Analiza 1

Vid Drobnič

Kazalo

1 Števila

1.1 Naravna števila

- Z njimi štejemo: 1, 2, 3
- Množico naravnih števil označimo z $\mathbb{N}$

$$\mathbb{N} = \{1, 2, 3, ...\}$$

- Vsako naravno število n ima naslednika n^+ ($n^+ = n + 1$)

Peanovi aksiomi:

$\mathbb{N}$ je množica skupaj s pravilom, ki vsakemu naravnemu številu n dodeli njegovega naslednika $n^+ \in \mathbb{N}$ in velja:

1. za vse $m, n \in \mathbb{N}$ če $m^+ = n^+$, potem $m = n$
2. obstaja $1 \in \mathbb{N}$, ki ni naslednik nobenega naravnega števila
3. Če je $A \subset \mathbb{N}$ in če je $1 \in A$ [1] in če velja: če $n \in A$, potem $n^+ \in A$ [2], potem $A = \mathbb{N}$

Aksiom (3) se imenuje **aksiom popolne indukcije**.

- Naravna števila lahko **seštevamo, množimo**.
- $\mathbb{N}$ so urejena po velikosti $1, 2, 3, 4, 5, ...$

$$\{3, 5, 6, 10\} \subset \mathbb{N}$$

$$\{3, 5, 7, 16, 23, ...\} \subset \mathbb{N}$$

- Vsaka neprazna podmnožica $\mathbb{N}$ ima najmanjši element.
- V splošnem ne velja[3], da ima vsaka neprazna podmnožica $\mathbb{N}$ največji element.

[1] indukcijska baza
[2] indukcijski korak
[3] ne velja za vse (množice)

1.2 Cela števila

Označimo jih z $\mathbb{Z}$

$$\mathbb{Z} = \{0, 1, -1, 2, -2, ...\}$$

- Seštevanje in množenje se iz $\mathbb{N}$ razširita na $\mathbb{Z}$.
- Poleg tega je definirano **odštevanje**.
- Množico celih števil uredimo na običajen način.
- Ni res, da bi imela vsaka neprazna podmnožica $\mathbb{Z}$ najmanjši element.
- V splošnem deljenje ni definirano ($\frac{3}{2}$)

1.3 Racionalna števila

Racionalna števila so kvocienti celih števil. Bolj natančno: kvoceinti celih in naravnih števil.

Dva ulomka $\frac{m}{n}, \frac{k}{l}$ predstavljata isto racionalno število če: $ml = nk$
lahko naredimo:

$$\mathbb{Z} \times \mathbb{N} = \{(m, n), m \in \mathbb{Z}, n \in \mathbb{N}\}$$

Množico $\mathbb{Z} \times \mathbb{N}$ razdelimo na razrede: urejena para (m, n) in (k, l) sta v istem razredu, če velja $ml = nk$.

Racionalno število je razred urejenih parov in ga označimo z $\frac{m}{n}$.

$$\mathbb{Q} = \{\frac{m}{n}, m \in \mathbb{Z}, n \in \mathbb{N}\}$$

Seštevanje v $\mathbb{Q}$:

$$\frac{m}{n} + \frac{k}{l} = \frac{ml + kn}{nl}, m, k \in \mathbb{Z}, n, l \in \mathbb{N}$$

Seštevanje ulomkov je *dobro definirano:*
če je: $\frac{m'}{n'} = \frac{m}{n}, \frac{k'}{l'} = \frac{k}{l}$
potem je: $\frac{m'}{n'} + \frac{k'}{l'} = \frac{m}{n} + \frac{k}{l}$

vemo: $m'n = mn'$ in $k'l = kl'$

Dokaz:

$$\frac{m'}{n'} + \frac{k'}{l'} =^{(def)} \frac{m'l' + n'k'}{n'l'} \frac{\cdot mk}{\cdot mk} =$$

$$= \frac{m'l'mk + n'k'mk}{n'ml'k} =$$

$$= \frac{m'mk'l + m'nk'k}{m'nk'l} = \frac{ml + nk}{nl} =^{(def)}= \frac{m}{n} + \frac{k}{l}$$

Množenje v $\mathbb{Q}$:

$$\frac{m}{n} \cdot \frac{k}{l} = \frac{mk}{nl}, m, k \in \mathbb{Z}, n, l, \in, \mathbb{N}$$

Množenje je dobro definirano (izpeljava doma).

Deljenje v $\mathbb{Q}$:

$$\frac{m}{n} : \frac{k}{l} = \frac{ml}{nk}, m, k \in \mathbb{Z}, n, l \in \mathbb{N}, k \neq 0$$

Lastnosti seštevanja

Naj bo A (številska) množica z operacijama $+$ in $\cdot$.

Osnovne lastnosti računskih operacij bomo imenovali **aksiomi**. Druge lastnosti izpeljemo iz aksiomov.

A1 asociativnost seštevanja

Za vse $a, b, c \in A$ velja $(a + b) + c = a + (b + c)$

A2 komutativnost seštevanja

Za vse $a, b \in A$ velja da $a + b = b + a$

A3 obstoj enote za seštevanje

Obstaja za element $0 \in A$ za katerega velja da: $0 + a = a$ za vse $a \in A$

A4 obstoj nasprotnega števila (elementa)

Za vsak $a \in A$ obstaja nasprotno število $-a \in A$ za katerega velja: $(-a) + a = 0$

Opomba: Množica A za operacijo $+$, ki ustreza aksiomom od A1 do A4 je **Abelova grupa** za $+$.

Trditev: Naj $(A, +)$ ustreza aksiomom od A1 do A4.

(1) $\forall a \in A$ ima eno samo nasprotno število

(2) **Pravilo krajšanja:** za vse $a, x, y \in A$ velja: $a + x = a + y \Rightarrow x = y$

(3) $-0 = 0$

Dokaz:

(1) izberemo poljubno število $a \in A$. Dokazujemo da ima a natanko 1 nasprotni element.

Po A4 nasprotno število obstaja. Denimo, da sta $b, c \in A$ nasprotni števili od a.

$$b + a = 0 \text{ in } c + a = 0$$

$$(a + b) + c \overset{\text{A2}}{=} (b + a) + c \overset{\text{predp.}}{=} 0 + c \overset{\text{A2}}{=} c$$

$$(a+b)+c \overset{\text{A2}}{=} (b+a)+c \overset{\text{A1}}{=} b+(a+c) \overset{\text{A2}}{=} b+(c+a) \overset{\text{predp.}}{=} b+0 \overset{\text{A2}}{=} 0+b \overset{\text{A3}}{=} b$$

$$c = b$$

(2)

$$a + x = a + y \overset{\text{A4}}{\Rightarrow}$$

$$\Rightarrow (-a) + (a + x) = (-a) + (a + y) \overset{\text{A1}}{\Rightarrow}$$

$$\Rightarrow ((-a) + a) + x = ((-a) + a) + y \overset{\text{A4}}{\Rightarrow}$$

$$\Rightarrow 0 + x = 0 + y \overset{\text{A3}}{\Rightarrow}$$

$$\Rightarrow x = y$$

(3) $-0 = 0$

$$0 \overset{\text{A4}}{=} (-0) + 0 \overset{\text{A2}}{=} 0 + (-0) \overset{\text{A3}}{=} -0$$

Odštevanje v A: razlika števil a in b je vsota a in nasprotnega elementa od b.

$$a - b := a + (-b)$$

$b - a$ je rešitev enačbe $a + x = b$

Pozor: odštevanje ne ustreza aksiomom od A1 do A4.

Lastnosti množenja

A5 asociativnost množenja

Za vse $a, b, c, \in A$ velja: $(ab)c = a(bc)$

A6 komutativnost množenja

Za vse $a, b, c \in A$ velja: $ab = ba$

A7 obstoj enote za množenje

$\exists 1 \in A : 1 \cdot a = a$, za $\forall a \in A$

A8 obstoj obratnega števila (elementa)

Vsak $a \in A, a \neq 0$, ima obratni element, tj.: $a^{-1} \in A : a^{-1} \cdot a = 1$

Množici A z operacijo $+$, ki ustreza A1-A4, rečemo **grupa za seštevanje** (Abelova grupa).

Množica $A \setminus \{0\}$ z operacijo $\cdot$, ki ustreza A5-A8 je **grupa za množenje.**

Podobno kot za seštevanje lahko izpeljemo:
Trditev: veljajo:

(1) Vsak $a \in A \setminus \{0\}$ ima eno samo obratno število

(2) (pravilo krajšanja za množenje)

Za vsak $a, x, y \in A$ velja: $ax = ay \Rightarrow x = y$

(3) $1^{-1} = 1$

A9 Števili 0 in 1 sta različni $0 \neq 1$

A10 Distributivnost

Za vsake $a, b, c \in A$ velja:

$$(a + b)c = ac + bc$$

Def: Množico A z operacijama $+$ in $\cdot$, ki ustreza aksiomom A1-A10, imenujemo **komutativen**[4] **obseg** ali **polje**.
Primer: $(\mathbb{Q}, +, \cdot)$ so polje.

V A vpeljemo urejenost z dvema aksiomoma:

A11: Za vsak $a \in A \setminus \{0\}$ velja, da je natanko eno od števil a, $-a$ pozitivno. Število 0 ni niti pozitivno niti negativno. (Število a je negativno, če je število $-a$ pozitivno).

A12: Za vsaka $a, b \in A$ velja: če sta a in b pozitivni števili, potem sta tudi $a + b$ in $a \cdot b$ pozitivni števili.

Def: Če ima obseg $(A, +, \cdot)$ urejenost, ki izpolnjuje A11 in A12, A imenujemo **urejen obseg** (urejeno polje).
Primer: $(\mathbb{Q}, +, \cdot)$ z običajno urejenostjo je urejen obseg.

$\frac{m}{n}$ je pozitiven, če $m \cdot n > 0$

Def: Naj bo A urejen obseg. Za poljubna $a, b \in A$ definiramo:

Pišemo $a > b$ natanko tedaj, kadar je $a - b$ pozitivno število.

V tem primeru pišemo tudi $b < a$

V posebnem primeru pišemo $a > 0$, kadar je a pozitivno število.

Def: Naj bo A urejen obseg. Za poljubna $a, b \in A$

$a \leq b$ natanko takrat, kadar $a < b$ ali $a = b$

Trditev: V urejenem obsegu A velja:

(1) Za poljubni števili $a, b \in A$ velja natanko ena od možnosti:

$$a < b,\ a = b,\ a > b$$

Sledi iz A11 uporabljen za $a - b$.

[4]komutativnost se nanaša na komutativnost množenja

(2) Za poljubne $a, b, c \in A$ velja:

če je $a > b \wedge b > c$, potem $a > c$ (tranzitivnost)

(3) Za poljubne $a, b, c \in A$ velja:

če je $a > b$, potem $a + c > b + c$

(4) Za poljubne $a, b, c, \in A, c > 0$:

če je $a > b$, potem je $ac > bc$

5 Za poljubne $a, b, c, d, \in A$:

če je $a > b > 0$ in $c > d > 0$, potem je $ac > bd$

Dokaz:

(2) $a > b \wedge b > c \Rightarrow a > c$

Po definiciji: $a - b > 0$ in $b - c > 0$

Zato po A12:

$$\begin{aligned} (a-b) + (b-c) &> 0 \\ a + (-b) + b + (-c) &> 0 \\ a + 0 + (-c) &> 0 \\ a - c &> 0 \end{aligned}$$

zato $a > c$

(3) denimo, da je $a > b$

dokazujemo, da je $a + b > b + c$, tj: $(a + c) - (b + c) > 0$

$$\begin{aligned} (a+c) - (b+c) =& a + c + (-(b+c)) = \\ & a + c + (-b) + (-c) = \\ & (a + (-b)) + (c + (-c)) = \\ & a + (-b) = a - b \end{aligned}$$

Dokaz da $-(b + c) = (-b) + (-c)$:

$-(b + c)$ je nasprotni element od $b + c$, kar pomeni da je njuna vsota enaka 0. Če velja $-(b + c) = (-b) + (-c)$, mora biti tudi $b + c + (-b) + (-c) = 0$:

$$b + c + (-b) + (-c) \stackrel{A2,A1}{=} (b + (-b)) + (c + (-c)) \stackrel{A4}{=} 0 + 0 \stackrel{A3}{=} 0$$

Če $a > b$ je $a - b > 0$, zato je $(a + c) - (b + c) > 0$, kar pomni $a + c > b + c$.

(5) $a > b > 0$ in $c > d > 0$

Dokazujemo $ac > bd$:

$a > b \stackrel{4}{\Rightarrow} ac > bc$ $(c > 0)$
$c > d \stackrel{4}{\Rightarrow} bc > bd$ $(b > 0)$

Z upoštevanjem tranzitivnosti (2) dobimo: $ac > bd\square$

Racionalna števila predstavimo na številski premici.

Racionalna števila so na številski premici **povsod gosta** tj: na vsakem nepraznem odprtem intervalu leži racionalno število.

Racionalna števila ne pokrijejo številske premice

Trditev: rešitev enačbe $x^2 = 2, x > 0$ ni racionalno število. ($\sqrt{2} \notin \mathbb{Q}$)
Dokaz: Dokazujemo da x ni ulomek.

Dokazujemo s protislovjem.

- privzamemo, da tisto kar dokazujemo ni res. (predpostavimo, da x je ulomek)
- sklepamo
- skepi nas privedejo v protislovje s predpostavko

$$x = \frac{m}{n}, m, n \in \mathbb{N}$$

Če je x ulomek, ga lahko zapišemo kot okrajšan ulomek, zato sta m in n tuji si števili.

$$\begin{aligned}
x^2 = 2 &\Rightarrow (\frac{m}{n})^2 = 2\\
\frac{m^2}{n^2} &= 2\\
m^2 &= 2n^2\\
2|m^2 &\Rightarrow 2|m\\
\exists l \in \mathbb{N} : m &= 2l\\
4l^2 &= 2n^2\\
2l^2 &= n^2\\
2|n^2 &\Rightarrow 2|n\\
&\rightarrow \leftarrow
\end{aligned}$$

Dokaz da $2|m^2 \Rightarrow 2|m$:
Če je m liho, potem $k \in \mathbb{N}_0$

$$\begin{aligned}
m &= 2k + +1\\
m^2 &= 4k^2 + 4k + 1\\
m^2 &\text{ je lih}
\end{aligned}$$

1.4 Dedekindov aksiom in Realna števila

Radi bi skonstruirali številsko množico, ki bo vsaj urejen obseg in, ki zapolni številsko premico.

Dedekindov pristop

Def: **Rez** je podmonožica $A \subset \mathbb{Q}$, za katero velja:

(i) $A \neq \varnothing, A \neq \mathbb{Q}$

(ii) Če je $p \in A$, potem za vsak $q \in \mathbb{Q}$ in $q < p$, velja $q \in A$

(iii) za vsak $p \in A$ obstaja $q \in A, q > p$ (A nima največjega elementa)

Def: Množica realnih števil je množica vseh rezov, označimo jo s $\mathbb{R}$
Primer: 16 ustreza rez: $\{p \in \mathbb{Q}; p < 16\} = B$

Trditev: Preslikava $\mathbb{Q} \to \mathbb{R}$ in je definirana s predpisom:

$$q \mapsto \{p \in \mathbb{Q}; p < q\} = p^*$$

vloži množico racionalnih števil v množico realnih števil.

Vpeljimo računski operaciji v $\mathbb{R}$.

Def: Naj bosta A in B reza. Vsota rezov A in B je

$$A + B = \{a + b, a \in A, b \in B\}$$

Opomba: $(p+q)^* = p * + q*$

Trditev: Če sta A in B reza, potem je tudi $A + B$ rez.
Dokaz(trditev): Denimo da sta A in B reza.

Dokazujemo da je $A + B$ rez:

(i) $\underline{A + B \neq \varnothing}$

Ker sta A in B reza, po lastnosti (i) obstaja $a \in A$ in $b \in B$. Potem je $a + b \in A + B$. Sledi $A + B \neq \varnothing$ $\square$

$\underline{A + B \neq \mathbb{Q}}$

Obstaja $c \in \mathbb{Q}, c \notin A$ in obstaja $d \in \mathbb{Q}, d \notin B$.

$$c + d \notin A + B$$

Denimo, da je $c + d \ \in A + B$.

Potem velja, da je $c + d = a + b$ za $a \in A, b \in B$.

Iz (ii) sledi: $c > a$ in $d > b \Rightarrow a + b < c + d \quad \to\leftarrow$

(ii) Denimo: $p \in A + B$, dokazujemo da za $q \in \mathbb{Q}, q < p$ velja $\underline{q \in A + B}$

Obstajata $a \in A$ in $b \in B$, da $p = a + b$

$$q = a + q - a$$

Če je $q - a < b$, potem $q - a \in B$

$$q < a + b$$
$$q < p$$
$$\square$$

(iii) $\underline{A + B \text{ nima največjega elementa.}}$

izberimo $p \in A + B$
iščemo $q \in A + B, q > p$

Obstajata $a \in A, b \in B$, da je $p = a_b$
Obstaja $a' \in A, a' > a$

$$q := a' + b \in A + B$$
$$q > p$$
$$\square$$

Ni težko preveriti, da za $(\mathbb{R}, +)$ veljajo A1-A4.
Asociativnost in komutatiovnost se dokaže z operacijami na elementih reza.
0^* je enota za seštevanje.

Nasprotni rez od A:

$$-A = \{r \in \mathbb{Q}, \text{obstaja } r' \in \mathbb{Q}, r' > r \text{ in } r' + p < 0 \text{ za vse } p \in A\}$$

(i) $-A \neq \varnothing$

$\underline{-A \neq \mathbb{Q}}$

$$q + a < 0 \text{ za vse } q \in \mathbb{Q}$$
$$q = -a$$

(ii) $q \in -A : r < q$

$q + a < 0$ za vse $a \in A$

$r + a < q + a$ za vse $a \in A$ po tranzitivnosti: $r + a < 0$

(iii) Izberemo poljuben $r \in A$. Iščemo $q \in A, q > r$.

$$q := \frac{r + r'}{2}(r' > r, r' \in \mathbb{Q} : r' + p < 0 \text{ za vse } p \in \mathbb{Q})$$

$$q \in \mathbb{Q}, r' > q$$

Def: Pravimo da je A pozitiven, če je $0^* \subset A, A \neq 0^*$. Denimo da sta A in B pozitivna reza:

$$A \cdot B = \{q \in \mathbb{Q}, \text{ obstajata } a \in A, a > 0 \text{ in } b \in B, b > 0, \text{ da je } q < ab\}$$

Želimo $(pq)^* = p^* \cdot q^*, p, q \in \mathbb{Q}$

Def: Naj bosta A in B poljubna reza.

$$A \cdot B = \begin{cases} A \cdot B & A > 0 \wedge B > 0 \\ -A \cdot (-B) & A > 0 \wedge B < 0 \\ -(-A) \cdot B & A < 0 \wedge B > 0 \\ (-A) \cdot (-B) & A < 0 \wedge B < 0 \end{cases}$$

Če je vsaj eden od rezov enak 0^*, potem $A \cdot B = 0^*$.

Ni težko preveriti, da množenje rezov izpolnjuje A5-A8 in A9, A10.

Enota za množenje je 1^*.

Urejenost izplonjuje A11 in A12.

$(\mathbb{R}, +, \cdot)$ je **urejen obseg** in vsebuje $\mathbb{Q}$ kot **urejen podobseg**.

Cilj: Obseg $\mathbb{R}$ izpolnjuje še dodaten aksion A13 (**Dedekindov aksiom**), ki pove, da $\mathbb{R}$ zapolnjuje številsko premico.

Aksioma A13 obseg $\mathbb{Q}$ ne izpolnjuje.

Def: Naj bo B urejen obseg in $A \subset B$. Pravimo, da je A navzgor omejena, če obstaja $M \in B$, da velja:

$$\forall a \in A : a \leq M$$

$\forall M$ s to lastnostjo pravimo zgornja meja množice A. Če je $A \subset \mathbb{Q}$(ali $\mathbb{R}$) in je množica navzgor omejena, potem ima A neskončno zgornjih mej.

Def: Naj bo A navzgor omejena množica. Če obstaja najmanjša od vseh zgornjih mej množice A v B, jo imenuje natančna zgornja meja množice A.

Torej je $\alpha \in B$ natančna zgornja meja množice A, če velja:

(i) α je zgornja meja $\forall a \in A : a \leq \alpha$

(ii) Če $b \in B, b < \alpha$, potem b ni zgornja meja množice A, t.j.: $\exists a \in A : a > b$

Natančno zgornjo mejo množice A imenujemo tudi **supremum** množice A in jo označimo z $\sup A$

Def: Če obstaja največji element množice A, ga imenujemo **maksimum** množice A in označimo z $\max A$.

Če ima A maksimum, potem velja:

$$\max A \in A \wedge \forall a \in A : a \leq \max A$$

Če ima A maksumum, potem $\max A = \sup A$. (Za a v (2) lastnosti definicije supremuma vzamemo $\max A$) *Dokaz:*

(1) $\max A$ je zgornja meja A (po definiciji maksimuma).

(2) če $b < \max A$, potem b ni zgornja meja.

$$\exists \max A, \text{ ki je večji}$$

Primeri:

1. $A = \{x \in \mathbb{Q}, x < 0\} \subset \mathbb{Q}$

   4 je zgornja meja množice A, ker $x \in A, x < 0, 0 < 4 \Rightarrow x < 4$

   $\Rightarrow A$ je navzgor omejena.

   0 je natančna zgornja meja množice A

   (a) $x \in A, x < 0$

   (b) Izberemo poljuben $b \in \mathbb{Q}, b < 0$ in dokazujemo, da b ni zgornja meja.
   $$b < \frac{b}{2} < 0; \frac{b}{2} \in A, \frac{b}{2} > b$$

   Množica A nima maksimuma: $0 \notin A$.

2. $C = \{x \in \mathbb{Q}, x^2 < 2\} \subset \mathbb{Q}$

   C je navzgor omejena z 2.

   $$x \in C : x^2 < 2 \wedge 2 < 4 \Rightarrow x^2 < 4 \Rightarrow x < 2$$

   (a) Vsako število $p \in \mathbb{Q}, p^2 > 2$ je zgornja meja množice C.

   (b) Nobeno racionalno število $q \in \mathbb{Q}, q^2 < 2$ ni zgornja meja množice C.

Vemo: Rešitev enačbe $x^2 = 2, x > 0, x \notin \mathbb{Q}$.
Sledi: $C \subset \mathbb{Q}$ nima natančne zgornje meje.

Dokaz:

(a)

$$x^2 < 2 < p^2$$

sledi: $x^2 < p^2 \Rightarrow x < p$ za vse $x \in C$ $\square$

(b) Iščemo $c \in C$, da je $c > q, c^2 < 2$

$$c := \frac{2q+2}{q+2} = q + \frac{2q+2-q^2-2q}{q+2} = q + \frac{2-q^2>0}{q+2} > 0$$

$(q^2 < 2)$

$$c^2 = (\frac{2q+2}{q+2}^2 = \frac{4(q^2+2q+1)}{q^2+4q+4}$$

$$c^2 - 2 = \frac{4q^2+8q+4-2q^2-8q-8}{(q+2)^2} = \frac{2q^2-4}{(q+2)^2} = \frac{2(q^2-2>0)}{(q+2)^2} > 0$$

$$q^2 < 0$$