Jedanaesto predavanje iz Teorije skupova 22/12/2005

Ponovimo iskaz Dedekindovog teorema rekurzije od prošli put:

Teorem 1 *(***Dedekindov teorem rekurzije***)*
Neka je S proizvoljan skup, te neka je

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

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

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

Korolar 1 *Neka je S proizvoljan skup i $s_0 \in S$, te $h : S \to S$ proizvoljna funkcija. Tada postoji jedinstvena funkcija $\varphi : \omega \to S$ za koju vrijedi:*

$$\begin{aligned}&\varphi(0) = s_0\\ &\varphi(m+1) = h(\varphi(m)), \quad \textit{za sve}\ m \in \omega\end{aligned}$$

Dokaz. Neka je Φ skup svih funkcija čija je domena neki prirodan broj, a kodomena je skup S. Definiramo funkciju $F : \Phi \to S$ tako da je $F(\emptyset) = s_0$, a za $f \in \Phi$ takvu da je $Dom(f) = n + 1$ definiramo $F(f) = h(f(n))$. Iz Dedekindovog teorema rekurzije slijedi da postoji funkcija $\varphi : \omega \to S$ koja ima traženo svojstvo.

Tada imamo $\varphi(0) = F(\varphi|0) = F(\emptyset) = s_0$, te $\varphi(m+1) = F(\varphi|m+1) = h(\varphi(m))$. Q.E.D.

Primjeri primjene Dedekindovog teorema rekurzije:

a) Pokažimo sada kako možemo definirati zbrajanje prirodnih brojeva u teoriji ZF. Tvrdimo da je pomoću jednakosti: $x + 0 = x$ i $x + (y + 1) = (x + y) + 1$, definirana jedinstvena funkcija.
Neka je Φ skup svih funkcija čije su domene neki prirodni brojevi n, a kodomena je ω.
Za svaki $m \in \omega$ promatramo funkciju $F_m : \Phi \to \omega$ tako da je $F(\emptyset) = m$, a za $f \in \Phi$, čija je domena $n + 1$, definiramo $F_m(f) = f(n) + 1$. Tada iz Dedekindovog teorema slijedi da postoji jedinstvena funkcija $\varphi_m : \omega \to \omega$ takva da za sve $n \in \omega$ vrijedi $\varphi_m(n) = F_m(\varphi_m|n)$. Tada imamo $\varphi_m(0) = F(\varphi_m|0) = F(\emptyset) = m$, te $\varphi_m(n+1) = F(\varphi_m|n+1) = \varphi_m(n) + 1$. Neka je $\varphi : \omega \times \omega \to \omega$ definirana sa $\varphi(m, n) = \varphi_m(n)$. Lako je vidjeti da vrijedi:

$$\varphi(m, 0) = m$$

$$\varphi(m, n + 1) = \varphi(m, n) + 1$$

b) Koristeći se Dedekindovom teorem rekurzije možemo definirati Fibonaccijev niz.
U tu svrhu definiramo funkciju $F : \Phi \to \omega$ na sljedeći način. Za $f \in \Phi$ čija je domena neki $n \in \omega$ definiramo:

$$F(f) = \begin{cases} 0, \text{ ako je } \ n = 0, \\ 1, \text{ ako je } \ n = 1, \\ f(m) + f(m+1), \text{ pri čemu je } \ n = m + 2 \end{cases}$$

Iz Dedekindovog teorema rekurzije slijedi da postoji jedinstvena funkcija φ tako da za sve $n \in \omega$ vrijedi $\varphi(n) = F(\varphi|n)$. Tada imamo:

$$\begin{aligned}
&\varphi(0) = F(\emptyset) = 0\\
&\varphi(1) = F(\varphi|1) = 1\\
&\varphi(n) + \varphi(n+1) = F(\varphi|n+2) = \varphi(n+2)
\end{aligned}$$

Kao što smo dokazali da u ZF za skup ω vrijedi princip mat. indukcije tako bi na analogni način mogli dokazati da skup ω zadovoljava i sve ostale **Peanove aksiome** koje sada navodimo:

1) $n + 1 \neq 0$

2) $n + 1 = m + 1 \ \Rightarrow \ n = m$

3) $n + 0 = n$

4) $m + (n + 1) = (m + n) + 1$

5) $n \cdot 0 = 0$

6) $m \cdot (n + 1) = m \cdot n + m$

Primijetite da smo dokazali da u ZF vrijede svojstva 1) i 2). Aksiomi 3)–6) su rekurzivne definicije zbrajanja i množenja. Iz Dedekindovog teorema rekurzije slijedi da su time stvarno definirane jedinstvene funkcije.

2.3. Skupovi brojeva Z, $\mathbb{Q}$ i $\mathbb{R}$

Cijeli brojevi: na skupu $\omega \times \omega$ definiramo binarnu relaciju $\sim$ sa:

$$(m_1, n_1) \sim (m_2, n_2) \ \text{ ako i samo ako } \ m_1 + n_2 = n_1 + m_2$$

Lako je provjeriti da je to relacija ekvivalencije. Za uređeni par (m, n) sa $[(m, n)]$ označavamo pripadnu klasu ekvivalencije. Skup cijelih brojeva **Z** definiramo kao skup svih klasa ekvivalencije relacije $\sim$, tj. $\mathbf{Z}{=}\omega \times \omega / \sim$

Zadatak. Na skupu **Z** definirajte zbrajanje, množenje i uređaj. Dokažite da definicije ne ovise o izboru reprezentanta klase ekvivalencije. Dokažite osnovna svojstva operacija (komutativnost, asocijativnost, ...) i relacije uređaja (irefleksivnost, tranzitivnost, kompatibilnost sa zbrajanjem i množenjem, ...) Upute:

$$\begin{aligned}
[(m_1, n_1)] \ + \ [(m_2, n_2)] \ &= \ [(m_1 + m_2, \ n_1 + n_2)]\\
[(m_1, n_1)] \cdot [(m_2, n_2)] \ &= \ [(m_1 \cdot m_2 + n_1 \cdot n_2, \ m_1 \cdot n_2 + n_1 \cdot m_2)]\\
-[(m, n)] \ &= \ [(n, m)]
\end{aligned}$$

$$[(m_1, n_1)] \ < \ [(m_2, n_2)] \ \text{ ako i samo ako } \ m_1 + n_2 < n_1 + m_2$$

Dokaz svojstva aritmetičkih operacija na skupu **Z** vidi u S. Kurepa, Uvod u matematiku, str. 104–121.

Racionalni brojevi: na skupu $\mathbf{Z}\times(\mathbf{Z}\backslash\{0\})$ definiramo binarnu relaciju $\sim$ sa:

$$(p_1, q_1) \sim (p_2, q_2) \text{ ako i samo ako } p_1 \cdot q_2 = q_1 \cdot p_2$$

Lako je provjeriti da je to relacija ekvivalencije. Za uređeni par (p, q) sa $[(p, q)]$ označavamo pripadnu klasu ekvivalencije.

Skup racionalnih brojeva $\mathbb{Q}$ definiramo kao skup svih klasa ekvivalencije relacije $\sim$, tj. $\mathbb{Q} = \mathbf{Z}\times(\mathbf{Z}\backslash\{0\})/\sim$.

Zadatak. Na skupu $\mathbb{Q}$ definirajte zbrajanje, množenje i uređaj. Dokažite da definicije ne ovise o izboru reprezentanta klase ekvivalencije. Dokažite osnovna svojstva operacija (komutativnost, asocijativnost, ...) i relacije uređaja (irefleksivnost, tranzitivnost, kompatibilnost sa zbrajanjem i množenjem, ...)

Upute:

$$\begin{aligned}
[(p_1, q_1)] \ + \ [(p_2, q_2)] &= [(p_1 \cdot q_2 \ + \ p_2 \cdot q_1, \ q_1 \cdot q_2)] \\
[(p_1, q_1)] \cdot [(p_2, q_2)] &= [(p_1 \cdot p_2, \ q_1 \cdot q_2)] \\
-[(p, q)] &= [(-p, q)]
\end{aligned}$$

$$[(p_1, q_1)] \ < \ [(p_2, q_2)] \text{ ako i samo ako } p_1 \cdot q_2 \ < p_2 \cdot q_1$$

(vidi S. Kurepa, Uvod u matematiku, str. 126–140)

Zadatak*. Definirajte skup realnih brojeva i operacije na njemu.
Skica. Ovdje opisujemo Dedekindovu konstrukciju koja se bazira na rezovima.
(vidi Drake, Singh str. 90)

Neka je (A, B) rez skupa $\mathbb{Q}$ takav da skup A nema najveći element. Skup A nazivamo realni broj. Skup svih realnih brojeva označavamo sa $\mathbb{R}$.

Na skupu $\mathbb{R}$ definiramo operacije:

zbrajanje: $A + C = \{r + q : r \in A, \ q \in C\}$

uređaj: $A < C$ ako i samo ako $A \subset C$

suprotni element: $-A = \{s \in \mathbb{Q} : (\exists r \in \mathbb{Q} \setminus A)(s < -r)\}$

(Npr. ako je $A = \langle -\infty, 3\rangle \cap \mathbb{Q}$ tada bi (intuitivno) $-A$ trebao biti $\langle -\infty, -3\rangle \cap \mathbb{Q}$.
No, pošto je $3 = \sup A$, tada je $-3 = \inf\{-x : x \in A\}$.
Iz toga slijedi da je po definiciji $-A = \langle -\infty, -3\rangle \cap \mathbb{Q}$.

skup pozitivnih realnih brojeva: $\mathbb{R}^+ = \{A \in \mathbb{R} : 0 \in A\}$

"realna" nula $0_R = \langle -\infty, 0\rangle \cap \mathbb{Q}$

množenje:
ako $X, Y \in \mathbb{R}^+$ tada definiramo $\quad X \cdot Y = \{r \cdot s : 0 \leq r \in X \ \text{ i } \ 0 \leq s \in Y\} \cup 0^*$

$0_{\mathbb{R}} \cdot X = X \cdot 0_{\mathbb{R}} = 0_{\mathbb{R}}$, za sve $X \in \mathbb{R}$

Zadatak. Definirajte množenje za slučajeve kada $x \in \mathbb{R}^+$ i $Y \notin \mathbb{R}^+$, te kada $X, Y \notin \mathbb{R}^+$

recipročni broj:
ako $X \in \mathbb{R}^+$ tada definiramo $X^{-1} = \{s \in Q : \exists r \notin X (s < r^{-1})\}$;

ako $-X \in \mathbb{R}^+$ tada definiramo $X^{-1} = -(-X)^{-1}$

$0_{\mathbb{R}}^{-1}$ se ne definira

Može se pokazati da je $\mathbb{R}$ uređeno Arhimedovo polje, te da je realno zatvoreno polje (tj. svaki polinom neparnog stupnja s koeficijentima iz $\mathbb{R}$ ima nultočku u $\mathbb{R}$).

Zatim, može se pokazati da za svaki $\emptyset \neq S \subseteq \mathbb{R}$, koji je odozgo ograničen, postoji supremum. Štoviše, vrijedi $\sup S = \cup S$.

Cantorova konstrukcija koristi Cauchyjeve nizove. Za niz $(a_n) \subseteq \mathbb{Q}$ kažemo da je Cauchyjev ako

$$(\forall \epsilon > 0)(\exists m \in \mathbb{N})(\forall k \in \mathbb{N})(|a_n - a_{n+k}| < \epsilon)$$

Na skupu svih racionalnih C–nizova definiramo relaciju $\sim$ ovako:

$$(a_n) \sim (b_n) \text{ ako i samo ako } \lim_{n \to \infty}(a_n - b_n) = 0.$$

Lako je provjeriti da je $\sim$ relacija ekvivalencije. Svaku klasu ekvivalencije nazivamo realan broj.

Literatura o uvođenju skupova brojeva:

1. Drake, Singh, Intermediate Set Theory, str. 85–93
2. S. Kurepa, Uvod u matematiku, Tehnička knjiga, Zagreb
3. D. Monk, Set Theory, skripta – (vrlo detaljno)

2.4. Ordinalni brojevi

Uvod. Još u osnovnoj školi uči se da svaki prirodan broj može biti promatran s dva aspekta. Prirodan broj određuje koliko čega ima, odnosno određuje redno mjesto. Nas ovdje upravo zanimaju redni brojevi: prvi, drugi, treći, ... No, ne zanimaju nas samo konačni redni brojevi već bismo željeli govoriti i o beskonačnim rednim brojevima.

Što znače redni brojevi? Prvi po redu znači da ispred njega nema nitko. Drugi znači da je ispred njega samo jedan, itd. Iz tog razloga se redni brojevi u teoriji skupova definiraju na sljedeći način:

$$
\begin{aligned}
&0. = \emptyset\\
&1. = \{\emptyset\}\\
&2. = \{0.,\ 1.\} = \{\emptyset,\ \{\emptyset\}\}\\
&3. = \{0.,\ 1.,\ 2.\}\\
&\qquad\qquad\vdots
\end{aligned}
$$

Kasnije ćemo vidjeti da su ordinalni broj dobro uređeni skupovi x koji imaju svojstvo da za sve $a \in x$ vrijedi $a = p_x(a)$.
Neka vas ne zbunjuje početak definicije $0. = \emptyset$ (prazan skup!). Kao što se npr. definira $0! = 1$ tako se i ovdje mora imati početak definicije. Napominjemo da u literaturi nije uobičajno koristiti oznake 0., 1., 2., 3., ..., već se jednostavno piše 0, 1, 2, 3, ... U daljnjem tekstu mi ćemo također konačne redne brojeve označavati s 0, 1, 2, 3, ...

Definicija 1 *Za skup x kažemo da je* **ordinalni broj** *ako je $(x, \in)$ tranzitivan i dobro uređen skup.*

Uočite da je u definiciji ordinalnog broja x dovoljno zahtijevati da je x tranzitivan skup, te je relacija $\in$ linearni uređaj na skupu x.
Irefleksivnost relacije $\in$, te svojstvo da svaki neprazni podskup od x ima najmanji element, slijedi iz aksioma dobre utemeljenosti.

Primjeri:

a) Prazan skup $\emptyset$, te $\{\emptyset\}$ i $\{\emptyset, \{\emptyset\}\}$ su ordinalni brojevi. Svaki prirodan broj je ordinalni broj. Skup ω je ordinalni broj.

b) Skupovi $\{\{\emptyset\}\}$ i $\{\{\{\emptyset\}\}, \{\emptyset\}, \emptyset\}$ nisu ordinalni brojevi.

c) Svaki tranzitivan skup nije ordinalni broj.
Skup $\{\emptyset,\ \{\emptyset\},\ \{\{\emptyset\}\}\}$ je tranzitivan, jer je očito svaki njegov element ujedno i njegov podskup. No, relacija $\in$ nije linearni uređaj, jer imamo $\emptyset \notin \{\{\emptyset\}\}$; $\quad \{\{\emptyset\}\} \notin \emptyset$; $\quad \emptyset \neq \{\{\emptyset\}\}$

Obično ćemo ordinalne brojeve označavati malim grčkim slovima: α, β, γ, δ, ...

Ako su α i β ordinalni brojevi tada definiramo:

$$\alpha < \beta \ \text{ ako i samo ako } \ \alpha \in \beta$$

Ako je α ordinalni broj i $x \in \alpha$ tada sa $p_\alpha(x)$ označavamo skup $\{y : y \in \alpha \text{ i } y \in x\}$.