Števila

Marsikdo ob besedi matematika najprej pomisli na števila in na aritmetiko. Tekom razvoja človeške civilizacije so se najprej uporabljala naravna števila za preštevanje objektov. Ker naravnih števil ne znamo niti odštevati niti deliti, uvedemo iz praktičnih razlogov cela oziroma racionalna števila. Vsa ta števila si grafično najlažje predstavljamo kot točke na številski premici. Racionalna števila zadoščajo večini potreb v vsakdanjem življenju, so pa ljudje že dokaj zgodaj ugotovili, da racionalna števila ne popišejo vseh točk na številski premici. To pa je pomanjkljivost, ki je ne moremo prezreti, če hočemo reševati polinomske enačbe ali pa zgraditi matematično korektno teorijo diferencialnega in pa integralskega računa. Števila, ki popišejo celotno številsko premico, in vsebujejo znana števila, kot so $\sqrt{2}$ in π, imenujemo realna števila. Na intuitivni ravni si realnih števil ni težko predstavljati, mi pa si bomo v tem poglavju pogledali njihovo matematično strukturo in jih poskušali karakterizirati s pomočjo aksiomov.

Poleg realnih števil se v matematiki in fiziki uporablja še precej objektov, ki imajo zelo podobne (vendar nekaj šibkejše) lastnosti kot realna števila. Na tem mestu omenimo predvsem kompleksna števila, kvaternione in pa matrike.

Naravna, cela in racionalna števila

Najbolj preprosta izmed števil so naravna števila. Množico naravnih števil označimo z

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

Naravna števila znamo med sabo seštevati in množiti, kar opišemo z dvema funkcijama

$$\begin{aligned} + : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \qquad & (x, y) \mapsto x + y, \\ \cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \qquad & (x, y) \mapsto x \cdot y = xy. \end{aligned}$$

Funkcijam tega tipa rečemo tudi *binarne operacije.*

Pri dokazovanju izrekov o naravnih številih nas pogosto ne zanima toliko kaj števila so, temveč kakšne so njihove lastnosti. Osnovne lastnosti naravnih števil so strnjene v Peanovih aksiomih.

- P1 1 je naravno število,
- P2 vsako naravno število n ima natanko določenega naslednika n^+,
- P3 različni naravni števili imata različna naslednika,
- P4 1 ni naslednik nobenega naravnega števila,
- P5 Če je $A \subset \mathbb{N}$, $1 \in A$ in če iz $a \in A$ sledi $a^+ \in A$, je $A = \mathbb{N}$.

Petemu Peanovemu aksiomu rečemo tudi *princip popolne indukcije.* Pogosto ga uporabljamo za dokazovanje, da neka lastnost naravnih števil velja za vsa naravna števila. Da to dokažemo, je dovolj preveriti, da ta lastnost velja za število 1 in da nam veljavnost za n implicira tudi veljavnost za n^+.

Zgled. Pokažimo s principom popolne indukcije, da formula

$$1 + 2 + 3 + \ldots + n = \frac{1}{2}n(n+1)$$

velja za vsa naravna števila n. Za $n = 1$ imamo enakost $1 = 1$.

Privzemimo sedaj, da za nek $n \in \mathbb{N}$ velja

$$1 + 2 + 3 + \ldots + n = \frac{1}{2}n(n+1).$$

Potem je

$$1 + \ldots + n + (n+1) = \frac{1}{2}n(n+1) + (n+1) = \frac{1}{2}(n+1)(n+2),$$

kar smo želeli dokazati.

Naravna števila znamo seštevati in množiti. Da pa bi jih lahko tudi odštevali, jih moramo najprej razširiti do celih števil

$$\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N} = \{\ldots, -2, -1, 0, 1, 2, \ldots\},$$

s tem, da jim dodamo število nič in pa k vsakemu naravnemu številu še njegovo nasprotno število. Če želimo števila tudi deliti, pa jim moramo dodati še vse možne ulomke. Tako pridemo do racionalnih števil

$$\mathbb{Q} = \left\{ \frac{m}{n} \,\middle|\, m \in \mathbb{Z}, n \in \mathbb{N}, n \geq 1 \right\}.$$

Racionalna števila tvorijo algebraično strukturo, ki jo imenujemo obseg in ki jo bomo podrobneje spoznali v naslednjem poglavju. Kot bomo videli, jih opredeljujejo skorajda isti aksiomi kot realna števila, razen enega. Le-ta pa igra ključno vlogo pri izgradnji matematično korektne teorije diferencialnega in integralskega računa.

Realna števila

Osnovne lastnosti realnih števil

V tem poglavju si bomo podrobneje pogledali osnovne lastnosti realnih števil, ki jih bomo podali v obliki aksiomov. Aksiomi si bodo sledili po vrsti v podobnem vrstnem redu, kot prehajamo iz celih v racionalna in nato k realnim številom. Prednost tega pristopa je v tem, da se bomo lahko v nadaljevanju pri dokazovanju izrekov sklicevali direktno na te aksiome, kar bo stvari napravilo bolj pregledne.

Realna števila $\mathbb{R}$ so množica, na kateri imamo dve (osnovni) operaciji

$$\begin{array}{lll} + : \mathbb{R} \times \mathbb{R} \to \mathbb{R} & (x, y) \mapsto x + y & \text{seštevanje,} \\ \cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R} & (x, y) \mapsto x \cdot y = xy & \text{množenje.} \end{array}$$

Ti dve operaciji morata zadoščati 13-im aksiomom, ki jih bomo sedaj našteli.

V prvo skupino aksiomov sodijo aksiomi za seštevanje:

AKSIOM 1	$x + (y + z) = (x + y) + z$	asociativnost,
AKSIOM 2	$x + y = y + x$	komutativnost,
AKSIOM 3	$x + 0 = x$	obstoj števila 0,
AKSIOM 4	$x + (-x) = 0$	obstoj nasprotnega števila.

Prva dva aksioma opisujeta dve dobro znani lastnosti realnih števil. Pri seštevanju namreč ni pomembno, kako postavimo oklepaje in v katerem vrstnem redu seštevamo. Tretji aksiom postulira obstoj števila 0, ki ima lastnost, da za vsako število $x \in \mathbb{R}$ velja $x + 0 = x$. Podobno nam četrti aksiom pove, da ima vsako število $x \in \mathbb{R}$ svoje nasprotno število, ki ga označimo z $-x$. Torej lahko smiselno definiramo tudi odštevanje s predpisom

$$x - y := x + (-y).$$

Prve štiri aksiome smo zbrali skupaj, ker določajo strukturo, ki se zelo pogosto pojavlja v matematiki. Množici, opremljeni z binarno operacijo, ki zadošča zgornjim štirim aksiomom, rečemo *Abelova grupa*. Poleg realnih števil so primeri Abelovih grup tudi cela in pa racionalna števila skupaj z operacijo seštevanja. Niso pa Abelova grupa naravna števila, ker ne izpolnjujejo četrtega aksioma. Poglejmo si nekaj lastnosti Abelovih grup.

Trditev 1. *V poljubni Abelovi grupi veljajo naslednje trditve:*

(1) Če je $x + y = x + z$, je $y = z$ (pravilo krajšanja).

(2) Enačba $b + x = a$ za spremenljivko x ima enolično rešitev $x = a - b$.

(3) Nasprotno število poljubnega realnega števila x je enolično določeno s pogojem $x + (-x) = 0$.

(4) $-0 = 0$.

(5) $-(x + y) = (-x) + (-y)$.

(6) $-(-x) = x$.

Dokaz. (1) Predpostavimo, da velja $x + y = x + z$. Potem je

$$y = 0 + y = (-x) + x + y = (-x) + x + z = 0 + z = z.$$

Pri izpeljavi smo uporabili lastnosti nasprotnega števila in pa števila 0 ter asociativnost seštevanja.

(2) Naj bo $x = a - b$. Iz enakosti

$$b + x = b + (a - b) = b + a + (-b) = b + (-b) + a = 0 + a = a$$

sledi, da ta x reši enačbo $b + x = a$. Tukaj smo uporabili komutativnost in asociativnost seštevanja ter lastnosti nasprotnega števila in števila 0. Če tudi število y zadošča enačbi $b+y = a$, dobimo $a = b+x = b+y$. Po pravilu krajšanja od tod sledi $x = y$, torej je enačba enolično rešljiva.

(3) Rešitev enačbe $x + y = 0$ je po prejšnji točki enolična in enaka $y = 0 - x = -x$, kar pomeni, da je nasprotno število enolično določeno.

(4) Opazimo, da število 0 reši enačbo $0 + y = 0$, zato je $0 = 0 - 0 = -0$.

(5) Tukaj si poglejmo enačbo $(x + y) + z = 0$ za spremenljivko z. Ker $z = (-x) + (-y)$ reši to enačbo, je $-(x + y) = (-x) + (-y)$.

(6) Za konec si poglejmo še enačbo $(-x) + y = 0$. Število x je rešitev te enačbe, torej je $-(-x) = x$. □

Vse omenjene lastnosti seveda že poznamo za realna števila. Prednost aksiomatskega pristopa pri dokazovanju (da torej vse izpeljemo samo iz omenjenih štirih aksiomov) pa je, da smo hkrati pokazali, da te lastnosti veljajo za vsako Abelovo grupo.

Poglejmo si sedaj drugo skupino aksiomov, ki opredeljujejo množenje:

AKSIOM 5	$x(yz) = (xy)z$	asociativnost,
AKSIOM 6	$xy = yx$	komutativnost,
AKSIOM 7	$1 \cdot x = x$	obstoj števila 1,
AKSIOM 8	$x \cdot \dfrac{1}{x} = 1, \text{ če } x \neq 0$	obstoj obratnega števila.

Vidimo, da so aksiomi za množenje precej podobni aksiomom za seštevanje, razlika je le med aksiomoma 4 in 8. Vsako realno število ima nasprotno število, medtem ko imajo obratno število le neničelna realna števila. Pišemo tudi $\frac{1}{x} = x^{-1}$ in označimo

$$x \cdot \frac{1}{y} = \frac{x}{y}.$$

Iz aksiomov sledi, da tvorijo neničelna realna števila Abelovo grupo za množenje, zato na podoben način kot Trditev 1 lahko dokažemo tudi naslednjo trditev.

Trditev 2. *(1) Če je $xy = xz$ in $x \neq 0$, je $y = z$ (pravilo krajšanja).*

(2) Naj bo $b \neq 0$. Potem ima enačba $bx = a$ enolično rešitev $x = \frac{a}{b}$.

(3) Obratno število poljubnega neničelnega števila x je enolično določeno s pogojem $x \cdot x^{-1} = 1$.

(4) $\frac{1}{1} = 1$.

(5) $\frac{1}{x \cdot y} = \frac{1}{x} \cdot \frac{1}{y}$.

(6) $(x^{-1})^{-1} = x$.

Tretja skupina aksiomov povezuje seštevanje in množenje.

AKSIOM 9	$1 \neq 0$,	
AKSIOM 10	$x(y + z) = xy + xz$	distributivnost.

Zahtevamo torej, da sta 0 in 1 različni realni števili in da lahko oklepaje odpravimo po distributivnostnem zakonu. Zapis $xy+xz$ kot običajno pomeni, da izračunamo najprej oba produkta in ju nato seštejemo.

Množici, ki je opremljena z dvema operacijama, ki zadoščata omenjenim desetim aksiomom, rečemo *obseg*. Poleg realnih števil sta precej znana še obsega racionalnih in pa kompleksnih števil.

Trditev 3. *V vsakem obsegu veljajo formule:*

(1) $x \cdot 0 = 0$.

(2) Iz $xy = 0$ sledi $x = 0$ ali $y = 0$.

(3) $x(y - z) = xy - xz$.

(4) $x(-z) = -(xz)$.

(5) $\frac{x}{y} + \frac{z}{y} = \frac{x+z}{y}$.

Dokaz. (1) Iz enakosti

$$x \cdot 1 + x \cdot 0 = x \cdot (1 + 0) = x \cdot 1 = x \cdot 1 + 0$$

dobimo po krajšanju $x \cdot 0 = 0$.

(2) Naj bo $xy = 0$ in denimo, da je $x \neq 0$. Pokazati moramo, da od tod sledi $y = 0$. Ker je $x \neq 0$, obstaja obratno število x^{-1}. Sedaj velja

$$0 = x^{-1} \cdot 0 = x^{-1}(xy) = (x^{-1}x)y = 1 \cdot y = y.$$

(3) Najprej pišimo $y = (y - z) + z$. Potem je

$$xy = x((y - z) + z) = x(y - z) + xz.$$

Če odštejemo xz na obeh straneh, dobimo željeno enakost.

(4) Sledi iz prejšnje enakosti, če je $y = 0$.

(5) Računajmo

$$\frac{x}{y} + \frac{z}{y} = xy^{-1} + zy^{-1} = (x+z)y^{-1} = \frac{x+z}{y}.$$

□

Četrta skupina aksiomov nam določa urejenost na množici realnih števil. Zahtevamo, da obstaja podmnožica $\mathbb{R}^+ \subset \mathbb{R}$ *pozitivnih* realnih števil, za katero veljata:

AKSIOM 11 $0 \notin \mathbb{R}^+$ in za poljubno število $x \in \mathbb{R} \setminus \{0\}$ je bodisi $x \in \mathbb{R}^+$ ali pa $x \notin \mathbb{R}^+$, ne pa oboje.

AKSIOM 12 Množica $\mathbb{R}^+$ je zaprta za seštevanje in množenje.

Aksiom 11 nam množico realnih števil razdeli na tri disjunktne kose

$$\mathbb{R} = \mathbb{R}^+ \cup \{0\} \cup \mathbb{R}^-,$$

kjer so $\mathbb{R}^- = \{-x \mid x \in \mathbb{R}^+\}$ *negativna* realna števila. Aksiom 12 dodatno še zahteva, da je vsota in produkt dveh pozitivnih števil spet pozitivno število.

S pomočjo pozitivnih realnih števil $\mathbb{R}^+$ lahko realna števila *uredimo po velikosti.* Formalno to naredimo, tako da uvedemo na množico $\mathbb{R}$ ustrezno relacijo. *Relacija* na množici A je neka podmnožica $R \subseteq A \times A$. To pomeni, da za vsak par (a, a') elementov množice A povemo ali je $(a, a') \in R$. Kadar je $(a, a') \in R$, rečemo, da je a v relaciji z a' in pišemo aRa'.

Na množico realnih števil lahko uvedemo relacijo urejenosti po velikosti

$$x < y \iff y - x \in \mathbb{R}^+.$$

To pomeni, da je po definiciji število y večje od števila x natanko takrat, ko je razlika $y - x$ pozitivno število. Podobno lahko definiramo relacijo

$$x \leq y \iff (x < y \text{ ali } x = y).$$

Pogosto uporabljamo tudi relaciji $x > y$ in $x \geq y$, ki pomenita $y < x$ oziroma $y \leq x$. Poskusimo sedaj iz aksiomov dokazati nekaj lastnosti urejenosti, ki jih že dobro poznamo.

Trditev 4. *(1) Iz $x < y$ in $y < z$ sledi $x < z$ (tranzitivnost relacije $<$).*

(2) Za poljubna $x, y \in \mathbb{R}$ velja natanko ena izmed možnosti

$$x < y, \quad x = y, \quad x > y \quad \textit{(zakon trihotomije)}$$

(3) Veljata ekvivalenci: $(x \in \mathbb{R}^+ \iff x > 0)$ in $(x \in \mathbb{R}^- \iff x < 0)$.

(4) Iz $x < y$ sledi $x + z < y + z$ za vsak $z \in \mathbb{R}$.

(5) Iz $x < y$ sledi $xz < yz$ za vsak $z \in \mathbb{R}^+$.

(6) Iz $x < 0$ in $y < 0$ sledi $xy > 0$.

(7) Iz $x < 0$ in $y > 0$ sledi $xy < 0$.

(8) $x^2 = x \cdot x > 0$ za vsak $x \neq 0$.

(9) $1 > 0$.

(10) Iz $x < y$ in $z < w$ sledi $x + z < y + w$.

Dokaz. (1) Ker je $y - x \in \mathbb{R}^+$ in $z - y \in \mathbb{R}^+$, je po aksiomu 12

$$(y - x) + (z - y) = z - x \in \mathbb{R}^+.$$

(2) Sledi iz aksioma 11.

(3) Prva ekvivalenca sledi iz definicije relacije $>$. Za drugi del pa si poglejmo naslednjo verigo ekvivalenc

$$x \in \mathbb{R}^- \iff -x \in \mathbb{R}^+ \iff 0 - x \in \mathbb{R}^+ \iff x < 0.$$

(4) Sledi iz $(y + z) - (x + z) = y - x \in \mathbb{R}^+$.

(5) Velja $yz - xz = (y - x)z$. Ker sta $y - x$ in z pozitivni števili, je tudi njun produkt po aksiomu 12 pozitiven.

(6) Naj bosta $x < 0$ in $y < 0$. Potem je $-x > 0$ in $-y > 0$ in zato sledi po aksiomu 12 tudi $(-x)(-y) > 0$. S pomočjo Trditve 3 (4) sledi

$$(-x)(-y) = -((-x)y) = -(y(-x)) = -(-(yx)) = -(-(xy)).$$

Iz Trditve 1 (6) sedaj sklepamo $(-x)(-y) = xy$ in zato $xy > 0$.

(7) Sklepamo na podoben način kot v prejšnjem primeru. Če je $x < 0$ in $y > 0$, je $(-x)y > 0$. Zato iz $(-x)y = -xy$ sledi $xy < 0$.

(8) Ločimo dve možnosti. Če je $x > 0$, je $x^2 > 0$ po aksiomu 12. Če pa je $x < 0$, pa velja $x^2 > 0$ zaradi (6).

(9) Velja $1 = 1 \cdot 1 = 1^2 > 0$ po (8).

(10) Naj bo $x < y$ in $z < w$. Potem iz (4) sledita

$$x + z < y + z,$$

$$y + z < y + w.$$

Zaradi tranzitivnosti relacije $<$ je potem $x + z < y + w$. □

Obseg, ki je urejen z aksiomoma 11 in 12, imenujemo *urejen obseg*. Poleg realnih števil so tudi racionalna števila urejen obseg, kar pomeni, da dosedaj omenjenih 12 aksiomov realnih števil ne določa natanko.

Preden navedemo še zadnji aksiom realnih števil, moramo definirati še nekaj izrazov, ki imajo sicer smisel v vsakem urejenem obsegu.

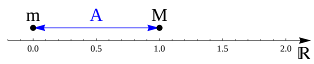
Definicija 5. *Naj bo $A \subset \mathbb{R}$ podmnožica.*

(1) Množica A je navzgor omejena, če obstaja $M \in \mathbb{R}$, tako da je $x \leq M$ za vsak $x \in A$. Takšen M imenujemo zgornja meja A.

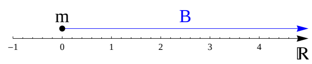
(2) Množica A je navzdol omejena, če obstaja $m \in \mathbb{R}$, tako da je $m \leq x$ za vsak $x \in A$. Takšen m imenujemo spodnja meja A.

(3) Množica A je omejena, če je navzgor in navzdol omejena.

Zgled. (1) Množica $A = (0, 1)$ je omejena. Za zgornjo mejo lahko vzamemo $M = 1$, za spodnjo pa $m = 0$.



(2) Množica $B = (0, \infty)$ je navzdol omejena z $m = 0$, navzgor pa ni omejena.



(3) Prazna množica $\emptyset$ je hkrati navzgor in navzdol omejena in vsako realno število je hkrati njena zgornja in spodnja meja.

Če je množica A navzgor omejena s številom M, je tudi vsako število, ki je večje od M, zgornja meja za A. Zato nas zanima predvsem število, ki je najmanjše izmed zgornjih mej. Število M je *najmanjša* (natančna) zgornja meja množice A oziroma *supremum* množice A, če velja:

· M je zgornja meja množice A.

· Če je tudi M' zgornja meja množice A, je $M \leq M'$.

Najmanjšo zgornjo mejo množice A označimo s $\sup(A)$. Število m je *največja* spodnja meja oziroma *infimum* množice A, če velja:

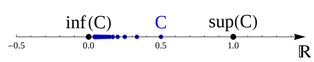
· m je spodnja meja množice A.

· Če je tudi m' spodnja meja množice A, je $m' \leq m$.

Infimum množice A označimo z $\inf(A)$.

Zgled. (1) Množica $A = (0, 1)$ ima $\sup(A) = 1$ in $\inf(A) = 0$.

(2) Množica $C = \{ \frac{1}{n} \,|\, n \in \mathbb{N}\}$ je omejena in $\inf(C) = 0$ ter $\sup(C) = 1$.



(3) Za konec si poglejmo še primer, ki nam ilustrira ključno razliko med realnimi in racionalnimi števili. Vzemimo realno število $e = 2,71827\ldots$ in množico njegovih končnih decimalnih približkov

$$\begin{aligned} r_1 &= 2 \\ r_2 &= 2,7 \\ r_3 &= 2,71 \\ r_4 &= 2,718 \\ &\vdots \end{aligned}$$

Množica racionalnih števil $E = \{r_1, r_2, r_3, \ldots\} \subset \mathbb{Q}$ je potem omejena. Njen infimum $\inf(E) = 2$ je spet racionalno število, medtem ko njen supremum $\sup(E) = e$ ni racionalno število. Množica E je torej primer omejene množice racionalnih števil, ki nima natančne zgornje meje v racionalnih številih. Kot bomo kmalu spoznali, je pomembna lastnost realnih števil ta, da ima vsaka omejena množica tako infimum kot supremum.

S supremumi in infimumi množic lahko tudi računamo. Najprej za poljubni podmnožici A in B realnih števil definirajmo njuno *vsoto*

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

za poljubno podmnožico A pa

$$-A = \{\, -a \mid a \in A\}.$$

Trditev 6. *Za poljubni (omejeni) podmnožici A in B realnih števil velja:*

(1) $\sup(A + B) = \sup(A) + \sup(B)$,

(2) $\inf(A + B) = \inf(A) + \inf(B)$,

(3) $\sup(A) = -\inf(-A)$ *in* $\inf(A) = -\sup(-A)$,

(4) če je $a \leq b$ za vsak $a \in A$ in $b \in B$, je $\sup(A) \leq \inf(B)$.

Dokaz. (1) Pokazati moramo, da je $\sup(A)+\sup(B)$ najmanjša zgornja meja množice $A + B$.

Ker velja $a \leq \sup(A)$ za vsak $a \in A$ in $b \leq \sup(B)$ za vsak $b \in B$, je $a + b \leq \sup(A) + \sup(B)$ za vsak $a \in A$ in $b \in B$. Od tod sledi, da je $\sup(A) + \sup(B)$ zgornja meja množice $A + B$.

Naj bo sedaj $c < \sup(A) + \sup(B)$. Potem je $c - \sup(A) < \sup(B)$ in zato iz definicije števila $\sup(B)$ sledi, da obstaja $b \in B$, da je $c - \sup(A) < b$ oziroma $c - b < \sup(A)$. Z istim premislekom lahko sedaj najdemo $a \in A$, da je $c - b < a$ oziroma $c < a + b$. Od tod sledi, da je $\sup(A) + \sup(B)$ najmanjša zgornja meja množice $A + B$.

(2) Dokaz je analogen dokazu točke (1).

(3) Za vsak $a \in A$ je $\inf(-A) \leq -a$ oziroma $a \leq -\inf(-A)$. Torej je $-\inf(-A)$ zgornja meja množice A. Če je $c < -\inf(-A)$, je $\inf(-A) < -c$, zato po definiciji največje spodnje meje obstaja $a \in A$, da velja $-a < -c$ oziroma $c < a$. Torej je $\sup(A) = -\inf(-A)$. Druga enakost sledi iz prve z zamenjavo množic A in $-A$.

(4) Pokazati moramo, da je število $\inf(B)$ zgornja meja množice A. Ker je $a \leq b$ za vsak $a \in A$ in vsak $b \in B$, je vsak $a \in A$ spodnja meja množice B. Od tod sledi, da je $a \leq \inf(B)$ za vsak $a \in A$, kar smo želeli dokazati. □

Zdaj lahko formuliramo zadnji aksiom realnih števil, ki nam bo omogočal ločiti realna števila od racionalnih.

AKSIOM 13 (DEDEKIND)

Vsaka neprazna, navzgor omejena podmnožica realnih števil ima najmanjšo zgornjo mejo.

Aksiomom $1-13$ zadošča le en urejen obseg: realna števila. Aksiomatski pristop je dober še za nekaj drugega; vse lastnosti realnih števil morajo biti namreč izpeljive iz teh trinajstih aksiomov.

Dosedaj smo se predvsem posvetili opisu lastnosti realnih števil, nič pa nismo povedali o tem, kaj realna števila so in kako jih predstavimo. Vsaki strukturi, ki zadošča omenjenim aksiomom, rečemo sistem realnih števil. Poleg običajnega modela z decimalnimi števili, ki ga bomo kmalu spoznali, v matematiki realna števila modeliramo tudi s Cauchyjevimi zaporedji racionalnih števil in pa s tako imenovanimi rezi.

Ne glede na to, kateri sistem realnih števil uporabljamo, lahko znotraj realnih števil zmeraj modeliramo naravna števila. Naravno število 1 je predstavljeno z elementom, ki ga določa aksiom 7 in je prav tako označen z 1. Število 2 nam predstavlja element $1 + 1$, število 3 element $1 + 1 + 1$ itd. Tako definirana podmnožica $\mathbb{N} \subset \mathbb{R}$ ustreza Peanovim aksiomom, ki smo jih navedli v prejšnjem razdelku. S pomočjo nasprotnih in pa obratnih elementov lahko iz podmnožice naravnih števil znotraj sistema realnih števil konstruiramo tudi cela števila in pa racionalna števila.

Poglejmo si sedaj nekaj posledic Dedekindovega aksioma.

Trditev 7. *Vsaka neprazna, navzdol omejena podmnožica realnih števil ima največjo spodnjo mejo.*

Dokaz. Naj bo $A \subset \mathbb{R}$ neprazna in navzdol omejena množica. Potem je množica $-A$ navzgor omejena, zato ima po aksiomu 13 najmanjšo zgornjo mejo $\sup(-A)$. Sledi $\inf(A) = -\sup(-A)$. □

Trditev 8. *Množica naravnih števil ni navzgor omejena.*

Dokaz. Če bi bila množica naravnih števil $\mathbb{N}$ navzgor omejena, bi obstajala njena najmanjša zgornja meja M v $\mathbb{R}$. Iz definicije potem sledi, da bi moral obstajati $n \in \mathbb{N}$, za katerega je $M - 1 < n$ oziroma $M < n + 1$. Ker je tudi $n + 1 \in \mathbb{N}$, je to v protislovju s predpostavko, da je M zgornja meja $\mathbb{N}$. □

Množica naravnih števil torej ni omejena, ima pa infimum $\inf(\mathbb{N}) = 1$.

Trditev 9. *Množica celih števil ni omejena niti navzgor niti navzdol.*

Dokaz. Velja $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$. Ker množica $\mathbb{N}$ ni navzgor omejena, množica $-\mathbb{N}$ (in zato tudi $\mathbb{Z}$) ni navzdol omejena. □

Trditev 10. *(1) Za vsak $x \in \mathbb{R}$ obstaja $n \in \mathbb{N}$, da velja $n > x$.*

(2) Za poljubni pozitivni realni števili a in b obstaja $n \in \mathbb{N}$, da velja $na > b$.

(3) Za poljubno pozitivno realno število a obstaja $n \in \mathbb{N}$, da velja $\frac{1}{n} < a$.

Dokaz. (1) Ker množica $\mathbb{N}$ ni navzgor omejena, število x ni njena zgornja meja. Zato obstaja $n \in \mathbb{N}$, da je $n > x$.

(2) Po prejšnji točki obstaja $n \in \mathbb{N}$, da velja $n > \frac{b}{a}$. Od tod sledi $na > b$, ker je $a > 0$.

(3) Po točki (1) obstaja $n \in \mathbb{N}$, da je $n > \frac{1}{a}$, od koder sledi trditev. □

Predstavitev realnih števil v decimalnem zapisu

Realna števila ponavadi predstavljamo v decimalnem zapisu, ki lahko število natančno določa (v primeru celih števil), včasih pa le približno (število $3,14$ je npr. približek za π). V tem razdelku si bomo pogledali, kako lahko realna števila predstavimo z neskončnim decimalnim zapisom in nekatere osnovne lastnosti takšne predstavitve.

Izberimo poljubno pozitivno realno število x. Potem obstaja natanko določen $a_0 \in \mathbb{N}$, da velja

$$a_0 \leq x < a_0 + 1.$$

Število a_0 igra vlogo celega dela realnega števila x in je največje naravno število, ki ne presega x. V naslednjem koraku izberimo natanko določen $a_1 \in \{ 0, 1, \ldots, 9 \}$, ki zadošča

$$a_0 + \frac{a_1}{10} \leq x < a_0 + \frac{a_1 + 1}{10}.$$

Ta a_1 igra vlogo cifre, ki je tik za decimalno vejico v zapisu števila x. V podobnem slogu lahko določimo tudi preostale cifre za decimalno vejico. Če smo že določili prvih $(k-1)$ cifer, je na k-tem mestu cifra a_k, za katero velja

$$a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_k}{10^k} \leq x < a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_k + 1}{10^k}.$$

Na ta način lahko vsakemu realnemu številu x priredimo neskončni decimalni zapis

$$x = a_0, a_1 a_2 \ldots a_k a_{k+1} \ldots$$

Različnima številoma pripadata različna zapisa, kar pomeni, da smo množico realnih števil injektivno preslikali v množico vseh neskončnih decimalnih zapisov. Moramo pa biti pri tej predstavitvi pozorni, saj omenjena preslikava ni bijekcija. Z omenjeno konstrukcijo dobimo namreč samo decimalne zapise, pri katerih se cifra 9 ne ponavlja od nekod naprej. Da bi bolje razumeli, zakaj takšni zapisi ne pridejo v poštev, si poglejmo decimalni zapis

$$0,99999\ldots$$

Če bi dani zapis predstavljal neko realno število x, bi to število bilo zgornja meja množice $S = \{\, s_k \,|\, k \in \mathbb{N}\}$ vseh končnih decimalnih približkov

$$s_k = 0,\underbrace{9\ldots9}_{k}$$

števila x. Torej bi veljalo $x \geq \sup S = 1$, kar pa bi pomenilo, da se decimalni zapis x ne začne z 0. To pa je v protislovju z našo predpostavko.

Razen ravnokar omenjenih decimalnih zapisov pa vsak decimalni zapis pripada nekemu realnemu številu. Poljubnemu zapisu $a_0, a_1 a_2 a_3 \ldots$ lahko namreč priredimo zaporedje racionalnih števil $\{q_k\}_{k\in\mathbb{N}}$, kjer je

$$q_k = a_0, a_1 \ldots a_k.$$

Množica $\{q_k \,|\, k \in \mathbb{N}\}$ je navzgor omejena in njena najmanjša zgornja meja je ravno realno število x, ki je predstavljeno z zapisom $a_0, a_1 a_2 a_3 \ldots$. Velja tudi ocena

$$x - q_k < 10^{-k},$$

kar pomeni, da lahko vsako realno število aproksimiramo poljubno natančno z racionalnimi števili. Rečemo tudi, da je množica racionalnih števil *gosta* v množici realnih števil.

Celim številom pri tej konstrukciji ustrezajo natanko decimalni zapisi, ki imajo za decimalno vejico same ničle, racionalnim številom pa zapisi, ki so od nekod dalje periodični (npr. $\frac{1}{3} = 0,3333\ldots$).

Negativnemu realnemu številu x priredimo decimalni zapis, tako da pred zapis števila $-x$ (ki je pozitivno število) dodamo negativen predznak.

Omenjena konstrukcija nam pokaže, kako lahko poljubnemu elementu nekega sistema realnih števil priredimo neskončen decimalni zapis. Zato bi lahko vzeli kar vse tako dobljene neskončne decimalne zapise kot našo množico realnih števil. Pomanjkljivost tega pristopa pa je v tem, da je za dva decimalna zapisa, ki predstavljata iracionalni števili, nekoliko težje definirati njuno vsoto in pa produkt. Zato ponavadi v teoriji raje uporabljamo kakšne druge sisteme realnih števil.

Iracionalna realna števila in obstoj korenov

Ena izmed motivacij za uvedbo realnih števil prihaja iz potrebe po reševanju polinomskih enačb. V tem razdelku si bomo pogledali, kako lahko s pomočjo aksiomov pokažemo, da ima vsako pozitivno realno število svoj kvadratni koren in pa, da niso vsa realna števila racionalna.

Izberimo si poljubno realno število a in si poglejmo enačbo v realnih številih

$$x^2 = a.$$

Če je $a < 0$, vemo, da ta enačba nima rešitev po Trditvi 4 (8), v primeru $a = 0$, pa je $x = 0$ njena edina rešitev.

Naj bo sedaj $a > 0$. Če je x_1 rešitev zgornje enačbe, je tudi število $-x_1$ rešitev iste enačbe. V tem primeru sta to tudi njeni edini rešitvi. Če namreč za nek y velja $y^2 = a$, sledi $y^2 = x_1^2$ oziroma $(y - x_1)(y + x_1) = 0$. Torej je $y = \pm x_1$. V naslednji trditvi bomo pokazali, da ima zgornja enačba zmeraj rešitev v realnih številih.

Trditev 11. *Naj bo a pozitivno realno število. Potem ima enačba $x^2 = a$ natanko eno pozitivno realno rešitev, ki jo označimo $x = \sqrt{a}$.*

Dokaz. Definirajmo podmnožico realnih števil

$$S = \{\, x > 0 \mid x^2 < a \,\}.$$

Najprej pokažimo, da je S neprazna množica. Iz neenakosti $a^2 < (1 + a)^2 a$ sledi $\left(\frac{a}{1+a}\right)^2 < a$. Ker je $0 < \frac{a}{1+a}$, je torej $\frac{a}{1+a} \in S$.

Poleg tega je $(1 + a)^2 > a > x^2$ za vsak $x \in S$, kar pomeni, da je $1 + a$ zgornja meja množice S. Po Dedekindovem aksiomu obstaja torej (pozitivno) število $b = \sup(S)$.

Sedaj imamo tri možnosti: $b^2 > a$, $b^2 < a$ in $b^2 = a$. Pokazati želimo, da velja $b^2 = a$, kar bo pomenilo, da je b rešitev enačbe $x^2 = a$.

(1) Recimo, da velja $b^2 > a$. Vzemimo število $c = b - \frac{b^2 - a}{2b} = \frac{1}{2}(b + \frac{a}{b})$. Iz zapisa je razvidno, da je $0 < c < b$. Poleg tega je

$$c^2 = b^2 - (b^2 - a) + \frac{(b^2 - a)^2}{4b^2} = a + \frac{(b^2 - a)^2}{4b^2} > a.$$

Od tod bi sledilo, da je c zgornja meja za S. Ker je $c < b$, je to v protislovju s predpostavko, da je b najmanjša zgornja meja množice S.

(2) Recimo sedaj, da velja $b^2 < a$. Potem lahko najdemo število c, za katerega velja $0 < c < b$ in $c < \frac{a - b^2}{3b}$. Sledi

$$(b + c)^2 = b^2 + c(2b + c) < b^2 + 3bc < b^2 + (a - b^2) = a.$$

Torej je $b + c \in S$. Ker je $b + c > b$, je to v nasprotju s predpostavko, da je b zgornja meja S.

(3) Preostane nam torej možnost $b^2 = a$, ki pove, da je b (edina) pozitivna rešitev enačbe $x^2 = a$. Njena druga rešitev $-b$ je namreč negativna. $\square$

Pri dokazu obstoja kvadratnih korenov pozitivnih števil je bila ključna lastnost realnih števil, ki jo opisuje Dedekindov aksiom. V naslednji trditvi bomo pokazali, da kvadratne enačbe zgornjega tipa niso vedno rešljive v obsegu racionalnih števil, kar bo pomenilo, da racionalna števila ne zadoščajo Dedekindovemu aksiomu.

Trditev 12. *Enačba $x^2 = 2$ nima rešitev v racionalnih številih.*

Dokaz. Recimo, da je $(\frac{m}{n})^2 = 2$, kjer je $\frac{m}{n}$ okrajšan ulomek. Sledi, da je $m^2 = 2n^2$. Zato sta m^2 in posledično m sodi števili. Torej lahko pišemo $m = 2k$ za neko celo število k. Sedaj dobimo enakost $m^2 = 4k^2 = 2n^2$ oziroma $n^2 = 2k^2$, ki nam pove, da je tudi n sodo število. Pridemo v protislovje s predpostavko, da je ulomek $\frac{m}{n}$ okrajšan. □

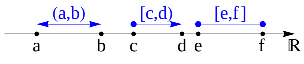
Kvadratni koreni so posebni primeri *algebraičnih števil*, to je števil, ki so rešitev kakšne polinomske enačbe s celimi koeficienti. Algebraična števila vsebujejo vsa racionalna števila in tudi sama tvorijo urejen obseg, ki pa spet ne zadošča Dedekindovemu aksiomu. Realnim številom, ki niso niti racionalna, niti algebraična, rečemo *transcendentna* števila. Kljub temu, da poznamo le nekaj transcendentnih števil kot sta npr. π in e, pa transcendentna števila tvorijo veliko večino realnih števil. V matematičnem jeziku to pomeni, da je množica realnih števil ekvipolentna množici transcendentnih števil.

Intervali, okolice in absolutna vrednost

V prejšnjih poglavjih smo se ukvarjali z algebraičnimi lastnostmi realnih števil. Dejstvo, da realna števila tvorijo urejen obseg pa nam omogoča, da govorimo tudi o tem ali sta dve realni števili blizu skupaj ali pa daleč narazen. S pomočjo teh pojmov definiramo ključne pojme v matematični analizi, kot so zveznost, odvedljivost in pa integracija.

Bistveno vlogo pri tem igrajo intervali. Poznamo *zaprte*, *polzaprte* in pa *odprte* intervale:

$$
\begin{aligned}
[a, b\,] &= \{\, x \in \mathbb{R} \,|\, a \leq x \leq b\},\\
(a, b\,] &= \{\, x \in \mathbb{R} \,|\, a < x \leq b\},\\
[a, b) &= \{\, x \in \mathbb{R} \,|\, a \leq x < b\},\\
(a, b) &= \{\, x \in \mathbb{R} \,|\, a < x < b\}.
\end{aligned}
$$



Točki a in b imenujemo *robni točki* intervala, točke v (a, b) pa *notranjost* intervala. V vseh štirih primerih je a največja spodnja meja, b pa najmanjša zgornja meja intervala. Ti primeri so tudi zgled, da je lahko najmanjša zgornja meja omejene množice včasih vsebovana v množici, včasih pa ne.

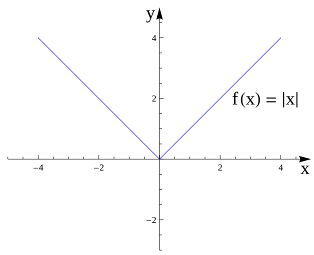
Razdaljo med dvema realnima številoma merimo s pomočjo absolutne vrednosti. Za vsak $x \in \mathbb{R}$ definiramo

$$|\,x\,| = \begin{cases} x & ;\ x \geq 0, \\ -x & ;\ x < 0. \end{cases}$$

Absolutno vrednost lahko torej smatramo kot funkcijo

$$|\,.\,| : \mathbb{R} \to \mathbb{R},$$

katere graf v $\mathbb{R} \times \mathbb{R}$ ima obliko



Razdalja med realnima številoma x in y je potem definirana kot

$$d(x, y) = d(y, x) = |x - y|.$$

Poglejmo si sedaj povezavo med absolutnimi vrednostmi in pa okolicami.

Definicija 13. *Naj bo $a \in \mathbb{R}$ in $\epsilon > 0$. Odprta krogla s središčem v a in s polmerom ϵ je množica*

$$(a - \epsilon, a + \epsilon) = \{\, x \in \mathbb{R} \,|\, a - \epsilon < x < a + \epsilon \} = \{\, x \in \mathbb{R} \,|\, |x - a| < \epsilon \}.$$

Označimo jo s $K(a, \epsilon)$.

Naj bo sedaj $A \subset \mathbb{R}$ poljubna podmnožica in $a \in A$.

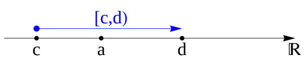
· Točka a je *notranja* točka množice A, če obstaja $\epsilon > 0$, da je $K(a, \epsilon) \subset A$.

· Množica A je *odprta*, če je vsaka njena točka notranja točka.

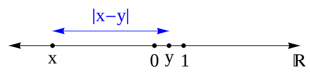
· Množica A je *zaprta*, če je množica A^c odprta.

Odprti intervali so odprte podmnožice, zaprti intervali pa zaprte podmnožice realnih števil. Množici $\emptyset$ in $\mathbb{R}$ sta hkrati odprti in zaprti. Polodprt interval ni niti odprt niti zaprt.

Če je a notranja točka množice A, rečemo, da je A *okolica* točke a. Okolica realnega števila a je takšna podmnožica realnih števil, ki vsebuje vsa realna števila, ki so dovolj blizu a. Polodprt interval je na primer okolica vseh svojih notranjih točk, ni pa okolica robne točke.



Realna števila si geometrično predstavljamo kot točke na realni premici. Število 0 igra vlogo koordinatnega izhodišča, število 1 pa je na enotski oddaljenosti od izhodišča v smeri desno. Z absolutno vrednostjo $|x-y|$ izmerimo razdaljo med številoma x in y.



Trditev 14. *Za poljubni realni števili x in y veljajo:*

1. $|\,x\,| \geq 0$ *in* $(|\,x\,| = 0 \iff x = 0)$,
2. $|xy| = |\,x\,||\,y\,|$,
3. $|x+y| \leq |\,x\,| + |\,y\,|$ *in* $|x-y| \leq |\,x\,| + |\,y\,|$,
4. $||\,x\,| - |\,y\,|| \leq |x+y|$ *in* $||\,x\,| - |\,y\,|| \leq |x-y|$.

Dokaz. Točki (1) in (2) sledita po kratkem premisleku direktno iz definicije absolutne vrednosti.

Pri dokazu točke (3) je dovolj pokazati samo prvo neenakost, saj druga sledi iz prve, če vstavimo namesto y število $-y$. V primeru, ko je $x = 0$ ali $y = 0$, ali pa sta x in y istega predznaka, imamo celo enakost, zato je dovolj pogledati primer, ko je npr. $x < 0$ in pa $y > 0$. Tukaj ločimo dva primera. Če je $x + y \geq 0$, se neenakost $|x + y| \leq |\,x\,| + |\,y\,|$ prevede v $x + y \leq -x + y$, kar pa drži, saj je $x < 0$. Če pa je $x + y < 0$, pa dobimo neenakost $-x - y \leq -x + y$, ki pa spet drži, ker je $y > 0$.

Za dokaz točke (4) je spet dovolj pokazati samo prvo neenakost. Iz točke (3) dobimo neenakost $|a+b| \leq |\,a\,| + |\,b\,|$ za poljubna $a, b \in \mathbb{R}$. Če vzamemo $a = x + y$ in $b = -x$, dobimo

$$|\,y\,| = |a+b| \leq |\,a\,| + |\,b\,| = |x+y| + |-x| = |x+y| + |\,x\,|,$$

kar nam da

$$-|x+y| \leq |\,x\,| - |\,y\,|.$$

V primeru $a = x + y$ in $b = -y$ pa dobimo na analogen način

$$|\,x\,| - |\,y\,| \leq |x+y|.$$

Sledi $||\,x\,| - |\,y\,|| \leq |x+y|$. □

Kompleksna števila

Videli smo že, da znamo v obsegu realnih števil reševati enačbe tipa $x^2 = a$, kjer je a pozitivno število. Vendar pa v realnih številih ni rešljiva že tako preprosta enačba, kot je

$$x^2 + 1 = 0.$$

Da bi znali rešiti to enačbo, moramo dodati realnim številom še rešitvi te enačbe, ki ju imenujemo $\pm i$. Tako pridemo do obsega kompleksnih števil. Osnovni izrek algebre (ki presega okvir tega predmeta) pravi, da znamo v obsegu kompleksnih števil rešiti poljubno polinomsko enačbo. To pomeni, da se tu, vsaj s stališča potrebe po reševanju enačb, naša pot konstruiranja različnih tipov števil ustavi. Seveda pa to ne pomeni, da ne obstajajo še kakšni drugi tipi objektov, ki imajo podobne lastnosti kot števila.

Obseg kompleksnih števil definiramo na naslednji način. Kot množica je

$$\mathbb{C} = \mathbb{R} \times \mathbb{R} = \{(a, b) \mid a, b \in \mathbb{R}\}.$$

Na njej definiramo operaciji

$$\begin{aligned} (a, b) + (a', b') &= (a + a', b + b'), \\ (a, b) \cdot (a', b') &= (aa' - bb', ab' + ba'). \end{aligned}$$

Poleg tega označimo še

$$\begin{aligned} 0 &= (0, 0), \\ 1 &= (1, 0), \\ -(a, b) &= (-a, -b), \\ (a, b)^{-1} &= \Big(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2}\Big). \end{aligned}$$

Rutinsko se da preveriti, da tako definirani operaciji zadoščata prvim desetim aksiomom, ki smo jih našteli v razdelku o realnih številih.

Trditev 15. *Kompleksna števila tvorijo obseg.*

Od tod sledi, da imajo kompleksna števila vse lastnosti, ki smo jih dokazali v prejšnjih razdelkih za poljuben obseg. Velja pa opozoriti, da kompleksna števila ne zadoščajo preostalim trem aksiomom realnih števil.

Kompleksna števila običajno označujemo s črkama z in w. Nasprotno število števila z označimo z $-z$, obratno pa z $z^{-1} = \frac{1}{z}$. Posebno vlogo igra število

$$i = (0, 1).$$

Velja namreč $i^2 = -1 = (-1, 0)$, kar pomeni, da sta števili $\pm i$ rešitvi enačbe $z^2 + 1 = 0$ v obsegu kompleksnih števil.

Realna števila so v obsegu $\mathbb{C}$ predstavljena s podmnožico števil oblike

$$\{(a, 0) \mid a \in \mathbb{R}\} \subset \mathbb{C},$$

kjer realnemu številu a ustreza kompleksno število $(a, 0)$. Množenje in seštevanje na tej podmnožici

$$\begin{aligned} (a, 0) + (a', 0) &= (a + a', 0), \\ (a, 0) \cdot (a', 0) &= (aa', 0), \end{aligned}$$

se ujema z ustreznima operacijama na množici realnih števil. Ponavadi realna števila kar identificiramo z elementi množice $\{(a, 0) \mid a \in \mathbb{R}\}$ in pišemo

$$a = (a, 0) \text{ za } a \in \mathbb{R}.$$

Poljubno kompleksno število $z = (a, b)$ lahko potem zapišemo v obliki

$$z = (a, 0) + (0, 1) \cdot (b, 0) = a + ib.$$

To je zapis kompleksnih števil, ki ga bomo večinoma uporabljali zaradi enostavnosti. Primeren je tudi za računanje, če upoštevamo, da velja

$$i^2 = -1, \quad , i^3 = -i, \quad i^4 = 1.$$

Tako je npr.

$$(a + ib)(a' + ib') = aa' + iba' + aib' + i^2bb' = (aa' - bb') + i(ba' + ab'),$$

kar se ujema z definicijo množenja v obsegu kompleksnih števil.

Vzemimo sedaj poljubno kompleksno število $z = a + ib$. S predpisom

$$\overline{z} = a - ib$$

definiramo *konjugirano* število števila z. Preprosto je preveriti, da velja

$$\begin{aligned}
\overline{z + w} &= \overline{z} + \overline{w}, \\
\overline{z \cdot w} &= \overline{z} \cdot \overline{w}, \\
\overline{a} &= a \qquad\qquad \text{za } a \in \mathbb{R}, \\
\overline{i} &= -i.
\end{aligned}$$

Če je $z = a + ib$, velja $z \cdot \overline{z} = a^2 + b^2 \geq 0$, zato lahko definiramo *absolutno vrednost* števila z s predpisom

$$|\, z \,| = \sqrt{z \cdot \overline{z}} = \sqrt{a^2 + b^2} \geq 0.$$

Podobno kot pri realnih številih velja $|\, z \,| = 0$ natanko takrat, ko je $z = 0$. Kot smo videli, igrata realni števili a in b v zapisu $z = a + ib$ pomembno vlogo. Zato uporabljamo oznaki

$$\begin{aligned}
\mathrm{Re}(z) &= a, \qquad && \text{realna komponenta števila } z, \\
\mathrm{Im}(z) &= b, \qquad && \text{imaginarna komponenta števila } z.
\end{aligned}$$

S pomočjo konjugacije si lahko pomagamo tudi pri deljenju kompleksnih števil. Naj bosta z in w kompleksni števili in naj velja $w \neq 0$. Potem velja

$$\frac{z}{w} = \frac{z \cdot \overline{w}}{w \cdot \overline{w}} = \frac{z \cdot \overline{w}}{|\, w \,|^2}.$$

Ker pa je $|\, w \,|^2$ pozitivno realno število, z njim ni težko deliti. Če je torej $z \cdot \overline{w} = x + iy$, je

$$\frac{z}{w} = \frac{x}{|\, w \,|^2} + i \frac{y}{|\, w \,|^2}.$$

Zgled. Za kompleksno število $z = \frac{a+i}{a-i}$, kjer je $a \in \mathbb{R}$, izračunajmo njegovo realno in imaginarno komponento, konjugirano kompleksno število in pa absolutno vrednost.

Pišimo
$$z = \frac{a+i}{a-i} = \frac{(a+i)(a+i)}{(a-i)(a+i)} = \frac{a^2+2ai-1}{a^2+1}.$$
Od tod sledi
$$\mathrm{Re}(z) = \frac{a^2-1}{a^2+1},$$
$$\mathrm{Im}(z) = \frac{2a}{a^2+1}.$$
Poleg tega je
$$\overline{z} = \frac{a-i}{a+i}$$
in zato
$$z \cdot \overline{z} = \frac{a+i}{a-i}\frac{a-i}{a+i} = 1 \Longrightarrow |\,z\,| = 1.$$

Trditev 16. *Za poljubni kompleksni števili z in w veljajo:*

(1) $|z \cdot w| = |\,z\,||\,w\,|$,

(2) $|z + w| \leq |\,z\,| + |\,w\,|$,

(3) $||\,z\,| - |\,w\,|| \leq |z + w|$.

Dokaz. Za dokaz točke (1) si poglejmo enakosti
$$|z \cdot w|^2 = z \cdot w \cdot \overline{z \cdot w} = z \cdot w \cdot \overline{z} \cdot \overline{w} = |\,z\,|^2|\,w\,|^2 = (|\,z\,||\,w\,|)^2,$$
od koder sledi $|z \cdot w| = |\,z\,||\,w\,|$.

Pišimo sedaj $z = a + ib$ in $w = x + iy$. Potem velja
$$\begin{aligned}|z+w| = |(a+x)+i(b+y)| &= \sqrt{(a+x)^2+(b+y)^2},\\ &= \sqrt{a^2+2ax+x^2+b^2+2by+y^2},\\ &= \sqrt{|\,z\,|^2+|\,w\,|^2+2(ax+by)}.\end{aligned}$$
Poleg tega velja tudi
$$|ax+by| = \sqrt{(ax+by)^2} = \sqrt{(a^2+b^2)(x^2+y^2)-(ay-bx)^2},$$
kar nam da oceno
$$|ax+by| \leq \sqrt{(a^2+b^2)(x^2+y^2)} = |\,z\,||\,w\,|.$$
Torej je
$$-|\,z\,||\,w\,| \leq ax+by \leq |\,z\,||\,w\,|$$

in zato iz enakosti $|z+w| = \sqrt{|\,z\,|^2 + |\,w\,|^2 + 2(ax+by)}$ sledi

$$\sqrt{|\,z\,|^2 + |\,w\,|^2 - 2|\,z\,||\,w\,|} \leq |z+w| \leq \sqrt{|\,z\,|^2 + |\,w\,|^2 + 2|\,z\,||\,w\,|}.$$

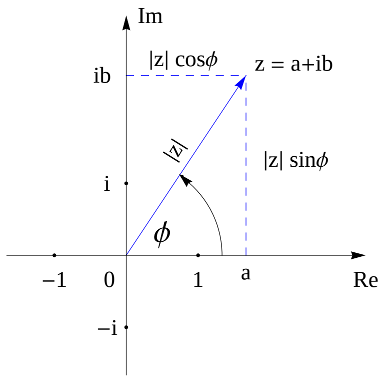
Tako smo prišli do neenakosti

$$||\,z\,| - |\,w\,|| \leq |z+w| \leq |\,z\,| + |\,w\,|,$$

ki dokažeta točki (2) in (3). $\square$

Geometrična upodobitev kompleksnih števil

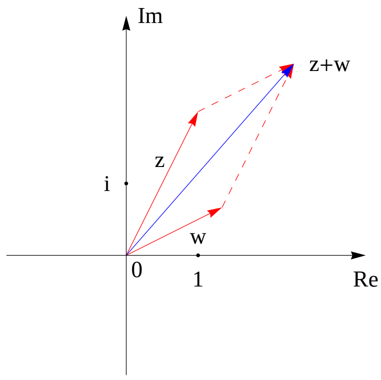
Geometrično si kompleksna števila predstavljamo s pomočjo kompleksne ravnine.



Kompleksno število z si predstavljamo kot vektor $(\mathrm{Re}(z), \mathrm{Im}(z))$ v ravnini. Absolutna vrednost $|\,z\,|$ nam predstavlja dolžino tega vektorja, argument

$$\arg(z) = \phi, \qquad \arg(z) \in [0, 2\pi)$$

kompleksnega števila z pa je kot med realno osjo in pa vektorjem, ki pripada številu z. Seštevanje kompleksnih števil pri tem ustreza seštevanju vektorjev.



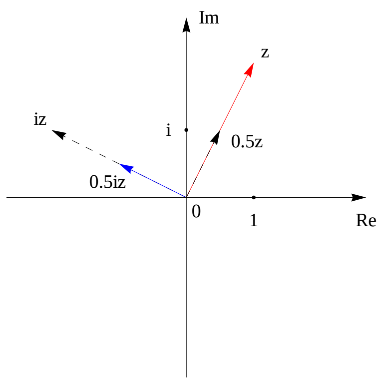
Pogosto nam pride prav tudi polarni zapis kompleksnega števila

$$z = |\, z\,|(\cos\phi + i\sin\phi).$$

Če pišemo $w = |\, w\,|(\cos\psi + i\sin\psi)$, namreč sledi

$$z{\cdot}w = |\, z\,||\, w\,|(\cos\phi{+}i\sin\phi)(\cos\psi{+}i\sin\psi) = |\, z\,||\, w\,|(\cos(\phi{+}\psi){+}i\sin(\phi{+}\psi))$$

Od tod lahko sedaj razberemo, kaj nam geometrično predstavlja množenje kompleksnih števil. Množiti dano število z s kompleksnim številom w pomeni hkrati skalirati vektor z za faktor $|\, w\,|$ in nato zavrteti za kot ψ okoli izhodišča. Če je w realno število, imamo torej množenje vektorja s skalarjem, če pa je $|\, w\,| = 1$, pa vrtenje vektorja za kot ψ. Na skici je prikazano množenje števila z s kompleksnim številom $0.5i$. Vidimo, da ustreza množenje s številom i ravno vrtenju za pravi kot okoli izhodišča.



De Moivrova formula in koreni enote

Poleg kartezičnega in polarnega zapisa kompleksnega števila nam pri računanju pride prav tudi Eulerjev zapis

$$z = |z|e^{i\phi},$$

kjer je $|z|$ absolutna vrednost, ϕ pa argument (polarni kot) števila z. Za nas bo Eulerjev zapis zaenkrat le pripomoček za računanje, kasneje pa bomo pokazali, da velja Eulerjeva formula

$$e^{i\phi} = \cos\phi + i\sin\phi.$$

Spomnimo se, da za množenje kompleksnih števil $z = |z|e^{i\phi}$ in $w = |w|e^{i\psi}$ velja

$$z \cdot w = |z||w|(\cos(\phi + \psi) + i\sin(\phi + \psi)).$$

Od tod lahko s pomočjo matematične indukcije izpeljemo, da za vsak $n \in \mathbb{N}$ velja

$$z^n = |z|^n(\cos n\phi + i\sin n\phi) = |z|^n e^{in\phi}.$$

Tej enakosti rečemo de Moivrova formula.

Zgled. Kot zgled uporabe de Moivrove formule si poglejmo, kako lahko računamo korene kompleksnih števil. Izberimo poljuben neničeln $w \in \mathbb{C}$ in si poglejmo enačbo

$$z^n = w$$

za nek $n \in \mathbb{N}$. Število w je torej fiksno, število z pa je neznanka. Najprej zapišimo obe števili v Eulerjevem zapisu: $z = |z|e^{i\phi}$ in $w = |w|e^{i\psi}$. Z uporabo de Moivrove formule se naša enačba prevede v enačbo

$$|z|^n e^{in\phi} = |w|e^{i\psi}.$$

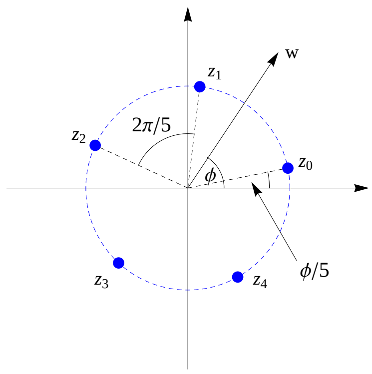
Ker sta dve kompleksni števili enaki, če imata enako dolžino in enak polarni kot, od tod sledi $|z|^n = |w|$ in $n\phi = \psi + 2k\pi$, oziroma

$$|z| = \sqrt[n]{|w|},$$
$$\phi = \frac{\psi}{n} + \frac{2k\pi}{n}.$$

Različne rešitve dobimo za $k \in \{0, 1, 2, \ldots, n-1\}$, zapišemo pa jih lahko v obliki

$$z_k = \sqrt[n]{|w|}e^{i\left(\frac{\psi}{n}+\frac{2k\pi}{n}\right)}, \qquad k \in \{0, 1, 2, \ldots, n-1\}.$$

Rešitve ležijo na krožnici s polmerom $\sqrt[n]{|w|}$ in tvorijo oglišča pravilnega n-kotnika. Poglejmo si primer $n = 5$.



Poseben, pomemben primer so koreni števila 1, ki jim rečemo koreni enote.

Kvadratne enačbe v kompleksnih številih

Za kvadratno enačbo $ax^2+bx+c = 0$ v realnih številih vemo, da ima natanko dve rešitvi, ki ju dobimo po formuli

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Če je diskriminanta $D = b^2 - 4ac$ negativna, enačba nima realnih rešitev. Na naslednjih primerih si bomo pogledali, kako se rešuje kvadratne enačbe v obsegu kompleksnih števil.

Zgled. (1) Rešimo najprej enačbo

$$z^2 = 2i$$

v kompleksnih številih. Pišimo $z = a + ib$. Potem se enačba $z^2 = 2i$ glasi

$$a^2 - b^2 + 2iab = 2i.$$

Od tod dobimo sistem dveh enačb v realnih številih

$$\begin{aligned} a^2 - b^2 &= 0, \\ 2ab &= 2. \end{aligned}$$

Iz druge enačbe sledi, da sta a in b neničelni števili in da je $b = \frac{1}{a}$. Če to vstavimo v prvo enačbo, dobimo enačbo $a^4 = 1$, ki ima rešitvi $a = \pm 1$. Potem pa je $b = \pm 1$ in zato sta rešitvi enačbe $z^2 = 2i$

$$z_{1,2} = \pm(1 + i).$$

(2) Malo bolj splošna je enačba

$$z^2 = u + iv,$$

kjer sta $u, v \in \mathbb{R}$. Z uporabo $z = a + ib$ pridemo do sistema enačb

$$\begin{aligned} a^2 - b^2 &= u, \\ 2ab &= v. \end{aligned}$$

Sedaj ločimo več možnosti.

Če je $v = 0$:

- $u = 0 \Longrightarrow z_{1,2} = 0$.
- $u > 0 \Longrightarrow a \neq 0$ in $b = 0$. Sledi $a = \pm\sqrt{u}$ in $z_{1,2} = \pm\sqrt{u} + i \cdot 0$.
- $u < 0 \Longrightarrow a = 0$ in $b \neq 0$. Sledi $b = \pm\sqrt{-u}$ in $z_{1,2} = 0 \pm i\sqrt{-u}$.

Naj bo sedaj $v \neq 0$. Potem iz druge enačbe sledi, da sta a in b neničelni števili in $b = \frac{v}{2a}$. Če to vstavimo v prvo enačbo, dobimo po preureditvi enačbo

$$4a^4 - 4a^2u - v^2 = 0.$$

Ob uvedbi nove spremenljivke $s = a^2 > 0$ pridemo do kvadratne enačbe

$$4s^2 - 4us - v^2 = 0$$

za spremenljivko s, katere rešitvi sta

$$s_{1,2} = \frac{4u \pm \sqrt{16u^2 + 16v^2}}{8} = \frac{u \pm \sqrt{u^2 + v^2}}{2}.$$

Ker pa je $\sqrt{u^2+v^2} > u$ in $s > 0$, je možna samo rešitev

$$s = \frac{u + \sqrt{u^2+v^2}}{2}.$$

Z upoštevanjem enakosti $a = \pm\sqrt{s}$ in $b = \frac{v}{2a}$, dobimo rešitev

$$z_{1,2} = \pm\Big(\frac{\sqrt{u+\sqrt{u^2+v^2}}}{\sqrt{2}} + i\frac{v}{\sqrt{2}\sqrt{u+\sqrt{u^2+v^2}}}\Big)$$

Vidimo torej, da ima enačba $z^2 = u + iv$ v kompleksnem vedno dve rešitvi (razen pri $u + iv = 0$), ki ju označimo z oznako $\pm\sqrt{u+iv}$. Za razliko od situacije pri realnih številih tukaj nimamo ene odlikovane rešitve; velja le, da sta rešitvi nasprotni si števili. Primer (1) bi torej lahko povzeli z enakostjo

$$\sqrt{2i} = \pm(1+i).$$

(3) Poglejmo si sedaj še splošno kvadratno enačbo

$$\alpha z^2 + \beta z + \gamma = 0,$$

kjer je $\alpha \neq 0$. Naredimo lahko podoben postopek kot v realnem primeru:

$$\begin{aligned} \alpha z^2 + \beta z + \gamma &= 0, \\ z^2 + 2\frac{\beta}{2\alpha}z + \frac{\gamma}{\alpha} &= 0, \\ \Big(z + \frac{\beta}{2\alpha}\Big)^2 + \frac{\gamma}{\alpha} - \frac{\beta^2}{4\alpha^2} &= 0, \\ \Big(z + \frac{\beta}{2\alpha}\Big)^2 &= \frac{\beta^2 - 4\alpha\gamma}{4\alpha^2}. \end{aligned}$$

Tako smo prišli do primera enačbe iz točke (2). Sledi

$$z + \frac{\beta}{2\alpha} = \pm\sqrt{\frac{\beta^2-4\alpha\gamma}{4\alpha^2}} = \pm\frac{\sqrt{\beta^2-4\alpha\gamma}}{2\alpha},$$

kar nam da

$$z_{1,2} = \frac{-\beta \pm \sqrt{\beta^2-4\alpha\gamma}}{2\alpha}.$$

Še enkrat opozorimo, da je tukaj mišljen kvadratni koren v kompleksnem, kot smo ga definirali v primeru (2).

Poglejmo si na hitro še neenačbe. Ker kompleksna števila niso urejena, direktno ne moremo študirati kompleksnih linearnih, kvadratnih in ostalih neenačb. Smisel imajo le neenačbe, kjer najprej kompleksno neznanko preslikamo v realna števila s kakšno funkcijo (kot so npr. absolutna vrednost ali realna oziroma imaginarna komponenta) in nato študiramo realno neenačbo.

Zgled. Opišimo množico rešitev neenačbe $|z-\lambda|<R$, kjer je $\lambda \in \mathbb{C}$.

Pišimo $z = x + iy$ in $\lambda = a + ib$. Potem je

$$|z-\lambda| = |(x-a)+i(y-b)| = \sqrt{(x-a)^2+(y-b)^2}.$$

Rešitve neenačbe $|z-\lambda|<R$ so torej točke (x,y) v kompleksni ravnini, za katere je

$$(x-a)^2+(y-b)^2<R^2.$$

To pa so točke, ki ležijo znotraj kroga s središčem v (a,b) in s polmerom R.