Poglavje 3

Množice

Teorija množic je razmeroma mlada veja matematike; njen začetnik je bil nemški matematik Georg Cantor v drugi polovici 19. stoletja. V začetku 20. stoletja so jo matematiki privzeli kot univerzalni jezik, v katerem je mogoče izražati matematične ideje in pojme. Preden lahko začnemo graditi stavbo matematike, torej definirati pojme in dokazovati izreke, si izberemo *osnovne pojme*, s pomočjo katerih definiramo vse druge pojme, in *aksiome*, iz katerih izpeljujemo vse druge trditve in izreke. Seveda si želimo, da bi bilo osnovnih (nedefiniranih) pojmov čim manj. V zgodovini matematike so bili osnovni pojmi npr. *točka, premica, ravnina, število, relacija, funkcija* itd., v teoriji množic pa je edini osnovni pojem *množica.* V 20. stoletju se je razvilo več alternativ teoriji množic, kot so npr. *teorija kategorij*, kjer sta osnovna pojma dva: *objekt* in *morfizem*, λ*-račun*, kjer je edini osnovni pojem *funkcija*, in še druge *teorije tipov*, vendar večina sodobne matematike še vedno temelji na teoriji množic. Obstaja več različic teorije množic, npr. von Neumann – Bernays – Gödlova teorija (NBG), Zermelo – Fraenklova teorija (ZF) ter Zermelo – Fraenklova teorija množic z aksiomom izbire (ZFC), ki jo bomo uporabljali tudi mi. V teoriji ZFC je *vsak* objekt neka množica.

Zgled 1 *V teoriji ZFC naravna števila definiramo kot množice takole:*

$$\begin{aligned}
0 &= \{\} = \emptyset \quad \text{prazna množica} \\
1 &= \{0\} \\
2 &= \{0, 1\} \\
&\vdots \\
n &= \{0, 1, 2, \ldots, n-1\} \\
&\vdots
\end{aligned}$$

Pripomba o pisavi. Kadar v logiki ali lingvistiki opisujemo jezik J_1 v jeziku J_2, imenujemo J_1 *objektni jezik*, J_2 pa *métajêzik.* V prejšnjem poglavju smo opisali jezik PR v slovenščini, torej je bil jezik PR objektni jezik, slovenščina pa metajezik. V nadaljevanju bo jezik PR naš metajezik, v katerem bomo opisovali objektni jezik teorije množic. Da bo šlo laže in hitreje, bomo v ta namen nekoliko razrahljali stroga pravila predikatnega računa. Za individualne spremenljivke bomo uporabljali vse črke (male in velike, z začetka in s konca abecede), za individualne konstante pa posebne simbole, kot so $\emptyset$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $0, 1, 2, \ldots$ Zaradi krajšega pisanja bomo univerzalne kvantifikatorje na začetku izjavnih formul pogosto opuščali in formule, ki niso zaprte, interpretirali kot njihova univerzalna zaprtja. Pri dokazovanju oziroma izpeljevanju implikacije $\varphi \Rightarrow \psi$ preko vmesnih posledic njenega antecedensa $\varphi_1, \varphi_2, \ldots, \varphi_n$ bomo namesto

$$(\varphi \Rightarrow \varphi_1) \wedge (\varphi_1 \Rightarrow \varphi_2) \wedge \cdots \wedge (\varphi_{n-1} \Rightarrow \varphi_n) \wedge (\varphi_n \Rightarrow \psi) \tag{3.1}$$

neformalno pisali kar

$$\varphi \Rightarrow \varphi_1 \Rightarrow \varphi_2 \Rightarrow \cdots \Rightarrow \varphi_{n-1} \Rightarrow \varphi_n \Rightarrow \psi \tag{3.2}$$

čeprav izraza (3.1) in (3.2) nista enakovredna. Da je v resnici mišljen izraz (3.1), bo razvidno iz konteksta. Podobno bomo ravnali tudi pri dokazovanju oziroma izpeljevanju ekvivalence $\varphi \Leftrightarrow \psi$ preko vmesnih ekvivalentnih formul.

3.1 Relacija pripadnosti ($\in$) in podajanje množic

Osnovna relacija v teoriji množic je ***relacija pripadnosti*** $\in$. Zapis $a \in A$ preberemo *a pripada A* ali *a je element A*. Zapis $a \notin A$ uporabljamo kot okrajšavo za formulo $\neg(a \in A)$.

Kako podamo množico? Odgovor nam ponuja

Aksiom ekstenzionalnosti (AE). $\forall x\colon (x \in A \Leftrightarrow x \in B) \implies A = B$.

Z besedami: *Množici, ki imata iste elemente, sta enaki*, oziroma: *Množica je določena s svojimi elementi.* Ta ugotovitev ni trivialna, saj bi lahko množice poleg elementov imele še druge atribute, npr. barvo, obliko ali okus. Potem bi rdeča in modra množica naravnih števil imeli iste elemente, a ne bi bili enaki. Po zaslugi aksioma ekstenzionalnost pa lahko množico določimo že s tem, da povemo, kaj so njeni elementi. Za majhne končne množice jih lahko kar naštejemo, npr.:

$$A \;=\; \{1, 4, 9\}.$$

V splošnem pa se to ne da. Zato množico definiramo z neko izjavno formulo $\varphi(x)$, v kateri prosto nastopa le spremenljivka x, in sicer takole:

$$A \;=\; \{x;\ \varphi(x)\} \tag{3.3}$$

Ta zapis pomeni, da množici A pripadajo natanko tisti objekti a, za katere je resnična izjava $\varphi(a)$, oziroma:

$$\forall x\colon (x \in A \;\Leftrightarrow\; \varphi(x)). \tag{3.4}$$

Zapis oziroma formula (3.3) je le okrajšava za formulo (3.4).

Zgled 2

$A_1 = \{x;\ x \in \mathbb{R} \ \wedge\ x > 0\}$ je množica vseh pozitivnih realnih števil.
$A_2 = \{x;\ \exists y\colon (y \in \mathbb{N} \ \wedge\ x = 2y + 1)\}$ je množica vseh lihih naravnih števil.
$A_3 = \{x;\ x = 1 \vee x = 4 \vee x = 9\}$ je množica $\{1, 4, 9\}$.
$A_4 = \{x;\ x \neq x\}$ je prazna množica $\emptyset$.
$A_5 = \{x;\ x \notin x\}$ je ***Russellova množica***.

Množico A_5 je definiral leta 1901 Bertrand Russell. Njeni elementi so vse "običajne" množice, ki ne vsebujejo same sebe kot element. Primeri množic, ki bi lahko vsebovale same sebe kot element:

– množica vseh nepraznih množic,
– množica vseh množic z vsaj tremi elementi,
– množica vseh množic.

Russell si je zastavil vprašanje: Ali je $A_5 \in A_5$? Po definiciji množice A_5 velja:

$$A_5 \in A_5 \iff \varphi(A_5), \quad \text{kjer je } \varphi(x) \text{ formula } x \notin x,$$

torej $A_5 \in A_5 \iff A_5 \notin A_5$. To protislovje, ki se imenuje ***Russellova antinomija***, je v začetku 20. stoletja povzročilo pravi pretres v osnovah matematike. Kako to protislovje razrešimo?

V enem od zgledov v prejšnjem poglavju smo pokazali, da je izjavna formula

$$\psi \;=\; \exists y \forall x\colon (R(x,y) \iff \neg R(x,x))$$

protislovna, torej lažna v vsaki interpretaciji. Vzemimo interpretacijo I, kjer je

$$D = \{x;\ x = x\} \ \ldots \ \text{razred vseh množic,}$$
$$R(x,y) \ \ldots \ \text{relacija pripadnosti } x \in y.$$

V tej interpretaciji se formula ψ glasi: $\exists y \forall x\colon (x \in y \iff x \notin x)$, oziroma:

Obstaja množica, ki vsebuje natanko vse tiste množice,
ki ne vsebujejo same sebe kot element.

Ker je formula ψ protislovna, je gornja izjava lažna. To pa pomeni, da Russellova množica A_5 ***ne obstaja***!

Nauk Russellove antinomije: Pri podajanju množic z izjavno formulo $\varphi(x)$ moramo biti previdni, saj nekatere takšne formule vodijo v protislovje. Teorije, v katerih lahko izpeljemo protislovje, imenujemo *protislovne teorije*; takšnih teorij pa se močno bojimo. Izjavni izraz $0 \Rightarrow p$ je namreč tavtologija, in če smo izpeljali protislovje 0, po pravilu MP dobimo

$$0,\ 0 \Rightarrow p \models p.$$

V protislovni teoriji lahko torej dokažemo *vsako* trditev, kar pomeni, da so takšne teorije povsem brez vrednosti.

Russellovi antinomiji se skušamo izogniti na različne načine.

A) V teoriji NBG za osnovni pojem vzamemo *razred*, množice pa definiramo kot poseben primer razredov.

Definicija 1 *Razred A je* množica*, če obstaja razred B, tako da je $A \in B$. V nasprotnem primeru imenujemo A* pravi razred*.*

Oznaka: Enomestni predikat $M(x)$ je okrajšava za izjavno formulo $\exists y : x \in y$. Preberemo ga kot "x je množica".

Razred definiramo z neko izjavno formulo $\varphi(x)$, v kateri prosto nastopa le spremenljivka x, pri čemer pa dodatno zahtevamo, da so elementi razreda le tisti razredi, *ki so množice:*

$$A \;=\; \{x;\ \varphi(x) \wedge M(x)\}. \tag{3.5}$$

Velja torej: $a \in A \;\Leftrightarrow\; \varphi(a) \wedge M(a)$. Definirajmo ***Russellov razred*** R takole:

$$R \;=\; \{x;\ x \notin x \,\wedge\, M(x)\}.$$

Ali je $R \in R$? Po definiciji razreda R velja: $R \in R \iff R \notin R \wedge M(R)$. Poenostavimo to ekvivalenco z uporabo enakovrednosti $p \Leftrightarrow q \sim (p\wedge q)\vee(\neg p\wedge\neg q)$, pa dobimo:

$$\begin{aligned}
& R \in R \iff R \notin R \wedge M(R) \\
\sim\ & (R \in R \wedge R \notin R \wedge M(R)) \ \vee\ (R \notin R \wedge \neg(R \notin R \wedge M(R))) \\
\sim\ & R \notin R \wedge \neg(R \notin R \wedge M(R)) \\
\sim\ & R \notin R \wedge (R \in R \vee \neg M(R)) \\
\sim\ & (R \notin R \wedge R \in R) \vee (R \notin R \wedge \neg M(R)) \\
\sim\ & R \notin R \wedge \neg M(R)
\end{aligned}$$

Za razliko od Russellove množice nas Russellov razred R ne pripelje do protislovja, temveč le do ugotovitve, da R ni množica, ampak je pravi razred (in zato seveda ne vsebuje samega sebe kot element, saj bi sicer bil množica).

Pravih razredov ne smemo uporabljati za elemente drugih razredov. V teoriji NBG privzamemo aksiome, ki za nekatere (ne "prevelike") razrede zagotavljajo, da so množice.

B) V teoriji ZFC je edini osnovni pojem množica, privzamemo pa eksistenčne aksiome, ki za nekatere (ne "prevelike") množice zagotavljajo, da obstajajo. Za množice, s katerimi delamo, najprej dokažemo, da obstajajo. Preden vstopimo v teorijo ZFC, privzemimo *standardno interpretacijo* I njenih izjavnih formul:

$$\begin{aligned} D = V = \{x;\ x = x\} & \ \ldots\ \text{razred vseh množic,} \\ x \in y & \ \ldots\ \text{relacija pripadnosti,} \\ x = y & \ \ldots\ \text{relacija enakosti.} \end{aligned}$$

3.2 Relacije med množicami

Oglejmo si še druge pomembne dvomestne relacije med množicami.

3.2.1 Relacija enakosti (=)

Enakost objektov v matematiki pojmujemo kot *istost* (oziroma *identičnost*). Privzamemo, da za relacijo enakosti velja:

Načelo zamenljivosti enakega z enakim (EE) Če je $A = B$, potem vse tisto, kar velja za A, velja tudi za B, in vse tisto, kar velja za B, velja tudi za A.

Trditev 1 $A = B \iff \forall x\colon (x \in A \Leftrightarrow x \in B)$

Dokaz: $(\Rightarrow)$ Naj bo $A = B$ in naj bo x neka množica. Če je $x \in A$, je po načelu EE tudi $x \in B$. In če je $x \in B$, je po načelu EE tudi $x \in A$, torej velja $x \in A \Leftrightarrow x \in B$. Ker je bila množica x poljubna, velja $\forall x\colon (x \in A \Leftrightarrow x \in B)$.

$(\Leftarrow)$ To je aksiom ekstenzionalnosti (AE). □

Množici sta torej enaki natanko tedaj, ko imata iste elemente.

Zgled 3 1. $\{a, b\} = \{b, a\}$ *(neurejen) par*

2. $\{a, a, a\} = \{a\}$ *enojček* ali *singleton*

3. $\{b, c, a, a, c, b, a\} = \{a, b, c\}$

Po trditvi 1 pri naštevanju elementov množice vrstni red ni pomemben, prav tako ne, kolikokrat navedemo posamezen element.

Posledica 1 (i) $A = A$ *(refleksivnost enakosti)*

(ii) $A = B \implies B = A$ *(simetričnost enakosti)*

(iii) $A = B \wedge B = C \implies A = C$ *(tranzitivnost enakosti)*

Dokaz: (i) Očitno velja $\forall x\colon (x \in A \Leftrightarrow x \in A)$, torej je po trditvi 1 $A = A$.

(ii) Iz formule $\forall x\colon (x \in A \Leftrightarrow x \in B)$ zaradi komutativnosti ekvivalence sledi $\forall x\colon (x \in B \Leftrightarrow x \in A)$, torej po trditvi 1 velja $A = B \implies B = A$.

(iii)

$$\begin{aligned} A = B \wedge B = C &\overset{\text{trd. 1}}{\iff} \forall x\colon (x \in A \Leftrightarrow x \in B) \wedge \forall x\colon (x \in B \Leftrightarrow x \in C) \\ &\overset{\text{PR}}{\iff} \forall x\colon ((x \in A \Leftrightarrow x \in B) \wedge (x \in B \Leftrightarrow x \in C)) \\ &\overset{2\times\text{ HS}}{\implies} \forall x\colon (x \in A \Leftrightarrow x \in C) \\ &\overset{\text{trd. 1}}{\iff} A = C \surd \end{aligned}$$

□

3.2.2 Relacija inkluzije ($\subseteq$)

Definicija 2

$$A \subseteq B \iff \forall x\colon (x \in A \Rightarrow x \in B)$$

Beremo: *A je podmnožica B*, ali tudi: *A je vsebovana v B*. Namesto $\neg(A \subseteq B)$ pišemo $A \nsubseteq B$.

Trditev 2

$$A = B \iff A \subseteq B \wedge B \subseteq A.$$

Dokaz:

$$\begin{aligned} A = B &\overset{\text{trd. 1}}{\iff} \forall x\colon (x \in A \Leftrightarrow x \in B) \\ &\overset{\text{IR}}{\iff} \forall x\colon ((x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)) \\ &\overset{\text{PR}}{\implies} \forall x\colon (x \in A \Rightarrow x \in B) \wedge \forall x\colon (x \in B \Rightarrow x \in A) \\ &\overset{\text{def. 2}}{\iff} A \subseteq B \wedge B \subseteq A \surd \end{aligned}$$

□

Aksiom, ki vsebuje poljubne izjavne formule, imenujemo *aksiomska shema*; takšna shema predstavlja neskončno mnogo aksiomov. Naslednja aksiomska shema, s katero se ZFC izogne Russellovi antinomiji, zagotavlja, da za vsako množico obstaja podmnožica vseh tistih elementov, ki zadoščajo dani izjavni formuli $\varphi(x)$.

Aksiomska shema o podmnožicah (ASP). Če množica B obstaja in je $\varphi(x)$ izjavna formula, v kateri le spremenljivka x lahko nastopa prosto, obstaja tudi množica $A = \{x;\ x \in B \ \land\ \varphi(x)\}$, ali s formulo:

$$\forall B\, \exists A\, \forall x\colon (x \in A \iff x \in B \ \land\ \varphi(x)).$$

Definicija 3 *Množica A je* prazna, *če velja $\forall x\colon x \notin A$.*

Posledica 2 *Prazna množica obstaja.*

Dokaz: V ASP za $\varphi(x)$ vzemimo izjavno formulo $x \neq x$. Potem velja:

$$\begin{aligned}
&\forall B\, \exists A\, \forall x\colon (x \in A \iff x \in B \ \land\ x \neq x) \\
\overset{\text{refl.}=}{\iff}\ &\forall B\, \exists A\, \forall x\colon (x \in A \iff x \in B \ \land\ 0) \\
\overset{\text{IR}}{\iff}\ &\forall B\, \exists A\, \forall x\colon (x \in A \iff 0) \\
\overset{\text{IR}}{\iff}\ &\forall B\, \exists A\, \forall x\colon x \notin A \\
\overset{\text{PR}}{\iff}\ &\exists A\, \forall x\colon x \notin A \ \surd
\end{aligned}$$

□

Posledica 3 *Razred vseh množic $V = \{x;\ x = x\}$ je pravi razred.*

Dokaz: Recimo, da je V množica. Potem po ASP obstaja tudi množica

$$A = \{x;\ x \in V \land x \notin x\} = \{x;\ 1 \land x \notin x\} = \{x;\ x \notin x\};$$

to pa je ravno Russellova množica A_5, za katero že vemo, da ne obstaja. Torej V ni množica, ampak pravi razred. □

Zaenkrat le za eno množico vemo, da zares obstaja, to je prazna množica. Obstoj nadaljnjih množic si v ZFC zagotovimo z *eksistenčnimi aksiomi.*

Aksiom o paru (AP). Če obstajata množici u in v, obstaja tudi množica $A = \{x;\ x = u \lor x = v\} = \{u, v\}$, ali s formulo:

$$\forall u\, \forall v\, \exists A\, \forall x\colon (x \in A \iff x = u \ \lor\ x = v).$$

Posledica 4 *Če obstaja množica u, obstaja tudi množica $A = \{x;\ x = u\} = \{u\}$.*

Dokaz: V aksiomu o paru vzamemo $v = u$ in dobimo množico $\{u, u\}$. $\square$

Zgled 4 Število $0 = \emptyset$ obstaja po posledici 2.
Število $1 = \{0\}$ obstaja po posledici 4.
Število $2 = \{0, 1\}$ obstaja po aksiomu o paru.

Izrek 1 (lastnosti inkluzije) *Za vse množice A, B, C velja:*
(i) $A \subseteq A$ *(refleksivnost inkluzije)*
(ii) $A \subseteq B \wedge B \subseteq A \implies A = B$ *(antisimetričnost inkluzije)*
(iii) $A \subseteq B \;\wedge\; B \subseteq C \implies A \subseteq C$ *(tranzitivnost inkluzije)*
(iv) $\emptyset \subseteq A$
(v) $A \subseteq \emptyset \iff A = \emptyset$

Dokaz: (ii): To je polovica trditve 2.
(v):

$$\begin{aligned} A \subseteq \emptyset &\overset{\text{def.}\subseteq}{\iff} \forall x\colon (x \in A \implies x \in \emptyset) \\ &\overset{\text{def.}\,\emptyset}{\iff} \forall x\colon (x \in A \implies 0) \\ &\overset{\text{IR}}{\iff} \forall x\colon x \notin A \\ &\overset{\text{def.}\,\emptyset}{\iff} A = \emptyset \;\checkmark \end{aligned}$$

$\square$