Osnove teorije množic

Jezik teorije množic je dandanes osnovni jezik, v katerem izražamo formule, enačbe, izreke in pa ostale matematične konstrukcije. *Množico* si intuitivno predstavljamo kot skupek reči, ki imajo ponavadi kakšno skupno lastnost. Kot primer lahko vzamemo množico študentov fizike ali pa npr. množico knjig v knjižnici. V fiziki so pogosto zanimive množice možnih konfiguracij kakšnega mehanskega sistema kot so npr. možni položaji točke na premici, ravnini ali pa v prostoru. Položaj točke v prostoru lahko preprosto opišemo s tremi parametri, že malo težje pa je opisati množico možnih orientacij nekega telesa v prostoru. Kar se tiče matematike, pa bodo za nas najbolj zanimive množice števil in pa množice, ki jih lahko iz njih konstruiramo.

Omeniti velja, da imamo v matematiki pogosto opravka z množicami, ki so opremljene še s kakšno dodatno strukturo. Števila znamo npr. seštevati in množiti, kar pomeni, da je množica števil opremljena z algebraično strukturo (matematična veja, ki se ukvarja s posplošitvami pojma števil, se imenuje algebra). Kot naslednji primer pa vzemimo množico položajev točke na premici, ki jo lahko enačimo kar z množico realnih števil. Na le-ti imamo mero, s pomočjo katere lahko rečemo, da sta dve števili blizu skupaj ali pa daleč narazen. Ti pojmi igrajo ključno vlogo pri študiju zveznosti in odvedljivosti funkcij. Matematična veja, ki nam omogoča definirati pojem 'bližine' na poljubni množici, se imenuje topologija.

Osnovne definicije in operacije

Kot smo že rekli, si množico predstavljamo kot skupino nekih reči. Vsako reč, ki spada v neko množico, imenujemo *element* te množice. Poznati neko množico pomeni natanko vedeti, katere reči so njeni elementi.

Običajno označujemo množice z velikimi črkami $A, B, C \ldots$, elemente pa z malimi črkami $a, b, c \ldots$ Zavedati pa se je treba, da so tudi množice same lahko elementi nekih večjih množic. Na začetku smo že omenili množico možnih položajev nekega mehanskega sistema. Kadar pa študiramo npr. kakšen fizikalni zakon, pa nas zanima množica mehanskih sistemov, za katere velja dani zakon. Imamo torej opravka z množico množic.

Celotna teorija množic temelji na pojmu 'biti element' oziroma na odnosu pripadnosti. Če je neka reč x element množice A, to zapišemo kot

$$x \in A,$$

v nasprotnem primeru pa pišemo $x \notin A$. Množic, ki imajo natanko iste elemente, med sabo ne ločimo. Definiramo, da sta množici A in B enaki (kar označimo z $A = B$) čee (če in samo če) imata iste elemente. To pomeni, da za poljuben x velja: $x \in A$ čee $x \in B$. Če množici A in B nista enaki, to označimo z $A \neq B$. V tem primeru mora obstajati ali $x \in A$ za katerega velja $x \notin B$ ali pa $y \in B$, da $y \notin A$.

Množico lahko konkretno navedemo, tako da naštejemo njene elemente eksplicitno. Oznaka

$$A = \{1, 3, 5, 7\}$$

nam npr. pove, da množica A vsebuje prva štiri liha števila. Množica, ki jo je najlažje opisati je *prazna množica*, ki jo označimo z $\emptyset$. Za njo velja, da nobena reč ni njen element (za poljuben x velja $x \notin \emptyset$). Omenimo, da iz definicije enakosti množic sledi

$$\{1, 3, 7, 9\} = \{1, 3, 7, 9, 9, 1\},$$

vendar pa

$$\emptyset \neq \{\emptyset\},$$

saj velja $\emptyset \notin \emptyset$ in $\emptyset \in \{\emptyset\}$.

Kadar imamo opravka z neskončnimi množicami, je zgornji zapis pogosto nepraktičen. V takšnih primerih množice definiramo kot *podmnožice* nekih že znanih množic. Naj bo A dana množica in L neka lastnost, ki je smiselna za elemente množice A. Definiramo lahko podmnožico

$$B = \{\, x \in A \,|\, x \text{ ima lastnost } L\},$$

vseh elementov množice A, ki imajo lastnost L. Kot primer lahko vzamemo množico A naravnih števil in njeno podmnožico B sodih števil. Lastnost L je v tem primeru 'biti sodo število'. To, da je B podmnožica A, označimo z $B \subset A$. V splošnem $B \subset A$ pomeni, da je vsak element množice B tudi element množice A. Za vsako množico A sta $\emptyset$ in pa A njuni podmnožici.

Poglejmo si sedaj osnovne *operacije* med danima množicama A in B.

1. *Presek*: $A \cap B = \{\, x \in A \,|\, x \in B\} = \{\, x \in B \,|\, x \in A\}$.
2. *Unija*: $A \cup B = \{\, x \,|\, x \in A \text{ ali } x \in B\}$.
3. *Razlika*: $A \setminus B = \{\, x \in A \,|\, x \notin B\}$.
4. *Produkt*: $A \times B = \{\, (x, y) \,|\, x \in A,\, y \in B\}$.

Presek $A \cap B$ vsebuje vse elemente, ki ležijo v obeh množicah in je zato podmnožica tako množice A kot množice B. Za množici A in B rečemo, da sta *disjunktni*, če velja $A \cap B = \emptyset$. Podobno lahko opazimo tudi, da je $A \setminus B$ podmnožica množice A, a ne nujno množice B. Unija dveh množic je definirana kot skupek vseh elementov, ki ležijo v eni izmed množic, zato je torej ne moremo definirati kot podmnožico. Produkt dveh množic si ponavadi predstavljamo kot množico urejenih parov elementov, pri čemer je prvi element iz prve množice, drugi pa iz druge. Fizikalno si lahko produkt množic predstavljamo kot prostor možnih položajev sistema, ki se lahko giblje v večih neodvisnih smereh. Položaje točke na premici lahko opišemo z množico realnih števil $\mathbb{R}$, položaje točke na ravnini pa z množico $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$.

Na podoben način lahko opišemo možne položaje sistema dveh različnih točk v prostoru z množico $\mathbb{R}^6 - B$, kjer je B množica vseh parametrov, pri katerih bi bili obe točki na istem mestu.

Včasih označujemo množice, ki imajo za elemente neke druge množice, s pisanimi črkami $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$,... in jih imenujemo tudi *razredi* ali pa družine množic. Denimo, da je $\mathcal{A}$ taka družina, in da so njeni elementi indeksirani z množico J. Potem zapišemo

$$\mathcal{A} = \{\, A_j \,|\, j \in J\}.$$

Tu je A_j neka množica, ki je prirejena elementu $j \in J$. Podobno kot za dve množici lahko definiramo tudi (neskončni) presek oziroma unijo

$$\bigcap \mathcal{A} = \bigcap_{j \in J} A_j = \{\, x \,|\, x \in A_j \text{ za vsak } j \in J\},$$

$$\bigcup \mathcal{A} = \bigcup_{j \in J} A_j = \{\, x \,|\, x \in A_j \text{ za vsaj en } j \in J\}.$$

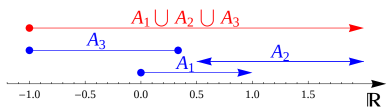
Zgled. (1) Imejmo končno indeksno množico $J = \{1, 2, 3\}$ in naj bo

$$A_1 = [0, 1) \subset \mathbb{R},$$
$$A_2 = \left(\frac{1}{2}, 2\right) \subset \mathbb{R},$$
$$A_3 = \left[-1, \frac{1}{3}\right] \subset \mathbb{R}.$$

Potem je

$$\bigcap_{j \in J} A_j = A_1 \cap A_2 \cap A_3 = \emptyset,$$
$$\bigcup_{j \in J} A_j = A_1 \cup A_2 \cup A_3 = [-1, 2).$$

Grafično lahko te množice predstavimo na naslednji način.



(2) Vzemimo sedaj neskončno indeksno množico $J = \mathbb{N}$ in naj bo

$$A_n = [0, n]$$

za vsak $n \in \mathbb{N}$. Potem je

$$\bigcap_{j \in J} A_j = A_1 \cap A_2 \cap A_3 \cap \ldots = [0, 1],$$
$$\bigcup_{j \in J} A_j = A_1 \cup A_2 \cup A_3 \cup \ldots = [0, \infty).$$

Definiramo lahko tudi produkt (neskončne) družine množic

$$\prod \mathcal{A} = \prod_{j \in J} A_j = \{\, (x_j)_{j \in J} \mid x_j \in A_j \text{ za vsak } j \in J\}.$$

Elemente produkta neskončno množic si lahko predstavljamo podobno kot zaporedja števil. Vsak element je namreč določen z izbiro po natanko enega elementa iz vsake množice.

V zvezi z neskončnim produktom množic moramo omeniti aksiom izbire. Brez oklevanja lahko verjamemo, da je produkt dveh nepraznih množic spet neprazna množica, zato se nam zdi upravičeno pričakovati, da bo produkt poljubne družine nepraznih množic spet neprazna množica. V teoriji množic to našo domnevo postuliramo z aksiomom izbire. Kljub temu, da se nam zdi v tej obliki aksiom izbire intuitivno upravičen, pa lahko iz njega izpeljemo nekatere posledice, ki se nam zdijo neobičajne. Kot primer navedimo paradoks Banacha in Tarskega. Le-ta pravi, da lahko trodimenzionalno kroglo razdelimo na končno število kosov, iz katerih lahko sestavimo dve identični kopiji prve krogle.

Včasih nas zanimajo samo množice, ki so podmnožice neke vnaprej dane množice U, ki jo imenujemo *univerzum* (pri nas bo univerzum pogosto množica števil). V tem kontekstu bomo uporabljali oznako A^c

$$A^c = U \setminus A = \{\, x \in U \mid x \notin A\}$$

za komplement množice A v U. Seveda velja $(A^c)^c = A$.

Poglejmo si sedaj povezavo med presekom, unijo in pa komplementi.

Trditev 1 (De Morganova zakona)**.** *Naj bodo A_j podmnožice množice U, indeksirane z indeksno množico J. Potem veljata enakosti*

$$\bigcup_{j \in J} A_j^c = \left(\bigcap_{j \in J} A_j \right)^c,$$

$$\bigcap_{j \in J} A_j^c = \left(\bigcup_{j \in J} A_j \right)^c.$$

Dokaz. Dokažimo prvo enakost. Iz definicije enakosti množic sledi, da je dovolj pokazati, da je vsak element $\bigcup_{j \in J} A_j^c$ tudi element $(\bigcap_{j \in J} A_j)^c$ in podobno v obratni smeri.

Vzemimo poljuben $x \in \bigcup_{j \in J} A_j^c$. Potem obstaja nek $j \in J$, da je $x \in A_j^c$. Od tod sledi, da $x \notin A_j$ in zato $x \notin \bigcap_{j \in J} A_j$. Zato je $x \in (\bigcap_{j \in J} A_j)^c$.

Naj bo sedaj $x \in (\bigcap_{j \in J} A_j)^c$ poljuben. Potem velja $x \notin \bigcap_{j \in J} A_j$, zato mora obstajati nek $j \in J$, da velja $x \notin A_j$. Torej je $x \in A_j^c$ in zato $x \in \bigcup_{j \in J} A_j^c$.

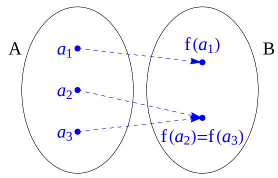
Drugo enakost lahko dokažemo na analogen način. □

Funkcije

Pojem, ki igra ključno vlogo v matematiki, je pojem funkcije. *Funkcija* ali preslikava f iz množice A v množico B je predpis, ki poljubnemu elementu $a \in A$ priredi natanko določen element $f(a) \in B$. Pišemo

$$f : A \to B.$$

Množico A imenujemo *domena* funkcije f, množico B pa *kodomena* f.



Dve funkciji sta enaki, če imata enaki domeni in kodomeni ter enak predpis. Vizualno funkcijo ponavadi ponazorimo z njenim *grafom*

$$\mathrm{Graf}(f) = \{\, (a, f(a)) \,|\, a \in A \,\} \subset A \times B.$$

V primeru realnih funkcij realne spremenljivke je graf funkcije tipično neka krivulja v ravnini, medtem ko je graf funkcije dveh spremenljivk neka ploskev v prostoru. Oba primera bomo podrobneje spoznali v nadaljevanju.

Slika oziroma zaloga vrednosti funkcije je množica vseh elementov v kodomeni, ki so slika kakšnega elementa domene

$$\mathrm{Im}(f) = \{\, f(a) \,|\, a \in A \,\} \subset B.$$

Zgled. (1) Pogosto imamo opravka s funkcijami, ki slikajo iz podmnožice realnih števil v realna števila. Če je domena funkcije neskončna množica, jo je najlažje definirati s pomočjo formule, ki nam pove, kam se preslika dano število. Kot primer vzemimo funkcijo $f : \mathbb{N} \to \mathbb{N}$, dano s predpisom

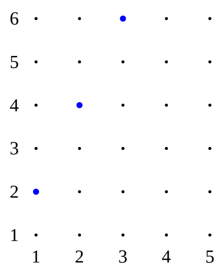
$$f(n) = 2n.$$

Domena in kodomena funkcije so naravna števila, njena slika pa so

$$\mathrm{Im}(f) = 2\mathbb{N} = \{\, 2n \,|\, n \in \mathbb{N} \,\}$$

soda naravna števila.

Graf funkcije f dobimo z vzorčenjem linearne funkcije po naravnih številih

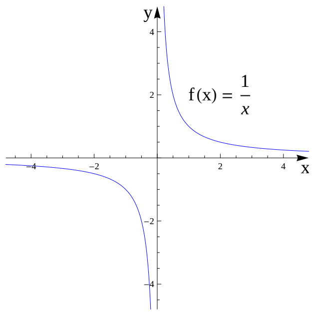


(2) Kadar je domena funkcije f končna množica, lahko funkcijo opišemo tudi tako, da povemo za vsak njen element, kam se preslika. Definirajmo na primer funkcijo $f : \{1, 3, 7\} \to \{0, 1\}$ s predpisom

$$\begin{aligned} f(1) &= 1, \\ f(3) &= 0, \\ f(7) &= 0. \end{aligned}$$

(3) Večino časa bomo posvetili funkcijam, katerih domene in kodomene so podmnožice realnih števil. V tem primeru smo pogosto malce površni. Če na primer definiramo funkcijo s predpisom $f(x) = \frac{1}{x}$, je s tem še nismo natančno določili, saj nismo povedali, kaj sta njena domena oziroma kodomena. Če jih eksplicitno ne omenimo, ponavadi privzamemo, da so v domeni vsa števila, za katera je predpis definiran, za kodomeno pa vzamemo kar vsa realna števila. V našem primeru bi torej vzeli $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$.

Graf funkcije f je sestavljen iz dveh krivulj



Slika funkcije f je $\mathrm{Im}(f) = \mathbb{R} \setminus \{0\}$. Lahko bi tudi definirali funkcijo $g : \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$ s predpisom $g(x) = \frac{1}{x}$, ki ima enak graf kot f, a je različna od funkcije f, saj ima različno kodomeno.

Kot primer funkcije, ki je različna od f, a ima isto domeno in kodomeno, pa navedimo funkcijo h s predpisom $h(x) = \frac{1}{x^2}$.

(4) Za poljubno množico A definiramo identično funkcijo $\mathrm{id}_A : A \to A$ s predpisom

$$\mathrm{id}_A(a) = a \text{ za vsak } a \in A.$$

(5) V fiziki se funkcije pogosto pojavljajo v obliki skalarnih polj (kot je na primer potencialna energija) ali pa vektorskih polj (gravitacijsko ali električno polje).

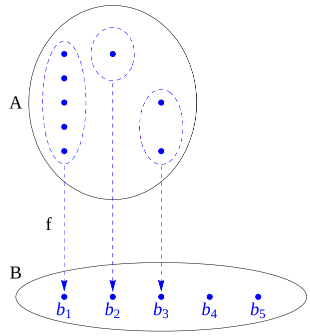
Bolj splošno lahko definiramo sliko podmnožice $X \subseteq A$

$$f(X) = \{\, f(a) \,|\, a \in X\} \subset B.$$

V posebnem primeru seveda velja $\mathrm{Im}(f) = f(A)$. Za poljubno podmnožico $Y \subset B$ definiramo njeno *inverzno sliko* oziroma *prasliko* vzdolž funkcije f

$$f^{-1}(Y) = \{\, a \in A \,|\, f(a) \in Y\} \subset A$$

in opazimo, da velja $f^{-1}(B) = A$. Prasliki $f^{-1}(b) := f^{-1}(\{b\})$ rečemo *vlakno* funkcije f nad točko $b \in B$. Funkcija f torej domeno razdeli na družino vlaken, po eno za vsako točko v sliki funkcije.



V sliki funkcije so ravno tiste točke, katerih vlakna so neprazna.

Definicija 2. *Naj bosta A in B množici in $f : A \to B$ funkcija.*

1. *Funkcija f je injektivna, če za poljubna $a, a' \in A$, $a \neq a'$, velja tudi $f(a) \neq f(a')$.*
2. *Funkcija f je surjektivna, če je $f(A) = B$. Torej je vsak $b \in B$ slika vsaj enega elementa iz A.*
3. *Funkcija f je bijektivna, če je hkrati surjektivna in injektivna.*

Zgled. Če imamo (lepo) funkcijo $f : \mathbb{R} \to \mathbb{R}$, si njen graf predstavljamo kot neko krivuljo v ravnini. V tem primeru je funkcija injektivna, če seka njen graf vsako vodoravnico največ enkrat ter surjektivna, če graf seka vsako vodoravnico vsaj enkrat. Sledi, da je f bijektivna, če seka njen graf vsako vodoravnico natanko enkrat.

Funkcija $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ s predpisom $f(x) = \frac{1}{x}$, je na primer injektivna, ni pa surjektivna. Če bi vzeli funkcijo z istim predpisom in isto domeno, kodomeno pa zožili na $\mathbb{R} \setminus \{0\}$, pa bi dobili bijektivno funkcijo.

Z zaporedno uporabo večih funkcij, definiranih na primernih množicah, pridemo do operacije *komponiranja* funkcij. Za funkciji $f : A \to B$ in $g : B \to C$ definiramo njun *kompozitum* $g \circ f : A \to C$ s predpisom

$$(g \circ f)(a) = g(f(a)) \qquad \text{za vsak } a \in A.$$

Pri komponiranju funkcij je zelo pomemben vrstni red, saj v splošnem velja

$$f \circ g \neq g \circ f.$$

Kot primer si poglejmo funkciji $f : \mathbb{R} \to \mathbb{R}$ in $g : \mathbb{R} \to \mathbb{R}$, definirani s predpisoma $f(x) = x^2$ ter $g(x) = 2x$. Tedaj je

$$(f \circ g)(x) = f(g(x)) = f(2x) = 4x^2,$$
$$(g \circ f)(x) = g(f(x)) = g(x^2) = 2x^2.$$

V zgornjem primeru so bile vse domene in kodomene enake, če pa je $A \neq C$, pa kompozituma $f \circ g$ niti ne moremo definirati. Rečemo, da komponiranje funkcij ni *komutativno*, za razliko od npr. množenja realnih števil, kjer vrstni red množenja ni pomemben.

Identični funkciji id_A in id_B igrata vlogo enice pri komponiranju

$$f \circ \mathrm{id}_A = f,$$
$$\mathrm{id}_B \circ f = f.$$

Kompozitum dveh funkcij lahko razširimo do kompozituma končnega števila funkcij. Če imamo še eno funkcijo $h : C \to D$, velja

$$(h \circ g) \circ f = h \circ (g \circ f).$$

Tej lastnosti rečemo *asociativnost* komponiranja. V praksi to pomeni, da ni važno, kako postavimo oklepaje, ki nam določajo, v kakšnem vrstem redu računamo kompozicije, če je le vrstni red funkcij enak.

Definicija 3. *Naj bo $f : A \to B$ funkcija.*

(1) Funkcija $g : B \to A$ je levi inverz f, če velja $g \circ f = id_A$.

(2) Funkcija $h : B \to A$ je desni inverz f, če velja $f \circ h = id_B$.

(3) Funkcija $w : B \to A$ je inverz f, če je hkrati levi in desni inverz f.

Recimo, da ima funkcija $f : A \to B$ levi inverz g in desni inverz h. Potem iz asociativnosti komponiranja sledi

$$(g \circ f) \circ h = g \circ (f \circ h),$$
$$\mathrm{id}_A \circ h = g \circ \mathrm{id}_B,$$
$$h = g,$$

kar pa pomeni, da je $g = h$ inverz funkcije f. Lahko se sicer zgodi, da ima neka funkcija več levih ali pa več desnih inverzov, kakor hitro pa ima hkrati levi in desni inverz, pa morata ti dve funkciji sovpadati. Od tod sledi, da je inverz funkcije enolično določen.

Definicija 4. *Funkcija $f : A \to B$ je obrnljiva, če ima inverz. V tem primeru inverz f označimo z $f^{-1} : B \to A$.*

Trditev 5. *Naj bo $f : A \to B$ funkcija, kjer je $A \neq \emptyset$. Potem velja:*

(1) Funkcija f je injektivna natanko takrat, ko ima levi inverz.

(2) Funkcija f je surjektivna natanko takrat, ko ima desni inverz.

(3) Funkcija f je bijektivna natanko takrat, ko je obrnljiva.

Dokaz. (1) Recimo, da velja $g \circ f = \mathrm{id}_A$ za neko funkcijo $g : B \to A$. Za poljubna različna $a, a' \in A$ potem velja $g(f(a)) \neq g(f(a'))$, od koder sledi $f(a) \neq f(a')$, kar pomeni, da je f injektivna. Privzemimo sedaj, da je f injektivna. Potem je vsak $b \in B$ ali slika nekega natanko določenega elementa A, ki ga označimo z $g(b)$, ali pa sploh ni v sliki funkcije f. Za vse $b \notin f(A)$ definiramo vrednost $g(b)$ na poljuben način. Iz definicije funkcije g potem sledi $g \circ f = \mathrm{id}_A$.

(2) Za dokaz druge ekvivalence pa uberimo naslednjo pot. Iz $f \circ g = \mathrm{id}_B$ sledi, da poljuben element $b \in B$ lahko zapišemo v obliki $b = f(g(b))$. Torej je b slika elementa $g(b) \in A$, kar pomeni, da je f surjektivna. Obratno, če je f surjektivna, lahko za poljuben $b \in B$ izberemo nek element iz A, ki ga označimo z $g(b)$, da je $f(g(b)) = b$. Za tako definirano funkcijo g potem velja enakost $f \circ g = \mathrm{id}_B$.

(3) Tretja ekvivalenca sledi iz prvih dveh. $\square$

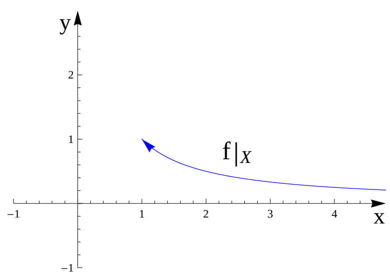
Naj bo $f : A \to B$ funkcija in $X \subset A$ podmnožica. *Zožitev* oziroma restrikcija funkcije f na množico X je funkcija

$$f|_X : X \to B,$$
$$f|_X : x \mapsto f(x).$$

Inkluzija množice X v množico A je preslikava

$$\mathrm{inc} : X \to A,$$
$$\mathrm{inc} : x \mapsto x.$$

Zgled. Poglejmo si še enkrat funkcijo $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ s predpisom $f(x) = \frac{1}{x}$ in vzemimo $X = (1, \infty)$. Graf restrikcije funkcije f na množico X dobimo, tako da pogledamo samo tisti del grafa funkcije f, ki leži nad množico X.



Moč množic

Poleg enakosti ločimo množice med sabo tudi glede na njihovo velikost. Pri končnih množicah z definicijo velikosti nimamo težav, se nam pa stvari lahko zdijo čudne, ko se začnemo ukvarjati z neskončnimi množicami. Pri matematični definiciji velikosti množic si pomagamo z bijekcijami.

Definicija 6. *Množici A in B sta ekvipolentni oziroma enako močni, če obstaja bijekcija med njima.*

Dejstvo, da sta množici A in B ekvipolentni, označimo z $|A| = |B|$. Ekvipolenca množic je ekvivalenčna relacija, kar pomeni, da iz $|A| = |B|$ in $|B| = |C|$ sledi $|A| = |C|$. Za nas bodo zanimive predvsem končne, števno neskončne in pa množice, ki imajo moč kontinuuma.

Naj bo sedaj A poljubna množica.

· A ima n *elementov*, če je ekvipolentna množici $\{1, 2, \ldots, n\}$ za nek $n \in \mathbb{N}$.

· A je *končna*, če je prazna ali ima n elementov za nek $n \in \mathbb{N}$.

· A je *neskončna množica*, če ni končna.

· A je *števno neskončna*, če je ekvipolentna množici naravnih števil $\mathbb{N}$.

· A je *števna*, če je končna ali števno neskončna.

Dve končni množici sta ekvipolentni natanko takrat, ko imata enako število elementov. Če je množica A števno neskončna, obstaja bijekcija $f : \mathbb{N} \to A$. V praksi to pomeni, da s preslikavo f elemente množice A oštevilčimo oziroma uredimo po vrsti.

Zgled. (1) Poglejmo si množico $2\mathbb{N}$ vseh sodih naravnih števil, torej

$$2\mathbb{N} = \{\, 2n \,|\, n \in \mathbb{N}\} = \{2, 4, 6, \ldots\}.$$

Po občutku bi rekli, da ima množica $2\mathbb{N}$ manj elementov kot množica $\mathbb{N}$, saj je pol manjša. Kljub temu pa sta ti dve množici enako močni, saj obstaja bijekcija $f : \mathbb{N} \to 2\mathbb{N}$, definirana s predpisom

$$f(n) = 2n.$$

Njen inverz je funkcija $f^{-1} : 2\mathbb{N} \to \mathbb{N}$, definirana s predpisom $f^{-1}(m) = \frac{m}{2}$.

(2) Pokažimo sedaj, da je množica $\mathbb{N} \times \mathbb{N}$ števno neskončna. Elemente množice $\mathbb{N} \times \mathbb{N}$ lahko razporedimo v tabelo

$$\begin{array}{cccc} (1,1) & (1,2) & (1,3) & \ldots \\ (2,1) & (2,2) & (2,3) & \ldots \\ (3,1) & (3,2) & (3,3) & \ldots \\ \vdots & \vdots & \vdots & \end{array}$$

Definirajmo sedaj bijekcijo $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, tako da elemente množice $\mathbb{N} \times \mathbb{N}$ štejemo po 'diagonalah' v vrstnem redu $(1, 1), (2, 1), (1, 2), (3, 1), (2, 2), \ldots$.

Lastnost, ki smo jo spoznali v zgornjem primeru, je ključna lastnost neskončnih množic. Neskončna množica je namreč lahko enako močna kot kakšne njene prave podmnožice; na kar se seveda moramo privaditi.

Poglejmo si nekaj načinov, kako lahko iz števnih množic konstruiramo nove števne množice.

Trditev 7. *Podmnožica števno neskončne množice je števna množica.*

Dokaz. Vsako števno neskončno množico si lahko s pomočjo bijekcije predstavljamo kar kot množico naravnih števil, zato je dovolj trditev pokazati za množico $\mathbb{N}$.

Naj bo $A \subseteq \mathbb{N}$. Izberimo najprej najmanjši element A, nato drugi najmanjši element A, nato tretji najmanjši element A in podobno naprej. Če se ta postopek ustavi po nekaj korakih, je množica A končna. V nasprotnem primeru pa nam opisani postopek definira neko funkcijo $f : \mathbb{N} \to A$, ki je injektivna po definiciji. Ker ima vsak element A le končno mnogo elementov pred njim, bomo z našim postopkom našteli vse elemente množice A. Torej je funkcija f tudi surjektivna, kar pomeni, da je A števno neskončna množica. $\square$

Trditev 8. *Unija števno mnogo števnih množic je števna množica.*

Dokaz. Brez škode za splošnost lahko predpostavimo, da so vse množice števno neskončne. Naj bo $\mathcal{A} = \cup_{i\in\mathbb{N}} A_i$. Ker so vse množice A_i števne, lahko elemente množice A_i npr. naštejemo po vrsti $a_{i1}, a_{i2}, a_{i3}, \ldots$ in vse skupaj razporedimo v tabelo

$$\begin{matrix} a_{11} & a_{12} & a_{13} & \cdots \\ a_{21} & a_{22} & a_{23} & \cdots \\ a_{31} & a_{32} & a_{33} & \cdots \\ \vdots & \vdots & \vdots & \end{matrix}$$

Definirajmo sedaj funkcijo $f : \mathbb{N} \to \mathcal{A}$, tako da elemente množice $\mathcal{A}$ štejemo po 'diagonalah' v vrstnem redu $a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, a_{14}, \ldots$ Tako definirana funkcija f je surjekcija, ni pa nujno injekcija, če množice A_i niso paroma disjunktne. V tem primeru lahko iz tabele izbrišemo nekaj elementov, tako da se vsak element pojavi samo enkrat. S to modifikacijo dobimo bijekcijo f, ki pokaže, da je $\mathcal{A}$ števna množica. $\square$

Če izberemo $A_i = \{\frac{n}{i} \,|\, n \in \mathbb{Z}\}$, dobimo kot posledico Trditve 8.

Posledica 9. *Množica racionalnih števil* $\mathbb{Q}$ *je števna.*

Trditev 10. *Produkt dveh (ali končno mnogo) števnih množic je števna množica.*

Dokaz. Spet lahko privzamemo, da je $A = B = \mathbb{N}$. Potem je

$$\mathbb{N} \times \mathbb{N} = \{\, (m, n) \,|\, m, n \in \mathbb{N}\} = \bigcup_{i=0}^{\infty} \{\, (i, n) \,|\, n \in \mathbb{N}\}.$$

Vse množice v zgornji uniji so števne, zato je tudi $\mathbb{N} \times \mathbb{N}$ števna množica po Trditvi 8. Če zgornji sklep nekajkrat ponovimo, lahko dokažemo trditev tudi za produkt končno mnogo množic. □

Zgoraj smo spoznali nekaj tipičih primerov števnih množic. Niso pa vse neskončne množice števne. Realnih števil, ki jih bomo podrobneje spoznali v naslednjem poglavju, je *neštevno* mnogo (torej jih ne moremo prešteti). Zaenkrat si poglejmo samo idejo dokaza tega dejstva.

Trditev 11. *Množica realnih števil* $\mathbb{R}$ *ni števna.*

Dokaz. Trditev bomo dokazali s protislovjem s pomočjo tako imenovanega diagonalnega trika.

Če bi bila $\mathbb{R}$ števna, bi bila po Trditvi 7 tudi množica $[0, 1) \subset \mathbb{R}$ števna. Denimo torej, da znamo elemente množice $[0, 1)$ prešteti

$$[0, 1) = \{x_1, x_2, x_3, \ldots\}.$$

Sedaj bomo uporabili dejstvo, da lahko vsako realno število $x \in [0, 1)$ enolično zapišemo v obliki $0, a_1 a_2 a_3 \ldots$, kjer je $a_k \in \{0, 1, 2, \ldots, 9\}$ in z dodatno predpostavko, da se cifra 9 ne ponavlja od nekod dalje. Potem je

$$\begin{aligned}
x_1 &= 0, a_1^1 a_2^1 a_3^1 \ldots, \\
x_2 &= 0, a_1^2 a_2^2 a_3^2 \ldots, \\
x_3 &= 0, a_1^3 a_2^3 a_3^3 \ldots, \\
&\vdots
\end{aligned}$$

Konstruirajmo sedaj število $y = 0, b_1 b_2 b_3 \ldots \in [0, 1)$ z zahtevo

$$b_k = \begin{cases} 1 & ;\ a_k^k \neq 1, \\ 2 & ;\ a_k^k = 1. \end{cases}$$

Število y se od števila x_k razlikuje na k-ti decimalki, kar pomeni, da je različno od vseh števil x_k. To pa nas privede v protislovje s predpostavko, da je $[0, 1) = \{x_1, x_2, x_3, \ldots\}$. □