# Množice in števila

## Osnovni pojmi o množicah

### *Množice*

- Množica je zbirka elementov, ki jih imenujemo elementi množice.
- Če x pripada množici A, zapišemo x∈ A, če ne pripada pa x∉ A.
- Prazno množico, ki nima nobenenega elementa zapišemo z ∅.
- A podmnožica B, zapišemo A⊆B in A je prava podmnožica B, A⊂ B. Unija AUB, presek A ∩ B, razlika ali komplement A\B.
- O komplementu $\overline{A}$ govorimo takrat, ko so vse množice , ki nas zanimajo, podmnožice neke vnaprej določene *univerzalne množice U*. Takrat je $\overline{A}$ , U\B

De Morganova izreka:

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

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

za poljuben objekt a velja:

$$a\in A\cap(B\cup C)\Leftrightarrow a\in A\wedge a\in B\cup C\Leftrightarrow a\in A\wedge(a\in B\wedge a\in C)\Leftrightarrow(a\in A\wedge a\in B)\vee(a\in A\wedge a\in C)\Leftrightarrow a\in A\cap B\vee a\in A\cap C\Leftrightarrow a\in(A\cap B)\cup(A\cap C)$$

### *Preslikave*

**Definicija**: preslikava množice A v B, je pravilo ki vsakemu elementu a∈ A priredi točno določen element v množici B,označimo ponavadi: $f:A\to B$. Element množice B, ki ga preslikava *f* priredi elementu a∈ A , je slika elementa a in ga zapišemo kot *f(a)*. Množico A imenujemo kot defenicijsko območje preslikave *f*, množico $f(A)=\{f(a),a\in A\}\subseteq B$ pa njeno zalogo vrednosti.

Med upodobitvami množice A vase zasluži posebno mesto identična upodobitev id: *A*→ *A*, ki vsak element množice A preslika nase: *id(a) = a*.

*Injektivna*

Preslikava *f: A*→ *B* je injektivna če sta sliki različnih elementov vedno različna elementa $a\neq b\Rightarrow f(a)\neq f(b)$. Za injektivne preslikave velja, da je vsak b ∈ B slika največ enega elementa *a* ∈ *A*.

*Surjektivna*

Preslikava *f: A*→ *B* je surjektivna kadar je njene 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.

*Bijektivna*

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

Številu elementov končne množice pravimo moč množice.

*Kompozitum*
Naj bo *f* upodobitev množice A v množico B in g upodobitev množice B v množico C. Tako lahko vsak $a \in A$ preslikamo naprej 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 $g(f(a)) \in C$. 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:* Naj bo f: R→ R dana s predpisom $f(x)=2x$ in g: R→R dana s predpisom $f(x)=x^2$. Potem sta preslikavi $f \circ g$ :R→R in $g \circ f$ :R→R določeni z $(f \circ g)(x) = 2(x^2) = 2x^2$ in $(g \circ f)(x) = (2x)^2 = 4x^2$.

Če je preslikava $f: A \to B$ inejktivna, je vsak element $b \in f(A)$ slika natanko enega elementa $a \in A$. Torej obstaja tak predpis, ki vsakemu elementu $b \in f(A)$ priredi natanko določen $a \in A$ (tisti za katerega velja $f(a)=b$). 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*.

Izrek: preslikava g: f(A)→A je preslikavi *f* inverzna, če velja $g \circ f = id : A \to A$ in $f \circ g = id : f(A) \to f(A)$

Definicija: graf preslikave $f:A \to B$ je podmnožica kartezičnega produkta $\Gamma(f) = \{(a, f(a)); a \in A\} \subset A \times B$.

# Realna števila

## Opis množice realnih števil

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

## Algebrajski opis števil

Množica realnih števil R je komutativen obseg. To pomeni da sta v R definirani dve binarni operaciji in sicer seštevanja in množenje, ki imata naslednje lasnosti:
Komutativnost
a + b = b + a in a * b = b * a
Asociativnost
(a + b) + c= a + (b + c)
Distributivnost
a * (b + c)=a * b + a * c
izrek:

1. za vsak par naravnih števil a,b velja natanko ena od možnosti (a = b; a < b; a > b)
2. če je a < b in b < c, je a < c
3. če je a < b, je a+c < b+c, kjer je c poljubno naravno število
4. če je a < b in c > 0 je a*c < b*c
5. če sta a in b pozitivni števili je a < b je 1/a > 1/b

Absolutna vrednost: je preslikava iz R v množico nenegativnih realnih, ki je določena s predpisom $|a| = {}^{a;a\geq 0}_{-a;a<0}$, zapišimo nekaj lasnosti absolutne vrednosti: ||a|-|b||<|a+b|<|a|+|b|, |ab|=|a||b|. Neenakostim pravimo trikotniški pravili.

## Številska premica

Geometrijsko lahko realna števila predstavimo kot točke na številski premici, kjer smo izbrali izhodišče, to je točka 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 $a \in R$ pripada natanko določena točka na številski premici: če je a pozitivno število, mu pripada točka desno od 0, ki je od 0 oddaljena za |a|, če je a negativno, paje ustrezna točka na levi, za |a| oddaljena od 0. Množico vseh števil na daljici imenujemo interval, ki je med dvema danima številoma.

$(a,b)=\{x : a<x<b\}$ odprt interval

$[a,b]=\{x : a \le x \le b\}$ zaprt interval

$[a,b)=\{x : a \le x < b\}$ poldoprt interval

$(a,b]=\{x : a < x \le b\}$ polodprt interval

Naj bo $\varepsilon$ majhno pozitivno število. Množica $\{x;|x-a|<\varepsilon\}$ vsebuje natanko tista števila x, ki so od a oddaljena za manj kot $\varepsilon$. Pravimo ji epsilon-okolica števila a in jo lahko zapišemo tudi kot odprt interval dolžine $2\varepsilon$ s središčem v točki a.

## Decimalne števila

Kadar računamo, zapišemo ponavadi realna števila v decimalni obliki. Decimalni zapis pozitivnega realnega števila a izgleda takole: $a = n \times d_1 d_2 d_3 \ldots$, kjer je n celo število in d je element naravnih števil 1-9.

## Številske podmnožice naravnih števil

### Naravna števila

Naj bo $1 \in R$ enota za množenje. Vsote 1+1=2; 1+1+1=3.... imenujemo naravna števila. Množice naravnih števil N={1,2,3,4....} je tesno povezana s štetjem. Tako kot R, je tudi množica N urejena z relacijo <. Vsako naravno število n ima glede na relacijo < v množici N svojega neposrednega naslednika- število n+1. v množici R o neposrednem nasledniku ne moremo govoriti.

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. (princip popolne indukcije pogosto uporabljamo za dokazovanje trditev in izrekov in to poteka v dveh fazah: 1.) najprej dokažimo da trditev velja za naravno število 1. 2.) nato dokažimo da iz veljavnosti trditve za naravno število n lahko sklepamo, da trditev velja tudi za naslednje naravno število n+1.

### Cela števila

Množico celih števil dobimo tako, da naravnim številom dodamo vsa njihova nasprotna števila in število 0: Z={...,-3,-2,-1,0,1,2,3...}. množica celih števil je zaprta za seštevanje in množenje, pa tudi za odštevanje.

### Racionalna števila

Če množici **Z** dodamo še vse kvociente $ab^{-1}$, kjer sta a∈ **Z** in b∈ **N**, dobimo množico racionalnih števil **Q**. Vsako racionalno število lahko predstavimo kot ulomek m/n, kjer je števec m celo, imenovalec n pa naravno število. Množica **Q** je zaprta za seštevanje, množenje

in odštevanje, torej je kolobar. Poleg tega je zaprta za deljenje z neničelnim številom. Znano je da obstajajo realna števila ki niso racionalna. Pravimo jim iracionalna. Primer takega števila je $\sqrt{2}$.

## Omejene podmnožice realnih števil

Definicija: množica A$\subset$ **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, to je, če je navzgor in navzdol omejena.

Definicija: naj bo $A \subset R$ navzgor omejena in $B \subset R$ navzdol omejena neprazna množica. Število M ej natančna zgornja meja ali supremum množice A, če je najmanjša med vsemi njenimi zgornjimi mejami , kara zapišemo *M=supA*. Podobno je m natančna spodnja meja ali infinimu množice B največja med vsemi njenimi spodnjimi mejami, kar zapišemo kot *m=infB*.

Trditev: *M=supA* 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=infB*, če je $m \leq b$ za vsak $b \in B$ ina za vsak $\varepsilon > 0$ obstaja tak element $b \in B$ da je m+$\varepsilon$ >b.

Dedekinov aksiom ali lasnosti kontinuuma: vsaka neprazna navzgor omejena množica realnih števil ima natačno zgornjo mejo. Podobno ima vsaka neprazna navzdol omejena podmnožica **R** natančno spodnjo mejo.

Izrek: (Arhimedova lasnost) če sta x in y poljubni realni števili in je y>0 obstaja tak $n \in N$, da je x<ny.

Trditev: vsako realno število a ima v vsaki svoji epsilon 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.

## Potence in koreni

Trditev: za vsak $n \in N$ velja: če je 0<a<b, je tudi $0 < a^n < b^n$
Navedimo brez dokaza znano formulo za potenciranje binoma, ki jo bomo velikokrat uporabili: $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$

Izrek: za vsak $y \geq 0$ in za vsak $n \in N$ obstaj tako natanko določeno število $x \geq 0$, da je $x^n = y$.

Definicija: 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/g; $q \in N$, $p \in Z$ za poljubno racionalno število, potem 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, le 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 te mprimeru 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 $a^{n+m}=a^n a^m$ in $(a^n)^m=a^{nm}$.

# Kompleksna števila

Definicija: kompleksno število $\alpha$ je urejen par realnih števil (a,b); prvo a=Re($\alpha$), imenujemo realna komponenta, drugo, b=Im($\alpha$), imaginarna komponenta. Množico kompleksnih števil označimo s simbolom **C**.

Izrek: množica C z operacijama (a,b)+(c,d)=(a+c,b+d) in (a,b)*(c,d)=(ac-bd,ad+bc) je obseg.

Definicija: številu $\alpha$ = a+bi konjugirano število je $\overline{\alpha}$=a-ib. Število $\alpha$ je realno natanko takrat kadar je $\alpha=\overline{\alpha}$ in imaginarno natanko takrat, kadar je $-\alpha=\overline{\alpha}$.

Definicija: absolutna vrednost kompleksnega števila $\alpha$ je kvadratni koren števila $\alpha\overline{\alpha}$.
$|\alpha|=\sqrt{\alpha\overline{\alpha}}=\sqrt{a^2+b^2}$.

Absolutna vresdnost ali modul kompleksnega števila $\alpha$ je dolžina daljice, ki povezuje koordinatno izhodišče s komplesksnim številom $\alpha$.
Če je $a\in R$ se ta definicija ujema z že znano definicijo absolutne vrednosti realnega števila. Podobno kot pri realnih številih velja $|\alpha\beta|=|\alpha||\beta|$ in $||\alpha|-|\beta||\leq|\alpha+\beta|\leq|\alpha|+|\beta|$.

## Polarni zapis kompleksnega števila

Lego kompleksnega števila z v ravnini lahko opišemo tudi s polarnimi koordinatami, tako, da podamo oddaljenost |z| števila z od izhodišča 0 in kotom $\varphi$, med poltrakom iz 0 skozi točko z in pozitivnim delom realne osi, ki mu pravimo argument števila z, kar zapišemo $\varphi$=argZ. Prehod od zapisa po komponentah do polarnega zapisa števila z=x+iy je določen z enačbami $r=\sqrt{x^2+y^2}$, $\cos\varphi=\frac{x}{\sqrt{x^2+y^2}}$, $\sin\varphi=\frac{y}{\sqrt{x^2+y^2}}$, obraten prehod pa x=rcos($\varphi$) in y=rsin($\varphi$). Tako dobimo polarni zapis kompleksnega števila $z=x+iy$; z=|z|(cos $\varphi$+isin $\varphi$).
Pogosto uporabljamo obliko $e^{i\varphi}=\cos\varphi+i\sin\varphi$. Tako dobimo zapis komplesksnega števila v eksponentni obliki z=|z| $e^{i\varphi}$.

## Koreni kompleksnih števil

Definicija: definirajmo $z^{p/q}$ s predpisom w= $z^{p/q}$ $\Leftrightarrow w^p=z^p$. 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 $p^q[\cos(q\vartheta)+i\sin(q\vartheta)]=r^p[\cos(p\varphi)+i\sin(p\varphi)]$. Število na levi je enako na desni, če je $p^q=r^p$ in $\vartheta=\frac{p\varphi+2k\pi}{q}$. izraz $z^{p/q}$ ni enolično določen, saj za vsak $k\in Z$ dobimo eno vrednost $w_k=z^{p/q}=r^{p/q}\left[\cos\frac{p\varphi+2k\pi}{q}+i\sin\frac{p\varphi+2k\pi}{q}\right]$.