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 definiramo **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 $\left(\frac{3}{2}\right)$

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 $b + c + (-b) + (-c) = 0$:

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

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 $ac>bd$:

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

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: Želimo si, da velja $(p+q)^* = p^* + q^*$

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 $d > b \Rightarrow a + b < c + d \quad \rightarrow\leftarrow$

(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) $A+B$ 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) $-A \neq \varnothing$

$-A \neq \mathbb{Q}$

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

(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 maksimum, 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 (ker je $\max A \in A$, b pa je manjši, velja da b ni zgornja meja od A, ker obstaja nek element is A, ki je večji od b).

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 $c > q, c^2 < 2$

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

$(q^2 < 2)$

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

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

$$q^2 < 2$$

Podobno kot zgornjo mejo, navzgor omejeno množico, supremum in maskimum, definiramo spodnjo mejo, navzdol omejeno množico, infimum in minimum.

A13 (Dedekindov aksiom): Vsaka neprazna navzgor omejena podmnožica v množici A ima supremum (v množici A).

Def: Če množica $(A, +, \cdot, <)$ izpolnjuje aksiome A1-A13 jo imenujem *poln urejen obseg* (poln se nanaša na A13).

Trditev: $(\mathbb{Q}, +, \cdot, <)$ je urejen obseg, ki ne izpolnjuje A13.

Izrek: vsaka nerpazna navzgor omejena podmnožica v $\mathbb{R}$ ima natančno določeno zgornjo mejo. ($\mathbb{R}$ izpolnjuje A13)

Posledica: $(\mathbb{R}, +, \cdot, <)$ je poln urejen obseg.

Posledica: Vsaka neprazna navzdol omejena podmnožica $\mathbb{R}$ ima natančno spodnjo mejo.

A neprazna navzdol omejena.

$$-A = \{x; -x \in A\}$$

$-A$ je neprazna, navzgor omejena (če m spodnja meja od A, je $-m$ zgornja meja od $-A$). $\Rightarrow -A$ ima supremum in velja: $-\sup A = \inf A$

Dokaz (izrek): Izberemo poljubno neprazno navzgor omejeno podmnožico $\mathcal{A}$ v $\mathbb{R}$.

$$C = \cup A, A \in \mathcal{A}$$

Dokazati je treba:

1. C je rez
2. $C = \sup \mathcal{A}$

1. (i) $C \neq \varnothing$
   Ker $\mathcal{A}$ ni prazna $\exists A \in \mathcal{A}$. Torej velja $A \subset C$, torej $C \neq \varnothing$.
   $C \neq \mathbb{Q}$
   Ker je $\mathcal{A}$ omejena, obstaja zgornja meja M množice $\mathcal{A}$, velja:

   $$\forall A \in \mathcal{A} : A \leq M$$
   $$\forall A \in \mathcal{A} : A \subset M$$

   Sledi: $C \subset M$, zato $C \neq \mathbb{Q}$ (ker $M \neq \mathbb{Q}/M$ je rez).

   (ii) $p \in C, q \in \mathbb{Q}, q < p \Rightarrow q \in C$
   $p \in C \Rightarrow \exists A \in \mathcal{A}$, da je $p \in A$. Ker je A rez, za $q \in \mathbb{Q}, q < p$ velja $q \in A$.
   Sledi: $q \in C$.

   (iii) $p \in C \Rightarrow \exists q \in \mathbb{Q}, q > p : q \in C$ $p \in C \Rightarrow \exists A \in \mathcal{A}$, da je $p \in A$. Ker je A rez, $\exists q \in A, q > p$.
   Sledi: $q \in C$.

2. (i) C je zgornja meja $\mathcal{A}$
   Ker je $A \subset C$ za vse $A \in \mathcal{A}$, velja $A \leq C$ za vse $A \in \mathcal{A}$. t.j.: C je zgornja meja.

   (ii) C je natančna zgornja meja $\mathcal{A}$
   Izberimo poljuben $D < C$. Dokazujemo, da D ni zgornja meja $\mathcal{A}$.
   Ker je $D < C, D \subset C$ in $D \neq C$, obstaja $p \in \mathbb{Q}, p \in C$ in $p \notin D$.
   Ker je $p \in C$, obstaja $A \in \mathcal{A}$, da je $p \in A$.
   Velja: $A > D$ in $A \in \mathcal{A}$ (vemo da sta vsaka reza primerljiva po velikosti.)
   Sledi: D ni zgornja meja. $\square$

Za radovedne: Poleg Dedekinda je realna števila definiral tudi Cantor. Ta je to naredil s Cauchyjevimi zaporedji.

Opomba: Med obsegoma $\mathbb{Q}$ in $\mathbb{R}$ je še veliko obsegov.

Definicija: Pravimo, da je x iracionalno število, če $x \notin \mathbb{Q}$.

Rešitvam polinomskih enačb s celimi koeficienti rečemo *algebraična števila.*

Primer: $\sqrt{2} : x^2 - 2 = 0$

Niso vsa iracionalna števila algebraična: π, e. Tem pravimo *transcendentna števila.*

1.5 Posledice Dedekindovega aksioma

- Množica $\mathbb{Z}$ ni navzgor omejena v $\mathbb{R}$.

  Dokaz: Denimo, da je $\mathbb{Z}$ navzgor omejena v $\mathbb{R}$. Potem obstaja $M \in \mathbb{R}$, da $M = \sup \mathbb{Z}$. Torej $M - 1$ ni zgornja meja $\mathbb{Z}$.

$$\exists a \in \mathbb{Z}, a > M - 1$$
$$a + 1 > M, a + 1 \in \mathbb{Z} \rightarrow\leftarrow$$

- $\forall a \in \mathbb{R} \exists b \in \mathbb{Z} : a < b$

  Dokaz: če to ne bi bilo res, bi bilo število a zgornja meja $\mathbb{Z}$. To pa ni res (prejšnja posledica).

- *Arhimedska lastnost:* Naj bosta $a, b \in \mathbb{R}^+$. Potem obstaja $n \in \mathbb{N} : na > b$.

  Dokaz: Obstajati mora $n \in \mathbb{N} : n > \frac{b}{a}$:. Po prejšnji posledici tak n obstaja. $\square$

- Naj bo $a \in \mathbb{R}^+$. Potem obstaja $n \in \mathbb{N}$, da $\frac{1}{n} < a$.

  Dokaz: uporabimo arhimedsko lastnost za $n = 1$.

- Naj bosta a, b poljubni $\mathbb{R}, a < b$. Obstaja $q \in \mathbb{Q}$, da velja $a < q < b$.

  *Dokaz:*če je $b - a > 1$, potem obstaja $m \in \mathbb{Z}, a < m < b$

$\{n \in \mathbb{Z}, n \leq a\}$ je navzdol omejena neprazna.

$$\sup\{n \in \mathbb{Z}, n \leq a\} = x, x \in \mathbb{Z}$$
$$m := x + 1$$

$$b > m > 0$$

$$b - a > 0$$
$$\exists n \in \mathbb{N} : n(b-a) > 1$$

Obstaja $m \in \mathbb{Z} : an < m < nb$.

$$a < \frac{m}{n} < b \; \square$$

Rečemo tudi: $\mathbb{Q}$ so v $\mathbb{R}$ *povsod gosta.*

1.6 Intervali

Def: Naj bosta $a, b \in \mathbb{R}, a < b$

1. $[a, b] = \{x \in \mathbb{R}, a \leq x \leq b\}$ *zaprti interval*
2. $(a, b) = \{x \in \mathbb{R}, a < x < b\}$ *odprti interval*
3. $[a, b) = \{x \in \mathbb{R}, a \leq x < b\}$ *polodprti interval*
   $(a, b] = \{x \in \mathbb{R}, a < x \leq b\}$
4. $(a, \infty) = \{x \in \mathbb{R}, x > a\}$
   $[a, \infty) = \{x \in \mathbb{R}, x \geq a\}$
   $(-\infty, a) = \{x \in \mathbb{R}, x < a\}$
   $(-\infty, a] = \{x \in \mathbb{R}, x \leq a\}$
   $(-\infty, \infty) = \mathbb{R}$

Def: Naj bo $a \in \mathbb{R}, \varepsilon > 0$. Interval $(a - \varepsilon, a + \varepsilon)$ imenujemo ε-*okolica* števila a.

Okolica točke a je vsaka taka podmnožica v $\mathbb{R}$, ki vsebuje kakšno ε-okolico točke a.

1.7 Decimalni ulomki

Vsako $\mathbb{R}$ število lahko zapišemo kot *decimalni ulomek*.

Naj bo $x \in \mathbb{R}^+$ in naj bo $n \in \mathbb{N}_0$ največje številko, ki ne presega x:

$$n \leq x < n + 1$$

Interval $[n, n+1]$ razdelimo na 10 enakih delov. Nato poiščemo $n_1 \in \{0, 1, 2, \ldots, 9\}$, da velja:

$$n + \frac{n_1}{10} \leq x < n + \frac{n_1 + 1}{10}$$

Postopek nadaljujemo in na ta način sestavimo zaporedje decimalnih približkov za x.

$$\mathcal{A} = \{n, n + \frac{n_1}{10}, n + \frac{n_1}{10} + \frac{n_2}{100}, \ldots\}$$

Trditev: $x = \sup \mathcal{A}$
Dokaz:

(i) x je zgornja meja množice $\mathcal{A}$
Velja po konstrukciji: $\forall a \in \mathcal{A} : a \leq x$.

(ii) x je najmanjša zgornja meja
Denimo da to ni res:

$$y := \sup \mathcal{A} < x$$
$$\exists n \in \mathbb{N} : \frac{1}{n} \leq x - y$$
$$\exists p \in \mathbb{N} : \frac{1}{10^p} < \frac{1}{n} < x - y$$

$$y + \frac{1}{10^p} < x$$

$$n + \frac{n_1}{10} + \frac{n_2}{100} + \ldots + \frac{n_p}{10^p} \leq y$$
$$n + \frac{n_1}{10} + \frac{n_2}{100} + \ldots + \frac{n_p + 1}{10^p} \leq y + \frac{1}{10^p} < x \rightarrow\leftarrow$$

Trditev utemelji, da x lahko zapišemo, kot neskončni decimalni ulomek.

$$x = n_0 + \frac{n_1}{10} + \ldots + \frac{n_p}{10^p} + \ldots = n_0, n_1 n_2 \ldots n_p \ldots$$

Trditev: Naj bosta $x, y \in \mathbb{R}^+$

(1) Denimo, da obstaja $k \in \mathbb{N}_0$, za katerega velja:

$$\begin{aligned} x &= n_0, n_1 n_2 \ldots n_{k-1} n_k 99 \ldots \\ y &= n_0, n_1 n_2 \ldots n_{k-1} (n_k + 1) 00 \ldots \end{aligned}$$

in $n_k \neq 9$, potem $x = y$.

(2) Za dva različna decimalna zapisa $x \in \mathbb{R}^+$ velja (1).

Dokaz: Naj bo $\mathcal{A}$ množica decimalnih preslikav za x.

(1)

$$\forall a \in \mathcal{A} : y \geq a \ (y \text{ je zgornja meja})$$

Zato $y \geq x$ (x je $\sup \mathcal{A}$)

Dokzujemo y je natančna zgornja meja od $\mathcal{A}$

Naj bo $l > k$ in a_l l-ti decimalni približek za x.

$$\begin{aligned} y - a_l &= \frac{1}{10^l} \\ y - \frac{1}{10^l} &= a_l \\ y - \frac{1}{10^l} &\leq a_l < a_{l+1} \end{aligned}$$

$\Rightarrow y - \frac{1}{10^l}$ ni zgornja meja za noben l, torej je y natančna zgornja meja.

(2) x naj ima dva decimalna zapisa:

$$\begin{aligned} x &= n_0, n_1 n_2 \ldots \\ x &= m_0, m_1 m_2 \ldots \end{aligned}$$

Obstaja najmanjši indeks $k \in \mathbb{N} : n_k \neq m_k$.

Predpostavimo, da je $m_k > n_k$

$m_0, m_1 m_2 \ldots m_k$ je zgornja meja množice decimalnih približkov za x.

$$m_0, m_1 m_2 \ldots m_k > m_0, m_1 m_2 \ldots m_{k-1} n_k n_{k+1} n_{k+2} \ldots$$

Če bi veljajo $n_k < m_k - 1$ (dokazujemo, da je razlika lahko največ 1, t.j: morajo se ponavljati 9-ke)

$$x \leq n_0, n_1 n_2 \ldots n_{k-1}(n_k + 1) < m_0, m_1 \ldots m_{k-1} m_k \leq x \to\leftarrow$$

($x < x$ ni možno)
Če bi bil $m_{k+1} \neq 0$ (ali za indeks $l > k$):

$$x \leq m_0, m_1 m_2 \ldots m_k < m_0, m_1 \ldots m_k m_{k+1} \leq x \to\leftarrow$$

Na podoben način dokažemo, da velja:

$$\forall l \in \mathbb{N} : n_{k+l} = 9$$

Podobno velja tudi za druge osnove. Primer v dvojiškem sistemu bi bil:

$$1101, 011 = 1101, 010\overline{1}$$

Trditev: Naj bo $x \in \mathbb{R}$. x ima periodičen decimalni zapis natanko tedaj, kadar $x \in \mathbb{Q}$ (tudi končen decimalni zapis je periodičen).

Dokaz: denimo, da je $x \in \mathbb{Q}^+$.

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

m delimo z n pisno. To pomeni da podpisujemo ostanke. Ker imamo na voljo n različnih ostankov: $o_j \in \{0, 1, \ldots, n-1\}$, se bo med $n+1$ zaporednimi ostanki vsaj eden zagotovo ponovil. Ko se ostanek ponovi, se ponovi tudi cel zapis, kar je perioda.

Denimo, da ima x periodičen decimalni zapis:

$$\begin{aligned} x &= d, d_1 d_2 \ldots d_n \overline{d_{n+1} d_{n+2} \ldots d_{n+k}} \\ 10^k x &= d \cdot 10^k + d_1 d_2 \ldots d_k, d_{k+1} \ldots d_n \ldots d_{n+k} \overline{d_{n+1} \ldots d_{n+k}} \\ 10^k x - x & \text{ ima končen decimalni zapis} = p \in \mathbb{Q} \\ x &= \frac{p}{10^k - 1} \in \mathbb{Q} \quad \square \end{aligned}$$

1.8 Absolutna vrednost

Def: če je $x \in \mathbb{R}$, potem

$$|x| = \begin{cases} x & \text{če } x \geq 0 \\ -x & \text{če } x < 0 \end{cases}$$

Število $|x|$ imenujemo *absolutna vrednost realnega števila* x.

Trditev: Naj bo $x \in \mathbb{R}$. Veljajo:

(i) $|x| \geq 0$

(ii) $|x| = 0 \Leftrightarrow x = 0$

(iii) $|x| = |-x|$

(iv) $-|x| \leq x \leq |x|$

(v) $|x|$ je razdalja x do 0 na številski premici

(vi) *Trikotniška neenakost:* $|x+y| \leq |x| + |y|$ za vse $x, y \in \mathbb{R}$

(vii) $|xy| = |x| \cdot |y|$ za vse $x, y \in \mathbb{R}$

Dokaz:

(vi) pregledamo vse možnosti glede na predznak

(1) $x \geq 0, y \geq 0$

$$|x+y| = x + y = |x| + |y|$$

(2) $x < 0, y < 0$

$$|x+y| = -(x+y) = -x - y = |x| + |y|$$

(3) $x \geq 0, y < 0$

$$\begin{aligned} |x| &= x, |y| = -y \\ x + y &= |x| - |y| \\ |x+y| &= \begin{cases} |x| - |y| & \text{če } |x| \geq |y|, \\ |y| - |x| & \text{če } |x| < |y| \end{cases} \\ |x+y| &\leq |x| + |y| \end{aligned}$$

(4) simetrična (3)

Posledica:

1) $||x| - |y|| \leq |x \pm y| \leq |x| + |y|$ za vse $x, y \in \mathbb{R}$

2) $|x_1 + \ldots + x_n| \leq |x_1| + \ldots + |x_n|$ za vse $x_1, \ldots x_n \in \mathbb{R}$

Dokaz:

1) Za $+$ je desna neenakost trikotniška neenakost.

   Leva neenakost:

$$|x| = |(x + y) - y| \leq |x + y| + |y|$$
$$|x| - |y| \leq |x + y|$$

   Podobno velja: $|y| - |x| \leq |x + y|$

   Iz tega sledi: $||x| - |y|| \leq |x + y| \quad \square$

1.9 Kompleksna števila

Motivacija za kompleksna števila je, da bi lahko rešili enačbo:

$$x^2 = -a, a \in \mathbb{R}^+$$

Definicija: Kompleksno število je urejeni par realnih števil: množica vseh kompleknih števil je množica vseh urejenih parov realnih števil, t.j.: $\mathbb{R} \times \mathbb{R}$ in jo označimo s $\mathbb{C}$.

$$\mathbb{C} = \{(a, b); a, b \in \mathbb{R}\}$$

Opomba (kdaj sta dve kompleksni števili enaki):

$$\alpha, \beta \in \mathbb{C}, \alpha = (a, b), \beta = (c, d) : \alpha = \beta \iff a = c \wedge b = d$$

V množico kompleksnih števil vpeljemo računski operaciji:

$$\alpha, \beta \in \mathbb{C}, \alpha = (a, b), \beta = (c, d) \text{ kjer } a, b, c, d \in \mathbb{R}$$

$$\alpha + \beta = (a + c, b + d)$$
$$\alpha \cdot \beta = (ac - bd, ad + bc)$$

Izrek: $(\mathbb{C}, +, \cdot)$ je komutativen obseg. Enota za seštevanje je $(0, 0)$, enota za množenja pa $(1, 0)$. V $\mathbb{C}$ se ne da vpeljati urejenosti, da bi bil urejen obseg. Drugače povedano: izraz kot npr. $z > 0$ je nesmiselen.

Dokaz: (veljavnosti nekaterih aksiomov)

(A3) $\alpha + (0, 0) = (a, b) + (0, 0) = (a + 0, b + 0) = (a, b) = \alpha \quad \square$

(A4) $\alpha = (a, b) \in \mathbb{C} \quad -\alpha = (-a, -b)$

$$(a, b) + (-a, -b) = (a + (-a), b + (-b)) = (0, 0) = 0 \quad \square$$

(A7) $(a, b) \cdot (1, 0) = (1a - 0b, 0a + 1b) = (a, b) \quad \square$

(A8) $\alpha \in \mathbb{C}, \alpha \neq 0 \qquad \alpha = (a, b)$

$$\alpha^{-1} = (\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2})$$
$$\alpha\alpha^{-1} = (\frac{a^2 + b^2}{a^2 + b^2}, \frac{-ab + ab}{a^2 + b^2}) = (1, 0) = 1 \quad \square$$

Opomba: Kompleksni števili $(0, 0) \equiv 0, (1, 0) \equiv 1$ poimenujemo 0 in 1.

Opomba: Preslikava $\mathbb{R} \to \mathbb{C}$ definirana s predpisom $a \mapsto (a, 0)$ inducira vložitev realnih števil v kompleksnem in je usklajena z računskima operacijama.

$$(a, 0) + (b, 0) = (a + b, 0)$$
$$(a, 0) \cdot (b, 0) = (ab - 0 \cdot 0, 0a + 0b) = (ab, 0)$$

Poleg te vložitve, bi si lahko zmislili tudi kakšno drugo, vendar ne bi bila dobra. Npr: $a \mapsto (a, 1)$ ni dobra vložitev, ker že pri seštevanju "pademo ven" iz realnih vrednosti $((a, 1) + (b, 1) + (a + b, 2))$.

Torej lahko kompleksna števila $(a, 0)$ *identificiramo* z realnimi: $(a, 0) = a$.

Definicija: Kompleksno število $(0, 1)$ označimo z i in ga imenujemo *imaginarna enota.*

$$i^2 = (0, 1)(0, 1) = (0 - 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0) = -1$$
$$(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) = a + bi$$

Od tu naprej bomo kompleksna števila obravnavali kot

$$\mathbb{C} = \{a + bi, a, b \in \mathbb{R}\}$$

Definirani računski operaciji inducirata običajno računanje s kompleksnimi števili

Definicija: Naj bo $\alpha \in \mathbb{C}, \alpha = a + bi, a, b \in \mathbb{R}$

- število a je realni del kompleksnega števila α in ga označimo: $a = \Re\alpha$
- število b je imaginarni del kompleksnega števila α in ga označimo: $b = \Im\alpha$. Opomba: $\Im\alpha \in \mathbb{R}$.
- številu $a - bi$ rečemo *konjugirano število* številu α in ga označimo z $\overline{\alpha}$
- šteilo $\sqrt{\alpha\overline{\alpha}}$ imenujemo *absolutna vrednost* kompleksnega števila α in označimo $|\alpha|$

  Opomba: $\alpha = a + bi, a, b \in \mathbb{R}$

  $\sqrt{\alpha\overline{\alpha}} = \sqrt{(a + bi)(a - bi)} = \sqrt{(a^2 - abi + abi + b^2)} = \sqrt{a^2 + b^2} \in \mathbb{R} \geq 0$

  $\alpha \in \mathbb{R} \Rightarrow \sqrt{\alpha\overline{\alpha}} = \sqrt{\alpha^2} = |\alpha|$

  To pojasni, zakaj lahko uporabljamo enako oznako za absolutno vrednost kompleksnega števila, kot za absolutno vrednost realnega števila.

Trditev: Za $\alpha, \beta \in \mathbb{C}$ velja:

(i) $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$

(ii) $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$

(iii)

$$\Re\alpha = \frac{1}{2}(\alpha + \overline{\alpha})$$
$$\Im\alpha = \frac{1}{2i}(\alpha - \overline{\alpha})$$

(iv) $\alpha\overline{\alpha} = (\Re\alpha)^2 + (\Im\alpha)^2$

(v) $\overline{\overline{\alpha}} = \alpha$

Dokaz:(ii) $\alpha = a + bi, \qquad \beta = c + di, a, b, c, d \in \mathbb{R}$

$$\overline{\alpha\beta} = \overline{(a+bi)(c+di)} = \overline{(ac - bd + (ad+bc)i)} =$$
$$= ac - bd - (ad+bc)i$$

$$\overline{\alpha} \cdot \overline{\beta} = \overline{(a+bi)(c+di)} = (a-bi)(c-di) =$$
$$= ac - bd - (ad+bc)i \quad \square$$

1.9.1 Lastnosti

Za vse $\alpha, \beta \in \mathbb{C}$ velja:

(i) $|\alpha| \geq 0$

(ii) $|\alpha| = 0 \iff \alpha = 0$

(iii) $|\alpha| = |\overline{\alpha}|$

(iv) $|\alpha\beta| = |\alpha||\beta|$

(v) $|\Re\alpha| \leq |\alpha|$
$|\Im\alpha| \leq |\alpha|$

(vi) $|\alpha + \beta| \leq |\alpha| + |\beta|$
$||\alpha| - |\beta|| \leq |\alpha \pm \beta| \leq |\alpha| + |\beta|$

Dokaz

(iv)
$$|\alpha\beta|^2 = (\alpha\beta)(\overline{\alpha\beta}) = \alpha\beta\overline{\alpha}\overline{\beta} = |\alpha|^2|\beta|^2$$

Ker je $|\alpha| \geq 0$, enakost sledi.

(vi)

$$|\alpha + \beta|^2 = (\alpha + \beta)(\overline{\alpha + \beta}) = (\alpha + \beta)(\overline{\alpha} + \overline{\beta}) =$$
$$= \alpha\overline{\alpha} + \alpha\overline{\beta} + \beta\overline{\alpha} + \beta\overline{\beta} =$$
$$= |\alpha|^2 + \alpha\overline{\beta} + \beta\overline{\alpha} + |\beta|^2$$

$$(|\alpha| + |\beta|)^2 = |\alpha|^2 + 2|\alpha||\beta| + |\beta|^2$$

Dovolj je dokazati $\alpha\overline{\beta} + \beta\overline{\alpha} \leq 2|\alpha||\beta|$

$$\alpha\overline{\beta} + \beta\overline{\alpha} = \alpha\overline{\beta} + \overline{\overline{\overline{\alpha}\beta}} = \alpha\overline{\beta} + \overline{\alpha\overline{\beta}} = 2\Re(\alpha\overline{\beta})$$

$$2\Re(\alpha\overline{\beta}) \leq 2|\alpha||\beta|$$
$$|\alpha\overline{\beta}| = |\alpha||\overline{\beta}| = |\alpha||\beta|$$

Neenakost velja zaradi (v).

1.9.2 Geometrijska interpretacija

Pri učenju geometrijske interpretacije toplo priporočam zvezek s skicami. Kot piše v datoteki README.md, skic v teh zapiskih ni in jih verjetno tudi ne bo. Če misliš, da imaš dovolj dobro domišljijo in se znajdeš samo iz tekstovnega opisa, potem pa kar pogumno, čeprav te pogum ne bo pripeljal do znanja.

Kompleksno število $\alpha \in \mathbb{C}, \alpha = a + bi, a, b \in \mathbb{R}$ predstavimo s točko (a, b) v izbranem koordinatnem sistemu. Te točki nam lahko predstavljata tudi krajevna vektorja in ker kompleksna števila seštevamo po komponentah, se to ujema s seštevanjem vektorjev.

Tako kot nam absolutna vrednost realnega števila predstavlja oddaljenost števila od 0, nam tudi tu absolutna vrednost kompleksnega števila predstavlja oddaljenost števila od izhodišča koordinatnega sistema. Drugače povedano: predstavlja nam "dolžino" tega števila. To lahko vidimo tudi iz enačbe $|\alpha| = \sqrt{(\Re\alpha)^2 + (\Im\alpha)^2}$, ki nam pravzaprav predstavlja pitagorov izrek.

Če si narišemo dve števili α in β v koordinatni sistem in nato vanj vrišemo še njuno vsoto $\alpha + \beta$ po paralelogramskem pravilu za seštevanje vekotjev, opazimo, da dobimo trikotnik s stranicami α, β in $\alpha + \beta$. Za trikotnik pa vemo, da je vsota dolžin dveh stranic v trikotniku večja od dolžine tretje stranice. Iz tu izhaja ime trikotniška neenakost.