Četrnaesto predavanje iz Teorije skupova

27. 01. 2006.

Kratki rezime prošlog predavanja:
Dokazali smo teorem rekurzije, te primjenom njega definirali zbrajanje ordinalnih brojeva.

Prvo ćemo navesti osnovna svojstva zbrajanja ordinalnih brojeva.
Sada ćemo definirati množenje i potenciranje ordinalnih brojeva.
Nakon toga ćemo definirati kardinalne brojeve.
Na samom kraju predavanja ćemo navesti sve aksiome Zermelo-Fraenkelove teorije skupova.

U sljedećoj propoziciji ističemo osnovna svojstva zbrajanja ordinalnih brojeva.
Sva svojstva se dokazuju primjenom principa transfinitne indukcije i posljednje leme s prošlog predavanja.

Propozicija 1 *(svojstva zbrajanja)*
Neka su α, β i γ proizvoljni ordinalni brojevi. Tada vrijedi:

(1) $0+\alpha=\alpha$

(2) $\alpha+(\beta+\gamma)=(\alpha+\beta)+\gamma$

(3) Ako je $\alpha+\beta=\alpha+\gamma$ tada je $\beta=\gamma$

Dokaz.
Za ilustraciju dokazujemo tvrdnju (2). Dokaz provodimo transfinitnom indukcijom po γ. Pretpostavimo da je γ ordinalni broj koji ima svojstvo da za sve $\delta<\gamma$, te sve ordinalne brojeve α i β vrijedi $(\alpha+\beta)+\delta=\alpha+(\beta+\delta)$. Promotrimo prvo slučaj kada je ordinalni broj γ prve vrste, tj. postoji ordinalni broj δ tako da vrijedi $\gamma=\delta+1$. Tada imamo:

$$\begin{aligned}
\alpha+(\beta+\gamma) &= \alpha+(\beta+(\delta+1))= \\
&= \text{(po def. zbrajanja)} = \alpha+((\beta+\delta)+1) \\
&= \text{(po def. zbrajanja)} = (\alpha+(\beta+\delta))+1 \\
&= \text{(po pret. indukcije)} = ((\alpha+\beta)+\delta)+1 \\
&= \text{(po def. zbrajanja)} = (\alpha+\beta)+(\delta+1) \\
&= (\alpha+\beta)+\gamma
\end{aligned}$$

Neka je sada γ granični ordinalni broj takav da za sve ordinalne brojeve $x<\gamma$, te sve ordinalne brojeve α i β vrijedi tvrdnja. Tada redom imamo:

$$\begin{aligned}
\alpha + (\beta + \gamma) &= \alpha + (\beta + \sup\{x : x < \gamma\}) \\
&= \text{(po def. zbrajanja)} = \alpha + \sup\{\beta + x : x < \gamma\} \\
&= \text{(po def. zbrajanja)} = \sup\{\alpha + (\beta + x) : x < \gamma\} \\
&= \text{(pret. indukcije)} = \sup\{(\alpha + \beta) + x : x < \gamma\} \\
&= \text{(po def. zbrajanja)} = (\alpha + \beta) + \sup\{x : x < \gamma\} \\
&= (\alpha + \beta) + \gamma
\end{aligned}$$

Q.E.D.

Napomena 1 *Zbrajanje ordinalnih brojeva općenito* **nije komutativno**. *Npr.* $1+\omega = \sup\{1+n : n \in \omega\} = \omega$, *ali* $\omega + 1 \neq \omega$, *jer znamo od prošli puta da vrijedi* $\omega < \omega + 1$.

Općenito iz $\beta + \alpha = \gamma + \alpha$ **ne mora slijediti** $\beta = \gamma$. *(npr.* $1 + \omega = 2 + \omega$*)*

Teorem 1 *(Teorem o oduzimanju)*
Neka su α *i* β *ordinalni brojevi takvi da je* $\beta \leq \alpha$. *Tada postoji jedinstveni ordinalni broj* γ *takav da vrijedi* $\alpha = \beta + \gamma$.

Dokaz. Označimo $A = \{x : \beta + x \leq \alpha\}$. Neka je $\gamma = \sup A$. Tada je $\beta + \gamma \leq \alpha$ (Zašto?). Pretpostavimo da je $\beta + \gamma < \alpha$. Tada iz propozicije s prošlog predavanja slijedi $(\beta + \gamma) + 1 \leq \alpha$, pa imamo $\alpha \geq (\beta + \gamma) + 1 = \beta + (\gamma + 1)$, iz čega slijedi da je $\gamma + 1 \in A$. No, to je nemoguće (jer bi tada imali $\gamma + 1 \leq \sup A = \gamma$).

Jedinstvenost slijedi iz propozicije 1 (3). Q.E.D.

Množenje ordinalnih brojeva

Definicija 1 *Primjenom teorema rekurzije slijedi da je s jednakostima koje slijede definirana jedinstvena funkcija* $\cdot : On \times On \to On$:

$$\alpha \cdot 0 = 0$$

$$\alpha \cdot (\beta + 1) = \alpha \cdot \beta + \alpha$$

$$\alpha \cdot \beta = \sup\{\alpha \cdot \gamma : \gamma < \beta\}, \quad \text{ako je } \beta \text{ granični ordinalni broj.}$$

Funkciju $\cdot$ *nazivamo* **množenje ordinalnih brojeva**.

Lema 1 *Neka su* $(A, <)$ *i* $(B, <')$ *dobro uređeni skupovi. Na Kartezijevom produktu* $A \times B$ *definiramo binarnu relaciju* $\prec$ *na sljedeći način:*

$$(a_1, b_1) \prec (a_2, b_2) \quad \Leftrightarrow \quad \begin{cases} b_1 <' b_2 \\ \text{ili} \\ b_1 = b_2 \ \text{ i } \ a_1 < a_2 \end{cases}$$

Lako je provjeriti da je $(A \times B, \prec)$ *dobro uređeni skup. Tada je* $o(A \times B) = \alpha \cdot \beta$.

Propozicija 2 *(svojstva množenja)*
Neka su α, β i γ proizvoljni ordinalni brojevi. Tada vrijedi:

(1) $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$

(2) $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$

(3) $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$

(4) Ako $\alpha \leq \beta$ *tada* $\alpha \cdot \gamma \leq \beta \cdot \gamma$

Napomena 2 *Množenje ordinalnih brojeva općenito* **nije komutativno**. *Npr.* $2 \cdot \omega =$ *(iz def.)* $= \sup\{2 \cdot n : n \in \omega\} = \omega$, *a po drugoj strani* $\omega \cdot 2 =$ *(iz def.)* $= \omega \cdot (1+1) = \omega + \omega \neq \omega$, *jer je očito (!)* $\omega + \omega > \omega + 1 > \omega$.

Općenito **ne vrijedi druga distributivnost**, *tj. ne mora vrijediti* $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$. *Npr.* $\omega = 2 \cdot \omega = (1+1) \cdot \omega \neq \omega + \omega$.

Teorem 2 *(Teorem o dijeljenju s ostatkom)*
Neka su α i β ordinalni brojevi, te neka je $\beta > 0$. Tada postoje jedinstveni ordinalni brojevi δ i ρ takvi da je $\alpha = \beta \cdot \delta + \rho$, i $\rho < \beta$.

Dokaz. Ako je $\alpha < \beta$ tada možemo uzeti $\delta = 0$ i $\rho = \alpha$. Ako je $\alpha = \beta$ tada možemo uzeti da je $\delta = 1$ i $\rho = 0$. Pretpostavimo sada da je $\alpha > \beta$. Neka je $\delta = \sup\{x : \beta \cdot x \leq \alpha\}$. Tada je $\beta \cdot \delta \leq \alpha$. Iz teorema o oduzimanju slijedi da postoji ordinalni broj ρ takav da je $\alpha = \beta \cdot \delta + \rho$.

Pretpostavimo da vrijedi $\beta \leq \rho$. Tada iz teorema o oduzimanju slijedi da postoji ordinalni broj γ takav da je $\rho = \beta + \gamma$. Sada iz toga slijedi $\alpha = \beta \cdot \delta + \rho = \beta \cdot \delta + (\beta + \gamma) = \beta \cdot (\delta + 1) + \gamma$, pa δ nije supremum skupa $\{x : \beta \cdot x \leq \alpha\}$, što je suprotno pretpostavci. To znači da mora vrijediti $\rho < \beta$.

Preostalo je dokazati jedinstvenost. Neka je $\alpha = \beta \cdot \delta + \rho$, gdje je $\rho < \beta$. Pretpostavimo da δ nije supremum skupa $\{x : \beta \cdot x \leq \alpha\}$. Tada je očito $\alpha > \beta \cdot \delta$, a onda je $\alpha \geq \beta \cdot (\delta + 1)$. Sada imamo:

$$\alpha \geq \beta \cdot (\delta + 1) = \beta \cdot \delta + \beta > \beta \cdot \delta + \rho = \alpha,$$

što je nemoguće. Time je dokazana jedinstvenost ordinalnog broja δ. Jedinstvenost ordinalnog broja ρ slijedi iz prije dokazane propozicije. Q.E.D.

Potenciranje ordinalnih brojeva

Definicija 2 *Primjenom teorema rekurzije slijedi da je sa jednakostima koje slijede definirana jedinstvena funkcija na* $On \times On$:

$$\alpha^0 = 1$$

$$\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$$

$$\alpha^\beta = \sup\{\alpha^\gamma : \gamma < \beta\}, \quad \textit{ako je } \beta \textit{ granični ordinalni broj.}$$

U sljedećoj propoziciji ističemo osnovna svojstva potenciranja ordinalnih brojeva. Dokazi se provode transfinitnom indukcijom po "krajnjem desnom" ordinalnom broju.

Propozicija 3 *(svojstva potenciranja)*
Neka su α, β i γ proizvoljni ordinalni brojevi. Tada vrijedi:

(1) $\alpha^{\beta} \cdot \alpha^{\gamma} = \alpha^{\beta+\gamma}$

(2) $(\alpha^{\beta})^{\gamma} = \alpha^{\beta\cdot\gamma}$

(3) Ako je $\alpha > 1$ i $\beta < \gamma$ tada je $\alpha^{\beta} < \alpha^{\gamma}$

Napomena 3 *Općenito ne vrijedi $\alpha^{\beta} \cdot \gamma^{\beta} = (\alpha \cdot \gamma)^{\beta}$.*
To ilustriramo sljedećim primjerom:

$$\begin{aligned}
(\omega \cdot 2)^{\omega} &= \sup\{(\omega \cdot 2)^{n} : n \in \omega\} \\
&= \sup\{(\omega \cdot 2) \cdot \ldots \cdot (\omega \cdot 2) : n \in \omega\} \\
&= \sup\{\omega \cdot (2 \cdot \omega) \cdot \ldots \cdot (2 \cdot \omega) \cdot 2 : n \in \omega\} \\
&= \sup\{\omega^{n} \cdot 2 : n \in \omega\} \ = \ \omega^{\omega}
\end{aligned}$$

$$\begin{aligned}
\omega^{\omega} \cdot 2^{\omega} &= \sup\{\omega^{\omega} \cdot 2^{n} : n \in \omega\} \\
&= \omega^{\omega} \cdot \omega \ = \ \omega^{\omega+1}
\end{aligned}$$

Teorem 3 *(logaritamski algoritam)*
Neka su $\alpha \neq 0$ i $\beta > 1$ ordinalni brojevi. Tada postoje jedinstveni ordinalni brojevi γ, δ i ρ takvi da je $0 < \delta < \beta$ i $\rho < \beta^{\gamma}$, te vrijedi

$$\alpha = \beta^{\gamma}\delta + \rho.$$

Dokaz. Neka je $\gamma = \sup\{x : \beta^{x} \leq \alpha\}$. Primjenom teorema o dijeljenju s ostatkom slijedi da postoje jedinstveni ordinalni broejvi δ i ρ, takvi da je $\rho < \beta^{\gamma}$ i $\alpha = \beta^{\gamma}\delta + \rho$.

Dokažimo da vrijedi $0 < \delta < \beta$. Ako bi vrijedilo $\delta = 0$ tada bi imali $\rho = \alpha \geq \beta^{\gamma} > \rho$, što je kontradikcija. Pretpostavimo da je $\delta \geq \beta$. Tada imamo:

$$\alpha < \beta^{\gamma+1} = \beta^{\gamma}\beta \leq \beta^{\gamma}\delta \leq \beta^{\gamma}\delta + \rho = \alpha,$$

što je kontradikcija.

Dokažimo sada jedinstvenost. Neka vrijedi $\alpha = \beta^{\gamma}\delta + \rho$, i pretpostavimo da γ nije supremum skupa $\{x : \beta^{x} \leq \alpha\}$. Tada imamo:

$$\alpha \geq \beta^{\gamma+1} = \beta^{\gamma}\beta \geq \beta^{\gamma}(\delta + 1) = \beta^{\gamma}\delta + \beta^{\gamma} > \beta^{\gamma}\delta + \rho = \alpha,$$

što je kontradikcija. Sada jedinstvenost ordinalnih brojeva δ i ρ slijedi iz teorema o dijeljenju. Q.E.D.

Teorem 4 *(teorem o normalnoj formi)*
Neka su α i β ordinalni brojevi i $\beta > 1$. Tada postoji jedinstveni prirodan broj n i konačni nizovi ordinalnih brojeva $\gamma_0, \ldots, \gamma_n$ i $\delta_0, \ldots, \delta_n$ tako da vrijedi:

$$\gamma_0 > \gamma_1 > \ldots > \gamma_n,$$
$$0 < \delta_i < \beta, \quad \textit{za sve} \quad i \leq n,$$

$$\alpha = \beta^{\gamma_0}\delta_0 + \beta^{\gamma_1}\delta_1 + \ldots + \beta^{\gamma_n}\delta_n$$

Dokaz. Primjenom teorema o logaritamskom algoritmu slijedi da postoje jedinstveni ordinalni brojevi γ_0, δ_0 i ρ_0 tako da vrijedi $0 < \delta_0 < \beta$, $\rho < \beta^{\gamma_0}$ i

$$\alpha = \beta^{\gamma_0}\delta_0 + \rho_0.$$

Ako je $\rho = 0$ tada je teorem dokazan. Ako pak je $\rho > 0$ tada na njega primjenimo teorem o logaritamskom algoritmu.

Važno je primijetiti da taj postupak mora stati u koančno mnogo koraka. Inače bi postojao beskonačan niz ordinalnih brojeva (γ_k) tako da za svaki k vrijedi $\gamma_k > \gamma_{k+1}$. To znači da taj niz ne bi imao najmanji element. No, to je nemoguće zbog aksioma dobre utemeljenosti.

Jedinstvenost slijedi iz teorema o logaritamskom algoritmu. Q.E.D.

Napomena 4 *Točan naziv prethodnog teorema je teorem o normalnoj formi po bazi β. Ako je $\beta = 2$ tada govorimo o diadskoj normalnoj formi, a ako pak je $\beta = \omega$ tada govorimo o* **Cantorovoj normalnoj formi**.
Dakle, za svaki ordinalni broj α postoji jedinstveni prirodan broj n i konačni nizovi ordinalnih brojeva $\gamma_0 > \gamma_1 > \ldots \gamma_n$ i $m_0, \ldots, m_n$, gdje su svi m_i konačni ordinalni brojevi, te vrijedi

$$\alpha = \omega^{\gamma_0}m_0 + \omega^{\gamma_1}m_1 + \ldots + \omega^{\gamma_n}m_n.$$

2.5. Kardinalni brojevi

Podsjetimo se da smo na samom početku kolegija u naivnoj teorij skupova spominjali pojam kardinalnosti (kao oznaku svojstva), tj. rekli smo da skupovi A i B imaju istu kardinalnost ako su ekvipotentni. No, nismo definirali što je zapravo kardinalni broj.

Definicija 3 **Kardinalni broj** λ *je ordinalni broj koji ima svojstvo da niti za jedan* $\alpha < \lambda$ *ne postoji bijekcija između* λ *i* α.

U sljedećem teoremu navodimo primjere kardinalnih brojeva.

Teorem 5 *Vrijede sljedeće tvrdnje:*

a) Svaki konačni ordinalni broj je kardinalni broj;

b) Skup ω *je kardinalni broj;*

c) Svaki beskonačni kardinalni broj je granični ordinalni broj.

(Svaki granični ordinalni broj nije kardinalni broj. Npr. $\omega + \omega$)

Neka je A proizvoljan skup. Iz Zermelovog teorema o dobrom uređenju (navest ćemo ga na sljedećem predavanju) slijedi da na skupu A postoji dobar uređaj. Iz teorema enumeracije tada slijedi da postoji ordinalni broj α takav da vrijedi $A \simeq \alpha$. To znači da je skup $\{\beta : \beta \in On \ \wedge \ A \sim \beta\}$ neprazan. Bili smo dokazali da svaki skup ordinalnih brojeva ima najmanji element. Ova razmatranja opravdavaju sljedeću definiciju.

Definicija 4 *Kardinalni broj proizvoljnog skupa* A *definiramo kao najmanji ordinalni broj* λ *za koji vrijedi* $A \sim \lambda$.
Primijetimo da za svaki skup postoji jedinstveni ordinalni broj. Iz tog razloga možemo uvesti oznaku $k(A)$ *za kardinalni broj skupa* A.

Uočite da je za sve skupove A ordinalni broj $k(A)$ zapravo kardinalni broj.
Ako je λ kardinalni broj tada je očito $k(\lambda) = \lambda$.
Očito je $k(\omega) = \omega$, te $k(\omega + 1) = \omega$ i $k(\omega^\omega) = \omega$.

Iz definicije očito slijedi da ekvipotentni skupovi imaju jednak kardinalni broj. Ta činjenica i sljedeća definicija operacija na kardinalnim brojevima omogućavaju nam da ovdje možemo samo istaknuti svojstva operacija na kardinalnim brojevima bez da ih moramo dokazivati. Dokazi tih svojstava bili bi sasvim isti kao u naivnoj teoriji skupova.

Definicija 5 *Neka su* λ *i* μ *kardinalni brojevi. Tada definiramo:*

a) $\lambda + \mu = k(\lambda \times \{0\} \cup \mu \times \{1\})$

b) $\lambda \cdot \mu = k(\lambda \times \mu)$

c) $\lambda^{\mu} = k(\{f |\ f : \mu \to \lambda\})$

Važna napomena: Važno je spomenuti da operacije zbrajanja, množenja i potenciranja za ordinalne i kardinalne brojeve isto označavamo. No, to nisu iste operacije. Npr. ako ω i 1 zbrajamo kao ordinalne brojeve tada je to $\omega + 1$ (što je različito od ω). No, ako ω i 1 zbrajamo kao kardinalne brojeve tada je to ω (jer je $\omega \times \{0\} \cup 1 \times \{1\} \sim \omega$.

Sada samo ističemo svojstva operacija na kardinalnim brojevima. Dokazi tih svojstava, kao što smo već bili napomenuli, su sasvim isti kao u naivnoj teoriji, pa ih ovdje nećemo ponavljati.

Teorem 6 *Neka su* λ, μ *i* ν *kardinalni brojevi. Tada vrijedi:*

a) $\lambda + (\mu + \nu) = (\lambda + \mu) + \nu$

b) $\lambda + \mu = \mu + \lambda$

c) $\lambda \cdot (\mu \cdot \nu) = (\lambda \cdot \mu) \cdot \nu$

d) $\lambda \cdot \mu = \mu \cdot \lambda$

e) $\lambda \cdot (\mu + \nu) = \lambda \cdot \mu + \lambda \cdot \nu$

f) $\lambda^{\nu} \cdot \mu^{\nu} = (\lambda \cdot \mu)^{\nu}$

g) $\lambda^{\mu + \nu} = \lambda^{\mu} \cdot \lambda^{\nu}$

h) $(\lambda^{\mu})^{\nu} = \lambda^{\mu \cdot \nu}$