Poglavje 5

Strukture urejenosti

5.3 Dobra urejenost in Zornova lema

Množice $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ so z relacijo $\leq$ (manjši ali enak) linearno urejene, niso pa dobro urejene. Enako velja za vsak interval pozitivne dolžine na realni osi. Oglejmo si še nekaj zgledov linearno urejenih množic, ki so dobro urejene.

Trditev 1 *1. Vsaka neprazna končna delno urejena množica ima minimalni element.*

2. Vsaka neprazna končna linearno urejena množica ima prvi element.

3. Vsaka končna linearno urejena množica je dobro urejena.

Dokaz:

1. Naj bo A neprazna končna delno urejena množica z n elementi. Z indukcijo po n dokažimo, da ima A vsaj en minimalni element.

   Osnova $(n = 1)$ V tem primeru obstaja a, tako da je $A = \{a\}$. Potem je a minimalni element množice A.

   Korak $(n \geq 1)$ Predpostavimo, da trditev velja za vse množice z n elementi, in pokažimo, da velja za vse množice z $n + 1$ elementi. Naj bo A neprazna končna delno urejena množica z $n+1$ elementi, $a \in A$ in $B = A \setminus \{a\}$. Potem je B neprazna končna delno urejena množica z n elementi. Po indukcijski predpostavki ima množica B minimalni element b. Ločimo dva primera:

   1.) $\neg(a \leq b)$: V tem primeru je b tudi minimalni element množice A.

   2.) $a \leq b$: Trdimo, da je v tem primeru a minimalni element množice A. Naj za $x \in A$ velja $x \leq a$. Po tranzitivnosti sledi $x \leq b$. Če je $x \in B$, je

$x = b$, saj je b minimalni element B. Potem je $b \leq a$ in po antisimetričnosti sledi $a = b$, kar ni mogoče, saj $a \notin B$. Torej $x \notin B$. Sledi $x = a$, kar pomeni, da je a minimalni element množice A.

2. Naj bo A neprazna končna linearno urejena množica. Po točki 1 ima A minimalni element, ki pa je zaradi linearne urejenosti tudi njen prvi element.

3. Naj bo A končna linearno urejena množica in $B \subseteq A$ poljubna neprazna podmnožica. Po točki 2 ima B prvi element, torej je A dobro urejena.

$\square$

Trditev 2 Množica $\mathbb{N}$ je z relacijo $\leq$ (manjši ali enak) dobro urejena.

Dokaz: Množica $\mathbb{N}$ je z relacijo $\leq$ linearno urejena, torej moramo pokazati še, da ima vsaka neprazna podmnožica prvi element. Naj bo $A \subseteq \mathbb{N}$ neprazna, $n_1 \in A$ in $B = \{n \in A;\ n \leq n_1\}$. Potem $n_1 \in B$, torej je B neprazna končna linearno urejena množica. Po trditvi 1.2 ima B najmanjši element $n_0 = \min B$. Potem je $n_0 \leq n_1$ in za vsak $n \in A$ velja:

a) $n \leq n_1 \implies n \in B \implies n_0 \leq n$, ali
b) $n > n_1 \implies n_0 \leq n_1 < n \implies n_0 < n$,

torej je $n_0 = \min A$. $\square$

V delno urejeni množici igrajo pomembno vlogo *verige*, t.j. podmnožice, na katerih je zožitev relacije delne urejenosti sovisna in so urejene linearno.

Definicija 1 *Naj relacija R delno ureja A in naj bo $V \subseteq A$. Če zožitev $R|_V$ linearno ureja V, je V* veriga *v A.*

Zgled 1 Ker je $\{\} \subset \{0\} \subset \{0,1\} \subset \{0,1,2\} \subset \{0,1,2,3\} \subset \cdots$, je množica $\{\{\},\{0\},\{0,1\},\{0,1,2\},\{0,1,2,3\},\ldots\}$ neskončna naraščajoča veriga v množici $\mathcal{P}\mathbb{N}$, delno urejeni z relacijo inkluzije $\subseteq$.

Ker je $\mathbb{N} \supset \mathbb{N}\setminus\{0\} \supset \mathbb{N}\setminus\{0,1\} \supset \mathbb{N}\setminus\{0,1,2\} \supset \mathbb{N}\setminus\{0,1,2,3\} \supset \cdots$, je množica $\{\mathbb{N}, \mathbb{N}\setminus\{0\}, \mathbb{N}\setminus\{0,1\}, \mathbb{N}\setminus\{0,1,2\}, \mathbb{N}\setminus\{0,1,2,3\},\ldots\}$ neskončna padajoča veriga v množici $\mathcal{P}\mathbb{N}$, delno urejeni z relacijo inkluzije $\subseteq$.

Ker $1 \mid 2 \mid 2^2 \mid 2^3 \mid 2^4 \mid \cdots$, je množica $\{1,\ 2,\ 2^2,\ 2^3,\ 2^4,\ \ldots\}$ neskončna naraščajoča veriga v množici $\mathbb{N}$, delno urejeni z relacijo deljivosti $|$.

Izrek 1 *Naj relacija $\leq$ linearno ureja A. Potem velja:*

Relacija $\leq$ dobro ureja A $\iff$ v A ne obstaja neskončna padajoča veriga oblike $a_0 > a_1 > a_2 > a_3 > \cdots$

Dokaz: ($\Longrightarrow$) Naj bo $a_0 > a_1 > a_2 > a_3 > \cdots$ neskončna padajoča veriga v A in $V = \{a_0, a_1, a_2, a_3, \dots\}$. Potem $V \neq \emptyset$ nima prvega elementa, saj za vsak $i \in \mathbb{N}$ velja: $a_{i+1} < a_i$. Torej množica A z relacijo $\leq$ ni dobro urejena.

($\Longleftarrow$) Recimo, da množica A z relacijo $\leq$ ni dobro urejena. Potem obstaja neprazna podmnožica $B \subseteq A$, ki nima prvega elementa. Pokažimo, da potem obstaja neskončna padajoča veriga v B in s tem tudi v A.

Ker B nima prvega elementa in je relacija $\leq$ sovisna, je $S_b = \{x \in B;\ x < b\} \neq \emptyset$ za vsak $b \in B$. Torej je $(S_b)_{b \in B}$ družina nepraznih množic. Po aksiomu izbire AC obstaja funkcija izbire $f : B \to \bigcup_{b \in B} S_b \subseteq B$, tako da za vsak $b \in B$ velja: $f(b) \in S_b$ oziroma $f(b) < b$. Sledi, da je $b > f(b) > f(f(b)) > f(f(f(b))) > \dots$ neskončna padajoča veriga v B za vsak $b \in B$. □

Izrek 2 (o dobri urejenosti, DU) *Za vsako množico A obstaja relacija R, ki jo dobro ureja.*

Dokaz: S pomočjo AC (zelo dolg ...) □

Pripomba 1 *Nihče si ne zna predstavljati, kakšna naj bi bila dobra urejenost npr. množice realnih števil* $\mathbb{R}$.

Izrek 3 (Zornova lema, ZL) *Naj relacija $\leq$ delno ureja A. Če ima vsaka veriga v A zgornjo mejo, ima A maksimalen element.*

Dokaz: S pomočjo AC (zelo dolg ...) □

Izkaže se, da lahko v teoriji ZF iz vsake od trditev AC, DU in ZL izpeljemo ostali dve. Vsi ti dokazi so dolgi razen dokaza aksioma izbire s pomočjo izreka o dobri urejenosti, ki gre takole:

(DU $\Longrightarrow$ AC) *Naj bo $(A_\lambda)_{\lambda \in \mathcal{I}}$ družina nepraznih množic. Po DU lahko množico $A = \bigcup_{\lambda \in \mathcal{I}} A_\lambda$ dobro uredimo, torej vsebuje vsaka množica A_λ enolično določen prvi element* $\min A_\lambda$. *Naj bo preslikava $f\colon\ \mathcal{I} \to A$ definirana s predpisom*

$$\forall \lambda \in \mathcal{I}\colon f(\lambda) = \min A_\lambda.$$

Ker je $f(\lambda) = \min A_\lambda \in A_\lambda$ za vse $\lambda \in \mathcal{I}$, je f funkcija izbire za družino $(A_\lambda)_{\lambda \in \mathcal{I}}$. Torej za vsako družino nepraznih množic obstaja funkcija izbire.

Zgled 2 Dokazi številnih pomembnih matematičnih izrekov uporabljajo Zornovo lemo (in s tem posredno aksiom izbire). Za zgled dokažimo, da ima vsak vektorski prostor bazo, torej podmnožico, ki je linearno neodvisna, hkrati pa je tudi ogrodje prostora. Če bazi dodamo še kak vektor, postane linearno odvisna, saj je vsak nebazni vektor linearna kombinacija baznih vektorjev, torej je baza prostora glede na relacijo inkluzije *maksimalna* linearno neodvisna množica.

Izrek 4 *Vsak vektorski prostor ima bazo.*

Dokaz: Naj bo X vektorski prostor in naj bo $\mathcal{N}$ množica vseh linearno neodvisnih množic prostora X, delno urejena z relacijo inkluzije. Po zgoraj omenjeni karakterizaciji baze zadošča pokazati, da ima $\mathcal{N}$ maksimalen element.

Uporabimo Zornovo lemo. Naj bo $\mathcal{V}$ veriga (torej linearno urejena podmnožica) v $\mathcal{N}$. Očitno je njena unija $\bigcup \mathcal{V}$ zgornja meja za $\mathcal{V}$ v $\mathcal{P}X$. Pokažimo, da je $\bigcup \mathcal{V} \in \mathcal{N}$, torej da je vsaka končna podmnožica množice $\bigcup \mathcal{V}$ linearno neodvisna.

Naj bo $k \in \mathbb{N}$ in $x_1, x_2, \ldots, x_k \in \bigcup \mathcal{V}$. Potem za vsak $i \in \{1, 2, \ldots, k\}$ obstaja $A_i \in \mathcal{V}$, tako da je $x_i \in A_i$. Tudi množica $\{A_1, A_2, \ldots, A_k\} \subseteq \mathcal{V}$ je veriga, torej obstaja permutacija p množice $\{1, 2, \ldots, k\}$, tako da je $A_{p(1)} \subseteq A_{p(2)} \subseteq \cdots \subseteq A_{p(k)}$. Od tod pa sledi, da je

$$\{x_1, x_2, \ldots, x_k\} \;\subseteq\; A_{p(k)}.$$

Ker je vsaka podmnožica linearno neodvisne množice linearno neodvisna, je tudi množica $\{x_1, x_2, \ldots, x_k\}$ linearno neodvisna. Dokazali smo, da je vsaka končna podmnožica množice $\bigcup \mathcal{V}$ linearno neodvisna, torej je $\bigcup \mathcal{V} \in \mathcal{N}$ in je zgornja meja verige $\mathcal{V}$ v $\mathcal{N}$. Ker je bila $\mathcal{V}$ poljubna veriga v $\mathcal{N}$, ima po Zornovi lemi množica $\mathcal{N}$ maksimalen element, to pa je baza prostora X. $\square$

5.4 Mreža

Definicija 2 *Delno urejena množica A je* mreža*, če za vse $a, b \in A$ obstajata tako* $\inf\{a, b\}$ *kot tudi* $\sup\{a, b\}$.

Zgled 3 1. Vsaka linearno urejena množica A je mreža, saj za vse $a, b \in A$ velja:

$$\begin{aligned} \inf\{a, b\} &= \min\{a, b\}, \\ \sup\{a, b\} &= \max\{a, b\}. \end{aligned}$$

2. $(\mathbb{N}, |\,)$ je mreža, saj za vse $a, b \in \mathbb{N}$ velja:

$$\begin{aligned} \inf\{a, b\} &= D(a, b), \\ \sup\{a, b\} &= v(a, b). \end{aligned}$$

2. Za vsako množico S je $(\mathcal{P}S, \subseteq)$ je mreža, saj za vse $A, B \subseteq S$ velja:

$$\begin{aligned} \inf\{A, B\} &= A \cap B, \\ \sup\{A, B\} &= A \cup B. \end{aligned}$$

Za tipe struktur urejenosti, ki smo jih definirali, velja:

<u>Dobra urejenost</u> je poseben primer <u>linearne urejenosti</u>, ki je poseben primer <u>mreže</u>, ta pa je poseben primer <u>delne urejenosti</u>.

Poglavje 6

Moč množic

6.1 Množica naravnih števil

Množico naravnih števil opisujejo *Peanovi aksiomi* iz l. 1889, ki se glasijo takole:

P1. 0 je naravno število.

P2. Vsako naravno število n ima točno določenega (neposrednega) naslednika n'.

P3. 0 ni naslednik nobenega naravnega števila.

P4. Različni naravni števili imata različna naslednika.

P5. (Aksiom indukcije) Naj bo L enomestni predikat. Če velja $L(0)$ in če za vsako naravno število n velja: $L(n) \implies L(n')$, potem za vsako naravno število n velja $L(n)$.

V teoriji ZFC vsak matematični objekt, torej tudi vsako naravno število, predstavimo z oziroma definiramo kot neko množico. Število n je smiselno definirati kot neko množico z n elementi, zato število 0 definiramo kot prazno množico: $0 = \emptyset$. Pojem naslednika pa definiramo kar za vse množice.

Definicija 3 *Za poljubno množico A je množica*

$$A' \;=\; A \cup \{A\}$$

naslednik *množice A.*

Množica A' obstaja po aksiomu o paru in aksiomu o uniji. Posamezna naravna števila zdaj definiramo takole:

$$\begin{array}{rclclcl}
0 & = & \emptyset & & & & \\
1 & = & 0' & = & 0 \cup \{0\} & = & \{0\} \\
2 & = & 1' & = & 1 \cup \{1\} & = & \{0, 1\} \\
3 & = & 2' & = & 2 \cup \{2\} & = & \{0, 1, 2\} \\
 & \vdots & & & & & \\
n+1 & = & n' & = & n \cup \{n\} & = & \{0, 1, 2, \ldots, n\} \\
 & \vdots & & & & &
\end{array}$$

Takó definirana naravna števila očitno zadoščajo Peanovim aksiomom P1, P2 in P3. S precej truda lahko že na podlagi doslej sprejetih aksiomov ZFC pokažemo, da naša naravna števila zadoščajo tudi aksiomu P4 in da ima množica, ki predstavlja število n, res n elementov. Ker se nam mudi, pa tega ne bomo storili, saj vsebuje teorija ZFC še dodaten aksiom, iz katerega to brž sledi.

Aksiom regularnosti (AR). Vsaka neprazna množica vsebuje element, s katerim si je tuja, oz. z izjavno formulo:

$$\forall A\colon (A \neq \emptyset \implies \exists x \in A\colon x \cap A = \emptyset).$$

Posledica 1

1. $\forall a\colon a \notin a$
2. $\forall a \forall b\colon \neg(a \in b \ \wedge \ b \in a)$

Dokaz: 1. Naj bo a poljubna množica. Po aksiomu o paru obstaja množica $A = \{a\}$, za katero po AR velja: $a \cap A = \emptyset$. Če $a \in a$, je $a \in a \cap A \neq \emptyset$, kar je protislovje. Torej $a \notin a$.

2. Naj bosta a in b poljubni množici. Po aksiomu o paru obstaja množica $A = \{a, b\}$, za katero po AR velja: $a \cap A = \emptyset \vee b \cap A = \emptyset$. Iz $a \in b$ sledi $a \in b \cap A \neq \emptyset$, iz $b \in a$ pa $b \in a \cap A \neq \emptyset$. Torej velja $a \notin b$ ali $b \notin a$. $\square$

Za vsako množico A torej velja: $A \subset A'$, saj je $A \in A'$ in $A \notin A$. Množica A' vsebuje natanko en element (namreč A) več kot množica A. Od tod sledi, da ima množica, ki predstavlja naravno število n, točno n elementov. Pokažimo še, da naravna števila, kot smo jih definirali, zadoščajo aksiomu P4, torej da iz $n \neq m$ sledi $n' \neq m'$. Dokažimo kontrapozicijo te implikacije:

$$\begin{aligned} n' = m' &\implies n \cup \{n\} = m \cup \{m\} \implies n \in m \cup \{m\} \wedge m \in n \cup \{n\} \\ &\implies (n \in m \vee n = m) \wedge (m \in n \vee m = n) \\ &\implies (n \in m \wedge m \in n) \vee n = m \implies 0 \vee n = m \implies n = m, \end{aligned}$$

kjer smo upoštevali posledico 1.2. – Končno želimo dokazati še, da naša naravna števila zadoščajo tudi aksiomu P5, in da obstaja množica vseh naravnih števil $\mathbb{N}$. Za to pa potrebujemo nov aksiom, saj je množica $\mathbb{N}$ neskončna, na podlagi doslej sprejetih aksiomov pa lahko konstruiramo le končne množice, kot so npr. posamezna naravna števila.

Definicija 4 *Množica M je* induktivna*, če velja:*

1. $\emptyset \in M$,
2. $\forall x \in M : x' \in M$.

Trditev 3 *Naj bo A neprazna množica induktivnih množic. Potem je tudi $\bigcap A$ induktivna množica.*

Dokaz: 1. $\forall y \in A : \emptyset \in y \implies \emptyset \in \bigcap A$
2. $x \in \bigcap A \implies \forall y \in A : x \in y \implies \forall y \in A : x' \in y \implies x' \in \bigcap A$ □

Aksiom neskončnosti (AN). Obstaja induktivna množica, oz. z izjavno formulo:

$$\exists M : (\emptyset \in M \wedge \forall x \in M : x' \in M).$$

Izrek 5 *Obstaja natanko ena množica $\mathbb{N}$, za katero velja:*

1. *$\mathbb{N}$ je induktivna,*
2. *$\forall A : (A$ induktivna $\implies \mathbb{N} \subseteq A)$.*

Dokaz: (obstoj) Po AN obstaja induktivna množica M. Naj bo

$$D = \{A \subseteq M; A \text{ induktivna}\}.$$

Ker $M \in D$, je $D \neq \emptyset$. Definirajmo $\mathbb{N} = \bigcap D$. Potem velja:

1. $\mathbb{N}$ je induktivna po trditvi 3,
2. A induktivna $\implies A \cap M$ induktivna $\implies A \cap M \in D$
$\implies \mathbb{N} = \bigcap D \subseteq A \cap M \subseteq A$ ✓

(enoličnost) Naj imata množici $\mathbb{N}_1$ in $\mathbb{N}_2$ lastnosti 1 in 2. Potem je $\mathbb{N}_1 \subseteq \mathbb{N}_2$ in $\mathbb{N}_2 \subseteq \mathbb{N}_1$, torej je $\mathbb{N}_1 = \mathbb{N}_2$. □