definirajmo ih formalnije.

- Varijable su *simboli* koji zamjenjuju objekte. Za njih najčešće koristimo velika i mala slova latinične abecede ($x, y, \dots$), ali ponekad koristimo i grčka ili druga slova. Svi logički objekti za nas će biti skupovi.
- Tvrdnje o objektima nazivaju se *formule* ili *logički izrazi*.
- Ako su x i y varijable, izrazi $x \in y$ i $x = y$ su formule, tzv. *atomarne formule*. Izraz $x \in y$ čitamo “ x je element od y ”, a $x = y$ čitamo “ x je jednako y ”.
- Pomoću *logičkih operacija* od jednih formula ϕ i ψ gradimo nove formule. Logičke operacije koje ćemo koristiti su $\neg\phi$ (“nije” ϕ), $\phi \wedge \psi$ (ϕ “i” ψ), $\phi \vee \psi$ (ϕ “ili” ψ), $\phi \rightarrow \psi$ (“iz ϕ slijedi ψ ”, ϕ “implicira” ψ) i $\phi \leftrightarrow \psi$ (ϕ “je ekvivalentno s” ψ , ϕ “ako i samo ako” ψ). Kada su tako složene formule istinite znamo iz prijašnjih kolegija.
- Varijable o kojima logički izraz nešto tvrdi nazivamo *slobodnim varijablama*. Istinitost takvog izraza u biti ovisi o tome koji objekt označava varijabla.
- Ako je ϕ logički izraz tada pomoću *kvantifikatora* gradimo nove izraze $\forall x \phi$ (“za svaki x vrijedi ϕ ”) i $\exists x \phi$ (“postoji x takav da vrijedi ϕ ”). Ako je x bio slobodna varijabla od ϕ on više nije slobodna varijabla od $\forall x \phi$ i $\exists x \phi$ jer izraz u cjelini ne govori o toj varijabli. Takvu varijablu nazivamo *vezana varijabla*.

Ako je potrebno u pisanju koristimo i zagrade. Naveli smo u načelu sve potrebne simbole za zapisivanje izraza. Njihovo je značenje intuitivno poznato. Ipak, u formalnoj logici formalizirani su intuitivno jasni načini zaključivanja. U to ovdje nećemo duboko ulaziti. Spomenimo samo da se koriste *aksiomi jednakosti* koji formaliziraju intuitivno značenje “biti jednak”. Primjerice, za logički izraz $\phi(x)$ koji ima slobodnu varijablu x i nema varijablu y (niti slobodnu niti vezanu) imamo aksiom

$$x = y \rightarrow (\phi(x) \rightarrow \phi(y)) \quad (1.1)$$

gdje je $\phi(y)$ isti taj logički izraz u kojem smo sve pojave varijable x zamijenili s y . Logičke aksiome nećemo navoditi među aksiome skupova nego ćemo ih smatrati jasnim.

Sve možemo zapisati u do sada objašnjenom jeziku. Ipak, za brže i jasnije zapisivanje koristimo neke pokrate. Slijedi vjerojatno nepotpuna lista logičkih pokrata:

- $\neg(x \in y)$ skraćeno pišemo $x \notin y$,
- $\neg(x = y)$ skraćeno pišemo $x \neq y$;

- $\forall x(x \in y \rightarrow \phi)$ skraćeno pišemo $(\forall x \in y)\phi$ i čitamo “za svaki x iz y vrijedi ϕ ”;
- $\exists x(x \in y \wedge \phi)$ skraćeno pišemo $(\exists x \in y)\phi$ i čitamo “postoji x iz y takav da vrijedi ϕ ”;
- $\exists y \forall x(x = y \leftrightarrow \phi)$ gdje y nije slobodna varijabla u ϕ skraćeno pišemo $\exists!x \phi$ i čitamo “postoji jedinstveni x takav da vrijedi ϕ ”.

Nadalje, za bilo koji logički izraz možemo uvesti skraćenu oznaku. Bitno je samo da se u oznaci spomenu sve slobodne varijable. Neke ćemo uvoditi u nastavku, a neke vjerojatno već poznate navedimo:

- $x \subseteq y$ (“ x je podskup od y ”) je pokratak za $\forall z \in x \ z \in y$, što smo već uveli kao pokratu za $\forall z(z \in x \rightarrow z \in y)$;
- $x \subset y$ (“ x je pravi podskup od y ”) je pokratak za $x \subseteq y \wedge x \neq y$;

Konačno, ako za logički izraz ϕ sa slobodnom varijablom y dokažemo $\exists!y \phi$, tom jedinstvenom y -u možemo dati naziv i oznaku koja ovisi o ostalim slobodnim varijablama od ϕ . Primjere ćemo uvoditi u nastavku.

2 Osnovni aksiomi

2.1 Aksiom ekstenzionalnosti

Prvi aksiom koji uvodimo formalizira intuitivnu predodžbu da je skup potpuno određen svojim elementima, tj. ako znamo elemente skupa, znamo sve o njemu.

Aksiom 1 (Aksiom ekstenzionalnosti). *Ako dva skupa imaju iste elemente, oni su jednaki. Formalno*

$$\forall z(z \in x \leftrightarrow z \in y) \rightarrow x = y.$$

Mogli smo uvesti i obostranu implikaciju $\leftrightarrow$ pa da iskaz aksioma izgleda kao definicija jednakosti. To međutim nije potrebno jer suprotna implikacija slijedi iz logičkih aksioma jednakosti, usporedi (1.1).

Aksiom ekstenzionalnosti glavno je oruđe za dokazivanje jednakosti skupova. Za dokazati da su x i y jednaki potrebno je dokazati da imaju iste elemente. To ćemo obično utvrđivati za dva smjera zasebno, tj. utvrdit ćemo da je svaki element od x element i od y , i obrnuto. Formalno, koristit ćemo ekvivalentan iskaz aksioma

$$(\forall z(z \in x \rightarrow z \in y) \wedge \forall z(z \in y \rightarrow z \in x)) \rightarrow x = y.$$

Koristeći pokratu s podskupovima to možemo zapisati kao

$$x \subseteq y \wedge y \subseteq x \rightarrow x = y.$$

2.2 Aksiom praznog skupa

Aksiom 2 (Aksiom praznog skupa). *Postoji skup koji nema elemenata. Formalno*

$$\exists x \forall y y \notin x.$$

Propozicija 2.1. *Skup koji nema elemenata je jedinstven, formalno $\exists! x \forall y y \notin x$.*

Dokaz. Koristimo aksiom ekstenzionalnosti. Pretpostavimo da su x_1 i x_2 dva skupa koji nemaju elemente. Potrebno je dokazati da je za svaki z $z \in x$ ekvivalentno sa $z \in y$. No obje su tvrdnje uvijek netočne, pa time i ekvivalentne. Zato je $x_1 = x_2$. $\square$

Zbog jedinstvenosti tom skupu možemo dati ime i oznaku u sljedećoj definiciji.

Definicija 2.2. *Jedinstveni skup bez elemenata zovemo prazan skup i označavamo $\emptyset$.*

2.3 Aksiom partitivnog skupa

Aksiom 3. Za svaki skup postoji skup njegovih podskupova, tj.

$$\forall x \exists y \forall z (z \in y \leftrightarrow z \subseteq x).$$

Slično kao za prazan skup, dokazat ćemo da je za svaki x takav skup jedinstven i dati mu ime i oznaku. Postupak je već standardan, pa detalje ostavljamo za domaću zadaću.

Propozicija 2.3. Za svaki x skup njegovih podskupova je jedinstven.

Dokaz. D.Z. □

Definicija 2.4. Za skup x skup njegovih podskupova nazivamo partitivni skup od x , u oznaci $\mathcal{P}(x)$.

2.4 Aksiom para

Aksiom 4. Za svaka dva skupa x i y postoji skup kojem su x i y jedini elementi, tj.

$$\forall a \forall b \exists y \forall z (z \in y \leftrightarrow (z = a \vee z = b)).$$

Propozicija 2.5. Za svaka dva skupa x i y skup kojem su x i y jedini elementi jedinstven je.

Dokaz. D.Z. □

Definicija 2.6. Za skupove x i y skup kojem su x i y jedini elementi jedinstven nazivamo (neuređeni) par od x i y , u oznaci $\{x, y\}$.

Ako je $x = y$ taj par zovemo singleton od x , u oznaci $\{x\}$.

Primijetimo da je $\{x, y\} = \{y, x\}$.

2.5 Aksiom unije

Aksiom 5. Za svaki skup x postoji skup kojem su elementi elemenata od x , tj.

$$\forall x \exists y \forall z (z \in y \leftrightarrow (\exists t \in x)(z \in t)).$$

Propozicija 2.7. Za svaki x taj je skup jedinstven.

Dokaz. D.Z. □

Definicija 2.8. Za skup x taj skup nazivamo unija od x , u oznaci $\cup x$.

Ovdje definirana unija jest unija svih elemenata od x . Uniju smo vjerojatno prvi put upoznali kao operaciju dvaju skupova koju sada definiramo kao:

$$x \cup y := \cup\{x, y\}. \quad (2.1)$$

Primijetimo da su za definiranje ove operacije potrebna dva aksioma, aksiom para i aksiom unije.

Aksiomom para mogli smo konstruirati dvočlane skupove. Aksiom unije zajedno s aksiomom para omogućuje nam da konstruiramo i veće skupove:

$$\{a, b, c\} := \cup\{\{a, b\}, \{c\}\},$$

$$\{a, b, c, d\} := \cup\{\{a, b, c\}, \{d\}\} \dots$$

Propozicija 2.9. Za svaki skup x vrijedi $\cup\mathcal{P}(x) = x$.

Dokaz. Dokazujemo dva smjera, da je $x \subseteq \cup\mathcal{P}(x)$ i $x \supseteq \cup\mathcal{P}(x)$. Najprije uzmimo $a \in x$. Treba dokazati da postoji $t \in \mathcal{P}(x)$ takav da je $a \in t$. No možemo uzeti cijeli $x \in \mathcal{P}(x)$ i znamo da je $a \in x$.

Obratno, uzmimo $a \in \cup\mathcal{P}(x)$. To znači da postoji $t \in \mathcal{P}(x)$ takav da je $a \in t$. Po definiciji partitivnog skupa je $t \subseteq x$, pa je $a \in x$. $\square$

2.6 Shema aksioma separacije

U naivnoj teoriji skupova skupove smo željeli definirati svojstvom, tj. logičkim izrazom s jednom slobodnom varijablom koji je ovisno o toj varijabli istinit ili lažan. No takvo nas je razmišljanje dovelo do paradoksa. Ipak, ako se ograničimo na već poznati skup, definiranje njegova podskupa pomoću svojstva ne dovodi do paradoksa, te se uvodi kao aksiom.

Aksiom 6 (Shema aksioma separacije ili Shema aksioma podskupa). Neka je $\phi(x)$ logička formula sa slobodnom varijablom x i bez slobodne varijable b . Tada

$$\forall a \exists b \forall x (x \in b \leftrightarrow (x \in a) \wedge \phi(x)).$$

Navedeno nije jedan aksiom, nego po jedan aksiom za svaku logičku formulu ϕ . Zato kažemo shema aksioma. Nije moguće pisati $\forall \phi$ jer ϕ nije objekt nego formula, a kvantificirati se mogu samo objekti u logici prvog reda.

Propozicija 2.10. Za formulu kao u aksiomu i za svaki a skup b iz aksioma je jedinstven.

Dokaz. D.Z. $\square$

Definicija 2.11. Za formulu $\phi(x)$ kao u aksiomu i za određen a jedinstveni skup b iz aksioma označavamo

$$\{x \in a \mid \phi(x)\}$$

i kažemo da je skup definiran separacijom iz a pomoću svojstva ϕ .

Za postojanje unije trebao nam je poseban aksiom. Za postojanje presjeka to nije potrebno, nego će ono slijediti iz aksioma separacije. Zato ga definiramo.

Definicija 2.12. *Neka je x neprazan skup. Presjek skupa x je skup*

$$\cap x = \{y \mid (\forall t \in x)y \in t\}.$$

Primijetimo da oznaka iz definicije presjeka nije oznaka koju smo definirali u Definiciji 2.11 jer nije naveden skup iz kojega separiramo. Zato ne možemo aksiom separacije direktno primijeniti i garantirati postojanje presjeka, nego to činimo u sljedećoj propoziciji.

Propozicija 2.13. *Presjek skupa x dobro je definiran, tj. postoji skup kojem su elementi točno oni koji zadovoljavaju navedeni uvjet.*

Dokaz. Jer je x neprazan, postoji $a \in x$. Elementi od $\cap x$ moraju biti u svakom elementu od x , pa onda i u a . Zato je

$$\cap x = \{y \in a \mid (\forall t \in x)y \in t\}.$$

Taj skup postoji po aksiomu separacije. □

U nastavku ćemo ponekad definirati skupove na sličan način, tj. koristeći oblik

$$\{\text{oznaka za objekte skupa} \mid \text{uvjet koji objekti moraju zadovoljavati}\}. \quad (2.2)$$

Da bismo mogli takvu oznaku koristiti moramo dokazati da su objekti s lijeva koji zadovoljavaju uvjet s desna sadržani u nekom (većem) skupu, iz čega će aksiom separacije garantirati postojanje definiranog skupa.

Napomena 2.14. *Čim znamo da postoji skup koji sigurno sadrži neke tražene elemente, a možda sadrži i još neke “uljeze”, pomoću aksioma separacije možemo konstruirati skup koji sadrži samo tražene elemente. Zato možemo do sada uvedene aksiome napisati jednostavnije, tako da garantiraju jednu inkluziju. Primjerice, aksiom para ekvivalentan je s*

$$\forall a \forall b \exists y (a \in y \wedge b \in y).$$

U ovoj formulaciji ne znamo sadrži li taj y možda još neke elemente osim a i b . No kakav god taj y bio, pomoću aksioma separacije možemo definirati

$$\{a, b\} := \{x \in y \mid x = a \vee x = b\},$$

i to je isti skup čije nam postojanje garantira originalni aksiom para.

Napomena 2.15. *U tom smislu posebno je zanimljiv aksiom praznog skupa. On je ekvivalentan jednostavnoj tvrdnji*

$$\exists a,$$

jer se prazan skup može konstruirati separacijom iz bilo kojeg skupa bilo kojim svojstvom koje je uvijek netočno, npr.

$$\emptyset = \{x \in a \mid x \neq x\}.$$

Primijetimo pritom da je aksiom praznog skupa jedini među do sada uvedenim aksiomima koji osigurava neovisno postojanje nekog skupa. Bez njega, u bilo kojem od ekvivalentnih oblika, bilo bi moguće da nijedan skup uopće ne postoji.

Aksiom praznog skupa (a i ostale elementarne aksiome) nastaviti ćemo navoditi u originalnom obliku prvenstveno iz pedagoških razloga. Prazan skup prvi je uveden jer je on skup od kojeg u biti konstruiramo sve ostale skupove.

2.7 Uređeni par

Par, tj. skup od dva elementa ne razlikuje koji je prvi, a koji drugi element. Od esencijalne će nam važnosti biti par, označimo ga (x, y) , koji neće biti isto što i (y, x) (za $x \neq y$). To se vjerojatno može postići na više načina, no sljedeći je standardan.

Definicija 2.16. Neka su x i y skupovi. Uređeni par skupova x i y je

$$(x, y) := \{\{x\}, \{x, y\}\}.$$

Idućom propozicijom provjerit ćemo da je to zaista struktura koju želimo. Prvo nam treba jedna lema.

Lema 2.17. Neka su x, y i z skupovi. Ako je $\{x, y\} = \{x, z\}$ onda je $y = z$.

Dokaz. Vrijedi $y \in \{x, y\} = \{x, z\}$, pa je po definiciji para $y = x$ ili $y = z$. U potonjem smo slučaju gotovi, pa nastavimo s pretpostavkom $x = y$. Analogno je $z = x$ ili $z = y$, i opet smo ili gotovi ili nastavimo s pretpostavkom $z = x$. No tada su svi jednaki, pa je također $y = z$. $\square$

Propozicija 2.18. Neka su a, b, c i d skupovi. Ako je $(a, b) = (c, d)$ onda je $a = c$ i $b = d$.

Dokaz. Pretpostavka kaže da je $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. Zato je $\{a\} = \{c\}$ ili $\{a\} = \{c, d\}$. U oba je slučaja $c \in \{a\}$, pa je po definiciji singletona $c = a$.

Sada imamo $\{\{a\}, \{a, b\}\} = \{\{a\}, \{a, d\}\}$. Lema implicira da je $\{a, b\} = \{a, d\}$, pa opet lema implicira da je $b = d$. $\square$

2.8 Kartezijev produkt

Definicija 2.19. Neka su a i b skupovi. Kartezijev produkt skupova a i b , u oznaci $a \times b$, jest skup svih uređenih parova (x, y) gdje je $x \in a$ i $y \in b$, tj.

$$a \times b := \{(x, y) \mid x \in a \wedge y \in b\} \quad (2.3)$$

što je pokrata za

$$\{p \mid (\exists x \in a)(\exists y \in b)p = (x, y)\}. \quad (2.4)$$

U ovoj definiciji ponovno nije naveden skup iz kojeg separiramo. Zato je potrebno provjeriti da takav skup postoji, tj. da je kartezijev produkt dobro definiran. Zato će nam trebati sljedeća lema.

Lema 2.20. *Ako je $x \in a$ i $y \in b$ onda je $(x, y) \in \mathcal{P}(\mathcal{P}(a \cup b))$.*

Dokaz. Iz $x \in a$ slijedi $\{x\} \subseteq a \subseteq a \cup b$, tj. $\{x\} \in \mathcal{P}(a \cup b)$. Slično je $\{x, y\} \subseteq a \cup b$, tj. $\{x, y\} \in \mathcal{P}(a \cup b)$. Zato je $(x, y) = \{\{x\}, \{x, y\}\} \subseteq \mathcal{P}(a \cup b)$, tj. $(x, y) \in \mathcal{P}(\mathcal{P}(a \cup b))$. $\square$

Propozicija 2.21. *Neka su a i b skupovi. Kartezijev produkt $a \times b$ dobro je definiran, tj. postoji skup koji zadovoljava definiciju.*

Dokaz. Iz leme direktno slijedi da je kartezijev produkt jednak

$$a \times b = \{p \in \mathcal{P}(\mathcal{P}(a \cup b)) \mid (\exists x \in a)(\exists y \in b)p = (x, y)\}, \quad (2.5)$$

a taj skup postoji po aksiomu separacije. $\square$

Jednakost (2.5) mogli smo koristiti kao definiciju, te bi iz nje odmah bilo jasno da definiramo nešto što postoji. Međutim tada ne bi odmah bilo jasno da su u tom skupu svi parovi (x, y) za $x \in a$ i $y \in b$, i to bi trebalo naknadno utvrditi. Oba su pristupa dobra.

3 Relacije i funkcije

Relacije i funkcije već su poznate iz prethodnih kolegija, posebno Elementarne matematike. Ovdje ćemo brzo proći kroz formalne definicije i dokaze, s naglaskom na specifičnostima iz perspektive teorije skupova.

3.1 Relacije

Definicija 3.1. Relacija je skup kojem su svi elementi uređeni parovi.

Ako je R relacija, tvrdnju $(x, y) \in R$ možemo zapisivati $x R y$.

Primjer 3.2. Svaki kartezijev produkt $a \times b$ je relacija. Podskup svake relacije je relacija.

Definicija 3.3. Neka su a i b skupovi. Kažemo da je relacija R između a i b ako je $R \subseteq a \times b$. Kažemo da je relacija R na a ako je $R \subseteq a \times a$.

Definicija 3.4. Neka je R relacija. Domena relacije R je

$$\text{dom}(R) := \{x \mid \exists y(x R y)\}. \quad (3.1)$$

Slika relacije R je

$$\text{rng}(R) := \{y \mid \exists x(x R y)\}. \quad (3.2)$$

Propozicija 3.5. Domena i slika dobro su definirane, tj. postoji skup kojem su elementi točno oni koji zadovoljavaju navedeni uvjet.

Dokaz. Ako je $(x, y) = \{\{x\}, \{x, y\}\} \in R$ onda su $\{x\}, \{x, y\} \in \cup R$ pa i $x, y \in \cup \cup R$. Zato domenu i sliku možemo dobiti separacijom iz $\cup \cup R$. $\square$

Napomena 3.6. Svaka relacija je relacija između svoje domene i svoje slike.

Neka je $\phi(x, y)$ logički izraz sa slobodnim varijablama x i y . Relaciju R često ćemo definirati oznakom

$$x R y :\Leftrightarrow \phi(x, y) \quad (3.3)$$

što je pokrata za

$$R := \{(x, y) \mid \phi(x, y)\}. \quad (3.4)$$

Pri tom, naravno, treba provjeriti da se relacija može dobiti separacijom iz nekog skupa.

Definicija 3.7. 1. Neka je R relacija. Inverz relacije R je relacija R^{-1} definirana sa

$$y R^{-1} x :\Leftrightarrow x R y.$$

3 Relacije i funkcije

2. Neka su R i S relacije. Kompozicija relacija R i S je relacija $S \circ R$ definirana sa

$$x(S \circ R)z :\Leftrightarrow \exists y(x R y \wedge y S z).$$

3. Neka je R relacija i c skup (obično je $c \subseteq \text{dom}R$, ali ne mora biti). Restrikcija od R na c je

$$R|_c := R \cap (c \times \text{rng}(R)).$$

Propozicija 3.8. Sve relacije u prethodnoj definiciji dobro su definirane.

Dokaz. D.Z. □

Definicija 3.9. Neka je R relacija.

- R je simetrična ako za svake x, y vrijedi $x R y \rightarrow y R x$.
- R je tranzitivna ako za svake x, y, z vrijedi $x R y \wedge y R z \rightarrow x R z$.
- R je irefleksivna ako ne postoji x takav da je $x R x$.
- Ako je R relacija na a i za svaki $x \in a$ je $x R x$ kažemo da je R refleksivna na a .

3.2 Parcijalni uređaj

Definicija 3.10. Neka je a skup i R relacija na a .

Relacija R je parcijalni uređaj na a ako je irefleksivna i tranzitivna.

Kažemo da je (a, R) parcijalno uređeni skup.

Za parcijalne uređaje obično koristimo notaciju $<, \prec, \triangleleft$ ili sl. Tada za inverznu relaciju obično koristimo simetrične notacije $>, \succ, \triangleright \dots$. Također uvodimo relaciju

$$x \leq y :\Leftrightarrow x < y \vee x = y, \quad (3.5)$$

koje se analogno označavaju $\preceq, \trianglelefteq \dots$ ovisno o oznaci parcijalnog uređaja, te se njihove inverzne relacije označavaju $\geq, \succeq, \trianglerighteq \dots$.

Iako je parcijalno uređeni skup definiran kao uređeni par $(a, <)$ često zlorabljavajući notaciju kažemo da je a parcijalno uređeni skup ako je jasno o kojem se uređaju radi na njemu.

Neka je $(a, <)$ parcijalno uređeni skup i $b \subseteq a$. Tada je $(b, < \cap b \times b)$ parcijalno uređeni skup. Ponovno zlorabljavajući notaciju taj parcijalno uređeni skup često označavamo s $(b, <)$. Čim spominjemo podskup parcijalno uređenog skupa promatrat ćemo ga kao parcijalno uređeni skup s ovako definiranim uređajem.

Definicija 3.11. Neka je $(a, <)$ parcijalno uređeni skup i $b \subseteq a$;

- $x \in a$ je minimalan (maksimalan) ako ne postoji $y \in a$ takav da je $y < x$ ($y > x$);

- $x \in a$ je najmanji element (najveći element) ako za svaki $y \in a$ vrijedi $x \leq y$ ($x \geq y$);
- $x \in a$ je donja međa (gornja međa) od b ako za svaki $y \in b$ vrijedi $x \leq y$ ($x \geq y$);
- $x \in a$ je supremum (infimum) od b ako je najmanja gornja (najveća donja) međa od b .

Propozicija 3.12. Neka je $(a, <)$ parcijalno uređeni skup.

Najmanji i najveći element u a , ako postoje, jedinstveni su.

Najmanji element je minimalan. Najveći element je maksimalan.

Dokaz. D.Z. □

Primjer 3.13. Neka je a skup i neka je

$$\subset_a := \{(x, y) \in \mathcal{P}(a) \times \mathcal{P}(a) \mid x \subset y\}$$

relacija na $\mathcal{P}(a)$. Lako se pokaže da je $(\mathcal{P}(a), \subset_a)$ parcijalno uređeni skup.

Primijetimo da je $\subset_a$ relacija, dok je $\subset$ logički izraz, no za $x, y \in \mathcal{P}(a)$ su $x \subset_a y$ i $x \subset y$ ekvivalentni. Zato zloupotrebljavajući notaciju parcijalno uređeni skup često označavamo $(\mathcal{P}(a), \subset)$.

U njemu je najmanji i jedini minimalni element $\emptyset$, a najveći i jedini maksimalni element a . Supremum skupa $b \subseteq \mathcal{P}(a)$ je $\cup b$. Infimum nepraznog $b \subseteq \mathcal{P}(a)$ je $\cap b$, dok je infimum od $\emptyset$ jednak a .

3.3 Totalni uređaj

Definicija 3.14. Neka je $(a, <)$ parcijalno uređeni skup.

Elemente x i y iz a zovemo neusporedivi ako nije $x < y$ niti $x > y$ niti $x = y$.

Ako ne postoje neusporedivi elementi u a kažemo da je uređaj $<$ totalan i da je $(a, <)$ totalno uređeni skup.

Propozicija 3.15. U totalno uređenom skupu pojmovi minimalnog (maksimalnog) i najmanjeg (najvećeg) elementa su ekvivalentni.

Dokaz. Nakon Propozicije 3.12 dovoljno je dokazati da je svaki minimalan (maksimalan) element najmanji (najveći). D.Z. □

Minimalan, odnosno najmanji element u totalno uređenom skupu $(a, <)$ označavamo $\min a$. Maksimalan, odnosno najveći element označavamo $\max a$.

Definicija 3.16. Totalno uređeni skup $(a, <)$ je dobro uređen ako svaki neprazan $b \subseteq a$ ima najmanji element.

3.4 Relacije ekvivalencije

Definicija 3.17. Neka je a skup i $\sim$ relacija na a .

Relacija $\sim$ je relacija ekvivalencije na a ako je refleksivna na a , simetrična i tranzitivna.

Lema 3.18. Neka je $\sim$ simetrična i tranzitivna relacija.

Tada postoji jedinstveni skup a takav da je $\sim$ relacija ekvivalencije na a .

Dokaz. Tvrdimo da je $a := \text{dom}(\sim)$ takav skup. Zaista, ako je $x \in \text{dom}(\sim)$ tada postoji y takav da je $x \sim y$. Zbog simetričnosti je $y \sim x$, a zatim zbog tranzitivnosti $x \sim x$. Stoga je $\sim$ refleksivna na $\text{dom}(\sim)$.

Skup na kojem je relacija refleksivna općenito je jedinstven jer je jednak $\{x \mid x \sim x\}$. $\square$

Definicija 3.19. Neka je a skup i R relacija ekvivalencije na a .

Klasa ekvivalencije od $x \in a$ s obzirom na R je

$$[x]_R := \{y \in A \mid x R y\}.$$

Pišemo i $[x]$ ako je relacija poznata.

Kvocijentni skup skupa a po relaciji R je skup svih klasa ekvivalencije:

$$a/R := \{[x]_R \in \mathcal{P}(a) \mid x \in a\}.$$

Propozicija 3.20. Neka je a skup, $\sim$ relacija ekvivalencije na a te $x, y \in a$. Tada je

1. $x \sim y$ ako i samo ako je $[x] = [y]$;
2. $x \not\sim y$ ako i samo ako je $[x] \cap [y] = \emptyset$.

Dokaz. D.Z. $\square$

3.5 Particije

Definicija 3.21. Neka su a i P skupovi. P je particija od a ako

- $\emptyset \notin P$;
- $\cup P = a$;
- za svake $x, y \in P$ je $x = y$ ili $x \cap y = \emptyset$.

Korolar 3.22. Neka je a skup i $\sim$ relacija ekvivalencije na a . Tada je kvocijentni skup $a/\sim$ particija od a .

Dokaz. D.Z. $\square$

Neka je P particija na a definirajmo relaciju $\tilde{P}$ kao

$$x \tilde{P} y :\Leftrightarrow \exists b \in P (\{x, y\} \subseteq b). \quad (3.6)$$

Propozicija 3.23. *Neka je a skup.*

1. *Za svaku particiju P od a $\tilde{P}$ je relacija ekvivalencije.*
2. *Za svaku particiju P od a ta particija jednaka je kvocijentnom skupu od $\tilde{P}$, tj. $P = a/\tilde{P}$.*
3. *Za svaku relaciju ekvivalencije $\sim$ na a vrijedi $\sim = \widetilde{a/\sim}$.*

Dokaz. D.Z. □

Zbog prethodne propozicije svaka relacija ekvivalencije na a ima pridruženu particiju na a , i svejedno je što od toga dvojice zadržamo.

3.6 Funkcije

Prisjetimo se da se funkcija standardno definira kao uređena trojka (f, a, b) gdje je a domena, b kodomena i f “pravilo preslikavanja” između a i b . Ovdje će nam funkcija biti samo f .

Definicija 3.24. *Relacija f je funkcija ako za svake x, y_1 i y_2 vrijedi $x f y_1 \wedge x f y_2 \rightarrow y_1 = y_2$, tj. svaki x je u relaciji f s najviše jednim elementom.*

Domenu funkcije ne treba posebno definirati jer je definirana za svaku relaciju. Kodomena nećemo formalno definirati, ali ćemo koristiti sljedeću notaciju.

Definicija 3.25. *Ako je f funkcija, $a = \text{dom}(f)$ i $b \supseteq \text{rng}(f)$ možemo zapisivati*

$$f : a \rightarrow b.$$

Skup b u ovoj notaciji možemo zvati kodomena. Primijetimo da kodomena nije jednoznačno određena, svaki nadskup od slike može se koristiti kao kodomena.

Definicija 3.26. *Funkcija f je injekcija ako je njen inverz f^{-1} funkcija.*

Funkcija $f : a \rightarrow b$ je surjekcija na b ako je $b = \text{rng}(f)$.

Funkcija $f : a \rightarrow b$ je bijekcija između a i b ako je injekcija i surjekcija na b .

Primijetimo da je svaka funkcija surjekcija na svoju sliku. Svaka injekcija je bijekcija između svoje domene i svoje slike.

Neka je $f : a \rightarrow b$. Budući da za svaki $x \in a$ postoji jedinstveni $y \in b$ takav da je $x f y$, za taj jedinstveni y uvodimo oznaku $f(x)$.

Primjer 3.27. *Neka je a skup. Tada je*

$$\text{id}_a := \{(x, x) \in a \times a \mid x \in a\} \tag{3.7}$$

funkcija. Zovemo je identiteta na a . Vrijedi $\text{id}_a : a \rightarrow a$, i ona je bijekcija između a i a .

Inverz i kompozicija već su definirani za svaku relaciju. Koristimo ih i kod funkcija.

3 Relacije i funkcije

- Propozicija 3.28.** 1. Ako je f funkcija, restrikcija $f|_c$ također je funkcija. Ako je $f : a \rightarrow b$ i $c \subseteq a$, tada je $f|_c : c \rightarrow b$.
2. Kompozicija funkcija je funkcija. Kompozicija injekcija je injekcija. Ako je $f : a \rightarrow b$ i $g : b \rightarrow c$, tada je $g \circ f : a \rightarrow c$.
3. Ako je f bijekcija između a i b , f^{-1} je bijekcija između b i a .
4. Ako je f bijekcija između a i b te g bijekcija između b i c , onda je $g \circ f$ bijekcija između a i c .

Dokaz. D.Z. □

Propozicija 3.29. Neka je $f : a \rightarrow b$. Funkcija f je bijekcija između a i b ako i samo ako postoji funkcija $g : b \rightarrow a$ takva da je $g \circ f = \text{id}_a$ i $f \circ g = \text{id}_b$.

Dokaz. D.Z. □

Neka su a i b skupovi. Skup svih funkcija $f : a \rightarrow b$ označavamo s

$${}^A B = B^A = \{f \in \mathcal{P}(a \times b) \mid f : a \rightarrow b\}. \quad (3.8)$$

4 Prirodni brojevi

Prirodne brojeve intuitivno poznajemo od početaka učenja matematike. Ipak, ovdje ih želimo strogo definirati, odnosno navesti njihova svojstva. Vjerojatno su nam poznati Peanovi aksiomi, to su posebni aksiomi koji aksiomatski opisuju prirodne brojeve. Ipak, teorija skupova je opća teorija u kojoj definiramo prirodne brojeve, bez posebnih aksioma samo za njih.

4.1 Definicija

U principu se prirodni brojevi mogu definirati na više načina, no u teoriji skupova jedan je standardan. Ideja je da svakako želimo da prirodan broj n bude neki skup s n elemenata. Stoga je za nulu jedini mogući izbor

$$0 := \emptyset. \quad (4.1)$$

Nastavljamo dalje s definicijom.

Definicija 4.1. *Neka je a skup. Sljedbenik od a je*

$$a^+ := a \cup \{a\}.$$

Definirajmo nekoliko brojeva koji slijede.

$$1 := 0^+ = \{\emptyset\}, \quad (4.2)$$

$$2 := 1^+ = \{0, 1\} = \{\emptyset, \{\emptyset\}\}, \quad (4.3)$$

$$3 := 2^+ = \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \dots \quad (4.4)$$

Definicija 4.2. *Skup I je induktivan ako*

- $\emptyset \in I$,
- za svaki $x \in I$ je $x^+ \in I$.

Aksiom 7 (Aksiom beskonačnosti). *Postoji induktivan skup, tj.*

$$\exists I(\emptyset \in I \wedge (\forall x \in I)(x \cup \{x\} \in I)).$$

Osnovni aksiomi garantiraju postojanje samo konačnih skupova. Ovo je prvi aksiom koji garantira postojanje skupa koji ne može biti konačan (kasnije ćemo formalno definirati pojam konačnosti). Zato se ovaj aksiom zove aksiom beskonačnosti.

Definicija 4.3. Skup prirodnih brojeva je skup

$$\omega := \{n \mid \forall \text{ induktivan } I(n \in I)\}.$$

Skup n je prirodan broj ako je element od ω , tj. ako je element svakog induktivnog skupa.

Propozicija 4.4. Skup prirodnih brojeva dobro je definiran.

Dokaz. Aksiom beskonačnosti implicira da postoji induktivan skup, nazovimo ga s J . Prirodni brojevi moraju biti elementi svakog induktivnog skupa, pa su i elementi od J . Zato ω možemo odrediti separacijom iz J :

$$\omega := \{n \in J \mid \forall \text{ induktivan } I(n \in I)\}.$$

Taj skup postoji zbog aksioma separacije. □

Propozicija 4.5. 1. Skup prirodnih brojeva ω je induktivan.

2. Ako je I induktivan, onda je $\omega \subseteq I$.

Dokaz. D.Z. □

Teorem 4.6 (Princip matematičke indukcije). Neka je $\phi(n)$ svojstvo, tj. logički izraz sa slobodnom varijablom n takav da vrijedi

- $\phi(0)$,
- $\phi(a) \rightarrow \phi(a^+)$.

Tada je za svaki $n \in \omega$ $\phi(n)$.

Dokaz. Neka je

$$S := \{a \in \omega \mid \phi(a)\}.$$

Znamo da je $0 \in \omega$ i $\phi(0)$, pa je $0 \in S$. Ako je $a \in S$ onda je $a \in \omega$ i $\phi(a)$. Jer je ω induktivan slijedi da je $a^+ \in \omega$, a tvrdnja iz teorema implicira da je $\phi(a^+)$, dakle $a^+ \in S$. Zbog toga je S induktivan, dakle $\omega \subseteq S$. Tj. svaki $n \in \omega$ je u S , pa za njega vrijedi $\phi(n)$. □

Kao što imamo shemu aksioma separacije, a ne jedan aksiom, tako je i prethodni teorem zapravo shema teorema, po jedan teorem za svaki logički izraz.

Princip matematičke indukcije često ćemo koristiti u nastavku. Upotrebljavamo standardne nazive: dokaz da je $\phi(0)$ nazivamo *bazom indukcije*, pretpostavku $\phi(a)$ nazivamo *pretpostavkom indukcije*, a dokaz kojim iz pretpostavke indukcije izvodimo $\phi(a^+)$ nazivamo *korakom indukcije*. Ponekad ćemo u dokazima preskočiti izričito navođenje pretpostavke indukcije ako je ona jasna.

4.2 Uređaj na prirodnim brojevima

Propozicija 4.7. Ako je $a \in b \in \omega$ onda je $a \in \omega$.

Dokaz. Dokažimo indukcijom po b .

Baza: $b = 0$. Tada nije moguće da je $a \in 0 = \emptyset$, pa je implikacije uvijek točna.

Pretpostavka: za svaki $a \in b$ vrijedi $a \in \omega$.

Korak: neka je $a \in b^+ = b \cup \{b\}$. Imamo dva slučaja: $a \in b$ ili $a = b$. U prvom slučaju pretpostavka indukcije implicira da je $a \in \omega$, a u drugom znamo da je $b \in \omega$. $\square$

Definicija 4.8. Na ω definiramo relaciju

$$a < b :\Leftrightarrow a \in b.$$

Lema 4.9. 1. Za svaki $n \in \omega$ je $0 \leq n$;

2. za svake $k, n \in \omega$ je $k < n^+$ ekvivalentno s $k < n \vee k = n$;

3. za svaki $n \in \omega$ je $n < n^+$.

Dokaz. TODO $\square$

Propozicija 4.10. Relacija $<$ je parcijalni uređaj, tj. $(\omega, <)$ je parcijalno uređeni skup.

Dokaz. TODO $\square$

Lema 4.11. Sljedbenik čuva uređaj, tj. za svake $k, n \in \omega$ $k < n$ povlači $k^+ < n^+$.

Dokaz. TODO $\square$

Propozicija 4.12. Relacija $<$ je totalni uređaj, tj. $(\omega, <)$ je totalno uređeni skup.

Dokaz. TODO $\square$

Propozicija 4.13. Za svake $a, b \in \omega$ $a < b$ ekvivalentno je s $a \subset b$.

Dokaz. TODO $\square$

Teorem 4.14 (Princip jake matematičke indukcije). Neka je $\phi(n)$ logički izraz sa slobodnom varijablom n takav da za svaki $n \in \omega$ vrijedi

$$((\forall k < n) \phi(k)) \rightarrow \phi(n).$$

Tada je za svaki $n \in \omega$ $\phi(n)$.

Dokaz. TODO $\square$

Propozicija 4.15. Totalno uređeni skup $(\omega, <)$ je dobro uređen.

Dokaz. TODO $\square$

4.3 Dedekindov teorem rekurzije

Definicija 4.16. Niz je funkcija kojemu je domena prirodan broj ili ω . Ako mu je domena ω zovemo ga beskonačni niz, a ako mu je domena prirodan broj n zovemo ga konačni niz ili uređena n -torka.

Za niz f vrijednost $f(n)$ često zapisujemo f_n .

Konačni niz f s domenom n možemo zapisivati $f = (f_0, f_1, \dots, f_n)$. Ponekad i beskonačni niz zapisujemo $f = (f_0, f_1, \dots)$.

Neka je $k \in \omega$, $n > k$ ili $n = \omega$ te $f : n \rightarrow S$ niz. Tada je restrikcija $f|_k : k \rightarrow S$ također niz.

Za skup t označimo s

$$t^* := \bigcup_{n \in \omega} {}^n t = \cup \{x \in \mathcal{P}(\omega \times t) \mid \exists n \in \omega (x \in {}^n t)\} \quad (4.5)$$

skup svih konačnih nizova na t .

Napomena 4.17. Prvi član unije, ${}^0 t$, jest skup svih funkcija s praznog skupa u t , tj.

$${}^0 t = \{f \subseteq \emptyset \times t \mid \forall x \in \emptyset \exists! y (x f y)\}.$$

Kako prazan skup nema članove uvjet $\forall x \in \emptyset \dots$ uvijek je zadovoljen. Zato je

$${}^0 t = \mathcal{P}(\emptyset \times t) = \mathcal{P}(\emptyset) = \{\emptyset\}.$$

Dakle postoji jedna funkcija kojoj je domena $\emptyset$ i ona je $\emptyset$.

Primjer 4.18. Fibonaccijev niz je niz f definiran sa

- $f_0 = 0$,
- $f_1 = 1$,
- $f_{n+2} = f_{n+1} + f_n$.

Intuitivno nam se čini da je ovo dovoljno za definirati cijeli niz $f : \omega \rightarrow \omega$. To će biti formalno dokazano u sljedećem teoremu.

Teorem 4.19 (Dedekindov teorem jake rekurzije). Neka je t skup i $F : t^* \rightarrow t$. Tada postoji jedinstvena funkcija $g : \omega \rightarrow t$ takva da je za svaki $n \in \omega$

$$g(n) = F(g|_n).$$

Dokaz. Potrebno je dokazati da postoji jedinstvena funkcija koja nešto zadovoljava. U konkretnom slučaju možemo definirati skup svih funkcija koje to zadovoljavaju:

$$G_\omega := \{g \in {}^\omega t \mid (\forall k \in \omega) g(k) = F(g|_k)\} \quad (4.6)$$

i onda treba dokazati da G_ω sadrži točno jedan element.

Za sada imamo oruđe za tvrdnje o prirodnim brojevima, ne baš cijelom ω . Zato ćemo prvo analizirati analogne skupove za prirodne brojeve. Za $n \in \omega$ definirajmo

$$G_n := \{g \in {}^n t \mid (\forall k < n) g(k) = F(g|_k)\}. \quad (4.7)$$

Očekujemo da će G_n također biti jednočlani. Dokažimo što možemo o njima.

Tvrdnja 1. *Za svaki $n \in \omega$ skup G_n je neprazan.*

Dokaz. Dokazujemo indukcijom po n .

Baza: $G_0 = \{g \in {}^0 t \mid (\forall k < 0) \dots\} = {}^0 t = \{\emptyset\} \neq \emptyset$.

Pretpostavka: $G_n \neq \emptyset$, tj. postoji funkcija $g_n: n \rightarrow t$ takva da za svaki $k < n$ vrijedi $g_n(k) = F(g_n|_k)$.

Korak: Definirajmo $g_{n^+}: n^+ \rightarrow t$ sa

$$g_{n^+}(k) = \begin{cases} g_n(k) & k < n \\ F(g_n) & k = n. \end{cases}$$

Provjerimo da je $g_{n^+} \in G_{n^+}$, tj. da $(\forall k < n^+) g_{n^+}(k) = F(g_{n^+}|_k)$. Za $k < n$ vrijedi

$$g_{n^+}(k) = g_n(k) = F(g_n|_k) = F(g_{n^+}|_k),$$

a za $k = n$ direktno po konstrukciji vrijedi

$$g_{n^+}(k) = F(g_n) = F(g_{n^+}|_n).$$

□

Sljedeću ćemo tvrdnju odmah proširiti i na G_ω jer je dokaz isti.

Tvrdnja 2. *Za svaki $n \in \omega$ i za $n = \omega$ skup G_n ima najviše jedan element.*

Dokaz. Pretpostavimo suprotno, da postoje različiti $g, g' \in G_n$. Neka je

$$k := \min\{m \in \omega \mid g(m) \neq g'(m)\}$$

najmanji prirodan broj u kojem se funkcije razlikuju. Tada je za svaki $m < k$ $g(m) = g'(m)$, tj. $g|_k = g'|_k$, pa je

$$g(k) = F(g|_k) = F(g'|_k) = g'(k),$$

što proturječi izboru k .

□

Sada znamo da za svaki $n \in \omega$ G_n sadrži točno jedan element. Nazovimo ga g_n .

Tvrdnja 3. *Za svake $m, n \in \omega$, $m < n$, vrijedi $g_n|_m = g_m$.*

Dokaz. Dovoljno je dokazati da je $g_n|_m \in G_m$. Provjerimo uvjet za $k < m$:

$$g_n|_m(k) = g_n(k) = F(g_n|_k) = F(g_n|_m|_k).$$

□

4 Prirodni brojevi

Definirajmo

$$g := \bigcup_{n \in \omega} g_n = \{(k, x) \in \omega \times t \mid (\exists n \in \omega) (k, x) \in g_n\}, \quad (4.8)$$

i tvrdimo da je g traženi element od G_ω .

Tvrdnja 4. Skup g je funkcija.

Dokaz. Pretpostavimo da su $(k, x_1), (k, x_2) \in g$. Tada po definiciji unije postoje $n, m \in \omega$ takvi da je $(k, x_1) \in g_n$ i $(k, x_2) \in g_m$. Mora vrijediti $k < n$ i $k < m$. Bez smanjenja općenitosti možemo pretpostaviti da je $n \leq m$. Zato je

$$(k, x_2) \in g_m|_n = g_n$$

zbog Tvrdnje 3. Kako su oba $(k, x_1), (k, x_2) \in g_n$, a g_n je funkcija, vrijedi $x_1 = x_2$, što je i trebalo dokazati. $\square$

Tvrdnja 5. Domena funkcije g je ω .

Dokaz. Domene svih funkcija g_n su $\subseteq \omega$, pa je i $\text{dom}(g) \subseteq \omega$.

Obratno, neka je $k \in \omega$. Vrijedi $k \in k^+ = \text{dom}(g_{k^+})$. Zato postoji x takav da je $(k, x) \in g_{k^+} \subseteq g$. Dakle $k \in \text{dom}(g)$. $\square$

Tvrdnja 6. Za svaki $n \in \omega$ $g|_n = g_n$.

Dokaz. Za dokazati jednakost dvaju funkcija s domenom n treba dokazati da su jednake za svaki $k \in n$:

$$g_n(k) = x \Leftrightarrow (k, x) \in g_n \Rightarrow (k, x) \in g \Leftrightarrow g(k) = x.$$

$\square$

Tvrdnja 7. Vrijedi $g \in G_\omega$, tj. za svaki $k \in \omega$ $g(k) = F(g|k)$.

Dokaz. Vrijedi

$$g(k) = g|_{k^+}(k) \stackrel{\text{Tv. 6}}{=} g_{k^+}(k) = F(g_{k^+}|_k) \stackrel{\text{Tv. 3}}{=} F(g_k) \stackrel{\text{Tv. 6}}{=} F(g|_k).$$

$\square$

Dakle G_ω sadrži neku funkciju, a zbog Tvrdnje 2. ta je funkcija jedinstvena, što je i trebalo dokazati. $\square$

Kod jake rekurzije, analogno jakoj indukciji, sljedeći član niza ovisi o svim vrijednostima do tada. U praksi će često biti potrebna samo vrijednost neposrednog prethodnika. Taj poseban slučaj navodimo u posebnom teoremu.

Teorem 4.20 (Primitivna rekurzija). *Neka je t skup, $s \in t$ i $F: t \rightarrow t$. Tada postoji jedinstvena funkcija $g: \omega \rightarrow t$ takva da*

- $g(0) = s$,
- $\forall n \in \omega \ g(n^+) = F(g(n))$.

Dokaz. TODO $\square$

4.4 Operacije na prirodnim brojevima

TODO

4.5 Rekurzija s logičkim funkcijama, shema aksioma zamjene

Pokušajmo definirati funkciju rekurzivno s

- $g(0) = \emptyset$,
- $g(n^+) = \{g(n)\}$.

Problem je što Teorem 4.20 zahtijeva da zadamo funkciju $F: t \rightarrow t$, dakle moramo unaprijed znati kodomenu t tražene funkcije g . U ovom primjeru

$$x \mapsto \{x\}$$

nije funkcije jer je preopćenito zadana, domena bi joj bila svi skupovi.

Zato želimo jači teorem rekurzije, neki u kojem će biti dovoljno zadati izraze koji će od jednog skupa jedinstveno definirati drugi, iako nisu funkcije. Prvo definirajmo takve izraze.

Definicija 4.21. Logički izraz $P(x, y)$ sa slobodnim varijablama x i y takav da $\forall x \exists! y P(x, y)$ nazivamo logička funkcija.

Primjer 4.22.

- $y = \{x\}$, tj. $\forall t (t \in y \leftrightarrow t = x)$,
- $y = x^+$, tj. $\forall t (t \in y \leftrightarrow t \in x \vee t = x)$.

Budući da kod logičkog izraza $P(x, y)$ svaki x jednoznačno definira y , taj y možemo označavati s $P(x)$.

Takav P sam ne definira funkciju jer je određen za svaki x . Možemo pokušati konstruirati funkciju ako ga “restringiramo” na neki skup A kao:

$$\{(x, P(x)) \mid x \in A\}. \quad (4.9)$$

Međutim niti to ne mora postojati ako ne znamo u kojem su skupu $P(x)$. Dosadašnji aksiomi nedovoljni su da dokažemo postojanje takvog skupa općenito. Zato uvodimo novi aksiom, točnije shemu aksioma.

Aksiom 8 (Shema aksioma zamjene). Za logičku funkciju $P(x, y)$ vrijedi $\forall A \exists B \forall x \in A P(x) \in B$.

Formalnije, za logički izraz $P(x, y)$ sa slobodnim varijablama x i y i bez slobodnih varijabli A i B vrijedi

$$\forall A (\forall x \in A \exists! y P(x, y) \rightarrow \exists B \forall y (\exists x \in A P(x, y) \leftrightarrow y \in B))$$

To nije jedan aksiom nego shema aksioma zato što imamo po jedan aksiom za svaki izraz $P(x, y)$, slično kao kod aksioma separacije.

U formalnom iskazu aksioma zaobišli smo definiciju logičke funkcije tako što smo uveli uvjet $\forall x \in A \exists! y P(x, y)$. Ako taj uvjet nije zadovoljen aksiom je trivijalno istinit.

Aksiom nam dozvoljava da definiramo funkcije kao u (4.9), točnije za logičku funkciju $P(x, y)$ i skup A definiramo

$$f = \{(x, y) \in A \times B \mid P(x, y)\} \quad (4.10)$$

gdje je B skup čije nam postojanje utvrđuje instanica aksioma zamjene s izrazom $P(x, y)$. Jasno je da je f funkcija.

Iznesimo sada jaču verziju teorema rekurzije.

Teorem 4.23 (Jaka rekurzija s logičkom funkcijom). *Neka je $F(x, y)$ logička funkcija. Tada postoji jedinstvena funkcija g na ω takva da je za svaki $n \in \omega$*

$$g(n) = F(g|_n),$$

tj. vrijedi $F(g(n), g|_n)$.

Primijetimo da je Teorem jake rekurzije s logičkom funkcijom shema teorema, po jedan teorem za svaku logičku funkciju.

Dokaz. Kopiramo dokaz Dedekindovog teorema rekurzije, imajući u vidu da ne možemo konstruirati skupove G_ω i G_n . Umjesto s tim skupovima, baratat ćemo s logičkim svojstvima. Pokazat će se da nije problem što ne znamo čine li objekti s tim svojstvom skup.

Neka je $G_\omega(g)$ logički izraz koji kaže

$$G_\omega(g) := g \text{ je funkcija} \wedge \text{dom}(g) = \omega \wedge (\forall k \in \omega) g(k) = F(g|_k). \quad (4.11)$$

Primijetimo da je jedino što fali ovom logičkom izrazu da bi definirao skup G_ω iz dokaza Teorema 4.19 tvrdnja $\text{rng}(g) \subseteq t$. Pokazat će se da ona nije bitna.

Za dokazati teorem trebamo dokazati da postoji jedinstveni g takav da je $G_\omega(g)$.

Nadalje, neka je $G(n, g)$ logički izraz koji kaže

$$G(n, g) := n \in \omega \wedge g \text{ je funkcija} \wedge \text{dom}(g) = n \wedge (\forall k \in n) g(k) = F(g|_k). \quad (4.12)$$

Tvrdnja 1. *Za svaki $n \in \omega$ postoji g takav da vrijedi $G(n, g)$.*

Dokaz. Dokazujemo indukcijom po n .

Baza: Provjerimo da vrijedi $G(0, \emptyset)$.

Pretpostavka: Postoji g_n takav da vrijedi $G(n, g_n)$.

Korak: Definirajmo $g_{n^+} : n^+ \rightarrow t$ sa

$$g_{n^+}(k) = \begin{cases} g_n(k) & k < n \\ F(g_n) & k = n. \end{cases}$$

Provjerimo da vrijedi $G(n^+, g_{n^+})$. □

Tvrdnja 2. 1. Za svaki $n \in \omega$ i za svake g, g' ako vrijedi $G(n, g)$ i $G(n, g')$ onda je $g = g'$.

2. Za svake g, g' ako vrijedi $G_\omega(g)$ i $G_\omega(g')$ onda je $g = g'$.

Dokaz. 1. Pretpostavimo suprotno, da postoje različiti g, g' takvi da je $G(n, g)$ i $G(n, g')$. Posebno, vrijedi da su g i g' funkcije s domenom n pa za $m \in n$ možemo koristiti notacije $g(m)$ i $g'(m)$. Neka je

$$k := \min\{m \in n \mid g(m) \neq g'(m)\}$$

najmanji prirodan broj u kojem se funkcije razlikuju. Tada je za svaki $m < k$ $g(m) = g'(m)$, tj. $g|_k = g'|_k$, pa $G(n, g)$ i $G(n, g')$ impliciraju

$$g(k) = F(g|_k) = F(g'|_k) = g'(k),$$

što proturječi izboru k .

2. Analogno kao 1. □

Tvrdnje 1. i 2. 1. povlače da za svaki $n \in \omega$ postoji jedinstveni g takav da vrijedi $G(n, g)$. Instanca aksioma zamjene za $G(n, g)$ tada implicira da postoji skup

$$S := \{g \mid (\exists n \in \omega) G(n, g)\}. \quad (4.13)$$

Ovo je ključan korak koji ne bismo mogli napraviti bez aksioma zamjene.

Za $n \in \omega$ pripadni g za koji vrijedi $G(n, g)$ nazovimo g_n .

Tvrdnja 3. Za svake $m, n \in \omega$, $m < n$, vrijedi $g_n|_m = g_m$.

Dokaz. Dovoljno je provjeriti da vrijedi $G(m, g_n|_m)$, pa jedinstvenost (Tvrdnja 2. 1.) povlači tvrdnju. □

Definirajmo

$$g := \cup S = \bigcup_{n \in \omega} g_n = \{(k, x) \mid (\exists n \in \omega) (k, x) \in g_n\}. \quad (4.14)$$

Tvrdnja 4. Skup g je funkcija.

Dokaz. Isto kao dokaz Tvrdnje 4 u dokazu Teorema 4.19. □

Tvrdnja 5. Domena funkcije g je ω .

Dokaz. Isto kao dokaz Tvrdnje 5 u dokazu Teorema 4.19. □

Tvrdnja 6. Za svaki $n \in \omega$ $g|_n = g_n$.

Dokaz. Isto kao dokaz Tvrdnje 6 u dokazu Teorema 4.19. □

Tvrdnja 7. Vrijedi $G_\omega(g)$.

4 Prirodni brojevi

Dokaz. Prve dvije tvrdnje iz $G_\omega(g)$ su Tvrdnja 4 i Tvrdnja 5, a za posljednju uzmimo $k \in \omega$ pa vrijedi

$$g(k) = g|_{k^+}(k) \stackrel{\text{Tv. 6}}{=} g_{k^+}(k) = F(g_{k^+}|_k) \stackrel{\text{Tv. 3}}{=} F(g_k) \stackrel{\text{Tv. 6}}{=} F(g|_k).$$

□

Dakle postoji g takav da vrijedi $G_\omega(g)$, a zbog Tvrdnje 2.2. taj je g jedinstven, što je i trebalo dokazati. □

Teorem 4.24 (Primitivna rekurzija s logičkom funkcijom). *Neka je $P(x, y)$ logička funkcija i neka je s skup. Tada postoji jedinstvena funkcija g na ω takva da je*

- $g(0) = s$,
- $\forall n \in \omega \ g(n^+) = P(g(n), g(n^+))$, tj. vrijedi $P(g(n), g(n^+))$.

Dokaz. D.Z. □

Primjer 4.25 (Uvod u ordinale). *Definirajmo funkciju s*

- $g(0) = \omega$,
- $g(n^+) = g(n)^+$.

Ta funkcija zadovoljava:

$$g(0) = \omega, \quad g(1) = \omega^+, \quad g(2) = \omega^{++}, \dots$$

Slika od g je

$$\text{rng}(g) = \{\omega, \omega^+, \omega^{++}, \dots\}.$$

U nastavku će biti zanimljiv skup

$$\omega \cup \text{rng}(g) = \{0, 1, 2, \dots, \omega, \omega^+, \omega^{++}, \dots\}.$$

Za nekoliko poglavlja definirat ćemo redne brojeve (ordinale) i vidjeti da su ω , ω^+ , ω^{++} i $\omega \cup \text{rng}(g)$ ordinali. Postojanje potonjeg skupa ne bi bilo moguće utvrditi bez aksioma zamjene.

5 Odnosi među skupovima

5.1 Ekvipotentnost

Definicija 5.1. Skupovi a i b su ekvipotentni, u oznaci $a \sim b$, ako postoji bijekcija $f : a \rightarrow b$.

Intuitivno, ekvipotentne skupove zamišljamo kao skupove koji imaju “jednak broj elemenata” ili su “jednako veliki”.

Propozicija 5.2. 1. Za svaki skup a vrijedi $a \sim a$.

2. Za svake skupove a, b ako je $a \sim b$ onda je i $b \sim a$.

3. Za svake skupove a, b, c ako je $a \sim b$ i $b \sim c$ onda je i $a \sim c$.

Dokaz. 1. Identiteta $\text{id}_a = \{(x, x) \in a \times a\}$ tražena je bijekcija.

2. $a \sim b$ implicira da postoji bijekcija $f : a \rightarrow b$. Po Propoziciji 3.28 3. je i $f^{-1} : b \rightarrow a$ bijekcija, pa je $b \sim a$.

3. $a \sim b$ i $b \sim c$ implicira da postoje bijekcije $f : a \rightarrow b$ i $g : b \rightarrow c$. Kompozicija $g \circ f : a \rightarrow c$ je bijekcija po Propoziciji 3.28 4. pa je $a \sim c$.

□

Svojstva iz propozicije slična svojstvima relacija refleksivnost, simetričnost i tranzitivnost. Ipak $\sim$ nije relacija jer nije skup. No “restrikcijom” na bilo koji skup A :

$$\{(x, y) \in A \times A \mid x \sim y\}$$

dobijamo stvarnu relaciju koja je refleksivna, simetrična i tranzitivna, dakle relacija ekvivalencije.

5.2 Konačni skupovi

Definicija 5.3. Skup a je konačan ako postoji $n \in \omega$ $n \sim a$.

Skup a je beskonačan ako nije konačan.

Lema 5.4. Za svaki $n \in \omega$ svaka injekcija $f : n \rightarrow n$ je i surjekcija.

5 Odnosi među skupovima

Dokaz. Dokazujemo indukcijom po n .

Baza: Slika svake funkcije $0 \rightarrow 0$ je podskup od $0 = \emptyset$, pa mora biti jednaka cijelom $\emptyset$, dakle f je surjekcija.

Pretpostavimo da je svaka injekcija $n \rightarrow n$ surjekcija i neka je $f : n^+ \rightarrow n^+$ injekcija. Pretpostavimo da ona nije surjekcija, tj. da postoji $\text{rng}(f) \neq n^+$. Imamo dva slučaja:

- I. $n \notin \text{rng}(f)$: Tada je $f : n^+ \rightarrow n$. Restrikcija $f|_n : n \rightarrow n$ ponovno je injekcija. Kada bi $f(n)$ bio u slici $\text{rng}(f|_n)$, postojao bi neki $k < n$ takav da je $f|_n(k) = f(k) = f(n)$ pa f ne bi bila injekcija. Dakle $f|_n$ nije surjekcija što proturječi pretpostavci indukcije.
- II. $n \in \text{rng}(f)$: Tada postoji neki drugi $k < n$, $k \notin \text{rng}(f)$. Neka je $l \in n^+$ takav da $f(l) = n$. Definirajmo funkciju $g : n \rightarrow n$ s

$$g(i) = \begin{cases} f(i) & i \neq l \\ k & i = l. \end{cases}$$

Posebno, ako je $k = l$ onda $g = f|_n$. Lako se provjeri da je g dobro definirana i da je injekcija. Analogno kao u prethodnom slučaju dokažemo da $f(n) \notin \text{rng}(g)$. Dakle g nije surjekcija što proturječi pretpostavci indukcije.

□

Teorem 5.5. 1. Neka su $n, m \in \omega$. Tada $n \sim m$ implicira $n = m$.

2. Za svaki konačan skup S postoji jedinstveni $n \in \omega$ takav da je $S \sim n$.
3. Za svaki konačan skup S svaka injekcija $f : S \rightarrow S$ je i surjekcija.
4. Skup ω je beskonačan.

Dokaz. 1. Pretpostavimo suprotno, tj. da postoji bijekcija $f : m \rightarrow n$, i da $n \neq m$. Bez smanjenja općenitosti možemo pretpostaviti da je $n < m$. Restrikcija $f|_n : n \rightarrow n$ je injekcija. Restrikcijom smo izbacili par $(n, f(n))$ iz funkcije, pa $f(n) \notin \text{rng}(f|_n)$. Dakle $f|_n$ nije surjekcija, što proturječi prethodnoj lemi.

2. Postojanje je definicija konačnosti. Jedinstvenost slijedi iz prethodne točke i Propozicije 5.2.
3. Jasno iz prethodne točke i Leme 5.4.
4. Pretpostavimo suprotno, tj. da postoji $n \in \omega$ i bijekcija $f : \omega \rightarrow n$. Dokaz se nastavlja identično kao u točki 1.

□

Zbog točke 2. prethodnog teorema možemo definirati kako slijedi.

Definicija 5.6. Neka je S konačan skup i $S \sim n$ za $n \in \omega$. Kažemo da je n kardinalni broj od S i zapisujemo $n = |S|$ ili $n = \aleph(S)$.

Za beskonačne skupove još uvijek ne možemo definirati kardinalni broj, iako možemo neformalno zapisivati $\aleph(A) = \aleph(B)$ misleći $A \sim B$.

Propozicija 5.7. *Neka je A konačan skup i $B \subseteq A$. Tada je B također konačan i $|B| \leq |A|$.*

Dokaz. Dokazujemo indukcijom po $|A|$.

Baza: Za $|A| = 0$ mora biti $A = \emptyset$, pa je i $B = \emptyset$, dakle konačan i $|B| = 0$.

Pretpostavka: Pretpostavimo da je za svaki konačan skup A takav da je $|A| = n$ i za svaki $B \subseteq A$ taj B također konačan i $|B| \leq n$.

Korak: Uzmimo proizvoljan A' takav da je $|A'| = n^+$ i $B' \subseteq A'$. Postoji bijekcija $f : n^+ \rightarrow A'$. Neka je $A := \text{rng}(f|_n)$, pa je $f|_n : n \rightarrow A$ bijekcija, dakle $|A| = n$. Imamo dva slučaja:

- I. $f(n) \in B'$: Neka je $B := B' \setminus \{f(n)\}$. Jasno je $B \subseteq A$, pa je po pretpostavci indukcije konačan i $m := |B| \leq n$. Uzmimo bijekciju $g : m \rightarrow B$ i definirajmo $h : m^+ \rightarrow B'$ sa

$$h(x) = \begin{cases} g(x) & x < m \\ f(n) & x = m. \end{cases}$$

Lako se pokaže da je h bijekcija. Dakle B' je konačan i $|B'| = m^+ \leq n^+$.

- II. $f(n) \notin B'$: Tada je $B' \subseteq A$, pa je po pretpostavci indukcije konačan i $|B'| \leq n < n^+$.

□

Primjer 5.8. *Neka je $f : \omega \rightarrow \omega$, $f(n) = n^+$. Funkcija f je injekcija, ali nije surjekcija jer $0 \notin \text{rng} f$. Dakle pravi podskup $\text{rng} f = \omega \setminus \{0\} \subset \omega$ ekvipotentan je s ω . To ne bi bilo moguće za konačne skupove zbog Teorema 5.5 točke 3.*

5.3 Cantorov osnovni teorem

Teorem 5.9 (Cantorov osnovni teorem). *Neka je a skup. Skup a i njegov partitivni skup $\mathcal{P}(a)$ nisu ekvipotentni.*

Dokaz. Pretpostavimo suprotno, da postoji bijekcija $g : a \rightarrow \mathcal{P}(a)$. Definirajmo

$$b := \{x \in a \mid x \notin g(x)\}. \quad (5.1)$$

Kako je f surjekcija na $\mathcal{P}(a)$ postoji $r \in a$ takav da je $b = f(r)$.

Je li $r \in b$? Kad bi bio, bio bi $r \in f(r)$, pa po definiciji od b vrijedi $r \notin b$. U suprotnom, ako $r \notin b = f(r)$ po definiciji od b treba biti $r \in b$. Kontradikcija. □

Uočimo sličnost navedenog dokaza s Russelovim paradoksom. Ta se ideja naziva *dijagonalni postupak* i koristi se na više mjesta u matematici.

Tvrđnja teorema intuitivno je poznata za konačne skupove. Mogli smo pomisliti da su svi beskonačni skupovi ekvipotentni jer “imaju jednako elemenata - beskonačno”, no Cantorov osnovni teorem implicira da nisu. Npr. ω i $\mathcal{P}(\omega)$ nisu ekvipotentni.

5.4 Cantor-Schröder-Bernsteinov teorem

Intuitivno shvaćamo da podskup ima “manje ili jednako” elemenata od nadskupa, ili je “manji ili jednako velik” kao nadskup. Od ideje da pravi podskup bude strogo manji od pravog nadskupa morali smo odustati jer to ne mora vrijedi za beskonačne skupove (Primjer 5.8).

Injekcija $f : B \rightarrow A$ je bijekcija na $\text{rng}(f) \subseteq A$, pa je B “manji ili jednako velik” kao A . Ako istovremeno postoji injekcija $A \rightarrow B$ je “manji ili jednako velik” kao B , dakle “jednako su veliki”. Postoji li zaista bijekcija među njima? Sljedeći teorem daje očekivan potvrđan odgovor, iako je dokaz možda neočekivano kompleksan.

Za $f : a \rightarrow b$ označimo s $f^\rightarrow : \mathcal{P}(a) \rightarrow \mathcal{P}(b)$ funkciju definiranu s

$$f^\rightarrow(c) := \text{rng}(f|_c) = \{y \in b \mid \exists x \in c, y = f(x)\}.$$

Teorem 5.10 (Cantor-Schröder-Bernstein). *Neka su A i B skupovi takvi da postoje injekcije $f : A \rightarrow B$ i $g : B \rightarrow A$. Tada su A i B ekvipotentni.*

Dokaz. Cilj je konstruirati bijekciju $h : A \rightarrow B$ koristeći poznate injekcije f i g , točnije neke ćemo elemente skupova A i B spariti pomoću f , a neke pomoću g . Elemente od

$$C_1 := A \setminus \text{rng}(g) = A \setminus g^\rightarrow(B)$$

moramo spariti pomoću f jer g^{-1} na njima nije definiran. Dakle želimo da je $h|_{C_1}(x) = f(x)$. Nakon toga želimo definirati ostatak bijekcije između ostataka skupova, dakle između $A \setminus C_1$ i $B \setminus f^\rightarrow(C_1)$. Sada je kodomena manja, pa analogno zaključujemo da elemente od

$$C_2 := A \setminus g^\rightarrow(B \setminus f^\rightarrow(C_1))$$

moramo spariti pomoću f . Isto će se zaključivanje nastavljati i dalje.

Dakle, formalno, rekursivno pomoću Teorema 4.20 definiramo niz $C : \omega \rightarrow \mathcal{P}(A)$ sa

- $C_0 = \emptyset$,
- $C_{n+1} = F(C_n)$

gdje je $F(x) := A \setminus g^\rightarrow(B \setminus f^\rightarrow(x))$. Neka je $C := \bigcup_{n \in \omega} C_n$. Sada definirajmo $h : A \rightarrow B$ sa

$$h(x) = \begin{cases} f(x) & x \in C \\ g^{-1}(x) & x \notin C. \end{cases}$$

Ako je $x \notin C \supseteq C_1 = A \setminus \text{rng}(g)$ onda je $x \in \text{rng}(g)$, tj. $g^{-1}(x)$ je dobro definiran, pa je h dobro definirana. Dokažimo da je h bijekcija između A i B .

Pretpostavimo da h nije injekcija, tj. da postoje različiti $x, y \in A$ takvi da je $h(x) = h(y)$. Ako su oba iz C moraju biti jednaki jer je f injekcija. Ako su oba iz $A \setminus C$ također moraju biti jednaki jer je g^{-1} injekcija. Zato bez smanjenja općenitosti možemo pretpostaviti da je $x \in C$ i $y \notin C$ i onda imamo $f(x) = g^{-1}(y)$, tj. $g(f(x)) = y$. $x \in C$ znači da postoji $n \in \omega$ takav da je $x \in C_n$. Iz toga slijedi da je $f(x) \in f^\rightarrow(C_n)$, tj. $f(x) \notin B \setminus f^\rightarrow(C_n)$. Budući da je

g injekcija slijedi da $y = g(f(x)) \notin g^{-1}(B \setminus f^{-1}(C_n))$, tj. $y \in A \setminus g^{-1}(B \setminus f^{-1}(C_n)) = C_{n+1} \subseteq C$. To proturječi pretpostavci da $y \notin C$, dakle h je injekcija.

Pretpostavimo da h nije surjekcija, tj. da postoji $y \in B$ koji nije u slici od h . Kad $g(y)$ ne bi bio u C , onda bi bilo $h(g(y)) = g^{-1}(g(y)) = y$, što bi proturječilo pretpostavci da y nije u slici od h . Dakle $g(y) \in C$, tj. postoji $n \in \omega$ takav da je $g(y) \in C_n$. C_0 je prazan, pa je $n > 0$ i neka je $n - 1$ njegov prethodnik. Sada $g(y) \in C_n = A \setminus g^{-1}(B \setminus f^{-1}(C_{n-1}))$ implicira da $y \notin B \setminus f^{-1}(C_{n-1})$, tj. $y \in f^{-1}(C_{n-1})$. Dakle $y = f(x)$ za neki $x \in C_{n-1} \subseteq C$, pa je i $h(x) = y$. $\square$

Napomena 5.11. Primijetimo da smo u dokazu Cantor-Schröder-Bernsteinovog teorema koristili znanja o prirodnim brojevima, pa konkretno i aksiom beskonačnosti. Intuitivno bismo pomislili da taj aksiom ne bi trebao biti potreban za ovaj teorem. Zaista, postoji dokaz Cantor-Schröder-Bernsteinovog teorema koji ne ovisi o aksiomu beskonačnosti. Ideja je da se rekursivna definicija od C pomoću $C_{n+1} = F(C_n)$ zamijeni unijom $C := \bigcup \{a \subseteq A \mid a \subseteq F(a)\}$.

5.5 Sličnost parcijalno uređenih skupova

Definicija 5.12. Neka su $(a, <)$ i $(b, \triangleleft)$ parcijalno uređeni skupovi i $f : a \rightarrow b$.

Kažemo da f čuva uređaj ako za svake $x, y \in a$, $x < y$ povlači $f(x) \triangleleft f(y)$.

Funkcija f je sličnost između a i b ako je bijekcija između a i b , čuva uređaj i f^{-1} čuva uređaj.

Ako postoji sličnost između a i b kažemo da su a i b slični i pišemo $(a, <) \simeq (b, \triangleleft)$.

Sljedeća propozicija analogna je Propoziciji 5.2.

Propozicija 5.13. 1. Za svaki parcijalno uređeni skup $(a, <)$ vrijedi $(a, <) \simeq (a, <)$.

2. Za svake parcijalno uređene skupove $(a, <), (b, <)$ ako je $(a, <) \simeq (b, <)$ onda je i $(b, <) \simeq (a, <)$.

3. Za svake parcijalno uređene skupove $(a, <), (b, <), (c, <)$ ako je $(a, <) \simeq (b, <)$ i $(b, <) \simeq (c, <)$ onda je i $(a, <) \simeq (c, <)$.

Dokaz. D.Z. $\square$

Propozicija 5.14. Neka su $(a, <)$ i $(b, \triangleleft)$ totalno uređeni skupovi i neka je $f : a \rightarrow b$ bijekcija između a i b koja čuva uređaj. Tada je f sličnost.

Dokaz. Samo treba dokazati da f^{-1} čuva uređaj. Neka su $y_1, y_2 \in b$, $y_1 < y_2$. Jer je f bijekcija postoje $x_1, x_2 \in a$ takvi da je $f(x_1) = y_1$, $f(x_2) = y_2$. Jer je $(a, <)$ totalno uređen x_1 i x_2 su usporedivi, a jer f čuva uređaj jedini mogući odnos je $x_1 < x_2$, što je trebalo dokazati. $\square$

Definicija 5.15. Neka je $(a, <)$ parcijalno uređen skup i $x \in a$.

(Otvoreni) početni komad od x u a je

$$p_a(x) := \{y \in a \mid y < x\}. \quad (5.2)$$

Zatvoreni početni komad od x u a je

$$\bar{p}_a(x) := \{y \in a \mid y \leq x\}. \quad (5.3)$$

Neka su $x, y \in a$, $x < y$. Tada je početni komad od x u a istovremeno početni komad i u početnom komadu $p_a(y)$, tj.

$$p_a(x) = p_{p_a(y)}(x). \quad (5.4)$$

Propozicija 5.16. Neka su $(a, <)$ i $(b, \triangleleft)$ parcijalno uređeni skupovi, $f : a \rightarrow b$ sličnost i $x \in A$. Tada je restrikcija $f|_{p_a(x)}$ sličnost između $p_a(x)$ i $p_b(f(x))$.

Dokaz. Ako funkcija čuva uređaj, čuva i njena restrikcija. Isto tako restrikcija injekcije je injekcija pa je jedino potrebno dokazati da je $f|_{p_a(x)}$ surjekcija na $p_b(f(x))$. Uzmimo $y \in p_b(f(x))$, tj. $y < f(x)$. Jer je f bijekcija postoji $x' \in a$ takav da je $y = f(x')$, a jer čuva uređaj mora biti $x' < x$, dakle $x' \in p_a(x)$. Stoga je y zaista u slici restrikcije na $p_a(x)$. $\square$

Teorem 5.17. Za svaki parcijalno uređen skup $(a, <)$ postoji $A \subset \mathcal{P}(a)$ takav da je $(a, <) \simeq (A, \subset)$.

Dokaz. Tvrdimo da je funkcija $\bar{p}_a : a \rightarrow \text{rng}(\bar{p}_a)$ koja svakom $x \in a$ pridružuje zatvoreni početni komad tražena sličnost. Ona je po definiciji surjekcija na $A := \text{rng}(\bar{p}_a)$. Uvijek je $x \in \bar{p}_a(x)$ pa $\emptyset \notin A$ što povlači $A \neq \mathcal{P}(a)$.

Pretpostavimo da je $\bar{p}_a(x) = \bar{p}_a(y)$. Zato je $x \in \bar{p}_a(y)$, tj. $x \leq y$. Analogno je $y \leq x$, pa je $x = y$. Dakle, $\bar{p}_a$ je injekcija, pa i bijekcija između a i A .

Ako je $x < y$ tranzitivnost povlači da za svaki $z \leq x$ vrijedi $z \leq y$, tj. $\bar{p}_a(x) \subseteq \bar{p}_a(y)$. Zbog injektivnosti ne mogu biti jednaki, pa je $\bar{p}_a(x) \subset \bar{p}_a(y)$. Dakle $\bar{p}_a$ čuva uređaj.

Sada Propozicija 5.14 implicira da je $\bar{p}_a$ sličnost. $\square$

6 Redni brojevi (ordinali)

6.1 Dobro uređeni skupovi

Prisjetimo se da je totalno uređeni skup $(A, <)$ dobro uređen ako svaki neprazan $B \subseteq A$ ima najmanji element, Definicija 3.16.

Lema 6.1. *Neka je $(A, <)$ dobro uređen skup i neka $f : A \rightarrow A$ čuva uređaj. Tada za svaki $x \in A$ vrijedi $f(x) \geq x$.*

Dokaz. Pretpostavimo suprotno, da postoji $x \in A$ takav da je $f(x) < x$. Neka je S skup svih takvih. Budući da je $(A, <)$ dobro uređen S ima najmanji element, pa neka je upravo x najmanji u S . Kako f čuva uređaj vrijedi $f(f(x)) < f(x)$, dakle $f(x) \in S$. To proturječi pretpostavci da je x najmanji u S . $\square$

Napomena 6.2. *Tehnika “najmanjeg protuprimjera” korištena u ovom dokazu standardna je tehnika dokazivanja kod dobro uređenih skupova. Ako želimo dokazati da nešto vrijedi za svaki element dobro uređenog skupa, možemo pretpostaviti suprotno i uzeti upravo najmanji koji to ne zadovoljava i dovesti do kontradikcije.*

Propozicija 6.3. 1. *Niti jedan dobro uređen skup nije sličan svom početnom komadu.*
2. *Identiteta je jedina sličnost dobro uređenog skupa sa samim sobom.*
3. *Ako su dobro uređeni skupovi slični, postoji jedinstvena sličnost između njih.*

Dokaz. 1. Pretpostavimo suprotno, da postoji x element dobro uređenog skupa A takav da postoji sličnost $f : A \rightarrow p_A(x)$. Tada je $f(x) \in p_A(x)$, dakle $f(x) < x$. Sličnost čuva uređaj, pa to proturječi Lemi 6.1.

2. Neka je $f : A \rightarrow A$ sličnost za dobro uređen A i neka je $x \in A$ proizvoljan. Sličnost f čuva uređaj pa Lema 6.1 implicira da je $f(x) \geq x$. Jednako tako f^{-1} čuva uređaj, pa ista lema implicira da je $x = f^{-1}(f(x)) \geq f(x)$, dakle $x = f(x)$.

3. Kad bi postojale dvije različite sličnosti $f, g : A \rightarrow B$, tada bi $g^{-1} \circ f$ bila sličnost $A \rightarrow A$ različita od identitete, protivno točki 2. $\square$

Teorem 6.4. *Za svaka dva dobro uređena skupa A i B vrijedi točno jedno od sljedećeg:*

- *A i B su slični,*
- *A je sličan početnom komadu u B , ili*

6 Redni brojevi (ordinali)

- B je sličan početnom komadu u A .

U potonja dva slučaja početni je komad jedinstven.

Dokaz. Definirajmo relaciju

$$f := \{(x, y) \in A \times B \mid p_A(x) \simeq p_B(y)\}.$$

Dokažimo da je f funkcija. Pretpostavimo da sa za različite $y_1, y_2 \in B$ $(x, y_1), (x, y_2) \in f$. Tada je $p_B(y_1) \simeq p_A(x) \simeq p_B(y_2)$. Bez smanjenja općenitosti možemo pretpostaviti da je $y_1 < y_2$, pa je početni komad $p_B(y_1)$ ujedno i početni komad u $p_B(y_2)$. Dakle $p_B(y_2)$ je sličan svom početnom komadu, što proturječi Propoziciji 6.3 1.

Analogno se dokazuje da je f^{-1} funkcija, tj. da je f injekcija. Dakle f je bijekcija između svoje domene i svoje slike.

Neka su $x_1, x_2 \in \text{dom}(f)$, $x_1 < x_2$. Po definiciji od f postoji sličnost između $p_A(x_2)$ i $p_B(f(x_2))$. Po Propoziciji 5.16 restrikcija te sličnosti na $p_A(x_1)$ je sličnost između $p_A(x_1)$ i nekog $p_{p_B(f(x_2))}(y_1) = p_B(y_1)$. Jer je f funkcija znamo da je $y_1 = f(x_1)$, no sada znamo da je $f(x_1) = y_1 < f(x_2)$. Dakle f čuva uređaj. Propozicija 5.14 implicira da je f sličnost između svoje domene i svoje slike.

Dokažimo da je $\text{dom}(f)$ ili cijeli A ili početni komad u A . Ako nije cijeli A neka je x najmanji element u $A \setminus \text{dom}(f)$. Dakle, svaki element manji od x je u domeni, tj. $p_A(x) \subseteq \text{dom}(f)$. Pretpostavimo da postoji $x' \in \text{dom}(f)$, $x' > x$. Dakle postoji sličnost između $p_A(x')$ i nekog $p_B(y')$. Tada Propozicija 5.16 implicira da je restrikcija te sličnosti na x sličnost između $p_A(x)$ i nekog $p_B(y)$. Zato je po definiciji od f $(x, y) \in f$, dakle $x \in \text{dom}(f)$. To proturječi izboru od x . Dakle zaista ne postoji $x' \in \text{dom}(f)$ takav da je $x' > x$, zbog čega je $\text{dom}(f) = p_A(x)$.

Analogno se dokazuje da je $\text{rng}(f)$ ili cijeli B ili početni komad u B .

Tvrdimo da je $\text{dom}(f) = A$ ili $\text{rng}(f) = B$. Pretpostavimo suprotno, tj. da postoje $x \in A$ i $y \in B$ takvi da je $\text{dom}(f) = p_A(x)$ i $\text{rng}(f) = p_B(y)$. No tada je sam f sličnost između početnih komada $p_A(x)$ i $p_B(y)$ pa po definiciji od f vrijedi $(x, y) \in f$, što proturječi pretpostavci.

Preostaju dakle točno tri tražene mogućnosti, f je sličnost između A i B , ili između A i početnog komada u B ili između početnog komada u A i B . Još treba provjeriti da nije moguća istovremeno još jedna opcija pomoću neke druge sličnosti. No u svakom od slučajeva višestrukih opcija skup bi bio sličan nekog svom početnom komadu, što proturječi Propoziciji 6.3 1.

Konačno, kad u potonja dva slučaja početni komad ne bi bio jedinstven, opet bismo dobili sličnost između većeg početnog komada i manjeg, koji je njegov početni komad, protivno Propoziciji 6.3 1. $\square$

6.2 Definicija i uvodna svojstva rednih brojeva

Definicija 6.5. Skup α je tranzitivan ako za svake x, y za koje je $x \in y \in \alpha$ vrijedi $x \in \alpha$.

Ekvivalentno, skup α je tranzitivan ako za svaki $x \in \alpha$ je $x \subseteq \alpha$.

Za skup S neka je

$$\in_S := \{(x, y) \in S \times S \mid x \in y\}. \quad (6.1)$$

Primijetimo da je $\in$ logička izjava s dvije varijable, dok je $\in_S$ relacija. Ipak, ako znamo da su oba $x, y \in S$ tada je $x \in y$ ekvivalentno s $x \in_S y$.

Definicija 6.6. Skup α je redni broj ili ordinal ako je tranzitivan i dobro uređen uređajem $\in_\alpha$.

Ordinale obično označavamo malim grčkim slovima.

Primjer 6.7. Provjerite da su $\emptyset$, $1 = \{\emptyset\}$ i $2 = \{\emptyset, \{\emptyset\}\}$ ordinali.

Propozicija 6.8. Za svaki redni broj α vrijedi $\alpha \notin \alpha$.

Dokaz. Pretpostavimo da je $\alpha \in \alpha$. Tada je α kao element u relaciji $\in_\alpha$ sa samim sobom, tj. $\alpha \in_\alpha \alpha$. To proturječi irefleksivnosti uređaja $\in_\alpha$. $\square$

Propozicija 6.9. Svaki element ordinala je ordinal.

Dokaz. Neka je α ordinal i $\beta \in \alpha$.

Uzmimo $x \in y \in \beta$. Jer je α tranzitivan $y \in \beta \in \alpha$ implicira $y \in \alpha$, a potom $x \in y \in \alpha$ implicira $x \in \alpha$. Dakle sva tri x, y, β su $\in \alpha$, pa $x \in y \in \beta$ implicira relacije $x \in_\alpha y \in_\alpha \beta$. Ta relacija je totalni uređaj na ordinalu α , pa njena tranzitivnost implicira $x \in_\alpha \beta$, odnosno $x \in \beta$. Dakle β je tranzitivan.

Jer je α ordinal $\beta \in \alpha$ implicira $\beta \subseteq \alpha$, pa je $\in_\beta$ restrikcija od $\in_\alpha$. Restrikcija dobrog uređaja je dobar uređaj. Dakle β je ordinal. $\square$

6.3 Uređaj na rednim brojevima

Definicija 6.10. Za redne brojeve α i β kažemo da je α manji od β i pišemo $\alpha < \beta$ ako je $\alpha \in \beta$. Sa $\alpha \leq \beta$ označavamo $\alpha < \beta$ ili $\alpha = \beta$.

Napomena 6.11. Oznaka $<$ nije relacija nego tek nova oznaka za već postojeću oznaku $\in$. Ipak, čim uvodimo ovakvu oznaku i terminologiju “manji od” očekivat ćemo da se ponašaju kao uređaj.

Zaista, zbog Propozicije 6.9 svaki ordinal je skup ordinala koji je po definiciji uređen upravo uređajem $\in$. To će vrijediti i za druge skupove ordinala kako ćemo vidjeti u nastavku.

Propozicija 6.12. Neka su α i β ordinali. Tada je

1. $\alpha \subset \beta$ ako i samo ako $\alpha < \beta$;
2. $\alpha \subseteq \beta$ ako i samo ako $\alpha \leq \beta$.

6 Redni brojevi (ordinali)

Dokaz. 1. Ako je $\alpha \in \beta$ tranzitivnost od β implicira $\alpha \subseteq \beta$. Propozicija 6.8 implicira da je $\alpha \neq \beta$ pa je $\alpha \subset \beta$.

Obratno, ako je $\alpha \subset \beta$ onda je $\beta \setminus \alpha$ neprazan podskup od β pa ima najmanji element γ u uređaju $\in_\beta$. Dakle, svaki $\delta < \gamma$ nije u tom skupu pa je u α . Drugim riječima, za svaki $\delta \in \gamma$ vrijedi $\delta \in \alpha$, tj. $\gamma \subseteq \alpha$.

Uzmimo $\delta \in \alpha \subset \beta$. Oba γ i δ su u β , pa su usporediva uređajem $\in_\beta$. Nije moguće da je $\delta = \gamma$ jer $\gamma \notin \alpha$. Nije moguće niti da je $\gamma \in \delta$ jer bi onda tranzitivnost od ordinala α također implicirala $\gamma \in \alpha$. Dakle vrijedi $\delta \in \gamma$. Zato je $\alpha \subseteq \gamma$, pa i $\alpha = \gamma \in \beta$.

2. Jasno iz 1. □

Lema 6.13. *Ako su α i β ordinali, $\alpha \cap \beta$ je također ordinal.*

Dokaz. Neka je $x \in y \in \alpha \cap \beta \subseteq \alpha$. Zato je $x \in \alpha$. Analogno je $x \in \beta$, pa je $x \in \alpha \cap \beta$, dakle $\alpha \cap \beta$ je tranzitivan.

Restrikcija dobrog uređaja je dobar uređaj. Dakle $\alpha \cap \beta$ je ordinal. □

Propozicija 6.14. *Za svaka dva redna broja α i β vrijedi točno jedno od sljedećeg: ili $\alpha < \beta$ ili $\alpha = \beta$ ili $\alpha > \beta$.*

Dokaz. Lema 6.13 implicira da je $\alpha \cap \beta$ ordinal. Ako je $\alpha \cap \beta = \alpha$ onda je $\alpha \subseteq \beta$ pa Propozicija 6.12 implicira $\alpha \leq \beta$.

Ako je $\alpha \cap \beta = \beta$ analogno je $\beta \leq \alpha$.

U preostalom slučaju je $\alpha \cap \beta \subset \alpha$ i $\alpha \cap \beta \subset \beta$, pa Propozicija 6.12 implicira da je $\alpha \cap \beta \in \alpha$ i $\alpha \cap \beta \in \beta$, dakle $\alpha \cap \beta \in \alpha \cap \beta$, a to proturječi Propoziciji 6.8.

Lako se vidi da ne može vrijediti više tvrdnji istovremeno zbog Propozicije 6.8. □

Korolar 6.15. *Neka je S skup ordinala. Tada je $\in_S$ totalni uređaj na S .*

Dokaz. TODO □

Propozicija 6.16. *Neka su α i β ordinali i neka je $\alpha < \beta$. Tada je α jednak svom početnom komadu u β , tj.*

$$\alpha = p_\beta(\alpha).$$

Dokaz. Propozicija 6.12 implicira $\alpha \subset \beta$, pa je

$$\alpha = \{\gamma \in \beta \mid \gamma \in \alpha\},$$

a to je upravo traženi početni komad. □

Korolar 6.17. *Ako su dva redna broja slična, onda su i jednaka.*

Dokaz. Dokazujemo obrat po kontrapoziciji. Ako dva ordinala α i β nisu jednaka, onda zbog Propozicije 6.14 bez smanjenja općenitosti možemo pretpostaviti da je $\alpha < \beta$, pa je α početni komad u β . Zbog Propozicije 6.3 1. ne mogu biti slični. □

6.4 Skupovi ordinala

Propozicija 6.18. *Neka je S skup ordinala. Tada je $\in_S$ dobar uređaj na S .*

Dokaz. Dovoljno je dokazati da svaki neprazan skup ordinala A ima najmanji element. Uzmimo $\alpha \in A$. Ako je $\alpha \cap A = \emptyset$, svaki drugi $\beta \in A$ nije element od α , pa po Propoziciji 6.14 mora biti $\alpha \in \beta$, dakle α je najmanji.

Ako je $\alpha \cap A$ neprazan, kao podskup od ordinala α ima najmanji element γ . Tvrdimo da je on najmanji i u A . U protivnom, ako postoji $\beta \in A$ takav da je $\beta \in \gamma$, po tranzitivnosti od α je i $\beta \in \alpha$, pa bi on bio manji od γ u α . $\square$

Korolar 6.19. *Svaki tranzitivni skup ordinala je ordinal.*

Dokaz. Direktno po definiciji ordinala. $\square$

Propozicija 6.20 (Burali-Fortijev paradoks). *Ne postoji skup svih rednih brojeva.*

Dokaz. Pretpostavimo suprotno, da postoji $\Omega = \{\alpha \mid \alpha \text{ je ordinal}\}$. Zbog Propozicije 6.9 element svakog ordinala je ordinal, pa je Ω tranzitivan. Zatim Korolar 6.19 povlači da je Ω ordinal, pa je $\Omega \in \Omega$, a to proturječi Propoziciji 6.8. $\square$

Propozicija 6.21. *Neka je S skup ordinala.*

1. $\cup S$ je ordinal.
2. $\cup S$ je gornja međa od S , tj. za svaki $\alpha \in S$ je $\alpha \leq \cup S$.
3. Ako S ima najveći element β , onda je $\cup S = \beta$.
4. Ako je ordinal β gornja međa od S , onda je $\cup S \leq \beta$.

Dokaz. 1. Neka je $x \in y \in \cup S$. Tada postoji ordinal $\alpha \in S$ takav da je $x \in y \in \alpha$, pa je $x \in \alpha \subseteq \cup S$. Dakle $\cup S$ je tranzitivan.

Po Propoziciji 6.9 svi elementi ordinala su ordinali, pa je $\cup S$ također skup ordinala. Budući da je tranzitivan Korolar 6.19 implicira da je ordinal.

U nastavku ćemo više puta koristiti Propoziciju 6.12 koja kaže da je za ordinale α i β $\alpha < \beta$ ekvivalentno s $\alpha \subset \beta$ te $\alpha \leq \beta$ ekvivalentno s $\alpha \subseteq \beta$. Bitno je prethodno provjeriti da su oba elementa zaista ordinali.

2. Za $\alpha \in S$ je $\alpha \subseteq \cup S$, pa i $\alpha \leq \cup S$.
3. Za svaki $\alpha \in S$ je $\alpha \leq \beta$, pa i $\alpha \subseteq \beta$. Dakle $\cup S \subseteq \beta$, pa i $\cup S \leq \beta$.

Točka 2. implicira da je $\beta \leq \cup S$.

4. Ako je β najveći element u S tvrdnja slijedi iz točke 3. U protivnom za svaki $\alpha \in S$ vrijedi $\alpha \in \beta$ pa i $\alpha \subset \beta$. To implicira da je $\cup S \subseteq \beta$, pa i $\cup S \leq \beta$.

□

Definicija 6.22. Neka je S skup ordinala. Skup $\cup S$ nazivamo supremum skupa S i označavamo $\sup S$.

Definicija je opravdana zbog točaka 2. i 4. prethodne propozicije. U nastavku ćemo nastaviti koristiti obje oznake $\cup S$ i $\sup S$.

Korolar 6.23. Za svaki ordinal α je $\cup \alpha \leq \alpha$.

Dokaz. Ordinal α je gornja međa samog sebe, pa točka 4. propozicije implicira tvrdnju. □

6.5 Sljedbenik rednog broja

Propozicija 6.24. Ako je α ordinal, sljedbenik α^+ također je ordinal.

Dokaz. Uzmimo $x \in y \in \alpha^+ = \alpha \cup \{\alpha\}$. Ako je $y \in \alpha$, jer je α ordinal slijedi $x \in \alpha \subseteq \alpha^+$. Ako je $x = \alpha$ onda je isto $y \in \alpha \subseteq \alpha^+$. Dakle α^+ je tranzitivan.

Jasno je da je α^+ skup ordinala, pa Korolar 6.19 povlači da je ordinal. □

Korolar 6.25. 1. Svaki prirodan broj $n \in \omega$ je ordinal.

2. Skup prirodnih brojeva ω je ordinal.

Dokaz. 1. Indukcijom iz propozicije.

2. Propozicija 4.7 implicira da je ω tranzitivan, pa točka 1. i Korolar 6.19 impliciraju tvrdnju. □

Propozicija 6.26. Neka su α i β ordinali. Tada je

1. $\alpha < \alpha^+$;
2. $\alpha < \beta^+$ ako i samo ako $\alpha \leq \beta$;
3. $\alpha < \beta$ ako i samo ako $\alpha^+ \leq \beta$;
4. $\alpha < \beta$ ako i samo ako $\alpha^+ < \beta^+$;
5. $\alpha^+ = \beta^+$ implicira $\alpha = \beta$;

Dokaz. 1. Jasno.

2. Jasno.

3. Neka je $\alpha^+ \leq \beta$, tj. $\alpha^+ = \beta$ ili $\alpha^+ < \beta$. U prvom slučaju točka 1., a u drugom slučaju tranzitivnost od β i točka 1. impliciraju $\alpha < \beta$.

Neka je $\alpha < \beta$. Uspoređujemo α^+ i β . Zbog Propozicije 6.14 dovoljno je isključiti $\beta < \alpha^+$. U tom bi slučaju točka 2. povlačila $\beta \leq \alpha < \beta$ što nije moguće.

4. Jasno iz točaka 2. i 3.;
5. Pretpostavimo suprotno, pa bez smanjenja općenitosti možemo pretpostaviti $\alpha < \beta$. Tada točka 4. povlači $\alpha^+ < \beta^+$, kontradikcija. $\square$

Definicija 6.27. Ordinal α je sljedbenik ako postoji β takav da je $\alpha = \beta^+$. Ordinal je granični ako nije ni 0 ni sljedbenik.

Primjer 6.28. Provjerite da je svaki prirodan broj osim 0 sljedbenik i da je ω granični ordinal.

Propozicija 6.29. 1. Ordinal α je sljedbenik ako i samo ako je $\alpha = (\cup \alpha)^+$.
2. Ordinal α je granični ili 0 ako i samo ako je $\alpha = \cup \alpha$.

Dokaz. 1. Pretpostavimo da je α sljedbenik, tj. $\alpha = \beta^+$ za neki β . Tada je

$$\cup \alpha = \cup(\beta \cup \{\beta\}) = \cup \beta \cup \beta = \beta$$

jer je $\cup \beta \subseteq \beta$ po Korolaru 6.23. Zato je $\alpha = (\cup \alpha)^+$.

Obrat proizlazi direktno iz definicije.

2. Pretpostavimo da je $\cup \alpha = \alpha$. Kada bi α bio sljedbenik onda bi po točki 1. bilo $\alpha = (\cup \alpha)^+ = \alpha^+$ što proturječi Propoziciji 6.26 1. Dakle α nije sljedbenik, pa je ili 0 ili granični.

Obratno, pretpostavimo da α nije sljedbenik. Korolar 6.23 povlači $\cup \alpha \subseteq \alpha$. S druge strane za proizvoljan $\beta \in \alpha$ Propozicija 6.26 3. povlači $\beta^+ \leq \alpha$. Ne mogu biti jednaki jer α nije sljedbenik, pa je $\beta^+ \in \alpha$. Budući da je $\cup \alpha$ gornja međa od α (Propozicija 6.21 2.) slijedi $\beta < \beta^+ \leq \cup \alpha$, tj. $\beta \in \cup \alpha$. Dakle zaista je $\alpha \subseteq \cup \alpha$, pa je $\alpha = \cup \alpha$. $\square$

6.6 Teorem enumeracije

Teorem 6.30. Svaki dobro uređen skup sličan je jedinstvenom rednom broju.

Dokaz. Neka je A dobro uređen skup i neka je

$$A' := \{x \in A \mid \exists \text{ ordinal } \beta \text{ takav da je } p_A(x) \simeq \beta\} \quad (6.2)$$

skup svih elemenata od A čiji su početni komadi slični nekom ordinalu. Za svaki $x \in A'$ taj je ordinal jedinstven zbog Korolara 6.17. Drugim riječima, logički izraz koji kaže

$$P(x, \beta) :\equiv \beta \text{ je ordinal } \wedge x \simeq \beta$$

zadovoljava da $\forall x \in A' \exists! \beta P(x, \beta)$, pa po aksiomu zamjene za taj $P(x, \beta)$ postoji skup

$$\alpha := \{f(x) \mid x \in A'\}$$

gdje je $f(x)$ jedinstven ordinal sličan s x . Zbog toga postoji i funkcija $f : A' \rightarrow \alpha$, $x \mapsto f(x)$.

Tvrdimo da je α tranzitivan. Uzmimo $\gamma \in f(x) \in \alpha$. Budući da je $f(x)$ ordinal, ordinal je i γ . Neka je $g : f(x) \rightarrow x$ sličnost i neka je $y := g(\gamma)$. Lako se provjeri da je restrikcija $g|_\gamma$ sličnost između γ i početnog komada $p_A(y)$. Dakle $y \in A'$ i $\gamma \in \alpha$. Dakle α je zaista tranzitivan, pa je po Korolaru 6.19 ordinal.

Na gotovo identičan način dokažemo da za svaki $x \in A'$ i svaki $y \in A$, $y < x$ implicira $y \in A'$ (detalji za D.Z.).

Lako se vidi da $f : A' = p_A(x) \rightarrow \alpha$ čuva uređaj. Stoga je i injekcija, a po definiciji od α je i surjekcija. Dakle ona je sličnost.

Tvrdimo da je $A' = A$. Pretpostavimo suprotno i uzmimo najmanji $x \in A$ koji nije u A' . Dakle, svaki $y < x$ je u A' , tj. $p_A(x) \subseteq A'$.

S druge strane, ako postoji $y \in A' \setminus p_A(x)$ postoji sličnost između $p_A(y)$ i nekog ordinala β . Propozicija 5.16 implicira da je restrikcija te sličnosti na $p_A(x)$ sličnosti između $p_A(x)$ i nekog početnog komada od β koji je po Propoziciji 6.16 ordinal. Zato je $x \in A'$ što proturječi pretpostavci da postoji traženi y . Zaključujemo da $y \in A' \setminus p_A(x)$ ne postoji, tj. $p_A(x) = A'$.

Dakle funkcija $f : A' = p_A(x) \rightarrow \alpha$ je sličnost između početnog komada u A i ordinala α , pa je $x \in A'$. To proturječi izboru od x , dakle zaista je $A' = A$.

Zato imamo $f : A \rightarrow \alpha$ sličnost, što je i trebalo pokazati. Jedinstvenost slijedi direktno iz Korolara 6.17. $\square$

6.7 Transfinitna indukcija

Teorem 6.31 (Jaka transfinitna indukcija). *Neka je $\phi(\beta)$ logički izraz sa slobodnom varijablom β takav da za svaki ordinal α*

$$((\forall \text{ ordinal } \beta < \alpha) \phi(\beta)) \rightarrow \phi(\alpha).$$

Tada za svaki ordinal α vrijedi $\phi(\alpha)$.

Primijetimo da je Teorem jake transfinitne indukcije shema teorema. Takva će biti i većina drugih teorema o transfinitnoj indukciji i rekurziji koje ćemo spomenuti u nastavku.

Dokaz. Pretpostavimo suprotno, tj. da postoji ordinal γ za koji ne vrijedi $\phi(\gamma)$. Neka je

$$\alpha := \min\{\beta \leq \gamma \mid \neg\phi(\beta)\}$$

najmanji ordinal manji ili jednak γ (dakle $\in \gamma^+$ po Propoziciji 6.26) za koji ne vrijedi $\phi(\alpha)$. Tada za sve ordinale $\beta < \alpha$ vrijedi $\phi(\beta)$, pa svojstvo iz teorema implicira $\phi(\alpha)$, što je kontradikcija. $\square$

Napomena 6.32. *Ordinal α iz dokaza definirali smo kao najmanji element skupa dobivenog separacijom iz γ^+ pomoću nekog svojstva. Postavlja se pitanje jesmo li mogli naprosto uzeti najmanji ordinal koji ima to svojstvo, budući da su svi ordinali “dobro uređeni”. Odgovor je: nismo direktno, jer ne postoji skup svih ordinala koji bi bio dobro uređen. Međutim, uvijek*

možemo napraviti trik kao u dokazu: ako postoji ordinal γ s nekim svojstvom dovoljno je razmatrati ordinale manje ili jednake njemu, a oni čine skup, i uzeti najmanji α među njima. Jasno je da α ne ovisi o izboru γ . Zbog toga možemo kratko reći da uzimamo najmanji ordinal koji ima dano svojstvo, što ćemo i raditi u nastavku.

Kao što indukcija i rekurzija prirodnih brojeva mogu biti jaka - koja uzima u obzir sve manje brojeve, i primitivna - koja uzima u obzir samo neposredne prethodnike, postoji i primitivna transfinitna indukcija. Ipak, redni su brojevi širi pojam od prirodnih brojeva pa je njihova primitivna indukcija nešto kompleksnija, što ćemo vidjeti u nastavku.

Teorem 6.33 (Primitivna transfinitna indukcija). *Neka je $\phi(\beta)$ logički izraz sa slobodnom varijablom β takav da vrijedi*

- $\phi(0)$;
- za svaki ordinal α $\phi(\alpha)$ povlači $\phi(\alpha^+)$;
- za svaki granični ordinal α ($\forall \beta < \alpha$) $\phi(\beta)$ povlači $\phi(\alpha)$.

Tada za svaki ordinal α vrijedi $\phi(\alpha)$.

Dokaz. Provjerit ćemo da za svaki ordinal α vrijedi uvjet Teorema 6.31, tj. implikacija $((\forall \text{ ordinal } \beta < \alpha) \phi(\beta)) \rightarrow \phi(\alpha)$.

Ako je $\alpha = 0$ $\phi(\alpha)$ vrijedi zbog prvog uvjeta.

Ako je α sljedbenik postoji γ takav da je $\alpha = \gamma^+$. Pretpostavimo da $(\forall \text{ ordinal } \beta < \alpha) \phi(\beta)$. Konkretno, $\gamma < \gamma^+ = \alpha$, pa slijedi $\phi(\gamma)$. Sada drugi uvjet povlači $\phi(\gamma^+)$, tj. $\phi(\alpha)$.

U preostalom slučaju, ako je α granični, treći uvjet ovog teorema identičan je uvjeti iz Teorema 6.31.

Dakle u svakom slučaju vrijedi uvjeti iz Teorema 6.31, pa on povlači $\phi(\alpha)$ za svaki ordinal α . $\square$

6.8 Transfinitna rekurzija

Prisjetimo se da logički izraz $P(x, y)$ za koji vrijedi $\forall x \exists! y P(x, y)$ nazivamo *logička funkcija*, Definicija 4.21. Za zadani x jedinstveni takav y označavamo s $P(x)$. Ako je $P(x, y)$ logička funkcija i X skup neka je

$$P|_X := \{(x, y) \mid x \in X \wedge P(x, y)\}. \quad (6.3)$$

To je jasno funkcija, a njeno postojanje slijedi iz aksioma zamjene.

Teorem 6.34 (Jaka transfinitna rekurzija). *Neka je $F(x, y)$ logička funkcija. Tada postoji logička funkcija $P(x, y)$ za koju vrijedi $(\forall \text{ ordinal } \alpha) P(\alpha) = F(P|_\alpha)$.*

Ponovno primijetimo da je navedeni teorem shema teorema, po jedan teorem za svaku logičku funkciju $F(x, y)$. Prisjetimo se da se sve tvrdnje ne mogu iznijeti u jednom teoremu jer za logičke izraze F ne možemo koristiti kvantifikator $\forall F$. No za logičke izraze ne možemo koristiti niti kvantifikator $\exists$, pa je tvrdnja teorema da postoji logička funkcija $P(x, y)$ problematična. Zaista, gore naveden iskaz teorema nepotpun je. Tvrdnja da postoji neka logička funkcija zapravo je nepotpuna skraćena tvrdnja koja eksplicitno navodi tu logičku funkciju. Logičku funkciju $P(x, y)$ konstruirat ćemo u dokazu i ona formalno mora biti dio iskaza teorema. Formalno ćemo iskazati teorem, odnosno teoreme, nakon dokaza.

Dokaz. Dokaz provodimo koliko možemo analogno dokazu Teorema 4.23.

Neka je $G(\alpha, g)$ logički izraz koji kaže

$$G(\alpha, g) := \alpha \text{ je ordinal} \wedge g \text{ je funkcija} \wedge \text{dom}(g) = \alpha \wedge (\forall \beta \in \alpha) g(\beta) = F(g|_\beta). \quad (6.4)$$

Tvrdnja 1. Za svaki ordinal α i za svake g, g' ako vrijedi $G(\alpha, g)$ i $G(\alpha, g')$ onda je $g = g'$.

Dokaz. Pretpostavimo suprotno, da postoje različiti g, g' takvi da je $G(\alpha, g)$ i $G(\alpha, g')$. Posebno, vrijedi da su g i g' funkcije s domenom α pa za $\beta \in \alpha$ možemo koristiti notacije $g(\beta)$ i $g'(\beta)$. Neka je

$$\gamma := \min\{\beta \in \alpha \mid g(\beta) \neq g'(\beta)\}$$

najmanji ordinal u kojem se funkcije razlikuju. Tada je za svaki $\beta < \gamma$ $g(\beta) = g'(\beta)$, tj. $g|_\gamma = g'|_\gamma$, pa $G(\alpha, g)$ i $G(\alpha, g')$ impliciraju

$$g(k) = F(g|_k) = F(g'|_k) = g'(k),$$

što proturječi izboru k . □

Tvrdnja 2. Neka su α i β ordinali takvi da je $\beta < \alpha$. Ako vrijedi $G(\alpha, g)$ onda vrijedi i $G(\beta, g|_\beta)$. □

Dokaz. Jasno.

Tvrdnja 3. Za svaki ordinal α postoji g takav da vrijedi $G(\alpha, g)$.

Dokaz. Dokazujemo primitivnom transfinitnom indukcijom po α .

Baza $\alpha = 0$: Provjerimo da vrijedi $G(0, \emptyset)$.

Sljedbenik $\alpha = \beta^+$: Pretpostavimo da vrijedi $G(\beta, g_\beta)$. Definirajmo funkciju g_α s domenom α :

$$g_\alpha(\gamma) := \begin{cases} g_\beta(\gamma) & \gamma < \beta \\ F(g_\beta) & \gamma = \beta. \end{cases} \quad (6.5)$$

Lako se provjeri da vrijedi $G(\alpha, g_\alpha)$.

Granični α : Pretpostavimo da za svaki ordinal $\beta < \alpha$ postoji g_β takav da vrijedi $G(\beta, g_\beta)$.

Tvrdnja 1 povlači da je za svaki β njegov pripadni g_β jedinstven. Stoga aksiom zamjene povlači da postoji skup

$$S_\alpha := \{g_\beta \mid \beta \in \alpha\}. \quad (6.6)$$

Neka je

$$g_\alpha := \cup S_\alpha. \quad (6.7)$$

Tvrdnja 3.1. Skup g_α je funkcija.

Dokaz. Dokazujemo slično kao Tvrdnju 4 Teorema 4.23, odnosno Teorema 4.19. Pretpostavimo da su $(\delta, x_1), (\delta, x_2) \in g_\alpha$. Po definiciji unije postoje $\beta, \gamma \in \alpha$ takvi da je $(\delta, x_1) \in g_\beta$ i $(\delta, x_2) \in g_\gamma$. Mora vrijediti $\delta < \beta$ i $\delta < \gamma$. Bez smanjenja općenitosti možemo pretpostaviti da je $\beta \leq \gamma$. Tvrdnja 2 povlači da je

$$g_\gamma|_\beta = g_\beta.$$

Zato su oba $(\delta, x_1), (\delta, x_2) \in g_\beta$, a kako je g_β je funkcija, vrijedi $x_1 = x_2$. $\square$

Tvrdnja 3.2. Domena funkcije g_α je α .

Dokaz. Dokazujemo slično kao Tvrdnju 5 Teorema 4.23, odnosno Teorema 4.19.

Domene svih funkcija g_β su $\subseteq \alpha$, pa je i $\text{dom}(g_\alpha) \subseteq \alpha$.

Obratno, neka je $\beta \in \alpha$. Zato je $\beta^+ \leq \alpha$, a kako je α granični mora biti $\beta^+ < \alpha$. Vrijedi $\beta \in \beta^+ = \text{dom}(g_{\beta^+})$. Zato postoji x takav da je $(\beta, x) \in g_{\beta^+} \subseteq g_\alpha$. Dakle $\beta \in \text{dom}(g_\alpha)$. $\square$

Transfinitnu indukciju završavamo sljedećom tvrdnjom.

Tvrdnja 3.3. Za svaki $\beta \in \alpha$ vrijedi $g_\alpha(\beta) = F(g_\alpha|_\beta)$.

Dokaz. Ponovno znamo da je $\beta^+ < \alpha$. Po pretpostavci indukcije vrijedi $G(\beta^+, g_{\beta^+})$, pa posebno $g_{\beta^+}(\beta) = F(g_{\beta^+}|_\beta)$, tj. $(\beta, F(g_{\beta^+}|_\beta)) \in g_{\beta^+} \subseteq g_\alpha$. Dakle $g_\alpha(\beta) = F(g_{\beta^+}|_\beta) = F(g_\alpha|_\beta)$. $\square$

Tvrdnje 3.1, 3.2 i 3.3 upravo impliciraju $G(\alpha, g_\alpha)$. Time je indukcija završena. $\square$

Dokazali smo da za svaki ordinal α postoji jedinstveni g_α takav da vrijedi $G(\alpha, g_\alpha)$. Svi ordinali ne čine skup, pa od ovoga ne možemo konstruirati generalnu funkciju na svim ordinalima. Ipak, možemo konstruirati logički izraz $P(\alpha, x)$ koji kaže $x = g_{\alpha^+}(\alpha)$, odnosno formalno:

$$P(\alpha, x) := (\alpha \text{ je ordinal} \wedge (\forall g) G(\alpha^+, g) \rightarrow (\alpha, x) \in g) \vee (\alpha \text{ nije ordinal} \wedge x = 0). \quad (6.8)$$

Tvrdnja 4. $P(\alpha, x)$ je logička funkcija, tj. za svaki α postoji jedinstveni x takav da vrijedi $P(\alpha, x)$.

Dokaz. Ako je α ordinal tvrdnje 1 i 3 impliciraju da postoji jedinstveni g_{α^+} takav da vrijedi $G(\alpha^+, g_{\alpha^+})$, dakle $P(\alpha, x)$ kaže da je $(\alpha, x) \in g_{\alpha^+}$. $G(\alpha^+, g_{\alpha^+})$ između ostalog povlači da je g_{α^+} funkcija s domenom α^+ , pa za $\alpha \in \alpha^+$ postoji jedinstveni x za koji je $(\alpha, x) \in g_{\alpha^+}$.

Ako α nije ordinal jasno je da $P(\alpha, x)$ vrijedi samo za $x = \emptyset$. $\square$

Dodatna opcija za α koji nije ordinal neće nikada biti korištena, ona služi samo da bismo zadovoljili formalnu definiciju logičke funkcije.

Sljedećom tvrdnjom završavamo ovaj dokaz.

Tvrdnja 5. Za svaki ordinal α vrijedi $P(\alpha) = F(P|_\alpha)$

6 Redni brojevi (ordinali)

Dokaz. Znamo da za $\beta \in \alpha$ vrijedi $P|_\alpha(\beta) = g_{\beta^+}(\beta)$. Tvrdnja 2 implicira da je to jednako $g_\alpha(\beta)$, pa je $P|_\alpha = g_\alpha$. Opet zbog tvrdnje 2 to je jednako $g_{\alpha^+}|_\alpha$.

Sada samo provjerimo da vrijedi $P(\alpha, F(g_\alpha))$, tj. $g_{\alpha^+}(\alpha) = F(g_{\alpha^+}|_\alpha)$. To direktno slijedi iz izbora g_{α^+} kao one funkcije koja zadovoljava $G(\alpha^+, g_{\alpha^+})$. $\square$

$\square$

Teorem (Formalni iskaz Sheme teorema jake transfinitne rekurzije). *Neka je $F(x, y)$ logička funkcija. Tada je sljedeća tvrdnja teorem.*

Teorem (Teorem jake transfinitne rekurzije za logičku funkciju $F(x, y)$). *Neka je $P(\alpha, x)$ logički izraz definiran u gornjem dokazu, tj.*

$$\begin{aligned} P(\alpha, x) : \equiv & (\alpha \text{ je ordinal} \wedge ((\forall g) g \text{ je funkcija} \wedge \text{dom}(g) = \alpha^+ \wedge \\ & (\forall \beta \in \alpha^+) g(\beta) = F(g|_\beta) \rightarrow (\alpha, x) \in g)) \\ & \vee (\alpha \text{ nije ordinal} \wedge x = \emptyset). \end{aligned}$$

Vrijedi sljedeće:

1. $P(\alpha, x)$ je logička funkcija, tj. za svaki α postoji jedinstveni x takav da je $P(\alpha, x)$.
2. Za svaki ordinal α vrijedi $P(\alpha) = F(P|_\alpha)$.

Iako je navedeno formalan logički iskaz teorema, mi ćemo i dalje neformalno govoriti da “postoji” ili da se “može konstruirati” logička funkcija te u iskazima teorema nećemo eksplicitno iznositi tu logičku funkciju. U konačnici nije nam bitno kako ona točno izgleda, nego su nam bitna njena svojstva koja iznosi teorem (u ovom slučaju $P(\alpha) = F(P|_\alpha)$). Prvu primjenu vidimo u sljedećem Teoremu primitivne transfinitne rekurzije.

Teorem 6.35 (Primitivna transfinitna rekurzija). *Neka je b skup te $S(x, y)$ i $G(x, y)$ logičke funkcije. Tada se može konstruirati logička funkcija $P(x, y)$ za koju vrijedi*

- $P(0) = b$;
- za svaki ordinal α je $P(\alpha^+) = S(P(\alpha))$;
- za svaki granični ordinal α je $P(\alpha) = G(P|_\alpha)$.

Dokaz. Konstruirajmo logički izraz:

$$\begin{aligned} F(x, y) : \equiv & x = \emptyset \wedge y = b \vee \\ & x \text{ je funkcija} \wedge (\exists \text{ ordinal } \alpha) (\text{dom}(x) = \alpha^+ \wedge S(x(\alpha), y) \vee) \\ & x \text{ je funkcija} \wedge (\exists \text{ granični ordinal } \alpha) (\text{dom}(x) = \alpha \wedge G(x, y)) \vee \\ & x \text{ nije funkcija ili mu domena nije ordinal} \wedge y = \emptyset. \end{aligned}$$

Za D.Z. pokažite da je $F(x, y)$ logička funkcija i primijenite Teorem jake transfinitne rekurzije za tu logičku funkciju. $\square$

6.9 Operacije na ordinalima

Slično kao kod prirodnih brojeva uvest ćemo operacije zbrajanja, množenja i eksponenciranja ordinala, ovaj put pomoću transfinite rekurzije.

Sve će one biti definirane logičkim izrazom $P(\alpha, \beta, \gamma)$ takvim da za svake ordinals α i β postoji jedinstveni γ za koji on vrijedi. Tada za navedeni γ možemo uvesti oznaku koja koristi α i β , pa je $P(\alpha, \beta, \gamma)$ ekvivalentno jednakosti $\gamma =$ (ta oznaka). Iako je pomalo neprecizno, u iskazima propozicija zbog jednostavnosti odmah ćemo koristiti tu jednakost umjesto P , čime impliciramo svojstvo jedinstvenosti γ .

Propozicija 6.36. Može se konstruirati logički izraz $\alpha + \beta = \gamma$ za koji vrijedi

- za svaki ordinal α je $\alpha + 0 = \alpha$;
- za svake ordinals α i β je $\alpha + \beta^+ = (\alpha + \beta)^+$;
- za svaki ordinal α i granični ordinal β je $\alpha + \beta = \sup\{\alpha + \gamma \mid \gamma \in \beta\}$.

Dokaz. Direktno primjenom Primitivne transfinite rekurzije, Teorem 6.35., za skup α te logičke funkcije $y = x^+$ i $y = \text{Urng}(x)$. $\square$

Propozicija 6.37. Može se konstruirati logički izraz $\alpha \cdot \beta = \gamma$ za koji vrijedi

- za svaki ordinal α je $\alpha \cdot 0 = 0$;
- za svake ordinals α i β je $\alpha \cdot \beta^+ = \alpha \cdot \beta + \alpha$;
- za svaki ordinal α i granični ordinal β je $\alpha \cdot \beta = \sup\{\alpha \cdot \gamma \mid \gamma \in \beta\}$.

Dokaz. D.Z. $\square$

Propozicija 6.38. Može se konstruirati logički izraz $\alpha^\beta = \gamma$ za koji vrijedi

- za svaki ordinal α je $\alpha^0 = 1$;
- za svake ordinals α i β je $\alpha^{\beta^+} = \alpha^\beta \cdot \alpha$;
- za svaki ordinal α i granični ordinal β je $\alpha + \beta = \sup\{\alpha^\gamma \mid \gamma \in \beta \setminus \{0\}\}$.

Dokaz. D.Z. $\square$

Propozicija 6.39. Za svake ordinals α, β i γ vrijedi

$0 + \alpha = \alpha$	$1 \cdot \alpha = \alpha \cdot 1 = \alpha$	$\alpha^1 = \alpha, \quad 1^\alpha = 1$
	$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$	$\alpha^{\beta+\gamma} = \alpha^\beta \alpha^\gamma$
$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$	$\alpha(\beta\gamma) = (\alpha\beta)\gamma$	
$\beta < \gamma \Rightarrow \alpha + \beta < \alpha + \gamma$	$\beta < \gamma \Rightarrow \alpha\beta < \alpha\gamma$ za $\alpha > 0$	$\beta < \gamma \Rightarrow \alpha^\beta < \alpha^\gamma$ za $\alpha > 1$
$\alpha + \beta = \alpha + \gamma \Rightarrow \beta = \gamma$	$\alpha\beta = \alpha\gamma \Rightarrow \beta = \gamma$ za $\alpha > 0$	$\alpha^\beta = \alpha^\gamma \Rightarrow \beta = \gamma$ za $\alpha > 1$
$\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$	$\alpha \leq \beta \Rightarrow \alpha\gamma \leq \beta\gamma$	$\alpha \leq \beta \Rightarrow \alpha^\gamma \leq \beta^\gamma$

Dokaz. Sve se dokazuje transfinite indukcijom. D.Z. $\square$

7 Aksiom izbora

7.1 Iskaz

Aksiom 9. *Neka je S skup nepraznih međusobno disjunktih skupova. Tada postoji skup A takav da je za svaki $x \in S$ presjek $x \cap A$ jednočlan.*

Formalno

$$(\forall S)((\emptyset \notin S) \wedge (\forall x, y \in S)(x = y \vee x \cap y = \emptyset)) \rightarrow (\exists A)(\forall x \in S)(\exists! y)(y \in A \cap x).$$

Aksiom izbora kaže da postoji skup A čiji su elementi po jedan element svakog $x \in S$. Takva se tvrdnja čini prirodnom, no zanimljivo je da ne slijedi iz dosadašnjih aksioma. Jasno je da je A podskup od $\cup S$, pa se postavlja pitanje zašto aksiom podskupa (separacije) ne može separirati A iz $\cup S$. Problem je što općenito ne možemo konstruirati logički izraz ϕ koji bi garantirao po jedan element iz svakog $x \in S$.

Svi dosadašnji aksiomi bili su “konstruktivni”, tj. “konstruirali” su novi skup jasno definirajući koji su mu elementi pomoću dosadašnjih skupova i logičkih izraza. Aksiom izbora bitno je drugačiji, on ne odgovara jasno na pitanje koji su elementi novog skupa A , on samo kaže da postoji skup A s traženim svojstvom. Općenito očekujemo da takvih skupova A ima mnogo, pa ipak moguće je da niti jedan ne možemo konstruirati. Ova “nekonstruktivnost” aksioma izbora uzrok je mnogih njegovih kontroverzi. Obično želimo da znamo koji su točno elementi skupa koji nas zanima, pa čim možemo postojanje nekog skupa utvrditi bez aksioma izbora, to je preferiran način. Ipak, matematičari obično prihvaćaju istinitost aksioma izbora i koriste ga kada je to nužno.

U mnogim slučajevima ipak nije nužno. Navedimo nekoliko takvih situacija.

Primjer 7.1. *Ako je S konačan, za dokazati postojanje skupa A nije nužan aksiom izbora. Dokažimo to indukcijom po $|S|$.*

Baza: Za $S = \emptyset$, $A = \emptyset$ zadovoljava tvrdnju.

Pretpostavka: Pretpostavimo da za svaki skup S ekvipotentan s $n \in \omega$ postoji A koji sadrži točno po jedan element svakog $x \in S$.

Korak: Neka je S ekvipotentan s n^+ . Uzmimo $x \in S$ i neka je $S' := S \setminus \{x\}$. Tada je $|S'| = n$ pa po pretpostavci indukcije postoji A' koji sadrži točno po jedan element svakog $x' \in A'$. Uzmimo $y \in x$. Lako se utvrdi da $A = A' \cup y$ sadrži točno po jedan element svakog $x \in A$.

U navedenom dokazu dva smo puta uzimali, tj. izabrali element nekog skupa ($x \in S$ i $y \in x$). Nije li to također “izbor”? Izbor jest, no ne treba mu aksiom izbora. To je jednostavno korištenje logike prvog reda: ako je x neprazan onda postoji $y \in x$, pa možemo nastaviti koristiti taj y .

Primjer 7.2. Ako postoji bilo koja opća metoda (funkcija, logički izraz isl.) kojom možemo iz $x \in S$ izdvojiti konkretan element, možemo separirati

$$A := \{y \in \cup S \mid (\exists x \in S)(y \text{ je izdvojen element u } x)\}.$$

Ovaj primjer slikovito možemo primijeniti na parove cipela. Ako je S skup parova cipela, A bi bio skup koji sadrži po jednu cipelu iz svakog para. Za to nam ne treba aksiom izbora, možemo jednostavno definirati A kao skup svih desnih cipela iz $\cup S$. Nasuprot tome, ako je S skup parova čarapa (koji općenito nemaju određenu lijevu i desnu čarapu) za postojanje skupa A koji sadrži po jednu čarapu iz svakog para potreban nam je aksiom izbora.

7.2 Funkcija izbora

Definicija 7.3. Neka je S skup nepraznih skupova. Funkcija f je funkcija izbora od S ako je $S = \text{dom}(f)$ i za svaki $x \in S$ vrijedi $f(x) \in x$.

Propozicija 7.4. Svaki skup nepraznih skupova ima funkciju izbora.

Dokaz. Neka je S skup nepraznih skupova. Za skup x definirajmo $\bar{x} := \{(x, y) \mid y \in x\}$ i neka je

$$S' := \{\bar{x} \mid x \in S\}.$$

Po konstrukciji su svi elementi od S' disjunktni. Neprazni su jer je svaki $x \in S$ neprazan, pa na S' možemo primijeniti aksiom izbora i dobiti A takav da za svaki $\bar{x} \in S'$ postoji jedinstveni $(x, y) \in A \cap \bar{x}$, tj. za svaki $x \in S$ postoji točno jedan par u A kojem je prvi član x . Drugi član po definiciji mora biti neki $y \in x$. Dakle A je upravo tražena funkcija izbora od S . □

Propozicija 7.5. Propozicija 7.4 ekvivalentna je aksiomu izbora.

Dokaz. Već smo dokazali propoziciju iz aksioma izbora. Obratno, pretpostavimo da svaki skup nepraznih skupova ima funkciju izbora i dokažimo aksiom izbora. Neka je S kao u aksiomu izbora. Posebno, S je skup nepraznih skupova, pa ima funkciju izbora f . Slika od f traženi je skup A . □

7.3 Zornova lema

Definicija 7.6. Neka je $(X, <)$ parcijalno uređeni skup i neka je $L \subseteq X$ takav da je $(L, <)$ totalno uređen, tj. svaka dva elementa u L usporediva su relacijom $<$. Tada kažemo da je L lanac u X .

Teorem 7.7 (Zornova lema). Neka je $(A, <)$ parcijalno uređeni skup u kojem svaki lanac ima gornju među. Tada u $(A, <)$ postoji maksimalan element.

Dokaz. Neka je $\mathcal{L} \subseteq \mathcal{P}(A)$ skup svih lanaca u A . Za svaki $L \in \mathcal{L}$ neka je

$$M_L := \{y \in A \mid (\forall x \in L)(x \leq y)\}$$

skup svih gornjih međa od L koji je neprazan po pretpostavci. Zato postoji funkcija izbora koja svakom M_L pridružuje njegov element. Kompozicijom s funkcijom $L \mapsto M_L$ dobivamo funkciju $g: \mathcal{L} \rightarrow A$ takvu da je $g(L)$ gornja međa od L za svaki lanac L .

Pretpostavimo suprotno, da u $(A, <)$ ne postoji maksimalan element, tj. za svaki $x \in A$ skup elemenata većih od x je neprazan. Na sličan način dobijemo funkciju $v: A \rightarrow A$ takvu da je $v(x) > x$ za svaki $x \in A$.

Uzmimo $x_0 \in A$. Primitivnom transfinitnom rekurzijom konstruiramo logičku funkciju $X(\alpha, x)$ koja za svaki ordinal α definira $X(\alpha)$ takav da

- $X(0) = x_0$,
- $X(\alpha^+) = v(X(\alpha))$,
- za granični α $X(\alpha) = g(\text{rng}(X|_\alpha))$.

Formalno za potrebe ove definicije možemo proširiti g na $\mathcal{P}(A)$ bilo kako, svakako ćemo u nastavku dokazati da je $\text{rng}(X|_\alpha)$ uvijek lanac.

Tvrđnja 1. *Za svaki ordinal α vrijedi:*

1. $\text{rng}(X|_\alpha)$ je lanac,
2. za svaki $\beta < \alpha$ vrijedi $X(\beta) < X(\alpha)$.

Dokaz. Dokazujemo jakom transfinitnom indukcijom po α .

Pretpostavimo da tvrdnje vrijede za svaki $\alpha' < \alpha$. Konkretno, tvrdnja 2. znači da za svake $\beta < \alpha' < \alpha$ je $X(\beta) < X(\alpha')$. To direktno povlači tvrdnju 1. za α .

Za dokazati tvrdnju 2. imat ćemo dva slučaja. Ako je α sljedbenik, tj. $\alpha = \gamma^+$ za neki γ vrijedi $X(\alpha) = v(X(\gamma)) > X(\gamma)$. Ako je $\beta < \alpha$ onda je $\beta \leq \gamma$. Pretpostavka zato implicira $X(\beta) \leq X(\gamma) < X(\alpha)$, što je i trebalo dokazati.

Ako je α granični već dokazana tvrdnja 1. implicirana da je $\text{rng}(X|_\alpha)$ je lanac, pa je $X(\alpha) = g(\text{rng}(X|_\alpha))$ gornja međa od $\text{rng}(X|_\alpha)$. Slika $\text{rng}(X|_\alpha)$ nema maksimum jer α nema maksimum (tvrdnja 2. pretpostavke), pa je $X(\alpha)$ strogo veći od svih elemenata od $\text{rng}(X|_\alpha)$, što je i trebalo dokazati. $\square$

Neka je $B := \{x \in A \mid (\exists \text{ ordinal } \alpha)(x = X(\alpha))\} \subseteq A$ skup svih elemenata od A koji se dobiju ovom rekurzijom.

Tvrdnja 1. između ostalog tvrdi da za svake različite ordinale α, β vrijedi $X(\alpha) \neq X(\beta)$, tj. $X(\alpha, x)$ i $X(\beta, x)$ povlači $\alpha = \beta$. Aksiom zamjene na (obrat od) X i skup B sada implicira da svi α , što su ovdje svi ordinali, čine skup. To proturječi Propoziciji 6.20. $\square$

7.4 Zermelov teorem

Teorem 7.8 (Zermelov teorem ili Teorem o dobrom uređaju). *Svaki se skup može dobro urediti*

Dokaz. Neka je S skup. Neka je $\mathcal{A}$ skup svih dobro uređenih skupova $(X, <)$ takvih da je $X \subseteq S$. Na $\mathcal{A}$ definiramo relaciju $(X, <_1) \triangleleft (Y, <_2)$ ako je X početni komad u Y i $<_1$ je restrikcija od $<_2$. Lako se provjeri da je $\triangleleft$ parcijalni uređaj.

Neka je $\mathcal{L} \subseteq \mathcal{A}$ lanac. Neka je

$$Z := \bigcup_{(X, <) \in \mathcal{L}} X$$

unija svih skupova u $\mathcal{L}$. Za $a, b \in Z$ definirajmo relaciju

$$a < b \iff (\exists (X, <) \in \mathcal{L})(a, b \in X \wedge a < b). \quad (7.1)$$

Budući da je L lanac, svi su njegovi elementi usporedivi, pa je uređaj na jednom restrikcija uređaja na drugom. Stoga, čim se a i b nalaze u jednom $(X, <_1) \in L$ i u njemu je $a <_1 b$, tada je $a <_2 b$ i u svakom drugom $(Y, <_2)$ čim su oba $a, b \in Y$. Zato smo mogli ekvivalentno definirati

$$a < b \iff (\forall (X, <) \in \mathcal{L})(a, b \in X \rightarrow a < b). \quad (7.2)$$

Uzmimo $a, b \in Z$, $a < b$. Tada postoji $(X, <) \in \mathcal{L}$ takav da su $a, b \in X$, $a < b$. Neka je $(Y, <_2) \in \mathcal{L}$ i neka je $b \in Y$. $(X, <)$ i $(Y, <_2)$ su usporedivi pa je jedan početni komad u drugom, ili su jednaki. U svakom slučaju mora biti $a \in Y$. Dakle ako imamo $a < b$, dovoljno je utvrditi da je b element nekog $(Y, <_2) \in \mathcal{L}$ da zaključimo $a <_2 b$.

Dokažimo da je $<$ parcijalni uređaj na Z . Irefleksivnost je jasna. Neka je $a < b < c$. To znači da postoji $(X, <) \in \mathcal{L}$ takav da je $b, c \in X$, $b < c$, a zbog upravo objašnjenog mora biti i $a \in X$, $a < b$. Tranzitivnost od $<$ povlači $a < c$, pa je po definiciji $a < c$.

Dokažimo da je $<$ dobar uređaj na Z . Neka je $W \subseteq Z$ neprazan i neka je $a \in W$. Postoji $(X, <) \in \mathcal{L}$ takav da je $a \in X$, pa je $W \cap X$ neprazan i ima minimum m u $(X, <)$. Tvrdimo da je m minimum od W u $(Z, <)$. Pretpostavimo suprotno, da postoji $b \in W$, $b < m$. No jer je $m \in X$ tada mora biti $b \in X$. Dakle $b \in W \cap X$, što proturječi izboru m kao njegova minimuma.

Dokažimo da je $(Z, <)$ gornja međa od $\mathcal{L}$. Uzmimo $(X, <) \in \mathcal{L}$ i treba dokazati da je $(X, <) \trianglelefteq (Z, <)$. Jasno je $X \subseteq Z$. Imat ćemo dva slučaja:

- Neka je $X = Z$. Iz (7.1) i (7.2) jasno je da je $a < b$ ekvivalentno s $a < b$, dakle $(X, <) = (Z, <)$.
- Neka je $X \subset Z$. Uzmimo $a \in Z \setminus X$. Postoji $(Y, <_2) \in \mathcal{L}$ takav da je $a \in Y$. $(X, <)$ i $(Y, <_2)$ su usporedivi, a jer a nije u X ne može biti $(Y, <_2) \trianglelefteq (X, <)$. Zato X mora biti početni komad u $(Y, <_2)$, tj. postoji $b \in Y$ takav da je $X = \{x \in Y \mid x <_2 b\}$. Iz (7.1) i (7.2) slijedi da je $X = \{x \in Y \mid x < b\}$, a iz činjenice da su svi manji od b u istom elementu lanca slijedi $X = \{x \in Z \mid x < b\}$, dakle X je početni komad u $(Z, <)$. Lako se vidi da je $<$ restrikcija od $<$, dakle $(X, <) \triangleleft (Z, <)$.

U oba slučaja $(Z, <)$ je gornja međa od $\mathcal{L}$, što je i trebalo dokazati.

Sada primijenimo Zornovu lemu i zaključimo da $\mathcal{A}$ ima maksimum $(M, <)$.

Pretpostavimo da je $M \neq S$, tj. da postoji $a \in S \setminus M$. Tada proširimo uređaj na M na $M \cup \{a\}$ tako da je a veći od svih ostalih. Jasno je da je i proširenje dobar uređaj, što proturječi maksimalnosti od $(M, <)$.

Dakle zaista je $M = S$, što povlači tvrdnju teorema. $\square$

Teorem 7.9. *Ekvivalentno je*

- *Aksiom izbora,*
- *Zornova lema,*
- *Zermelov teorem.*

Dokaz. Dovoljno je dokazati aksiom izbora iz Zermelovog teorema. Neka je S skup iz aksioma izbora. Po Zermelovom teoremu uzmimo dobar uređaj $<$ na $\cup S$. Neka je

$$A := \{\min(x) \mid x \in S\}.$$

Najmanji element postoji jer je uređaj dobar. Jasno je da A zadovoljava traženo svojstvo iz aksioma izbora. $\square$

8 Kardinalni brojevi (kardinali)

8.1 Definicija

Zermelov teorem implicira da se svaki skup može dobro urediti, i onda zbog teorema enumeracije sličan je nekom ordinalu. Posebno, on je ekvipotentan nekom ordinalu. Želimo definirati kardinalni broj kao neki skup koji će predstavljati sve skupove ekvipotentne s njime. Sada vidimo da je dovoljno usredotočiti se na redne brojeve, gdje se nameće prirodan izbor: najmanji redni broj koji je ekvipotentan zadanom skupu.

Definicija 8.1. Ordinal α je kardinalni broj ili kardinal ako niti jedan $\beta \in \alpha$ nije ekvipotentan s α .

Primjer 8.2. Svi prirodni brojevi i ω su kardinali.

Kardinalne brojeve uglavnom označavamo grčkim slovima $\kappa, \lambda, \mu, \dots$

Teorem 8.3. Za svaki skup S postoji jedinstveni kardinalni broj α ekvipotentan s njim.

Dokaz. Prema Zermelovom teoremu na S postoji dobar uređaj $<$. Prema teoremu enumeracije postoji ordinal β sličan s $(S, <)$. Posebno vrijedi da je $\beta \sim S$. Neka je α najmanji ordinal ekvipotentan s β (c.f. Napomena 6.32). Zato je $S \sim \alpha$, a α je kardinal jer nije ekvipotentan manjem ordinalu.

Za jedinstvenost pretpostavimo da postoje dva različita kardinala, α i β , ekvipotentna s S . Tada je $\alpha \sim \beta$ i bez smanjenja općenitosti možemo pretpostaviti da je $\alpha < \beta$. Zato β nije kardinal. $\square$

Definicija 8.4. Neka je S skup. Kardinalni broj κ ekvipotentan s S nazivamo kardinalni broj od S i označavamo $\kappa = |S|$ ili $\kappa = \aleph(S)$.

Propozicija 8.5. Neka su a i b skupovi. Tada vrijedi:

1. $|a| = |b|$ ako i samo ako je $a \sim b$,
2. $|a| \leq |b|$ ako i samo ako postoji injekcija $a \rightarrow b$,
3. $|a| \leq |b|$ ako i samo ako je $a = \emptyset$ ili postoji surjekcija $b \rightarrow a$.

Dokaz. 1. Jasno.

2. Ako je $|a| \leq |b|$ onda je inkluzija $|a| \rightarrow |b|$ injekcija. Komponiranjem s bijekcijama iz definicije kardinalnog broja dobivamo injekciju $a \rightarrow b$.

Ako postoji injekcija $a \rightarrow b$, komponiranjem s bijekcijama iz definicije kardinalnog broja dobivamo injekciju $|a| \rightarrow |b|$. Pretpostavimo suprotno, da je $|a| > |b|$, pa je inkluzija $|b| \rightarrow |a|$ injekcija. Cantor-Schröder-Bernsteinov teorem tada povlači da je $|a| \sim |b|$, dakle $|a| = |b|$, što proturječi pretpostavci.

3. Zbog točke 2. dovoljno je dokazati da postoji injekcija $a \rightarrow b$ ako i samo ako je $a = \emptyset$ ili postoji surjekcija $b \rightarrow a$.

Pretpostavimo da postoji injekcija $f : a \rightarrow b$. Ako je $a = \emptyset$ gotovi smo. U protivnom uzmimo $t \in a$ i definirimo funkciju $g : b \rightarrow a$ sa

$$g(y) = \begin{cases} x & (\exists x \in a)(f(x) = y) \\ t & \text{inače.} \end{cases}$$

Lako se vidi da je g dobro definirana i surjekcija, što je trebalo pokazati.

Obratno, ako je $a = \emptyset$, prazan skup je i tražena injekcija. Ako postoji surjekcija $g : b \rightarrow a$, za svaki $y \in a$ skup $g^{-1}(\{y\}) = \{x \in b \mid g(x) = y\}$ je neprazan. Postoji funkcija izbora koja svakom takvom skupu pridružuje jedan njegov element, pa komponirana s funkcijom $y \mapsto g^{-1}(\{y\})$ daje funkciju $f : a \rightarrow b$ koja svakom $y \in a$ pridružuje neki $x \in b$ takav da je $g(x) = y$. Dobivena je funkcija jasno injekcija. $\square$

8.2 Operacije na kardinalima

Definicija 8.6. Neka su κ i λ kardinalni brojevi.

- $\kappa + \lambda := |\kappa \times \{0\} \cup \lambda \times \{1\}|$,
- $\kappa \cdot \lambda := |\kappa \times \lambda|$,
- $\kappa^\lambda := |\{f : \lambda \rightarrow \kappa\}|$.

Propozicija 8.7. Neka su a i b skupovi.

1. Ako su a i b disjunktni, onda je $|a \cup b| = |a| + |b|$.
2. $|a \times b| = |a| \cdot |b|$.
3. $|a|^{|b|} = |\{f : b \rightarrow a\}|$.
4. $|\mathcal{P}(a)| = 2^{|a|}$.

Dokaz. D.Z. $\square$

Propozicija 8.8. Za svake kardinale κ , λ i μ vrijedi

$$\begin{array}{lll}
0 + \kappa = \kappa & 0 \cdot \kappa = 0, \quad 1 \cdot \kappa = \kappa & \kappa^0 = 1, \quad 0^\kappa = 0 \text{ za } \kappa > 0 \\
\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu & \kappa \cdot (\lambda \cdot \gamma) = (\kappa \cdot \lambda) \cdot \mu & \kappa^1 = \kappa, \quad 1^\kappa = 1 \\
\kappa + \lambda = \lambda + \kappa & \kappa \cdot \lambda = \lambda \cdot \kappa & \kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu, \quad \kappa^{\lambda \cdot \mu} = (\kappa^\lambda)^\mu \\
& \kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu & (\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu \\
\kappa \leq \lambda \Rightarrow \kappa + \mu \leq \lambda + \mu & \kappa \leq \lambda \Rightarrow \kappa \cdot \mu \leq \lambda \cdot \mu & \kappa \leq \lambda \Rightarrow \kappa^\mu \leq \lambda^\mu \\
& & \lambda \leq \mu \Rightarrow \kappa^\lambda \leq \kappa^\mu \text{ za } \kappa \geq 1
\end{array}$$

Dokaz. D.Z. □

8.3 Hijerarhija alefa

Iz Cantorova osnovnog teorema znamo da za svaki kardinalni broj κ postoji veći kardinalni broj $|\mathcal{P}(\kappa)| = 2^\kappa$. Ne znamo postoje li kardinalni brojevi između, no možemo definirati

$$\kappa^\dagger := \min\{\lambda \leq 2^\kappa \mid \lambda \text{ je kardinalni broj i } \lambda > \kappa\}, \quad (8.1)$$

što je prvi kardinalni broj veći od κ , tj. *sljedbenik* među kardinalnim brojevima.

Propozicija 8.9. Neka je S skup kardinalnih brojeva. Tada je $\cup S$ kardinalni broj.

Dokaz. Znamo da je $\cup S$ redni broj, i da je on supremum od S . Pretpostavimo suprotno, da on nije kardinalni broj, tj. da postoji kardinalni broj $\kappa < \cup S$ takav da je $\kappa \sim \cup S$. Uzmimo bijekciju $f: \cup S \rightarrow \kappa$. Kako je $\cup S$ supremum od S postoji kardinalni broj $\lambda \in S$ takav da je $\kappa < \lambda$. Restrikcija $f|_\lambda: \lambda \rightarrow \kappa$ je injekcija, pa je $\lambda \leq \kappa$, što je kontradikcija. □

Sada možemo transfinitnom rekurzijom za svaki ordinal α definirati kardinalni broj $\aleph_\alpha$:

- $\aleph_0 = \omega$,
- $\aleph_{\alpha^+} = \aleph_\alpha^\dagger$,
- za granični α $\aleph_\alpha = \cup\{\aleph_\beta \mid \beta < \alpha\}$.

Propozicija 8.10. 1. Za svake ordinale α i β $\alpha < \beta$ povlači $\aleph_\alpha < \aleph_\beta$.

2. Za svaki ordinal α vrijedi $\alpha \leq \aleph_\alpha$.

Dokaz. 1. D.Z.

2. Dokazujemo primitivnom transfinitnom indukcijom.

Za $\alpha = 0$ jasno je $0 \leq \aleph_0$.

Pretpostavimo da za neki ordinal α vrijedi $\alpha \leq \aleph_\alpha$. Jasno je $\aleph_{\alpha^+} > \aleph_\alpha \geq \alpha$, pa je $\aleph_{\alpha^+} \geq \alpha^+$.

Neka je α granični ordinal i neka za svaki $\beta < \alpha$ vrijedi $\beta \leq \aleph_\beta < \aleph_\alpha$. Dakle $\aleph_\alpha$ je gornja međa od α , pa mora biti $\aleph_\alpha \geq \sup \alpha = \alpha$ (c.f. Propozicija 6.29). □

Teorem 8.11. *Svaki kardinalni broj je ili konačan ili jednak $\aleph_\alpha$ za neki redni broj α .*

Dokaz. Pretpostavimo da je κ beskonačan kardinalni broj. Zbog Propozicije 8.10 2. vrijedi $\kappa \leq \aleph_\kappa$. Neka je α najmanji ordinal takav da je $\kappa \leq \aleph_\alpha$. Tvrdimo da vrijedi jednakost. Pretpostavimo suprotno, da je $\kappa < \aleph_\alpha$.

Ako je $\alpha = 0$ imamo $\kappa < \aleph_0 = \omega$, dakle κ je konačan što proturječi pretpostavci.

Ako je α sljedbenik, tj. postoji β takav da je $\alpha = \beta^+$, imamo $\kappa \leq \aleph_\beta$ jer ne postoji kardinal između $\aleph_\beta$ i $\aleph_{\beta^+}$. To proturječi izboru α .

Ako je α granični ordinal $\aleph_\alpha = \sup\{\aleph_\beta \mid \beta < \alpha\}$, pa κ nije gornja međa od $\{\aleph_\beta \mid \beta < \alpha\}$, tj. postoji $\beta < \alpha$ takav da je $\kappa < \aleph_\beta$. To također proturječi izboru α . $\square$

Nismo odgovorili na pitanje koji je odnos 2^κ i κ^+ . Posebno, koji je odnos $2^{\aleph_0}$ i $\aleph_1$? Jasno je $2^{\aleph_0} \geq \aleph_1$, no je li jednako? Tvrdnja da je $2^{\aleph_0} = \aleph_1$ naziva se *hipoteza kontinuuma*.

Odgovor je vrlo zanimljiv. Naprednim metodama u matematičkoj logici, tzv. forcingom, može se dokazati da je hipoteza kontinuuma neodgovoriva u Zermelo–Fraenkelovoj teoriji skupova. To znači da se ne može dokazati niti opovrgnuti pomoću navedenih aksioma.

8.4 Teorem o kvadratu

Propozicija 8.12. *Svaki beskonačni kardinalni broj je granični ordinal.*

Dokaz. D.Z. $\square$

Teorem 8.13. *Za svaki beskonačni kardinalni broj vrijedi $\kappa^2 = \kappa$.*

Dokaz. Lako se vidi da je $\kappa^2 \geq \kappa$, pa je dovoljno dokazati da je $\kappa^2 \leq \kappa$. Pretpostavimo suprotno, da postoji beskonačni kardinalni broj takav da je $\kappa^2 > \kappa$, i neka je κ upravo najmanji takav.

Neka je $f : \kappa \times \kappa \rightarrow \kappa \times \kappa \times \kappa$ zadana sa $f(\alpha, \beta) = (\alpha, \beta, \max(\alpha, \beta))$ i neka je $M := \text{rng}(f)$. Jasno je f bijekcija između $\kappa \times \kappa$ i M , pa je $\kappa^2 \sim M$ te je po pretpostavci je $|M| > \kappa$.

$M \subseteq \kappa \times \kappa \times \kappa$ je dobro uređen antileksikografskim uređajem, i κ je dobro uređen kao ordinal. Zbog $|M| > \kappa$ Teorem 6.4 povlači da je κ sličan početnom komadu u M , tj. postoji $u = (\alpha, \beta, \gamma) \in M$ takav da je $\kappa \simeq p_M(u)$.

Jer je κ granični ordinal (Propozicija 8.12) vrijedi $\gamma^+ < \kappa$ pa je $v := (\gamma^+ \gamma^+, \gamma^+) \in M$ i u antileksikografskom uređaju je $u < v$. Zato je $\kappa \leq |p_M(v)|$. Za svaki $(\alpha', \beta', \gamma') \in p_M(v)$ vrijedi $\alpha', \beta' \leq \gamma' \leq \gamma^+$, pa je $p_M(v) \subseteq \gamma^+ \times \gamma^+ \times \gamma^+$. To povlači da je $\kappa \leq |\gamma^+|^3$. Nazovimo $\lambda := |\gamma^+|$. Vrijedi $\lambda \leq \gamma^+ < \kappa$, pa imamo $\lambda < \kappa \leq \lambda^3$.

Kardinal λ nije konačan zbog $\kappa \leq \lambda^3$ i manji je od κ , pa po izboru od κ mora biti $\lambda^2 = \lambda$. No tada je $\lambda^3 = \lambda \cdot \lambda^2 = \lambda \cdot \lambda = \lambda^2 = \lambda$, u kontradikciji s $\lambda < \lambda^3$. $\square$

Sljedeća propozicija implicira da su zbrajanje i množenje beskonačnih kardinalnih brojeva zapravo trivijalne operacije.

Propozicija 8.14. *Neka su κ i λ kardinalni brojevi od kojih je barem jedan beskonačan. Tada vrijedi*

$$1. \kappa + \lambda = \max(\kappa, \lambda);$$

$$2. \text{ ako niti jedan od } \kappa \text{ i } \lambda \text{ nije } 0, \text{ onda je } \kappa \cdot \lambda = \max(\kappa, \lambda)$$

Dokaz. Bez smanjenja općenitosti je $\lambda \leq \kappa$ i onda κ mora biti beskonačan. Imamo

$$\kappa = \kappa + 0 \leq \kappa + \lambda \leq \kappa + \kappa = \kappa \cdot 2 \leq \kappa \cdot \kappa = \kappa^2 = \kappa.$$

Zato je $\kappa = \kappa + \lambda$. Slično ako je $\lambda \geq 1$

$$\kappa = \kappa \cdot 1 \leq \kappa \cdot \lambda \leq \kappa \cdot \kappa = \kappa^2 = \kappa.$$

Zato je $\kappa = \kappa \cdot \lambda$.

□

9 Skupovi brojeva

9.1 Skup cijelih brojeva

Na ω^2 definirajmo relaciju

$$(a, b) \sim (c, d) :\Leftrightarrow a + d = b + c. \quad (9.1)$$

Lako se utvrdi da je to relacija ekvivalencije (D.Z.).

Skup cijelih brojeva je kvocijentni skup $\mathbb{Z} := \omega^2 / \sim$.

Na $\mathbb{Z}$ definiramo operacije i uređaj:

$$(a, b) + (c, d) = (a + c, b + d), \quad (9.2)$$

$$(a, b) \cdot (c, d) = (ac + bd, ad + bc), \quad (9.3)$$

$$(a, b) < (c, d) :\Leftrightarrow a + d < c + b. \quad (9.4)$$

Propozicija 9.1. 1. Operacije $+$ i $\cdot$ te relacija $<$ dobro su definirane, tj. ne ovise o izboru reprezentanta.

2. $(\mathbb{Z}, +, \cdot)$ je integralna domena.

3. $(\mathbb{Z}, <)$ je totalno uređeni skup. Zbrajanje čuva uređaj.

4. $\omega \rightarrow \mathbb{Z}$, $n \mapsto [(n, 0)]$ je ulaganje, tj. injekcija koja čuva operacije i uređaj.

Dokaz. D.Z. □

Propozicija 9.2. Svaki cijeli broj x je oblika $[(n, 0)]$ ili oblika $[(0, n)]$. Jedini broj koji je oba oblika je $[(0, 0)]$.

Dokaz. D.Z. □

Brojevi oblika $[(n, 0)]$ mogu se dobiti inkluzijom $\omega \rightarrow \mathbb{Z}$ i jednostavno se označavaju s n . Brojevi oblika $[(0, n)]$ označavaju se s $-n$.

Skup pozitivnih cijelih brojeva je $\mathbb{Z}_+ := \{x \in \mathbb{Z} \mid x > 0\}$.

9.2 Skup racionalnih brojeva

Na $\mathbb{Z} \times \mathbb{Z}_+$ definirajmo relaciju

$$(a, b) \sim (c, d) : \Leftrightarrow ad = bc. \quad (9.5)$$

Lako se utvrdi da je to relacija ekvivalencije (D.Z.).

Skup racionalnih brojeva je kvocijentni skup $\mathbb{Q} := \mathbb{Z} \times \mathbb{Z}_+ / \sim$.

Klasu ekvivalencije $[(a, b)]$ označavamo s $\frac{a}{b}$.

Na $\mathbb{Q}$ definiramo operacije i uređaj:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}, \quad (9.6)$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad (9.7)$$

$$\frac{a}{b} < \frac{c}{d} : \Leftrightarrow ad < cb. \quad (9.8)$$

Propozicija 9.3. 1. Operacije $+$ i $\cdot$ te relacija $<$ dobro su definirane, tj. ne ovise o izboru reprezentanta.

2. $(\mathbb{Q}, +, \cdot, <)$ je uređeno polje karakteristike 0.
3. $(\mathbb{Q}, <)$ je totalno uređeni skup. Zbrajanje čuva uređaj.
4. $\mathbb{Z} \rightarrow \mathbb{Q}, x \mapsto \frac{x}{1}$ je ulaganje, tj. injekcija koja čuva operacije i uređaj.

Dokaz. D.Z. □

9.3 Skup realnih brojeva

Realne brojeve definiramo Dedekindovim rezovima, što nam je poznato iz drugih kolegija. Ovdje nećemo detaljno sve definirati i dokazati. Ponovimo samo definiciju i osnovna svojstva koja su nam zanimljiva iz perspektive skupova.

Definicija 9.4. Skup $a \subseteq \mathbb{Q}$ je realan broj ako je

- $\emptyset \subset a \subset \mathbb{Q}$,
- a zatvoren prema dolje, tj. za svaki $y \in a$ i $x \in \mathbb{Q}$ $x < y$ povlači $y \in a$,
- a nema najveći element.

Skup svih realnih brojeva označavamo s $\mathbb{R}$.

Za $a, b \in \mathbb{R}$ definiramo uređaj

$$a < b : \Leftrightarrow a \subset b. \quad (9.9)$$

Funkcija $\mathbb{Q} \rightarrow \mathbb{R} q \mapsto \{x \in \mathbb{Q} \mid x < q\}$ je ulaganje, tj. injekcija koja čuva operacije i uređaj.

9.4 Invarijante sličnosti

Definicija 9.5. Za svojstvo (logički izraz) P totalno uređenih skupova kažemo da je invarijanta sličnosti ako za svake totalno uređene skupove A i B $P(A)$ i $A \simeq B$ povlači $P(B)$.

Definicija 9.6. Neka je $(A, <)$ totalno uređeni skup i $B \subseteq A$.

Kažemo da je B gust u $(A, <)$ ako za svake $x, y \in A$, $x < y$ postoji $z \in B$ takav da je $x < z < y$.

Kažemo da je $(A, <)$ gust u sebi ili gust ako je A gust u $(A, <)$.

Definicija 9.7. Totalno uređeni skup $(A, <)$ je separabilan ako postoji prebrojiv $B \subseteq A$ gust u $(A, <)$.

Definicija 9.8. Totalno uređeni skup $(A, <)$ je potpun ako svaki odozgo ograničen $B \subseteq A$ ima supremum u $(A, <)$.

Propozicija 9.9. Sljedeća svojstva totalno uređenog skupa $(A, <)$ su invarijante sličnosti:

1. za fiksni kardinalni broj κ $|A| = \kappa$;
2. $(A, <)$ ima najmanji (najveći) element;
3. $(A, <)$ je dobro uređen;
4. $(A, <)$ je gust;
5. $(A, <)$ je separabilan;
6. $(A, <)$ je potpun.

Dokaz. D.Z. □

Propozicija 9.10. 1. Skupovi $\mathbb{Z}$ i $\mathbb{Q}$ su prebrojivi, tj. kardinalni broj im je $\aleph_0$.

2. Skupovi $\mathbb{Z}$, $\mathbb{Q}$ i $\mathbb{R}$ nemaju ni minimum ni maksimum.
3. $\mathbb{Q}$ je gust u sebi. $\mathbb{Q}$ je gust u $\mathbb{R}$. $\mathbb{R}$ je separabilan.
4. $\mathbb{R}$ je potpun.

Dokaz. 1. D.Z.

2. D.Z.

3. Uzmimo $q, r \in \mathbb{Q}$, $q < r$. Neka je $s := (q + r) \cdot \frac{1}{2}$. Lako se vidi da je $q < s < r$. Zato je $\mathbb{Q}$ gust u sebi.

Primijetimo da formalno $\mathbb{Q}$ nije podskup od $\mathbb{R}$. No $\mathbb{Q}$ poistovjećujemo sa slikom ulaganja $u: q \mapsto \{x \in \mathbb{Q} \mid x < q\} \in \mathbb{R}$ koju ćemo isto, zloupotrebom notacije, označavati s $\mathbb{Q}$. Dokažimo da je takav $\mathbb{Q}$ gust u $\mathbb{R}$.

Neka su $a, b \in \mathbb{R}$, $a < b$. Tj. $a \subset b$, pa postoji $q \in b \setminus a$. Jer b nema maksimum postoji $r \in b$ veći od q . Zbog zatvorenosti od a prema dolje vrijedi i $r \notin a$.

Svaki $x \in u(r)$ manji je od $r \in b$, pa zatvorenost od b prema dolje povlači $x \in b$, dakle $u(r) \subseteq b$. No $r \notin u(r)$, pa vrijedi $u(r) \subset b$, tj. $u(r) < b$.

Uzmimo $x \in a$ i usporedimo ga s r . Jer $r \notin a$ ne može biti $x = r$. Kada bi bilo $x > r$ zbog zatvorenosti prema dolje od a bilo bi i $r \in a$, što nije. Dakle $x < r$, tj. $x \in u(r)$. Kako je $x \in a$ bio proizvoljan zaključujemo da je $a \subseteq u(r)$. Primijetimo da je $q \in u(r)$, ali $q \notin a$, dakle $a \subset u(r)$, tj. $a < u(r)$.

Dakle, konstruirali smo $u(r)$ u (poistovjećenju slici od) $\mathbb{Q}$ takav da je $a < u(r) < b$. Zato je $\mathbb{Q}$ gust u $\mathbb{R}$.

Separabilnost od $\mathbb{R}$ slijedi direktno iz činjenice da je $\mathbb{Q}$ prebrojiv.

4. D.Z.

□

9.5 Uređajne karakterizacije

Definicija 9.11. Za svojstvo (logički izraz) P totalno uređenih skupova kažemo da je uređajna karakterizacija ako za totalno uređene skupove A i B $P(A)$ i $P(B)$ povlači $A \simeq B$.

Svojstvo P je uređajna karakterizacija totalno uređenog skupa A ako je uređajna karakterizacija i vrijedi $P(A)$.

Teorem 9.12 (Uređajna karakterizacija konačnog skupa). Neka je $(A, <)$ totalno uređeni skup i $n \in \omega$. Ako je $A \sim n$ onda je $(A, <) \simeq (n, <)$.

Dokaz. D.Z.

□

Teorem 9.13 (Uređajna karakterizacija skupa prirodnih brojeva). Neka je $(A, <)$ totalno uređeni skup. Ako je A beskonačan i svaki početni komad u $(A, <)$ je konačan, onda je $(A, <) \simeq (\omega, <)$.

Dokaz. Definirajmo funkciju $f : A \rightarrow \omega$, $f(x) = |p_A(x)|$. Jer je svaki početni komad konačan, rezultat je zaista u ω . Tvrdimo da je f sličnost. Dovoljno je dokazati da čuva uređaj i da je surjekcija.

Neka su $x, y \in A$, $x < y$. Tada je $p_A(x) \subset p_A(y)$ pa Propozicija 5.7 povlači $|p_A(x)| \leq |p_A(y)|$. Jednakost nije moguća jer bi onda bijekcija $p_A(y) \rightarrow p_A(x)$ bila injekcija $p_A(y) \rightarrow p_A(y)$, pa i surjekcija zbog Teorema 5.5 3. što je jasno da nije. Dakle $f(x) = |p_A(x)| < |p_A(y)| = f(y)$, tj. f čuva uređaj.

Dokažimo indukcijom da je $\text{rng}(f) = \omega$.

Baza: Uzmimo $x \in A$. Ako je $p_A(x) = \emptyset$ onda je $f(x) = 0$ pa smo gotovi. U protivnom $p_A(x)$ je neprazan i konačan, pa ima minimum $m := \min p_A(x)$. Lako se vidi da je m najmanji i u A , što povlači da je $p_A(m) = \emptyset$, dakle $f(m) = 0$.

Pretpostavka: Za $n \in \omega$ postoji $x \in A$ takav da je $f(x) = n$.

Korak: Jer je A beskonačan, a $\bar{p}_A(x) = p_A(x) \cup \{x\}$ konačan, postoji $y \in A \setminus \bar{p}_A(x)$. Jasno je $\bar{p}_A(x) \subseteq p_A(y)$.

Ako je $\bar{p}_A(x) = p_A(y)$ onda je $f(y) = |p_A(y)| = |\bar{p}_A(x)| = |p_A(x)| + 1 = n + 1$, čime je korak indukcije završen.

Ako je $\bar{p}_A(x) \subset p_A(y)$ neka je $m := \min(p_A(y) \setminus \bar{p}_A(x))$. Lako se vidi da je $p_A(m) = \bar{p}_A(x)$ pa analogno dobijemo da je $f(m) = n + 1$. $\square$

Definicija 9.14. Neka je $(A, <)$ totalno uređeni skup i $x, y \in A$, $x \leq y$. Segment od x i y u $(A, <)$ je $[x, y]_A := \{z \in A \mid x \leq z \leq y\}$.

Teorem 9.15 (Uređajna karakterizacija skupa cijelih brojeva). Neka je $(A, <)$ totalno uređeni skup. Ako je A neprazan, $(A, <)$ nema ni minimum ni maksimum i svaku segment u $(A, <)$ je konačan, onda je $(A, <) \simeq (\mathbb{Z}, <)$.

Dokaz. Fiksirajmo $a \in A$. Neka su $P := \{x \in A \mid x \geq a\}$ i $N := \{x \in A \mid x < a\}$. Jasno je $A = P \cup N$, $P \cap N = \emptyset$ i za svake $x \in N$ i $y \in P$ je $x < y$.

Kad bi P bio konačan imao bi maksimum koji bi bio maksimum i od A . Dakle P je beskonačan.

Neka je $x \in P$. Zatvoreni početni komad $\bar{p}_P(x) = [a, x]_A$ je segment u A , dakle konačan je. Otvoreni početni komad je njegov podskup, dakle također je konačan.

Sada Teorem 9.13 povlači da postoji sličnost $f: \omega \rightarrow (P, <)$. Na analogan se način konstruira sličnost $g: \omega \rightarrow (N, >)$. Neka je $h: \mathbb{Z} \rightarrow A$

$$h(n) = \begin{cases} f(n) & n \geq 0 \\ g(-n-1) & n < 0. \end{cases}$$

Lako se provjeri da h čuva uređaj i da je $\text{rng}(h) = P \cup N = A$, dakle h je sličnost. $\square$

Teorem 9.16 (Uređajna karakterizacija skupa racionalnih brojeva). Neka je $(A, <)$ totalno uređeni skup. Ako je A prebrojiv, $(A, <)$ je gust i nema ni minimum ni maksimum, onda je $(A, <) \simeq (\mathbb{Q}, <)$.

Dokaz. A i $\mathbb{Q}$ su prebrojivi, pa ih poredajmo u nizove $A = \{a_0, a_1, \dots\}$ i $\mathbb{Q} = \{q_0, q_1, \dots\}$. Konstruiramo niz $f: \omega \rightarrow A \times \mathbb{Q}$. Cilj je da $\text{rng}(f)$ bude tražena sličnost $A \rightarrow \mathbb{Q}$. Dakle želimo sve elemente a_i i q_i spariti tako da se svaki pojavljuje točno jednom u nekom paru $f(n)$. Konstrukcija je rekurzivna:

- $f(0) = (a_0, q_0)$.
- Neka je n paran i neka su već konstruirani parovi $f(0), f(1), \dots, f(n-1)$. Neka je

$$A_n := \{x \in A \mid (\exists i \in \omega)(\exists q \in \mathbb{Q}) f(i) = (x, q)\}$$

skup svih već iskorištenih elemenata od A . Neka je $a \in A$ prvi član niza $(a_0, a_1, \dots)$ koji nije u A_n . Neka su $V := \{x \in A_n \mid x > a\}$ i $M := \{x \in A_n \mid x < a\}$. Imamo 3 slučaja:

- $V \neq \emptyset$ i $M \neq \emptyset$. Neka je $a_p := \max M$ i $a_s := \min V$, tj. a se nalazi između a_p i a_s od već iskorištenih elemenata od A . Neka su $(a_p, q_p), (a_s, q_s) \in \text{rng}(f|_n)$, tj. q_p i q_s su već konstruirani parovi od a_p i a_s . Želimo da par od a bude između q_p i q_s . Pa uzmimo prvi neiskorišteni q u nizu $(q_0, q_1, \dots)$ koji se nalazi između q_p i q_s . Takav postoji (štoviše postoji beskonačno takvih) zbog gustoće od $\mathbb{Q}$. Neka je $f(n) = (a, q)$.
- $V = \emptyset$ i $M \neq \emptyset$. Neka je $a_p := \max M$. Neka je $(a_p, q_p) \in \text{rng}(f|_n)$, tj. q_p je već konstruiran par od a_p . Neka je q prvi neiskorišteni u nizu $(q_0, q_1, \dots)$ koji je veći od q_p . Takav postoji (štoviše postoji beskonačno takvih) jer $\mathbb{Q}$ nema maksimum. Neka je $f(n) = (a, q)$.
- $V \neq \emptyset$ i $M = \emptyset$. Analogno prethodnoj točki definiramo $f(n) = (a, q)$ gdje je q prvi neiskorišteni manji od para od $\min V$.

Slučaj kada je $V = \emptyset$ i $M = \emptyset$ nije moguć jer je $a_0 \in A_n$.

- Neka je n neparan. Konstruiramo $f(n)$ na analogan način pri čemu zamijenimo uloge A i $\mathbb{Q}$. Dakle uzmemo $q \in \mathbb{Q}$ prvi neiskorišteni element od $\mathbb{Q}$ i nađemo $a \in A$ koji je u prikladnom odnosu s q .

Neka je $s := \text{rng}(f) \subseteq A \times \mathbb{Q}$. Tvrdimo da je s sličnost između A i $\mathbb{Q}$.

Rekurzivna konstrukcija od f upravo je takva da se indukcijom lako pokaže da je za svaki $n \in \omega$ slika $\text{rng}(h|_n)$ funkcija koja čuva uređaj. Zato je s , koji je jednak uniji svih $\text{rng}(h|_n)$, također funkcija koja čuva uređaj. Još samo treba dokazati da mu je domena A i slika $\mathbb{Q}$.

Beskonačno smo puta (za svaki parni n) birali najmanji neiskorišteni član niza $(a_0, a_1, \dots)$, pa smo sigurno izabrali sve, tj. $\text{dom}(h) = A$. Analogno se pokaže da je $\text{rng}(h) = \mathbb{Q}$. $\square$

Teorem 9.17 (Uređajna karakterizacija skupa realnih brojeva). *Neka je $(A, <)$ totalno uređeni skup. Ako je $(A, <)$ separabilan, potpun i nema ni minimum ni maksimum, onda je $(A, <) \simeq (\mathbb{R}, <)$.*

Dokaz. Budući da je A separabilan, postoji prebrojiv $B \subseteq A$ gust u A . Tada je i gust u sebi.

Pretpostavimo da B ima minimum m . A nema minimum, pa postoji $a \in A$, $a < m$. Jer je B gust u A postoji $b \in B$ takav da je $a < b < m$, što proturječi izboru m . Dakle B nema minimum. Analogno nema ni maksimum.

Dakle B zadovoljava uređajnu karakterizaciju racionalnih brojeva (Teorem 9.16) pa postoji sličnost $f : \mathbb{Q} \rightarrow B$.

Neka je $x \in \mathbb{R}$. Iz definicije realnih brojeva proizlazi da je x neprazan odozgo ograničen podskup od $\mathbb{Q}$. Jer f čuva uređaj $f^{-1}(x) \subseteq B$ također je neprazan odozgo ograničen skup. Sada, zbog potpunosti od A , $f^{-1}(x)$ ima supremum u A .

Zato možemo definirati funkciju $F : \mathbb{R} \rightarrow A$, $x \mapsto \sup f^{-1}(x)$. Dokažimo da je F sličnost.

Dokažimo prvo da čuva uređaj. Neka su $x, y \in \mathbb{R}$ takvi da je $x < y$, tj. $x \subset y$. Uzmimo $q \in y \setminus x$. Jer je x zatvoren prema dolje $q \notin x$ povlači da je q gornja međa od x . Jer y nema maksimum q nije gornja međa od y . Jer f čuva uređaj to povlači da je $f(q)$ gornja međa od $f^{-1}(x)$, ali nije gornja međa od $f^{-1}(y)$. Zato je

$$F(x) = \sup f^{-1}(x) \leq f(q) < \sup f^{-1}(y) = F(y),$$

dakle $F(x) < F(y)$.

Još treba dokazati da je F surjekcija na A . Uzmimo $a \in A$. Neka je $S := \{b \in B \mid b < a\}$. Tvrdimo da je $x := f^{\leftarrow}(S)$ realan broj i da je $F(x) = a$.

Za dokazati da je x realan broj treba dokazati da nije jednak praznom skupu niti cijelom $\mathbb{Q}$, da je zatvoren prema dolje i da nema maksimum. Budući da je f sličnost dovoljno je dokazati iste stvari za S (gdje $\mathbb{Q}$ zamijenimo s B).

A nema ni minimum ni maksimum, pa postoje $m', M' \in A$ takvi da je $m' < a < M'$. Jer je B gust u A postoje $m, M \in B$ takvi da je $m' < m < a < M < M'$. Vrijedi $m \in S$, pa je $S \neq \emptyset$. Slično $M \notin S$ povlači $S \neq B$.

Jasno je da je S zatvoren prema dolje.

Pretpostavimo da je $m \in S$ najveći element. Jer je B gust u A postoji $b \in B$ takav da je $m < b < a$. Zato je $b \in S$ veći od m , što proturječi izboru od m kao najvećeg. Dakle S nema najveći element.

Dakle x je zaista realan broj.

Vrijedi $F(x) = \sup f^{\rightarrow}(x) = \sup S$. Po definiciji je a gornja međa od S . Pretpostavimo da je $\sup S < a$. Gustoća od B u A povlači da postoji $b \in B$ takav da je $\sup S < b < a$. No tada je $b \in S$ veći od supremuma, kontradikcija. Dakle zaista vrijedi $F(x) = \sup S = a$. $\square$

10 Dobra utemeljenost skupova

10.1 Aksiom dobre utemeljenosti

Svi skupovi koje smo konstruirali u ovom kolegiju, a praktički i svi skupovi koji se koriste u matematici, dobijaju su raznim konstrukcijama počevši od praznog skupa: prirodni brojevi dobiveni su operacijom sljedbenik počevši od $\emptyset$; ordinali još koriste uniju; cijeli, racionalni i realni brojevi konstruiraju se počevši od prirodnih, itd. Ipak, navedeni aksiomi ne zabranjuju da postoje i drugačiji skupovi. Na primjer skup koji bi bio element samog sebe ne može nastati nikakvom konstrukcijom počevši od $\emptyset$, a za sada nije zabranjen. Zbog toga se u teoriji skupova obično dodaje aksiom koji zabranjuje sve skupove koji nisu “dobro utemeljeni”.

Aksiom 10 (Aksiom dobre utemeljenosti ili Aksiom regularnosti). *Za svaki neprazan skup x postoji $y \in x$ disjunktan s x . Formalno*

$$(\forall x)(x \neq \emptyset \rightarrow (\exists y \in x)(x \cap y = \emptyset)).$$

Ovaj aksiom nigdje nismo koristili i uglavnom ga nije potrebno koristiti. Skupovi koji nisu dobro utemeljeni mogu se jednostavno ignorirati i ne koristiti u matematici. Ipak, može se činiti jasnijim da takvi skupovi niti ne postoje. Za neke analize teorije skupova to je i nužno.

Propozicija 10.1. *Za svaki skup x vrijedi $x \notin x$.*

Dokaz. Pretpostavimo suprotno, da je $x \in x$. Promotrimo skup $\{x\}$ (dobiven Aksiomom para). Taj je skup neprazan, pa po Aksiomu dobre utemeljenosti postoji njegov element, koji mora biti x , disjunktan s $\{x\}$. No oni nisu disjunktni jer je x element oba. $\square$

Sljedeća propozicija povlači da ako izaberemo element nekog skupa, pa zatim element tog elementa, itd., nakon konačno koraka doći ćemo do praznog skupa.

Propozicija 10.2. *Ne postoji beskonačan niz a takav da za svaki $n \in \omega$ vrijedi $a(n^+) \in a(n)$.*

Dokaz. Pretpostavimo suprotno, da postoji takav niz. Promotrimo skup $\text{rng}(a)$ i uzmimo neki njegov element $a(n)$. Vrijedi $a(n^+) \in a(n)$ i $a(n^+) \in \text{rng}(a)$. Kako je $a(n) \in \text{rng}(a)$ bio proizvoljan to proturječi Aksiomu dobre utemeljenosti. $\square$

10.2 Kumulativna hijerarhija skupova

Jedna od praktičnih posljedica Aksioma dobre utemeljenosti jest kumulativna hijerarhija, točnije rezultat da se svaku skup nalazi negdje u toj hijerarhiji.

Skupove kumulativne hijerarhije definiramo primitivnom transfinitnom indukcijom: za ordinal α definiramo V_α sa

- $V_0 = \emptyset$,
- $V_{\alpha^+} = \mathcal{P}(V_\alpha)$,
- za granični α $V_\alpha = \cup\{V_\beta \mid \beta < \alpha\}$.

Propozicija 10.3. 1. Za svaki ordinal α V_α je tranzitivan skup.

2. Neka su α i β ordinali, $\beta < \alpha$. Tada je $V_\beta \subseteq V_\alpha$.

Dokaz. 1. Dokažimo transfinitnom indukcijom.

Za $\alpha = 0$ tvrdnja je jasna.

Fiksirajmo α i pretpostavimo da za svaki $x \in V_\alpha$ vrijedi $x \subseteq V_\alpha$. Uzmimo $x \in y \in V_{\alpha^+} = \mathcal{P}(V_\alpha)$. To znači da je $x \in y \subseteq V_\alpha$ pa pretpostavka povlači da je $x \subseteq V_\alpha$, dakle $x \in \mathcal{P}(V_\alpha) = V_{\alpha^+}$, što je i trebalo pokazati.

Neka je α granični i pretpostavimo da tvrdnja vrijedi za svaki $\beta < \alpha$. Neka je $x \in V_\alpha$. Tada je $x \in V_\beta$ za neki $\beta < \alpha$ pa pretpostavka povlači da je $x \subseteq V_\beta \subseteq V_\alpha$, što je i trebalo pokazati.

2. Dokažimo transfinitnom indukcijom po α .

Za $\alpha = 0$ tvrdnja je jasna jer ne postoji $\beta < \alpha$.

Fiksirajmo α i pretpostavimo da za svaki $\beta < \alpha$ vrijedi $V_\beta \subseteq V_\alpha$. Uzmimo $\beta' < \alpha^+$, tj. $\beta' < \alpha$ ili $\beta' = \alpha$. U prvom slučaju pretpostavka povlači da je $V_{\beta'} \subseteq V_\alpha$. Točka 1. ove propozicije povlači da je $V_\alpha \subseteq V_{\alpha^+}$, pa u oba slučaja imamo $V_{\beta'} \subseteq V_{\alpha^+}$.

Ako je α granični ordinal tvrdnja slijedi direktno iz definicije.

□

Propozicija 10.4. Za svaki skup S postoji tranzitivan skup T takav da je $S \in T$.

Dokaz. Rekurzijom (na prirodnim brojevima) za $n \in \omega$ definiramo niz a :

- $a(0) = \{S\}$,
- $a(n^+) = \cup a(n)$.

Neka je $T := \text{Urng}(a)$. $S \in a(0)$ povlači $S \in T$.

Uzmimo neki $x \in T$. Tada je $x \in a(n)$ za neki $n \in \omega$. Vrijedi $x \subseteq \cup a(n) = a(n^+) \subseteq T$. Dakle, T je tranzitivan skup.

□

Lema 10.5. *Neka je S skup. Ako za svaki $x \in S$ postoji ordinal β takav da je $x \in V_\beta$, onda postoji ordinal α takav da je $S \in V_\alpha$.*

Dokaz. Za $x \in S$ neka je β_x najmanji ordinal takav da je $x \in V_{\beta_x}$ i neka je $\alpha := \sup\{\beta_x \mid x \in S\}$. Propozicija 10.3 2. povlači da je za svaki $x \in S$ i $x \in V_\alpha$, dakle $S \subseteq V_\alpha$. Zbog toga je $S \in \mathcal{P}(V_\alpha) = V_{\alpha^+}$. $\square$

Teorem 10.6. *Za svaki skup S postoji redni broj α takav da je $S \in V_\alpha$.*

Dokaz. Pretpostavimo suprotno, da postoji skup S koji nije element niti jednog V_α . Neka je T tranzitivan skup koji sadrži S (Propozicija 10.4). Neka je

$$U := \{x \in T \mid (\forall \text{ ordinal } \alpha)(x \notin V_\alpha)\}$$

skup svih elemenata od S koji nisu elementi niti jednog V_α . U je neprazan jer je $S \in U$, pa Aksiom regularnosti povlači da postoji $m \in U$ takav da je $m \cap U = \emptyset$.

Budući da je $m \in U \subseteq T$ tranzitivnost od T povlači $m \subseteq T$. Disjunktnost s U povlači da je $m \in T \setminus U$, dakle za svaki element od $x \in m$ postoji ordinal α takav da je $x \in V_\alpha$. Lema 10.5 povlači da postoji ordinal β takav da je $m \in V_\beta$, dakle $m \notin U$, kontradikcija. $\square$

Bibliografija

- [1] Hrbáček K. i Jech T. *Introduction to Set Theory*. Chapman & Hall/CRC Pure and Applied Mathematics. Taylor & Francis, 1999. ISBN: 9780824779153
- [2] Čačić V. *Teorija skupova - predavanja 2024./25*.
- [3] Bašić, B. *Ordinalni kalkulator*. Mag. rad. PMF–MO, rujan 2020.