Deseto predavanje iz Teorije skupova 16/12/2005

§2. Aksiomatska teorija skupova

U prethodnom poglavlju, koje je imalo naziv *Naivna teorija skupova*, naučili smo osnovne pojmove kao što su: (ne)prebrojivost, dobro uređeni skupovi, ... Tu smo već uočili probleme prilikom definicije kardinalnog broja. Zapravo govorili smo o kardinalnosti, a ne o kardinalnim brojevima. Naučili smo da svi beskonačni skupovi nemaju istu kardinalnost, te smo proučavali operacije kako bi dobili nove kardinalnosti. No, ne znamo što je kardinalni broj. To ćemo znati kada definiramo ordinalne ili redne brojeve. Dakle, imamo barem tri razloga za definiciju ordinalnog broja:

a) Moramo odgovoriti što je "nivo" u kumulativnoj hijerarhiji.

b) Prije smo već bili postavili problem kako definirati beskonačne redne brojeve.

c) Pomoću ordinalnih brojeva ćemo definirati kardinalne brojeve.

Ordinalni brojevi su neki dobro uređeni skupovi, pri čemu je relacija uređaja $\in$. Kardinalni brojevi su neki posebni ordinalni brojevi. (Svaki konačni ordinalni broj je kardinalni broj.)

Želimo naglasiti da bez obzira na naslov ovog poglavlja *Aksiomatska teorija skupova* sada se nećemo baviti aksiomima i formalnim dokazima. Naslov poglavlja je takav jer egzistencija objekata koje promatramo može biti dokazana pomoću aksioma Zermelo–Fraenkelove teorije.

Naveli smo većinu aksioma Zermelo–Fraenkelove teorije koji su nam bili potrebni kako bi definirali neke pojmove, odnosno dokazali neke tvrdnje. Preostalo je još iskazati aksiom beskonačnosti i shemu aksioma zamjene. Nakon definicije ordinalnog broja, navest ćemo teoreme enumeracije i rekurzije. Usput ćemo navesti kako uvesti, odnosno strogo definirati, skupove brojeva $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ i $\mathbb{R}$.

Definirat ćemo aritmetiku ordinalnih brojeva, tj. zbrajanje, množenje i potenciranje, te dokazati teorem o oduzimanju, teorem o ostatku, teorem o logaritamskom algoritmu i teorem o normalnoj formi za ordinalne brojeve. Posebno predavanje će biti posvećeno kardinalnim brojevima. Na samom kraju ćemo razmatrati aksiom izbora.

2.1. Prirodni brojevi

Često se može čuti da je teorija skupova osnova matematike. Razlog tome je da se mnogi matematički objekti mogu definirati u teoriji ZF, te se tu mogu dokazati njihova osnovna svojstva. Mi ćemo sada definirati skupove brojeva. Na taj način želimo upravo ilustrirati tvrdnju da je teorija skupova osnova matematike. Prvo ćemo definirati prirodne brojeve. Kasnije ćemo vidjeti da su prirodni brojevi zapravo konačni ordinalni brojevi. Dakle, prirodni brojevi su nam i dobra motivacija prije razmatranja ordinalnih brojeva.

Definicija 1 *Za skup x kažemo da je* **induktivan** *ako vrijedi $\emptyset \in x$ i za sve $y \in x$ vrijedi $(y \cup \{y\}) \in x$. Sa $Ind(x)$ označavamo formulu*

$$\emptyset \in x \ \wedge \ \forall y(y \in x \rightarrow y \cup \{y\} \in x).$$

Kažemo da je skup x **prirodan broj** *ako za sve induktivne skupove y vrijedi $x \in y$. Sa $Pri(x)$ označavamo formulu $\forall y(Ind(y) \rightarrow x \in y)$.*

Primjeri prirodnih brojeva: $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$

Iz do sada uvednih aksioma teorije ZF ne možemo dokazati egzistenciju skupa svih prirodnih brojeva. To nam omogućava sljedeći aksiom.

Aksiom beskonačnosti: Postoji induktivan skup, tj. formalno

$$\exists x\Big(\emptyset \in x \wedge \forall y(y \in x \rightarrow (y \cup \{y\}) \in x)\Big).$$

Ako je F neka tvrdnja[1] u daljnjem tekstu ćemo sa $ZF \vdash F$ označavati činjenicu da je tvrdnja F dokaziva u teoriji ZF.

Kako bi barem malo ilustrirali netrivijalnost navedene definicije prirodnih brojeva u teoriji ZF, dokazat ćemo da je aksiom matematičke indukcije dokaziv u teoriji ZF. Prvi korak prema tome je sljedeća lema.

Lema 1 *Klasa $\omega = \{x : Pri(x)\}$ je skup, tj. vrijedi*

$$ZF \vdash \exists! x \forall y(y \in x \leftrightarrow Pri(y)).$$

Skup ω je najmanji induktivan skup.

Dokaz. Aksiom beskonačnosti jednostavno tvrdi da postoji barem jedan induktivan skup. Označimo sa I jedan induktivan skup. Očito vrijedi $\{x : Pri(x)\} = \{x : x \in I \ \wedge \ Pri(x)\}$, jer po definiciji prirodnih brojeva imamo da je svaki prirodan broj element proizvoljnog induktivnog skupa. Sada iz aksioma separacije slijedi da je ω skup. Jedinstvenost skupa ω slijedi iz aksioma ekstenzionalnosti. Očito je $\omega \subseteq I$, tj. ω je najmanji induktivan skup. Q.E.D.

Ako je x prirodan broj tada sa $x + 1$ označavamo $x \cup \{x\}$.

[1] Točnije, F je proizvoljna formula teorije ZF. Ovdje nećemo strogo definirati pojam formule. Grubo govoreći F može biti sastavljena od varijabli, simbola $\in$, bulovskih veznika i kvantifikatora. Za strogu definiciju vidite npr. skriptu M. Vuković, Matematička logika 1, PMF-MO, Zagreb, 2004.

Teorem 1 *U teoriji ZF je dokaziv aksiom matematičke indukcije. Odnosno, ako je φ proizvoljna formula tada vrijedi:*

$$ZF \vdash \Big(\varphi(\emptyset) \wedge \forall x(Pri(x) \wedge \varphi(x) \to \varphi(x+1))\Big) \to \forall x(Pri(x) \to \varphi(x)).$$

Dokaz. Neka je φ proizvoljna formula tako da vrijedi

$$ZF \vdash \Big(\varphi(\emptyset) \wedge \forall x(Pri(x) \wedge \varphi(x) \to \varphi(x+1)\Big) \qquad (*)$$

Označimo $X = \{x : Pri(x) \ \text{ i } \ ZF \vdash \varphi(x)\}$. Iz leme 1 slijedi da je tada $X = \{x : x \in \omega \ \text{ i } ZF \vdash \varphi(x)\}$. Iz aksioma separcije slijedi da je X skup.

Pošto po pretpostavci $(*)$ posebno vrijedi $ZF \vdash \varphi(\emptyset)$ tada imamo $\emptyset \in X$. Zatim, ako je $x \in X$ tada je $x \in \omega$ i vrijedi $ZF \vdash \varphi(x)$. Po pretpostavci $(*)$ tada vrijedi (!) $ZF \vdash \varphi(x+1)$, tj. imamo da je $x + 1 \in X$. To znači da je X induktivan skup.

Po definiciji svaki induktivan skup sadrži svaki prirodan broj. Posebno imamo da za sve prirodne brojeve x vrijedi $x \in X$, a onda iz definicije skupa X slijedi da vrijedi $ZF \vdash \varphi(x)$. Q.E.D.

Komentar za studente koji slušaju predavanja iz kolegija Mat. logika: Uočite da nismo dokazali da je aksiom matematičke indukcije dokaziv u teoriji ZF, već shema aksioma mat. indukcije. U dokazu prethodnog teorema koristi se teorem dedukcije. Na mjestima gdje su u dokazu stavljeni uskličnici trebalo bi napisati i pretpostavke s lijeve strane.

Za prirodne brojeve uvodimo oznake: $0 := \emptyset$, $1 := \{\emptyset\}$, $2 := \{0, 1\}$, $3 := \{0, 1, 2\}$, ...

Indukcijom po n lako je dokazati da za sve n vrijedi $n \in \omega$. To znači da vrijedi $\{0, 1, 2, \ldots\} \subseteq \omega$. Sada primjenom prethodnog teorema slijedi $\omega = \{0, 1, , 2, \ldots\}$.

2.2. Tranzitivni skupovi

Sada definiramo pojam tranzitivnog skupa koji će nam trebati prilikom definicije ordinalnih brojeva.

Definicija 2 *Kažemo da je skup x tranzitivan ako vrijedi:*

$$\forall y \forall z(y \in z \in x \ \to y \in x)$$

Sa $Trans(x)$ označavamo formulu $\forall y \forall z(y \in z \ \wedge \ z \in x \ \to y \in x)$.

Osnovne primjere tranzitivnih skupova navodimo u sljedećoj propoziciji.

Propozicija 1 *Svaki prirodan broj je tranzitivan skup. Skup ω je tranzitivan.*

Dokaz. Želimo dokazati da vrijedi $ZF \vdash \forall x(Pri(x) \to Trans(x))$. Tu tvrdnju dokazujemo indukcijom, tj. primjenom dokazanog teorema o aksiomu matematičke indukcije.

Iz aksioma praznog skupa slijedi da vrijedi $ZF \vdash y \in z \in \emptyset \to y \in \emptyset$, tj. $ZF \vdash Trans(\emptyset)$.

Pretpostavimo da je neki prirodan broj x tranzitivan, te neka imamo $y \in z \in x + 1$.

Tada je $z \in x \cup \{x\}$, tj. $z \in x$ ili $z = x$. Lako je vidjeti da u oba slučaja vrijedi $y \in x$. Pošto je $x \subseteq x+1$ tada imamo i traženu tvrdnju, tj. $y \in x+1$.

Dokažimo sada da je ω tranzitivan skup. Moramo dokazati da $y \in z \in \omega$ povlači $y \in \omega$. Iz leme s prošlog predavanja (prije teorema o aksiomu matematičke indukcije) slijedi da je ta tvrdnja ekvivalentna sa: $Pri(z) \wedge y \in z \in \omega$ povlači $y \in \omega$. Posljednja tvrdnja se lako dokaže indukcijom po z. Q.E.D.

Korolar 1 *Ako je x prirodan broj i $y \in x$ tada je i y prirodan broj.*

Dokaz. Pošto x prirodan broj tada $x \in \omega$. Pošto je ω tranzitivan skup tada iz $y \in x \in \omega$ slijedi $y \in \omega$. Sada iz $\omega = \{z : Pri(z)\}$ slijedi da je y prirodan broj. Q.E.D.

Zadatak. Navedite neke skupove koji nisu tranzitivni. Neka je $x = \{\{\emptyset\}\}$. Taj skup nije tranzitivan jer vrijedi $\emptyset \in \{\emptyset\} \in x$, ali ne i $\emptyset \in x$. Skupovi $\{\emptyset, \{\{\emptyset\}\}\}$ i $\{\emptyset, \{\{\{\emptyset\}\}\}\}$ također nisu tranzitivni.

Zadatak. Dokažite da za svaki skup x vrijedi:

a) skup x je tranzitivan ako i samo ako skup $\mathcal{P}(x)$ tranzitivan;

b) ako je skup x tranzitivan tada je i skup $\cup x$ tranzitivan;

Odredite neki skup x tako da je $\cup x$ tranzitivan skup, a x nije tranzitivan skup.

Zadatak. Neka su m i n prirodni brojevi. Kažemo da je m **manji** od n, i pišemo $m < n$, ako vrijedi $m \in n$. Dokažite da je taj uređaj linearan. Napomena. Kada dokažemo da je svaki prirodan broj ordinalni broj, te da je uređaj $<$ na ordinalnim brojevima linearan, tada će tvrdnja zadatka biti jednostavna posljedica.

Kako bismo na skupu ω mogli definirati zbrajanje i množenje, a i druge funkcije, moramo prvo dokazati Dedekindov teorem rekurzije. Taj teorem jednostavno govori da rekurzijom smijemo definirati funkcije na ω. Dedekindov teorem rekurzije, a i njegov dokaz, nam je dobra motivacija za teorem rekurzije (za ordinalne brojeve).

U iskazu i dokazu Dedekindovog teorema koristimo da za sve $n \in \omega$ vrijedi $n = \{0, 1, \ldots, n-1\}$, te da je $\omega = \{0, 1, 2, \ldots\}$ Ako je $f : \omega \to S$ neka funkcija i $n \in \omega$ tada nam $f|n$ označava restrikciju funkcije f na skup n.

Teorem 2 *(***Dedekindov teorem rekurzije***)*
Neka je S proizvoljan skup, te neka je

$$\Phi = \{f| \ postoji \ \ n \in \omega \ \ t.d. \ \ \ f : n \to S\}$$

Neka je $F : \Phi \to S$ proizvoljna funkcija. Tada postoji jedinstvena funkcija $\varphi : \omega \to S$ takva da za svaki $n \in \omega$ vrijedi

$$\varphi(n) = F(\varphi|n).$$

Dokaz. Ideja dokaza je vrlo jednostavna. Očito mora vrijediti $\varphi(0) = F(\emptyset)$. Zatim, $\varphi(1) = F(F(\emptyset))$, $\varphi(2) = F(F(F(\emptyset))), \ldots$ Upravo ta jednostavnost je razlog zašto se teorem prihvaća u svakodnevnoj praksi bez da se postavlja pitanje njegovog dokaza. No, važno je uočiti da zapravo nije glavno pitanje je li tvrdnja teorema istinita, već može li se dokaz provesti u teoriji ZF.

Neka je $\mathcal{G}$ skup svih funkcija g čija je domena neki $n \in \omega$ a kodomena ω, te za sve $m < n$ vrijedi $g(m) = F(g|m)$. (Funkcije koje pripadaju skupu G možemo zamisliti kao konačne aproksimacije tražene funkcije φ.) Dokaz provodimo po koracima dokazujući redom tvrdnje.

Tvrdnja 1. Ako su $g, h \in \mathcal{G}$ takve da je $g : m \to \omega$ i $h : n \to \omega$, te je $m < n$, tada vrijedi $g = h|n$. Tvrdnju je lako dokazati indukcijom po $i < m$. (Dokaz koraka indukcije: $g(i) = F(g|i) = F(h|i) = h(i) = (h|m)(i)$.)

Tvrdnja 2. Za svaki $m \in \omega$ postoji funkcija $g \in \mathcal{G}$ takva da je $m \in Dom(g)$.
Dokaz se provodi indukcijom po m.
Za $m = 0$ možemo uzeti funkciju $g : 1 \to S$ definiranu s $g(0) = F(\emptyset)$. Pretpostavimo da za neki $m \in \omega$ postoji funkcija $g \in \mathcal{G}$ takva da je $m \in Dom(g)$. Ako je $m + 1 \in Dom(g)$ tada je dokaz gotov. Pretpostavimo zato da $m + 1 \notin Dom(g)$. Definiramo funkciju $h : (m + 1) \to S$ sa:

$$h(i) = \begin{cases} g(i), & \text{ako je } \ i \in m, \\ F(g), & \text{ako je } \ i = m. \end{cases}$$

Lako je provjeriti da je $h \in \mathcal{G}$.

Sada definiramo $\varphi = \cup_{g \in \mathcal{G}} \, g$. Dokažimo prvo da je φ funkcija.
Neka $(a, b), \ (a, c) \in \varphi$. Iz definicije φ slijedi da postoje funkcije $g, h \in \mathcal{G}$ tako da vrijedi $f(a) = b$ i $h(a) = c$. Radi određenosti možemo pretpostaviti da je $Dom(g) = m$ i $Dom(h) = n$, te je $m < n$. Iz dokazane tvrdnje 1. slijedi $g \subseteq h$. Zato je $b = c$.

Očito je $Dom(\varphi) \subseteq \omega$. Pokažimo i obratnu inkluziju. Neka je $m \in \omega$ proizvoljan. Tada iz dokazane tvrdnje 2. slijedi da postoji funkcija $g \in \mathcal{G}$ takva da je $m \in Dom(g)$. Tada je očito $m \in Dom(\varphi)$. Time smo dokazali $\omega = Dom(\varphi)$.

Primijetimo da je slika funkcije φ sadržana u skupu S. (Ako je $m \in \omega$ tada prema dokazanoj tvrdnji 2. slijedi da možemo izabrati funkciju $g \in \mathcal{G}$ tako da vrijedi $m \in Dom(g)$. Pošto je kodomena funkcije g upravo skup S, te je $\varphi(m) = g(m)$, tada je $\varphi(m) \in S$).

Dokažimo sada da za sve $m \in \omega$ vrijedi $\varphi(m) = F(\varphi|m)$.
Neka je $m \in \omega$ proizvoljan. Tada iz dokazane tvrdnje 2. slijedi da postoji $g \in G$ tako da je $m \in Dom(g)$. Iz dokazane tvrdnje 1. slijedi da za sve $i < m$ vrijedi $i \in Dom(g)$, te je $\varphi(i) = g(i)$. Tada imamo:

$$\varphi(m) = g(m) = F(g|m) = F(\varphi|m).$$

Preostalo je još dokazati jedinstvenost funkcije φ.
Pretpostavimo da je $\theta : \omega \to S$ funkcija takva da za svaki $m \in \omega$ vrijedi $\theta(m) = F(\theta|m)$. Indukcijom po m dokazujemo da vrijedi $\varphi(m) = \theta(m)$. Redom imamo $\varphi(0) = F(\varphi|0) = F(\emptyset) = F(\theta|0) = \theta(0)$. Neka je $m \in \omega$ koji ima svojstvo da za sve $i < m$ vrijedi $\varphi(i) = \theta(i)$. Tada imamo: $\varphi(m) = F(\varphi|m) = F(\theta|m) = \theta(m)$. Q.E.D.