Poglavje 1

Množice in števila

1.1 Osnovni pojmi o množicah

1.1.1 Množice

Množica je zbirka objektov, ki jih imenujemo *elementi množice.* Če x pripada množici A pravimo, da je x element množice A, kar napišemo $x \in A$. Za objekt y, ki ne pripada množici A pravimo, da ni element množice A, kar napišemo $y \notin A$.

Množico lahko opredelimo tako, da naštejemo vse njene elemente, na primer:

$$A = \{1, 2, \sqrt{2}, 5, \pi\},$$

ali pa s pomočjo pravila, ki natanko določa elemente, ki ji pripadajo, na primer:

$$B = \{x;\ x \text{ je realno število, } x > 0\}.$$

Med množicami ima posebno mesto tista množica, ki nima nobenega elementa. Pravimo ji *prazna množica* in jo zapišemo s simbolom $\emptyset$. Tako je

$$\{x;\ 0 \cdot x = 1\} = \emptyset.$$

Množici A in B sta enaki natanko takrat, kadar imata iste elemente, kar zapišemo $A = B$. Na primer, množica vseh realnih števil je enaka množici

$$A = \{x;\ x \text{ je realno število, } 0 \cdot x = 0\}.$$

Kadar za dve množici A in B velja, da je vsak element množice A tudi element množice B pravimo, da je A *podmnožica* množice B, kar zapišemo $A \subseteq B$. Za vsako množico A veljata relaciji $A \subseteq A$ in $\emptyset \subseteq A$.

Kadar je $A = B$, veljata relaciji $A \subseteq B$ in $B \subseteq A$. Če je $A \subseteq B$ in $A \neq B$ pravimo, da je množica A *prava* podmnožica množice B in to zapišemo $A \subset B$.

Z množicami lahko tudi računamo. Naštejmo osnovne operacije nad množicami, ki jih bomo uporabljali v nadaljevanju:

> *Unija* $A \cup B$ je množica, ki vsebuje vse elemente, ki so v množici A ali v množici B
> $$A \cup B = \{x;\ x \in A \text{ ali } x \in B\}.$$
>
> *Presek* $A \cap B$ je množica, ki vsebuje vse elemente, ki so v obeh množicah, v A in v B.
> $$A \cap B = \{x;\ x \in A \text{ in } x \in B\}.$$
>
> Če je $A \cap B = \emptyset$, pravimo, da sta množici A in B *disjunktni.*
>
> *Razlika* $A \setminus B$ dveh množic je množica, ki vsebuje vse elemente množice A, ki niso elementi množice B.
> $$A \setminus B = \{x;\ x \in A \text{ in } x \notin B\}.$$
>
> Razliki $A \setminus B$ pravimo tudi *komplement* množice B glede na množico A.
>
> O *komplementu* $\bar{A}$ govorimo takrat, kadar so vse množice, ki nas zanimajo, podmnožice neke vnaprej določene *univerzalne množice* U. Komplement $\bar{A}$ je v tem primeru razlika $U \setminus A$.
>
> *Premi (kartezični) produkt* $A \times B$ je množica, katere elementi so urejeni pari (x, y), kjer je prvi element v paru iz množice A, drugi pa iz množice B
> $$A \times B = \{(x, y) : x \in A \text{ in } y \in B\}.$$

Primer 1.1.1. Dokažimo *de Morganova zakona*[1] :

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

[1] Augustus de Morgan (1806–1871), angleški matematik. Ukvarjal se je predvsem z matematično logiko.

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Za poljuben objekt a velja

$$\begin{aligned} a \in A \cap (B \cup C) &\iff a \in A \text{ in } a \in B \cup C \\ &\iff a \in A \text{ in } (a \in B \text{ ali } a \in C) \\ &\iff (a \in A \text{ in } a \in B) \text{ ali } (a \in A \text{ in } a \in C) \\ &\iff a \in A \cap B \text{ ali } a \in A \cap C \\ &\iff a \in (A \cap B) \cup (A \cap C). \end{aligned}$$

Dokaz druge enakosti je podoben in ga prepuščamo bralcu. ■

Pri matematiki pogosto srečujemo množice, katerih elementi so števila. V glavnem bomo srečevali naslednje številske množice in njihove oznake:

Naravna števila	$\mathbb{N}$
Cela števila	$\mathbb{Z}$
Racionalna števila	$\mathbb{Q}$
Realna števila	$\mathbb{R}$
Kompleksna števila	$\mathbb{C}$.

1.1.2 Preslikave

Dani naj bosta množici A in B.

Definicija 1.1.1. *Preslikava* množice A v množico B ali *upodobitev* množice A v množici B je pravilo, ki vsakemu elementu $a \in A$ priredi točno določen element v množici B. Preslikave običajno označujemo z malimi latinskimi ali grškimi črkami, npr.:

$$f : A \to B.$$

Element množice B, ki ga preslikava f priredi elementu $a \in A$, je *slika* elementa a in ga zapišemo kot $f(a)$. Množico A imenujemo *definicijsko območje* preslikave f, množico

$$f(A) = \{f(a), a \in A\} \subseteq B$$

pa njeno *zaloga vrednosti*.

Primer 1.1.2. Navedimo nekaj preslikav:

1. Preslikavi $f : A \to B$, ki vsem elementom $a \in A$ priredi isti element $b \in B$ pravimo *konstantna preslikava.* Zaloga vrednosti konstantne preslikave je točka $\{b\} \subset B$.

2. Preslikava $f : \mathbb{N} \to \mathbb{N}$, ki vsakemu naravnemu številu n priredi število $f(n) = 2n$, ima za zalogo vrednosti vsa soda naravna števila.

3. Pogosto bomo imeli opravka s preslikavo $f : \mathbb{R} \to \mathbb{Z}$, ki številu a priredi največje celo število, ki ni večje od a. Sliki $f(a)$ pravimo *celi del* števila a in jo običajno označujemo z $f(a) = \lfloor a \rfloor$. ■

Slika 1.1: Preslikava množice A v množico B

Če se zgodi, da je $A = B$, je $f(a) \in A$. Množico A smo tako upodobili vase. Med upodobitvami množice A vase zasluži posebno mesto *identična* upodobitev $id : A \to A$, ki vsak element množice A preslika nase: $\mathrm{id}(a) = a$.

Preslikava $f : A \to B$ je *injektivna*, če sta sliki različnih elementov vedno različna elementa

$$a \neq b \Longrightarrow f(a) \neq f(b).$$

Za injektivne preslikave velja, da je vsak $b \in B$ slika največ enega elementa $a \in A$. Preslikava $f : A \to B$ je *surjektivna*, kadar je njena zaloga vrednosti enaka celi množici B, torej $f(A) = B$. Za surjektivne preslikave velja, da je vsak element množice B slika vsaj enega elementa iz množice A.

Naj bo upodobitev $f : A \to B$ surjektivna in injektivna. V tem primeru je vsak element iz množice B slika natančno enega elementa iz množice A. Tako upodobitev imenujemo *bijektivna* ali *povratno-enolična* preslikava.

Primer 1.1.3. Navedimo nekaj zgledov:

1. Druga preslikava iz primera 1.1.2, $f : \mathbb{N} \to \mathbb{N}$, $f(n) = 2n$, je očitno injektivna, saj je za $n_1 \neq n_2$ tudi $2n_1 \neq 2n_2$. Vendar pa ni surjektivna, ker liha števila niso v zalogi vrednosti.

Preslikava $f : \mathbb{R} \to \mathbb{R}$, ki je dana z istim predpisom, in ima za definicijsko območje vsa realna števila, je tako injektivna kot surjektivna, torej bijektivna.

2. Tretja preslikava iz primera 1.1.2, $f : \mathbb{R} \to \mathbb{Z}$, $f(a) = \lfloor a \rfloor$ je surjektivna, injektivna pa ne, saj je na primer
$$\lfloor 1 \rfloor = \left\lfloor \frac{4}{3} \right\rfloor .$$

3. Preslikava $f : \mathbb{Z} \to \mathbb{Z}$, dana s predpisom $f(z) = -z$ je injektivna in surjektivna, torej bijektivna. ■

Če sta A in B množici s končno mnogo elementi in $f : A \to B$ bijektivna preslikava med njima, pripada vsakemu elementu iz A natanko en element iz B in vsak element iz B je slika natanko enega elementa iz A, torej imeta obe množici isto število elementov. Številu elementov končne množice pravimo *moč* množice. Množici A in B imata torej v tem primeru isto moč. Moč neskončnih množic je teže definirati, vendar tudi v tem primeru velja, da imata dve množici isto moč (torej, ohlapno rečeno, isto število elementov), če obstaja bijektivna preslikava med njima.

Primer 1.1.4. Moč neskončne množice je včasih v nasprotju z intuitivno predstavo o številu elementov, ki smo se je navadili pri končnih množicah:

1. Preslikava $f : \mathbb{N} \to \{2n, n \in \mathbb{N}\}$ je bijektivna preslikava. Množica naravnih števil ima torej isto moč kot množica sodih naravnih števil.

2. Množici
$$A = \{x \in \mathbb{R};\ 0 \leq x \leq 1\} \quad \text{in} \quad B = \{x \in \mathbb{R};\ 0 \leq x \leq 10\}.$$
predstavljata daljici na številski premici — prva ima dolžino 1, druga pa dolžino 10. Preslikava $f : A \to B$, dana s predpisom $f(x) = 10x$, je očitno bijektivna preslikava, torej sta obe daljici (različnih dolžin) množici z isto močjo. Nasploh lahko poiščmo bijektivno preslikavo med poljubnima daljicama, torej so vse daljice množice z isto močjo.

3. Preslikava $f : (-\pi/2, \pi/2) \to \mathbb{R}$, dana s predpisom $f(x) = \operatorname{tg} x$, je bijektivna preslikava. Cela množica $\mathbb{R}$ ima torej isto moč kot jo imajo intervali. ■

Slika 1.2: Sestavljena upodobitev

Naj bo f upodobitev množice A v množico B in g upodobitev množice B v množico C. Tako lahko vsak $a \in A$ preslikamo najprej v $f(a) \in B$, tega pa v element $g(f(a)) \in C$. Enak učinek lahko dosežemo tudi z eno samo preslikavo, ki $a \in A$ preslika v $g(f(a)) \in C$ (glej sliko 1.2). Taki upodobitvi pravimo *sestavljena preslikava* ali *kompozitum* in jo označimo s simbolom $g \circ f$. Tako je $(g \circ f)(a) = g(f(a))$.

Primer 1.1.5. Navedimo dva zgleda za kompozitum:

1. Naj bo $f : \mathbb{N} \to \mathbb{N}$ preslikava iz primera 1.1.2, tj. $f(n) = 2n$. Potem je $(f \circ f)(n) = 4n$.

2. Naj bo $f : \mathbb{R} \to \mathbb{R}$ dana s predpisom $f(x) = 2x$ in $g : \mathbb{R} \to \mathbb{R}$ dana s predpisom $f(x) = x^2$. Potem sta preslikavi $f \circ g : \mathbb{R} \to \mathbb{R}$ in $g \circ f : \mathbb{R} \to \mathbb{R}$ določeni z

$$(f \circ g)(x) = 2(x^2) = 2x^2 \quad \text{in} \quad (g \circ f)(x) = (2x)^2 = 4x^2.$$

■

Če je preslikava $f : A \to B$ injektivna, je vsak element $b \in f(A)$ slika natanko enega elementa $a \in A$. Torej obstaja predpis, ki vsakemu elementu $b \in f(A)$ priredi natanko določen $a \in A$ — tisti a, za katerega je $f(a) = b$. Preslikavi iz $f(A) \subseteq B$ v A, ki smo jo s tem definirali, pravimo preslikavi f *inverzna* preslikava in jo zapišemo kot $f^{-1} : f(A) \to A$. Definicijsko območje preslikave f^{-1} je zaloga vrednosti $f(A)$ preslikave f, njena zaloga vrednosti je definicijsko območje A preslikave f. Če je f tudi surjektivna preslikava, je definicijsko območje preslikave f^{-1} cela množica B. Inverzno preslikavo lahko opišemo tudi takole:

Izrek 1.1.1. *Preslikava $g : f(A) \to A$ je preslikavi f inverzna, če velja:*

$$g \circ f = \mathrm{id} : A \to A \quad \textit{in} \quad f \circ g = \mathrm{id} : f(A) \to f(A)$$

Primer 1.1.6. Preslikava $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x$, je injektivna, njena inverzna preslikava $f^{-1} : \mathbb{R} \to \mathbb{R}$ pa je dana s predpisom $f^{-1}(x) = \frac{1}{2}x$.

Tudi preslikava $g : \mathbb{Z} \to \mathbb{Z}$, dana s predpisom $g(z) = -z$, ima inverzno preslikavo $g^{-1} : \mathbb{Z} \to \mathbb{Z}$, ki je dana s predpisom $g^{-1}(z) = -z$. V tem primeru je torej $g^{-1} = g$. ■

Pogosto bomo imeli opravka z *grafi* preslikav.

Definicija 1.1.2. *Graf preslikave* $f : A \to B$ je podmnožica kartezičnega produkta

$$\Gamma(f) = \{(a, f(a)); a \in A\} \subset A \times B.$$

Primer 1.1.7. Če je $f : \mathbb{R} \to \mathbb{R}$, je njen graf

$$\{(x, f(x));\ x \in \mathbb{R}\} \subset \mathbb{R} \times \mathbb{R} = \mathbb{R}^2.$$

Kartezični produkt $\mathbb{R}^2$ si lahko predstavljamo kot množico točk v ravnini, v kateri smo izbrali pravokotni koordinatni sistem, graf $\Gamma(f)$ pa je, če je funkcija f dovolj lepa, krivulja v $\mathbb{R}^2$.

Na primer, graf preslikave $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x$ je premica skozi izhodišče. ■

1.2 Realna števila

1.2.1 Opisi množice realnih števil

Realna števila si lahko predstavljamo vsaj na tri načine: kot abstraktne elemente neke množice, v kateri so definirane določene operacija (algebrajsko), kot točke na številski premici (geometrijsko) in kot neskončna decimalna števila.

Algebrajski opis realnih števil

Množica realnih števil $\mathbb{R}$ je *komutativen obseg.* To pomeni, da sta v $\mathbb{R}$ definirani dve binarni operaciji: *seštevanje* in *množenje*, ki imata naslednje lastnosti. Obe sta *komutativni*

$$a + b = b + a \quad \text{in} \quad a \cdot b = b \cdot a,$$

in *asociativni*

$$(a + b) + c = a + (b + c) \quad \text{in} \quad (a \cdot b) \cdot c = a \cdot (b \cdot c),$$

množenje pa je *distributivno* glede na seštevanje:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Dve realni števili imata posebno vlogo: število 0 je *nevtralni element za seštevanje* (ali ničla), torej je $a + 0 = a$ za vsak $a \in \mathbb{R}$, število 1 pa je *nevtralni element za množenje* (ali enota), za katero je $a \cdot 1 = a$ za vsak $a \in \mathbb{R}$. Vsako realno število ima svoje nasprotno število $-a$, za katero velja $a + (-a) = 0$, če je $a \neq 0$ ima tudi svoje inverzno število a^{-1}, za katero velja $a \cdot a^{-1} = 1$.

Vsoto $a + (-b) = a - b$ imenujemo *razlika* števil a in b, produkt $a \cdot b^{-1}$, kjer je $b \neq 0$ pa *kvocient* števil a in b. Tako smo pridobili še dve novi operaciji — *odštevanje* in *deljenje.*

Obseg $\mathbb{R}$ je *urejen.* Do ureditve realnih števil pridemo tako, da razdelimo realna števila na tri podmnožice — *pozitivna števila, negativna števila* in *število* 0, tako da velja: za vsako število $a \neq 0$ je natanko eno od števil a in $-a$ pozitivno, množica pozitivnih števil pa je zaprta za seštevanje in množenje, tj. če sta a in b pozitivni števili, sta $a + b$ in $a \cdot b$ pozitivni števili.

S pomočjo te delitve realna števila *uredimo*, tako da definiramo relacijo *manjši*: število a je manjše od števila b, kar zapišemo $a < b$ ali pa $b > a$, natanko takrat, kadar je $b - a$ pozitivno število.

Relacija $<$ ima nekaj lastnosti, ki jih pogosto uporabljamo pri računanju z neenačbami:

Izrek 1.2.1.

1. Zakon trihotomije: *Za vsak par realnih števil a, b velja natanko ena od treh možnosti: $a = b$, $a < b$ ali pa $a > b$.*

2. Zakon tranzitivnosti: *če je $a < b$ in $b < c$, je $a < c$.*

3. *Če je $a < b$, je $a + c < b + c$, kjer je c poljubno realno število.*

4. *Če je $a < b$ in $c > 0$, je $a \cdot c < b \cdot c$.*

5. *Če sta a in b pozitivni števili in je $a < b$, je $a^{-1} > b^{-1}$.*

Pozor! Četrta lastnost pravi, da lahko neenačbo množimo s pozitivnim številom. Če neenačbo množimo z negativnim številom se neenačaj obrne: če je $a < b$ in $c < 0$, je $ac > bc$.

Vsaki množici, ki ima vse doslej naštete lastnosti, pravimo *urejen komutativen obseg*.

Pogosto uporabljamo tudi relacijo *manjši ali enak*: število a je manjše ali enako številu b, kar zapišemo $a \leq b$ oziroma $b \geq a$, če je $a < b$ ali pa $a = b$.

Absolutna vrednost je preslikava iz $\mathbb{R}$ v množico nenegativnih realnih števil, ki je določena s predpisom:

$$|a| = \begin{cases} a & \text{če je} \quad a \geq 0 \\ -a & \text{če je} \quad a < 0. \end{cases}$$

Zapišimo nekaj lastnosti absolutne vrednosti:

$$||a| - |b|| \leq |a + b| \leq |a| + |b|, \tag{1.1}$$

$$|ab| = |a| \cdot |b|. \tag{1.2}$$

Neenakostima (1.1) pravimo *trikotniški pravili.* Vse tri zveze bomo dokazali v širšem okviru v poglavju o kompleksnih številih. S pomočjo absolutne vrednosti lahko merimo razdalje med realnimi števili: razdalja med številoma a in b je enaka $|a - b|$.

Številska premica

Geometrijsko lahko realna števila predstavimo kot točke na *številski premici*, kjer smo izbrali *izhodišče*, tj. točko, ki predstavlja število 0, in (običajno desno od nje) točko, ki predstavlja število 1. S tem smo določili *koordinatni sistem* na številski premici in enoto za merjenje dolžine. Vsakemu številu $a \in \mathbb{R}$ pripada natanko določena točka na številski premici: če je a pozitivno

$\sqrt{2}$

Slika 1.3: Število, katerega kvadrat je enak 2, na številski premici

število, mu pripada točka desno od 0, ki je od 0 oddaljena za $|a|$, če je a negativno, pa je ustrezna točka na levi, za $|a|$ oddaljena od 0.

Konstrukcija števila $\sqrt{2}$ na realni osi je prikazana na sliki 1.3.

Na številski premici se nazorno pokažejo nekatere relacije med števili. Na primer, število $-a$ je simetrično številu a glede na izhodišče 0. Relacija $b < a$ se odraža tako, da je b levo od a (slika 1.4). Vsoto števil a in b dobimo tako, da število a premaknemo po številski premici v smeri in za dolžino, ki ju določa b, tako kot kaže slika 1.5.

Množico vseh števil na daljici med dvema danima številoma $a < b$, imenujemo omejen *interval*. Interval je *odprt*, *zaprt* ali *polodprt*, glede na to, ali vsebuje svoja krajišča ali ne:

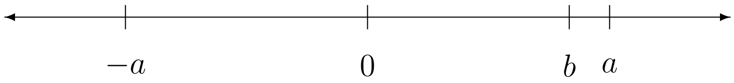
$$
\begin{array}{rcll}
(a,b) & = & \{x : a < x < b\} & \text{odprt interval} \\
[a,b] & = & \{x : a \leq x \leq b\} & \text{zaprt interval} \\
[a,b) & = & \{x : a \leq x < b\} & \text{polodprt interval} \\
(a,b] & = & \{x : a < x \leq b\} & \text{polodprt interval}
\end{array}
$$

Absolutna vrednost razlike $|a - b|$ je enaka *dolžini intervala*, (a,b), to je *razdalja* med številoma a in b na številski premici.

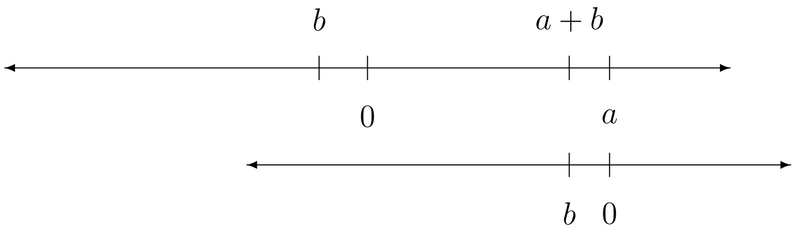
Naj bo ε majhno pozitivno število. Množica

$$\{x;\ |x - a| < \varepsilon\}$$

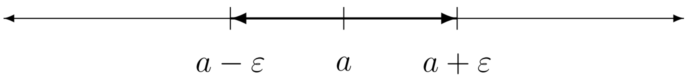
vsebuje natanko tista števila x, ki so od števila a oddaljena za manj kot ε. Pravimo ji *ε-okolica števila a* in jo lahko zapišemo tudi kot odprt interval dolžine 2ε s središčem v točki a, torej $(a - \varepsilon, a + \varepsilon)$ (slika 1.6).



Slika 1.4: Relacije med števili na številski premici



Slika 1.5: Seštevanje na številski premici



Slika 1.6: ε-okolica števila a

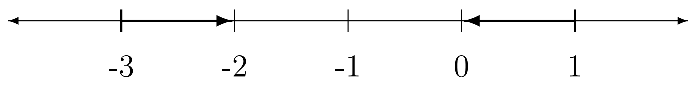
Poznamo tudi *neomejene intervale*, to so poltraki na številski premici ali pa cela številska premica:

$$\begin{array}{rcll}
(a,\infty) & = & \{x : a < x\} & \text{odprt navzgor neomejen interval} \\
[a,\infty) & = & \{x : a \leq x\} & \text{zaprt navzgor neomejen interval} \\
(-\infty,a) & = & \{x : x < a\} & \text{odprt navzdol neomejen interval} \\
(-\infty,a] & = & \{x : x \leq a\} & \text{zaprt navzdol neomejen interval} \\
(-\infty,\infty) & = & \mathbb{R} & \text{Vsa realna števila}
\end{array}$$

Pozor! Simbola ∞ ali $-\infty$ v zapisu neomejenih intervalov ne predstavljata realnih števil, temveč sta le znaka, ki nam povesta, da interval v tisto smer ni omejen.

Primer 1.2.1. Katera realna števila določa neenačba

$$1 < |x+1| \leq 2 \ ? \tag{1.3}$$



Slika 1.7: Rešitve neenačbe $1 < |x+1| \leq 2$

Če je $x+1 \geq 0$, neenačbo lahko prepišemo kar brez absolutne vrednosti

$$1 < x+1 \leq 2,$$

torej mora biti $0 < x \leq 1$.

Če pa je $x+1 < 0$, moramo izrazu pod absolutno vrednostjo spremeniti predznak

$$1 < -(x+1) \leq 2,$$

torej je $-3 \leq x < -2$.

Neenačba (1.3) torej določa unijo intervalov $[-3,-2) \cup (0,1]$. ■

Decimalna števila

Kadar računamo, zapišemo realna števila običajno v obliki decimalnih števil. Decimalni zapis pozitivnega realnega števila a izgleda takole:

$$a = n.d_1 d_2 d_3 \ldots,$$

kjer je n celo število in $d_1, d_2, \ldots \in \{0,1,2,\ldots 9\}$. Pozitivnemu realnemu številu a priredimo decimalno število takole: celi del $n = \lfloor a \rfloor$ je največje celo število, ki ni večje od a in ga določimo tako, da poltrak $[0,\infty)$ razdelimo na polodprte intervale dolžine 1, $[n, n+1)$, $n \in \mathbb{Z}$, in poiščemo tistega, ki vsebuje a. Interval $[n, n+1)$ potem razdelimo na polodprte intervale dolžine $\frac{1}{10}$ in določimo prvo decimalko d_1 tako, da je $a \in [n + \frac{d_1}{10}, n + \frac{d_1+1}{10})$. Ostale decimalke določimo podobno. Negativnemu številu a pripredimo decimalni zapis tako, da ga zapišemo v obliki $a = -|a| = -n.d_1 d_2 d_3 \ldots$, število 0 pa ima decimalni zapis $0.000\ldots$.

Opisani postopek ni edini možen in lahko se zgodi, da dve različni decimalni števili predstavljata isto realno število. Na primer: čtevilo $0.999\ldots$ lahko zapišemo kot *geometrijsko vrsto*

$$0.999\ldots = \frac{9}{10} + \frac{9}{100} + \frac{9}{1000} + \ldots,$$

katere vsota je enaka

$$\frac{9}{10}\frac{1}{1-1/10} = -\frac{9}{9} = 1,$$

zato je

$$0.99999\ldots = 1.00000\ldots\ .$$

Realna števila, zapisana v decimalni obliki je lahko primerjati po velikosti. Ne samo, da takoj vidimo, katero od dveh števil je večje, vidimo tudi, za koliko večje je. Velja namreč:

Če se decimalni števili a in b ujemata v celem delu in v prvih m decimalkah, je $|a-b| < 10^{-m}$.

Na primer, če števili

$$\frac{17}{20} \quad \text{in} \quad \frac{45}{53}$$

zapišemo v decimalni obliki

$$\frac{17}{20} = 0.85000 \quad \text{in} \quad \frac{45}{53} = 0.84905\ldots$$

je očitno da je prvo večje in to za manj kot 10^{-1} (celo za manj kot 10^{-3}).

Pri računanju uporabljamo (razen, če računamo z ulomki) le končna decimalna števila, ki jih dobimo tako, da neskončne decimalke *zaokrožimo* na določeno število decimalnih mest.

Realna števila smo zapisali v najbolj običajni obliki - v desetiškem številskem sistemu. Prav tako bi lahko uporabili kakšno drugo osnovo, na primer 2, 8, 16,. . . .

1.2.2 Številske podmnožice realnih števil

Naravna števila

Naj bo $1 \in \mathbb{R}$ enota za množenje. Vsote

$$1+1=2, 1+1+1=3, \ldots$$

imenujmo *naravna števila.* Množica naravnih števil

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$$

je tesno povezana s štetjem. Očitno je zaprta za seštevanje in množenje (vsota in produkt dveh naravnih števil sta spet naravni števili).

Tako kot $\mathbb{R}$, je tudi množica $\mathbb{N}$ urejena z relacijo $<$. Vsako naravno število n ima glede na relacijo $<$ v množici $\mathbb{N}$ svojega neposrednega naslednika — število $n+1$. V množici $\mathbb{R}$ o neposrednem nasledniku ne moremo govoriti.

Množica $\mathbb{N}$ ima še eno ključno lastnost, ki jo razlikuje od ostalih osnovnih številskih množic, pravimo pa ji

Princip popolne indukcije: *Vsaka podmnožica naravnih števil, ki vsebuje število 1 in je v njej hkrati s številom n tudi njegov naslednik $n+1$, vsebuje vsa naravna števila.*[2]

Princip popolne indukcije pogosto uporabljamo za dokazovanje trditev in izrekov. Vsak tak dokaz poteka v dveh fazah:

1. Najprej dokažemo, da trditev velja za naravno število 1.
2. Nato dokažemo, da iz veljavnosti trditve za naravno število n (*indukcijska predpostavka*) lahko sklepamo, da trditev velja tudi za naslednje naravno število $n+1$.

Primer 1.2.2. Dokažimo, da enačba

$$1+2+\cdots+n=\frac{n(n+1)}{2} \tag{1.4}$$

velja za vsa naravna števila n.

1. Za $n=1$ je veljavnost trditve očitna.
2. Predpostavimo, da enačba velja za neko naravno število k.

   Označimo $S_k=1+2+\cdots+k$ in izračunajmo S_{k+1}. Zaradi indukcijske predpostavke velja

   $$S_{k+1}=1+2+\cdots+k+(k+1)=S_k+(k+1)=\frac{k(k+1)}{2}+(k+1).$$

   Desno stran te enakosti spravimo na skupen imenovalec, pa že imamo

   $$S_{k+1}=\frac{(k+1)(k+2)}{2},$$

   kar pomeni, da enačba (1.4) velja tudi za $k+1$.

Enačba (1.4) torej velja za vsa naravna števila. ∎

[2] Princip popolne indukcije lahko uporabimo tudi za množice, ki jih lahko bijektivno preslikamo na $\mathbb{N}$, na primer $\{x\in\mathbb{Z};\ x>a\}$

Primer 1.2.3. Dokažimo, da so vsa števila oblike

$$f(n) = 10^n + 3 \cdot 4^{n+2} + 5; \quad n \in \{0\} \cup \mathbb{N}$$

deljiva z 9.

1. $f(0) = 1 + 3 \cdot 4^2 + 5 = 54 = 9 \cdot 6$.
2. Predpostavimo, da je število $f(k) = 10^k + 3 \cdot 4^{k+2} + 5$ za neko naravno število k deljivo z 9. Potem je

$$\begin{aligned} f(k+1) - f(k) &= 10^{k+1} + 3 \cdot 4^{k+3} + 5 - 10^k - 3 \cdot 4^{k+2} - 5 \\ &= 9(10^k + 4^{k+2}), \end{aligned}$$

   kar pomeni, da je razlika $f(k+1) - f(k)$ deljiva z 9, zaradi predpostavke pa mora biti tudi $f(k+1)$ deljivo z 9. ■

Cela števila

Množico celih števil dobimo tako, da naravnim številom dodamo vsa njihova nasprotna števila in število 0:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Množica celih števil je zaprta za seštevanje in množenje, pa tudi za odštevanje (kar za množico $\mathbb{N}$ ne velja). Vsaki množici, v kateri so definirane operacije seštevanje, množenje in odštevanje, z vsemi naštetimi lastnosti, pravimo *kolobar.*

Racionalna števila

Če množici $\mathbb{Z}$ dodamo še vse kvociente $a \cdot b^{-1}$, kjer sta $a \in \mathbb{Z}$ in $b \in \mathbb{N}$, dobimo množico racionalnih števil $\mathbb{Q}$. Vsako racionalno število lahko predstavimo kot *ulomek* m/n, kjer je *števec* m celo, *imenovalec* n pa naravno število. Dva različna ulomka m/n in p/q predstavljata isto racionalno število, če je $mq = np$. Ulomek p/q je *okrajšan*, če sta p in q tuji si števili.

Množica $\mathbb{Q}$ je zaprta za seštevanje, množenje in odštevanje, torej je kolobar. Poleg tega je zaprta tudi za deljenje z neničelnim številom, torej je, podobno kot $\mathbb{R}$, obseg. Za računanje v $\mathbb{Q}$ uporabljamo dobro znana pravila za računanje z ulomki.

Znano je, da obstajajo realna števila, ki niso racionalna (to so vedeli že starogrški matematiki). Pravimo jim *iracionalna števila.* Primer takega števila je $\sqrt{2}$, tj. dolžina diagonale kvadrata s stranico 1. Omenimo le, da je iracionalnih števil zelo veliko — celo mnogo več kot racionalnih (za dokaz glej [6, str.117]).

Trditev 1.2.2. *Število $\sqrt{2}$ ni racionalno.*

Dokaz: Če bi bilo $\sqrt{2}$ racionalno število, bi ga lahko zapisali kot

$$\sqrt{2} = \frac{m}{n},\ m, n \in \mathbb{Z},$$

kjer števili m in n nimata skupnih deliteljev. Potem je

$$m^2 = 2n^2,$$

torej je m^2 sodo število. Potem je tudi m sodo (saj imata m in m^2 iste prafaktorje), torej $m = 2k$ in

$$4k^2 = 2n^2.$$

Od tod sledi $n^2 = 2k^2$, torej je n sodo število, to pa je v nasprotju s predpostavko, da m in n nimata skupnih deliteljev. Tako smo na podlagi predpostavke, da je $\sqrt{2}$ racionalno število, zašli v protislovje, predpostavka da je $\sqrt{2}$ racionalno število je bila napačna. ∎

Sklep, ki smo ga opisali, imenujemo *dokaz s protislovjem.* Tak način dokazovanja v matematiki pogosto uporabljamo.

1.2.3 Omejene podmnožice realnih števil

Definicija 1.2.1. Množica $A \subset \mathbb{R}$ je *navzgor omejena*, če obstaja tako realno število M, da za vsak $a \in A$ velja $a \leq M$. Število M imenujemo *zgornja meja* množice A.

Množica A je *navzdol omejena*, če obstaja tako število m, da za vsak element $a \in A$ velja $a \geq m$. Število m je *spodnja meja* množice A.

Množica A je *omejena*, če obstaja tako število M, da je $|a| \leq M$ za vsak $a \in A$, tj. če je navzgor in navzdol omejena.

Primer 1.2.4. Interval (a, ∞) je navzdol omejena množica s spodnjo mejo a, navzgor pa ni omejena. Interval $(-\infty, b]$ je navzgor omejena množica z zgornjo mejo b, navzdol pa ni omejena. Nazadnje, interval $[a, b]$ je primer omejene množice. ■

Navzgor omejena množica še zdaleč nima ene same zgornje meje – če je M njena zgornja meja in $N > M$, je očitno tudi N njena zgornja meja. Podobno velja tudi za spodnjo mejo.

Definicija 1.2.2. Naj bo $A \subset \mathbb{R}$ navzgor omejena in $B \subset \mathbb{R}$ navzdol omejena neprazna množica. Število M je *natančna zgornja meja* ali *supremum* množice A, če je najmanjša med vsemi njenimi zgornjimi mejami, kar zapišemo $M = \sup A$. Podobno je m *natančna spodnja meja* ali *infimum* množice B največja med vsemi njenimi spodnjimi mejami, kar zapišemo kot $m = \inf B$.

Če od števila $M = \sup A$ odštejemo še tako majhen ε, dobljena razlika $M - \varepsilon$ ni več zgornja meja množice A. Zato lahko natančno zgornjo (in podobno tudi natančno spodnjo) mejo množice opišemo tudi takole:

Trditev 1.2.3. *$M = \sup A$ natanko takrat, kadar je $a \leq M$ za vsak $a \in A$ in za vsak $\varepsilon > 0$ obstaja tak element $a \in A$, da je $a > M - \varepsilon$.*

Podobno je $m = \inf B$, če je $m \leq b$ za vsak $b \in B$ in za vsak $\varepsilon > 0$ obstaja tak element $b \in B$, da je $m + \varepsilon > b$.

Za intervale velja:

$$\sup(a, b) = b \quad \text{in} \quad \inf(a, b) = a,$$

pa tudi

$$\sup[a, b] = b \quad \text{in} \quad \inf[a, b] = a.$$

Za splošne navzgor omejene podmnožice realnih števil pa še zdaleč ni tako očitno, da imajo tudi natančno zgornjo mejo. Ena od ključnih lastnosti realnih števil je:

1.2.4. Dedekindov[3] aksiom ali lastnost kontinuuma. *Vsaka neprazna navzgor omejena množica realnih števil ima natančno zgornjo mejo. Podobno ima vsaka neprazna navzdol omejena podmnožica $\mathbb{R}$ natančno spodnjo mejo.*

[3]Julius Richard Wilhelm Dedekind (1831–1916), nemški matematik. Ukvarjal se je z algebro in s teorijo števil.

Lastnost kontinuuma je tista ključna lastnost, ki loči obseg realnih števil od obsega racionalnih števil. Množica racionalnih števil $\mathbb{Q}$, ki je prav tako kot $\mathbb{R}$ urejen obseg, te lastnosti nima. Na primer, množica

$$A = \{x \in \mathbb{Q}; x^2 < 2\}$$

je neprazna in navzgor omejena, vendar v obsegu $\mathbb{Q}$ nima natančne zgornje meje. Njena natančna zgornja meja v obsegu $\mathbb{R}$ seveda obstaja in je enaka $\sqrt{2}$, to pa, kot smo se prepričali, ni racionalno število.

Kar nekaj pomembnih lastnosti realnih števil, ki jih pri računanju in sklepanju pogosto uporabljamo, temelji na lastnosti kontinuuma. Na primer:

Izrek 1.2.5. *[Arhimedova lastnost] Če sta x in y poljubni realni števili in je $y > 0$, obstaja tak $n \in \mathbb{N}$, da je $x < ny$.*

Dokaz. Recimo, da je $x \geq ny$ za vsak $n \in \mathbb{N}$. To pomeni, da je x zgornja meja množice

$$A = \{ny;\ n \in \mathbb{N}\}.$$

Ker je to omejena množica, mora imeti svojo najmanjšo zgornjo mejo $M = \sup A$, torej število $M - y$ ni več zgornja meja množice A, saj je $y > 0$. To pomeni, da obstaja tak $n \in \mathbb{N}$, da je $ny > M - y$. Vendar pa je potem $(n+1)y > M$. Ker je $(n+1)y \in A$, je to v nasprotju s predpostavko, da je M natančna zgornja meja množice A. □

Če v zgornjem izreku vzamemo $y = 1$, sledi, da je množica $\mathbb{N}$ navzgor neomejena. Če pa v izreku vzamemo $x = 1$, pa sledi, da za vsako pozitivno število y obstaja tak n, da je ulomek $1/n$ manjši od y. Drugače povedano, v poljubno majhni okolici (y-okolici) števila 0 je vsaj eno racionalno število $1/n$.

Arhimedova lastnost ima še eno posledico, ki pa je pomembna čisto s praktičnega stališča:

Trditev 1.2.6. *Vsako realno število a ima v vsaki svoji ε-okolici vsaj eno racionalno število p/q. Drugače povedano, vsako realno število lahko poljubno natančno aproksimiramo z racionalnim številom. Pravimo tudi, da so racionalna števila povsod gosta v množici realnih števil.*

Dokaz. Za število $a = 0$ smo trditev dokazali že zgoraj. Recimo, da je $a > 0$. Potem obstaja tak $q \in \mathbb{N}$, da je $\varepsilon > 1/q$. Po drugi strani, ker je množica $\mathbb{N}$ neomejena, obstaja tak $p \in \mathbb{N}$, da je $p - 1 \leq qa$ in $p > qa$, torej je

$$\frac{p-1}{q} \leq a < \frac{p}{q}$$

in

$$\left|a - \frac{p}{q}\right| \leq \left|\frac{p-1}{q} - \frac{p}{q}\right| = \frac{1}{q} < \varepsilon.$$

Če pa je $a < 0$, lahko najdemo racionalno število p/q v ε-okolici števila $-a$, torej je $-p/q$ v ε-okolici števila a. $\square$

Dobro se je zavedati pomena te zadnje trditve. Pri računanju namreč uporabljamo izključno racionalna števila — iracionalna števila so za nas zgolj idealni objekti, za katere vemo, da obstajajo, vendar njihove natančne vrednosti ne moremo doseči. Vendar se jim lahko, zaradi Arhimedove lastnosti realnih števil, poljubno natančno približamo.

1.2.4 Potence in koreni

Naj bo a realno število. Spomnimo se definicije potence a^n, $n \in \mathbb{N}$:

$$a^1 = a,\ a^2 = a \cdot a,\ \ldots,\ a^n = a^{n-1} \cdot a,\ \ldots$$

Če je $a \neq 0$ lahko definiramo tudi potence $a^0 = 1$ in $a^{-n} = 1/a^n$, torej je za števila $a \neq 0$ definirana potenca a^n za vsak $n \in \mathbb{Z}$.

Trditev 1.2.7. *Za vsak $n \in \mathbb{N}$ velja: če je $0 < a < b$, je tudi*

$$0 < a^n < b^n.$$

Dokaz. Trditev najlaže dokažemo z indukcijo. Za $n = 1$ nimamo kaj dokazovati, ker je po predpostavki $0 < a^1 < b^1$. Recimo, da je $0 < a^{n-1} < b^{n-1}$. Če ti dve neenačbi pomnožimo z $a > 0$, dobimo

$$0 < a^n < b^{n-1}a.$$

Po drugi strani, če neenačbo $a < b$ pomnožimo z b^{n-1}, dobimo $ab^{n-1} < b^n$, torej zaradi tranzitivnosti relacije $<$ sledi

$$0 < a^n < b^{n-1}a < b^n$$

in trditev je dokazana. $\square$

Navedimo brez dokaza znano formulo za potenciranje binoma, ki jo bomo večkrat uporabili:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k.$$

Koeficienti

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n\cdot(n-1)\cdots(n-k+1)}{1\cdot\ \ 2\ \ \cdots\ \ \ k}$$

so *binomski simboli.*

Za negativne eksponente velja ravno obratna relacija kot za pozitivne: če je $0 < a < b$, je $0 < b^{-n} < a^{-n}$.

Naj bo $n \in \mathbb{Z}$. Če je $a > 0$ je tudi $a^n > 0$ za vsak $n \in \mathbb{Z}$. Za $a < 0$, pa je predznak potence a^n odvisen od eksponenta: za sode eksponente $n = 2k$ je $a^n > 0$, za lihe eksponente $n = 2k+1$ pa je $a^n < 0$.

Na sliki 1.3 smo konstruirali na številski premici število $\sqrt{2}$, za katero velja $(\sqrt{2})^2 = 2$. Velja pa še dosti več:

Izrek 1.2.8. *Za vsak $y \geq 0$ in vsak $n \in \mathbb{N}$ obstaja tako natanko določeno število $x \geq 0$, da je $x^n = y$.*

Dokaz. Oglejmo si množico $A = \{a \in \mathbb{R}; a^n \leq y\}$. Očitno je $0 \in A$, torej je A neprazna množica. Če je $0 \leq y \leq 1$, je 1 zgornja meja za množico A, kajti za vsako število $b > 1$, je tudi $b^n > 1 \geq y$, torej $b \notin A$. Če je $y > 1$, pa je y zgornja meja za množico A, kajti za vsak $b > y$ velja $b^n > y^n \geq y$, torej $b \notin A$.

Množica $A \subset \mathbb{R}$ je torej neprazna in navzgor omejena in ima svojo natančno zgornjo mejo $x = \sup A$, to pa je ravno število, ki ga iščemo. Pokažimo (brez podrobnosti), da je $x^n = y$.

Recimo, da bi bilo $x^n < y$ in $z = x + h$, kjer je $0 < h < 1$. Potem bi veljalo

$$\begin{aligned} z^n = (x+h)^n &= \sum_{k=0}^{n} \binom{n}{k} x^{n-k} h^k \\ &= x^n + h \sum_{k=1}^{n} \binom{n}{k} x^{n-k} h^{k-1} \\ &< x^n + h \sum_{k=1}^{n} \binom{n}{k} x^{n-k} \\ &= x^n + h((x+1)^n - x^n). \end{aligned}$$

Če izberemo

$$h < \frac{y - x^n}{(x+1)^n - x^n},$$

dobimo

$$z^n < x^n + \frac{y - x^n}{(x+1)^n - x^n} \cdot ((x+1)^n - x^n) = y,$$

torej $z > x$ in $z \in A$. To pa je v protislovju s tem, da je $x = \sup A$.

Če pa bi bilo $x^n > y$, bi na podoben način pokazali, da je število $u = x - k$, kjer je

$$0 < k < 1, \quad k < x \quad \text{in} \quad k < \frac{x^n - y}{(x+1)^n - x^n},$$

zgornja meja množice A in $u < x$, kar spet ni mogoče, ker je x najmanjša zgornja meja za A. Veljati mora torej $x^n = y$. $\square$

Izrek, ki smo ga dokazali, omogoča, da za pozitivna realna števila definiramo tudi potence z racionalnimi eksponenti:

Definicija 1.2.3. Če je $y \geq 0$, imenujemo število x, ki zadošča enačbi $x^n = y$, *n-ti koren števila* y, kar zapišemo $x = \sqrt[n]{y}$.

Če je $y \geq 0$, in p/q; $q \in \mathbb{N}$, $p \in \mathbb{Z}$ poljubno racionalno število, definiramo:

$$y^{p/q} = (\sqrt[q]{y})^p.$$

Če je $n = 2k$ sodo število, je $x^n > 0$ za vsak $x \neq 0$. Enačba $x^n = y$ v tem primeru nima rešitve, če je $y < 0$, torej koren $\sqrt[n]{y}$ za $y < 0$ ne obstaja. Če je $n = 2k + 1$ liho število, pa za $x < 0$ velja $x^n = -(-x)^n < 0$. V tem primeru lahko razširimo definicijo korena še na negativna števila: za $y < 0$ je $\sqrt[n]{y} = -\sqrt[n]{-y}$.

Za računanje s potencami veljata dobro znani pravili (ki jih ne bomo dokazovali):

$$a^{n+m} = a^n \cdot a^m \quad \text{in} \quad (a^n)^m = a^{(nm)}.$$

1.3 Kompleksna števila

Za vsak $a \in \mathbb{R}$ je $a^2 \geq 0$. To pomeni, da v okviru realnih števil enačba $x^2 = -1$ ni rešljiva. Enačbam oblike

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0$$

pravimo *algebraične enačbe* naš primer kaže, da take enačbe v obsegu $\mathbb{R}$ nimajo vedno rešitev.

Množica kompleksnih števil je razširitev množice realnih števil z rešitvami algebraičnih enačb. Vsebuje tako vsa realna števila, kot tudi vse rešitve algebraičnih enačb (z realnimi, pa tudi s kompleksnimi koeficienti).

Definicija 1.3.1. *Kompleksno število* α je urejen par realnih števil (a, b); prvo, $a = \operatorname{Re} \alpha$, imenujemo *realna komponenta*, drugo, $b = \operatorname{Im} \alpha$, *imaginarna komponenta*. Množico vseh kompleksnih števil označimo s simbolom $\mathbb{C}$.

Dve kompleksni števili sta enaki, kadar imata enaki realni in enaki imaginarni komponenti.

Vsoto in produkt kompleksnih števil definiramo s predpisoma

$$(a, b) + (c, d) = (a + c, b + d), \tag{1.5}$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc). \tag{1.6}$$

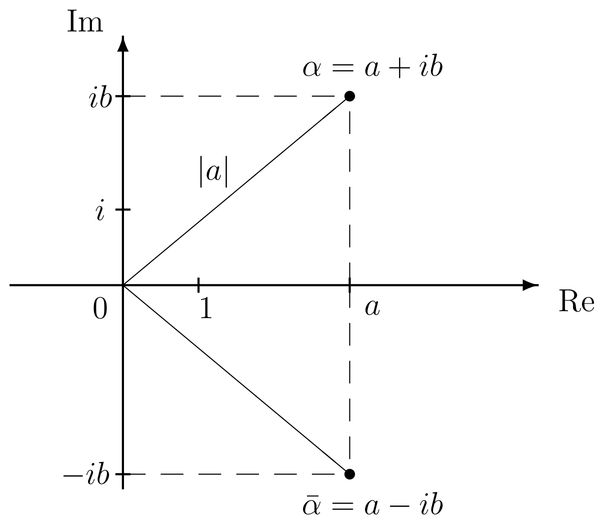
Izrek 1.3.1. *Množica $\mathbb{C}$ z operacijama (1.5) in (1.6) je obseg.*

Za dokaz tega izreka bi bilo potrebno preveriti, da velja komutativnost in asociativnost vsote in produkta in distributivnost produkta glede na seštevanje, da je število $(0,0)$ ničla za seštevanje in število $(1,0)$ enota za množenje. Za vsak $\alpha = (a,b)$ je število $-\alpha = (-a,-b)$ njegovo nasprotno število, če je $\alpha \neq (0,0)$ pa je

$$\alpha^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \right)$$

njegovo inverzno število. Vse te preproste izračune prepuščamo bralcu.

Kompleksna števila lahko upodobimo s točkami ravnine. V ravnini narišemo pravokotni koordinatni sistem. Na abscisno os, ki ji v tem primeru pravimo *realna os*, nanesemo realno komponento kompleksnega števila, na ordinatno os, ki ji pravimo *imaginarna os*, pa imaginarno komponento.



Slika 1.8: Kompleksna ravnina

Množica kompleksnih števil, ki ležijo na realni osi, tj. števil oblike $(a,0)$, ima vse lastnosti realnih števil, saj je zaprta za seštevanje in množenje, vsebuje tako ničlo $(0,0)$ kot enoto $(1,0)$, pa tudi obratno in inverzno število vsakega svojega števila (razen števila $(0,0)$). Kompleksno število $\alpha = (a,0)$ imamo lahko za zastopnika realnega števila a v množici $\mathbb{C}$, zato ga običajno pišemo kar a.

Kompleksnemu številu oblike $(0, b)$ na imaginarni osi pravimo *čisto imaginarno število.* Kvadrat čisto imaginarnega števila

$$(0, b) \cdot (0, b) = (-b^2, 0) = -b^2$$

je negativno realno število. Imaginarno število $(0, 1)$, katerega kvadrat je enak -1, imenujemo *imaginarna enota* in ga zaznamujemo z i. (V elektrotehniki se pogosto uporablja oznaka j.)

Vsako kompleksno število se da zapisati kot

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

Računski pravili (1.5) in (1.6) lahko zdaj zapišemo v bolj domači obliki:

$$\begin{aligned} (a + ib) + (c + id) &= (a + c) + i(b + d) \\ (a + ib) \cdot (c + id) &= (ac - bd) + i(ad + bc). \end{aligned}$$

Poleg seštevanja in množenja poznamo v množici $\mathbb{C}$ še eno enočleno operacijo, ki jo imenujemo *konjugiranje*.

Definicija 1.3.2. Številu $\alpha = a + bi$ *konjugirano število* je $\bar{\alpha} = a - ib$.

Število $\bar{\alpha}$ je simetrično številu α glede na realno os (slika 1.8). Naštejmo nekaj lastnosti konjugiranja. Dokazi so povsem preprosti, zato jih prepuščamo bralcu.

1. Konjugiranost števil je vzajemna: $\bar{\bar{\alpha}} = \alpha$
2. $\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}$
3. $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$
4. $\overline{(\alpha^{-1})} = (\bar{\alpha})^{-1}$

Število α je realno natanko takrat, kadar je $\bar{\alpha} = \alpha$ in imaginarno natanko takrat, kadar je $\bar{\alpha} = -\alpha$.

Za poljubno kompleksno število α je $\alpha + \bar{\alpha} = 2\,\mathrm{Re}(\alpha) \in \mathbb{R}$ realno in $(\alpha - \bar{\alpha}) = 2i\,\mathrm{Im}(\alpha)$ čisto imaginarno število. Število $\alpha\bar{\alpha} = a^2 + b^2$ je nenegativno realno število, ki je enako 0 samo, če je $\alpha = 0$, torej za vsak $\alpha \in \mathbb{C}$ obstaja kvadratni koren $\sqrt{\alpha\bar{\alpha}}$.

Definicija 1.3.3. *Absolutna vrednost* kompleksnega števila α je kvadratni koren števila $\alpha\bar{\alpha}$

$$|\alpha| = \sqrt{\alpha\bar{\alpha}} = \sqrt{a^2 + b^2}.$$

Absolutna vrednost ali *modul* kompleksnega števila α je dolžina daljice, ki povezuje koordinatno izhodišče s kompleksnim številom α.

Če je $a \in \mathbb{R}$, se ta definicija ujema z že znano definicijo absolutne vrednosti realnega števila. Podobno kot pri realnih številih velja

$$|\alpha\beta| = |\alpha| \cdot |\beta|. \tag{1.7}$$

$$||\alpha| - |\beta|| \leq |\alpha + \beta| \leq |\alpha| + |\beta| \tag{1.8}$$

Dokaz enakosti (1.7) je preprost:

$$|\alpha \cdot \beta|^2 = (\alpha \cdot \beta)(\overline{\alpha \cdot \beta}) = (\alpha\bar{\alpha}) \cdot (\beta\bar{\beta}) = |\alpha|^2 \cdot |\beta|^2,$$

torej je

$$|\alpha \cdot \beta| = |\alpha| \cdot |\beta|.$$

Dokažimo še *trikotniški pravili* (1.8):

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

Ker je

$$(\alpha \cdot \bar{\beta} + \beta \cdot \bar{\alpha}) = \alpha\bar{\beta} + \overline{\alpha\bar{\beta}} = 2\,\mathrm{Re}(\alpha\bar{\beta}) \leq 2|\alpha| \cdot |\beta|$$

in

$$\mathrm{Re}(\alpha\bar{\beta}) \leq |\alpha\bar{\beta}| = |\alpha| \cdot |\beta|,$$

je

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

in prvo trikotniško pravilo je dokazano.

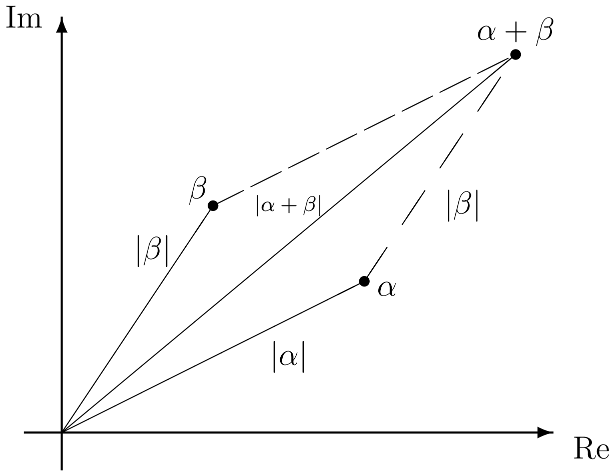
Drugo trikotniško pravilo je posledica prvega:

$$|\alpha| = |(\alpha + \beta) - \beta| \leq |\alpha + \beta| + |-\beta| = |\alpha + \beta| + |\beta|,$$

zato je $|\alpha| - |\beta| \leq |\alpha + \beta|$. Prav tako pokažemo, da je $|\beta| - |\alpha| \leq |\alpha + \beta|$, torej mora biti tudi $||\alpha| - |\beta|| \leq |\alpha + \beta|$. □

Na sliki (1.9) vidimo, da sta trikotniški pravili (1.8) enakovredni dobro znanemu dejstvu iz geometrije: vsaka stranica v trikotniku je daljša od razlike in krajša od vsote ostalih dveh stranic.

S pomočjo absolutne vrednosti lahko merimo razdalje med kompleksnimi števili: razdalja med α in β je enaka $|\alpha - \beta|$.



Slika 1.9: Upodobitev kompleksnega števila

Primer 1.3.1. Predstava o absolutni vrednosti kot o razdalji med dvema številoma nam včasih olajša razmišljanje:

1. Poiščimo množico

$$A = \{z \in \mathbb{C};\ |z-1| = |z-i|\}.$$

   Množica A vsebuje vsa tista kompleksna števila, ki so enako oddaljena od 1 in od i, torej ležijo na simetrali lihih kvadrantov (slika 1.10)

2. Množica

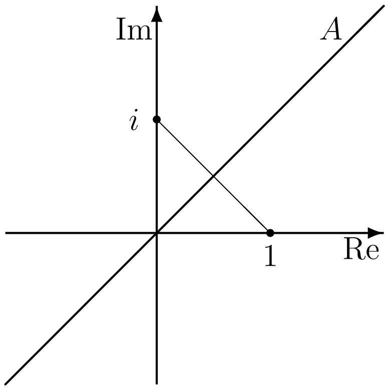
$$B = \{z \in \mathbb{C};\ |z-z_0| = r\}$$

   je krožnica s središčem v z_0 in radijem r.

3. Množica

$$C = \{z \in \mathbb{C};\ |z-z_1| + |z-z_2| = r\}$$

   je elipsa z goriščema z_1 in z_2 (*klasična* definicija elipse: elipsa je množica točk, za katere je vsota razdalj do dveh fiksnih točk (*gorišč*) konstantna). ■



Slika 1.10: Množica A iz primera 1.3.1

Polarni zapis kompleksnega števila

Lego kompleksnega števila $z \neq 0$ v ravnini lahko opišemo tudi v polarnih koordinatah, tako, da podamo oddaljenost $|z|$ števila z od izhodišča 0 in kotom φ, med poltrakom iz 0 skozi točko z in pozitivnim delom realne osi, ki mu pravimo *argument* števila z, kar zapišemo $\varphi = \arg z$. Argument kompleksnega števila ni enolično določen, saj določajo vsi argumenti $\varphi + 2k\pi, k \in \mathbb{Z}$ isti poltrak v kompleksni ravnini. Če izberemo argument tako, da leži na intervalu $[0, 2\pi)$, pravimo, da smo izbrali *glavno vrednost* argumenta in ta je določena enolično za vsak $z \neq 0$.

Prehod od zapisa po komponentah do polarnega zapisa kompleksnega števila $z = x + iy$ je določen z enačbami

$$r = \sqrt{x^2 + y^2}, \quad \cos\varphi = \frac{x}{\sqrt{x^2 + y^2}}, \quad \sin\varphi = \frac{y}{\sqrt{x^2 + y^2}},$$

obratni prehod pa z

$$x = r\cos\varphi, \quad y = r\sin\varphi.$$

Tako dobimo *polarni zapis* kompleksnega števila $z = x + iy$:

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

Primer 1.3.2. Prehod od zapisa po komponentah do polarnega zapisa in obratno:

1. Število $z = -4\sqrt{3} + 4i$ zapišimo v polarni obliki.

   Najprej izračunamo absolutno vrednost

   $$|z| = \sqrt{(-4\sqrt{3})^2 + 4^2} = 8,$$

   nato iz enačb

   $$\cos\varphi = \frac{-4\sqrt{3}}{8} = -\frac{\sqrt{3}}{2}; \quad \sin\varphi = \frac{4}{8} = \frac{1}{2}$$

   ugotovimo, da je glavna vrednost argumenta enaka $\varphi = 5\pi/6$, torej

   $$z = 8\left(\cos\frac{5\pi}{6} + i\sin\frac{5\pi}{6}\right).$$

2. Kompleksno število z absolutno vrednostjo $|z| = 3$ in argumentom $\arg z = -\pi/10$ zapišimo po komponentah.

   $$\begin{aligned} z &= 3\left(\cos\frac{-\pi}{10} + i\sin\frac{-\pi}{10}\right) \\ &= 3\left(\cos\frac{\pi}{10} - i\sin\frac{\pi}{10}\right) \approx 2.85 - 0.93i. \end{aligned}$$

■

Kompleksni števili zapisani v polarni obliki $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$ in $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$ sta enaki natanko tedaj, ko je $r_1 = r_2$ in $\varphi_1 - \varphi_2 = 2k\pi$.

Produkt dveh kompleksnih števil v polarni obliki

$$z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1) \quad \text{in} \quad z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$$

je enak

$$\begin{aligned} z_1 z_2 &= r_1 r_2[(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2) \\ &\quad + i(\sin\varphi_1\cos\varphi_2 + \cos\varphi_1\sin\varphi_2)] \\ &= r_1 r_2[\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)]. \end{aligned}$$

Pri množenju se torej moduli množijo: $|z_1 z_2| = |z_1| \cdot |z_2|$, argumenti pa seštevajo: $\arg(z_1 z_2) = \arg z_1 + \arg z_2$.

Kvocient dveh kompleksnih števil z_1 in $z_2 \neq 0$,

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}[\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)],$$

ima modul $|z_1/z_2| = |z_1|/|z_2|$ in $\arg(z_1/z_2) = \arg z_1 - \arg z_2$.

Če pravilo za produkt uporabimo za n enakih faktorjev

$$z_1 = z_2 = \cdots = z_n = z = r(\cos\varphi + i\sin\varphi),$$

dobimo znano pravilo za potenciranje kompleksnih števil, imenovano tudi de Moivreov[4] obrazec

$$z^n = r^n(\cos n\varphi + i\sin n\varphi).$$

Primer 1.3.3. Izračunajmo z^{10}, če je $z = 1 + i$.

Zapišimo z v polarni obliki:

$$z = \sqrt{2}(\cos(\pi/4) + i\sin(\pi/4))$$

in izračunajmo po de Moivrejevem obrazcu

$$z^{10} = \sqrt{2}^{10}\left(\cos\frac{10\pi}{4} + i\sin\frac{10\pi}{4}\right) = 2^5\left(\cos\frac{5\pi}{2} + i\sin\frac{5\pi}{2}\right) = 32i.$$

■

Pogosto uporabljamo oznako

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

Tako dobimo zapis kompleksnega števila v *eksponentni obliki*:

$$z = |z|e^{i\varphi}.$$

Pravila za računanje v eksponentni obliki izgledajo takole:

$$\begin{aligned} z_1 \cdot z_2 &= |z_1||z_2|e^{i(\varphi_1+\varphi_2)} \\ \frac{z_1}{z_2} &= \frac{|z_1|}{|z_2|}e^{i(\varphi_1-\varphi_2)} \\ z^n &= |z|^n e^{in\varphi}. \end{aligned}$$

[4] Abraham de Moivre (1667–1754), Francoski matematik

Koreni kompleksnih števil

Naj bo p/q racionalno število, kjer $p \in \mathbb{Z}$ in $q \in \mathbb{N}$ nimata skupnega delitelja.

Definicija 1.3.4. Definirajmo $z^{p/q}$ s predpisom

$$w = z^{p/q} \quad \Longleftrightarrow \quad w^q = z^p.$$

Števili w in z naj bosta dani v polarni obliki: $w = \rho(\cos\vartheta + i\sin\vartheta)$ in $z = r(\cos\varphi + i\sin\varphi)$. Iz zgornje definicije sledi

$$\rho^q[\cos(q\vartheta) + i\sin(q\vartheta)] = r^p[cos(p\varphi) + i\sin(p\varphi)].$$

Število na levi je enako številu na desni, če je $\rho^q = r^p$ in $q\vartheta - p\varphi = 2k\pi$, od koder dobimo

$$\rho = r^{p/q} \quad \text{in} \quad \vartheta = \frac{p\varphi + 2k\pi}{q}.$$

Izraz $z^{p/q}$ ni enolično določen, saj za vsak $k \in \mathbb{Z}$ dobimo eno vrednost

$$w_k = z^{p/q} = r^{p/q}\left[\cos\frac{p\varphi + 2k\pi}{q} + i\sin\frac{p\varphi + 2k\pi}{q}\right]. \tag{1.9}$$

Zaradi periodičnosti funkcij sin in cos, je le q vrednosti med seboj različnih $w_0, w_1, \ldots, w_{q-1}$, potem pa se števila w_k začnejo ciklično ponavljati, tako da je $w_q = w_0,\ w_{q+1} = w_1,\ \ldots$.

V kompleksni ravnini ležijo koreni $w_0, w_1, \ldots, w_{q-1}$ na ogliščih pravilnega q-kotnika s središčem v točki 0, središčni kot med dvema sosednjima ogliščema je $2\pi/q$.

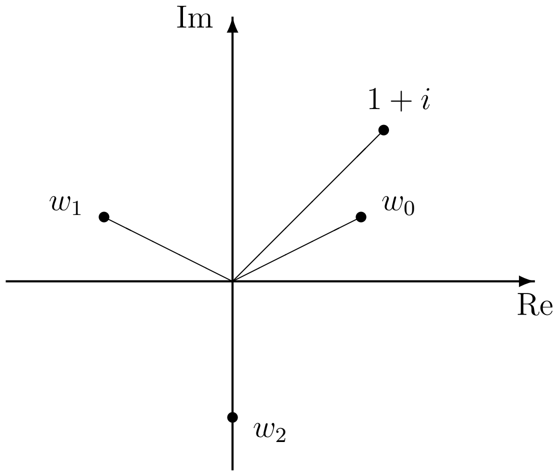
Primer 1.3.4. Izračunajmo vse vrednosti izraza $(1+i)^{2/3}$.

Najprej število $z = 1 + i$ zapišemo v polarni obliki

$$z = \sqrt{2}(\cos\pi/4 + i\sin\pi/4),$$

nato pa uporabimo enačbo (1.9) pri $p = 2$ in $q = 3$:

$$\begin{aligned} w_k &= \left(\sqrt{2}\right)^{2/3}\left[\cos\frac{\pi/2 + 2k\pi}{3} + i\sin\frac{\pi/2 + 2k\pi}{3}\right] \\ &= \sqrt[3]{2}\left(\cos\frac{(1+4k)\pi}{6} + i\sin\frac{(1+4k)\pi}{6}\right). \end{aligned}$$



Slika 1.11: Koreni $(1+i)^{2/3}$

Za $k = 0, 1, 2$ dobimo zaporedoma vse tri vrednosti:

$$\begin{aligned}
w_0 &= \sqrt[3]{2}(\cos\tfrac{\pi}{6} + i\sin\tfrac{\pi}{6}) &&= \sqrt[3]{2}\left(\frac{\sqrt{3}}{2} + \frac{i}{2}\right)\\
w_1 &= \sqrt[3]{2}(\cos\tfrac{5\pi}{6} + i\sin\tfrac{5\pi}{6}) &&= \sqrt[3]{2}\left(-\frac{\sqrt{3}}{2} + \frac{i}{2}\right)\\
w_2 &= \sqrt[3]{2}(\cos\tfrac{9\pi}{6} + i\sin\tfrac{9\pi}{6}) &&= -i\sqrt[3]{2}.
\end{aligned}$$

$\blacksquare$

Literatura

[1] K. G. Binmore: *Mathematical Analysis (a straightforeward approach), 2 ed.*, Cambridge University Press, Cambridge, 1982.

[2] C. H. Edwards Jr. in D. E. Penney: *Calculus and Analytic Geometry*, Prentice-Hall International, Inc., Englewood Cliffs, 1990.

[3] R. Jamnik: *Matematika*, Partizanska knjiga, Ljubljana, 1981.

[4] P. Lax, S. Burstein in A. Lax: *Calculus with Applications and Computing, Vol I*, Springer-Verlag, New York, 1976.

[5] N. Piskunov: *Differential and Integral Calculus, vol. I*, Mir Publishers, Moscow, 1974.

[6] N. Prijatelj: *Uvod v matematično analizo, 1. del*, DMFA, Ljubljana, 1980.

[7] G. B. Thomas, Jr: *Calculus and Analytic Geometry*, Addison-Wesley Publishing Company, Reading, 1972.

[8] I. Vidav: *Višja matematika I* (10. natis), DMFA, Ljubljana, 1990.