Logika in množice

Andrej Bauer | Davorin Lešnik

© 2026 Andrej Bauer in Davorin Lešnik

To delo je objavljeno pod licenco Creative Commons Priznanje avtorstva-Nekomercialno-Brez predelav 4.0 Mednarodna (CC BY-NC-ND 4.0). Izvorna koda učbenika je dostopna na naslovu github.com/andrejbauer/ucbenik-logika-in-mnozice.

Kazalo

Predgovor **1**

1 Osnovno o množicah in preslikavah **3**
1.1 Pravilo ekstenzionalnosti 4
1.2 Končne množice 5
1.3 Preslikave 8
1.4 Vaje 20

2 Aritmetika množic **21**
2.1 Zmnožek 22
2.2 Vsota 24
2.3 Eksponent 26
2.4 Preslikave višjega reda 26
2.5 Izomorfizem množic 28
2.6 Aritmetika množic 32
2.7 Vaje 36

3 Simbolni zapis **39**
3.1 Pisave in simboli 40
3.2 Izrazi 42
3.3 Slike in diagrami 45
3.4 Logične formule 46
3.5 Kako beremo in pišemo simbolni zapis 52
3.6 Definicije 57
3.7 Enolični obstoj 59

3.8 Enolični opis 60
3.9 Vaje 60

4 Dokazi **63**
4.1 Kaj je matematični dokaz? 63
4.2 Struktura dokaza 65
4.3 Pravila vpeljave in uporabe 69
4.4 Enakost in ekvivalenca 76
4.5 Pravilo o izključenem tretjem 78
4.6 Brez izgube za splošnost 83

5 Boolova algebra **85**
5.1 Izjavni in predikatni račun 85
5.2 Resničnostne tabele 86
5.3 Tavtologije 87
5.4 Disjunktivna in konjunktivna oblika 89
5.5 Boolova algebra 91

Literatura **97**

Predgovor

Pri predmetu Logika in množice v prvem letniku študija matematike na Fakulteti za matematiko in fiziko Univerze v Ljubljani se študenti učijo osnov matematičnega izražanja—kako beremo in pišemo matematično besedilo in simbolni zapis—hkrati pa spoznavajo temelje matematične logike in teorije množic. Pred študenti matematike je torej težka naloga učiti se novo snov v novem žargonu.

Da bo učbenik v pomoč, bomo pri matematičnem izražanju bolj natančni, kot je to običajno za matematično besedilo. Pojasnjevali bomo, kako matematiki pišejo, govorijo in razmišljajo v praksi ter marsikaj raje zapisali na dolgo, da bo začetniku bolj prijazno. Bližnjice, ki jih ubirajo izkušeni matematiki, bomo vpeljali zlagoma, hkrati pa opozarjali na nedoslednosti, ki so večinoma ostanki zgodovinskega razvoja matematike in ki se jim matematična tradicija stežka odreče. Ne zamerite nam, če dobrohotno ponudimo še kak nasvet o študiju matematike.

Zahvala. Za pomoč pri urejanju zapiskov in opozarjanje na napake se zahvaljujeva študentkam in študentom: Luka Debevc, Milan Djaković, Matija Fajfar, Ema Grmšek, Miha Gyergyek, Peter Jereb, Jan Kastelic, Jan Malej, Matej Marinko, Jan Pantner, Luka Ponikvar, Lev Rus, Jakob Schrader, Matija Sirk, Matej Šafarič, Gal Zmazek, Marjetka Zupan, Patrik Žnidaršič in vsi, ki sva jih pozabila omeniti. Vse preostale napake so najina last.

Andrej Bauer in Davorin Lešnik

1

Osnovno o množicah in preslikavah

Temeljni gradniki sodobne matematike so ***množice***, ki so skupki ali zbirke matematičnih objektov, lahko spet množic. Vsaka množica sestoji iz ***elementov*** in je z njimi natančno določena. Kadar je a element množice M, to zapišemo

$$a \in M$$

in beremo »*a je element M*« ali »*a pripada M*«. Slišali boste tudi »*a je vsebovan v M*«, a to rabo odsvetujemo, ker tudi $A \subseteq M$ beremo »*A je vsebovan v M*«.

V splošni razpravi o množicah, ki bi presegala meje ožje matematične vede, bi se opirali na zgodovinski in družbeni kontekst, jezikovni izvor in rabo besed ‘množica’, ‘skupek’ in ‘zbirka’, kognitivno analizo, eksperimente, filozofijo itn. Vsi ti vidiki so za matematike izjemno koristni, saj iz takih ‘predmatematičnih’ obravnav črpamo sveže zamisli in matematiko naredimo zares uporabno. Ko pa delujemo znotraj matematike, zunanje vplive odmislimo in se zanašamo le še na pravila logičnega sklepanja in dogovorjene matematične zakone, da ne prihaja do nejasnosti in dvomljivih sklepov.

Kot matematiki lahko ustvarimo takšen ali drugačen pojem množice in pri tem imamo popolno svobodo. Se množica lahko spreminja ali vedno vsebuje iste elemente? Je pomemben vrstni red elementov v množici? Sme množica biti element same sebe? Ali morajo biti elementi množice izračunljivi? To so

vprašanja, ki nimajo enoznačnega odgovora. In res je znanih več med seboj nezdružljivih zvrsti teorije množic, ki matematično opredeljujejo različne vidike običajnega razumevanja besede ‘množica’. Mi bomo spoznali tisto, ki jo uporablja velika večina matematikov.

Še enkrat poudarimo, da ima vsakdo, še posebej pa mladi um, popolno svobodo matematičnega ustvarjanja. Želite razmišljati o drugačnih množicah, ki ne zadoščajo pravilom iz tega učbenika? Ali pa o številih, ki zadoščajo zakonu $x + x = 0$? O geometriji, v kateri skozi točko lahko potegnemo dve vzporednici k dani premici? Kar dajte! Pri tem vas le prosimo, celo zahtevamo, da razmišljate temeljito, vztrajno in globoko, da ste iskreni do sebe in ostalih ter da svoje zamisli in spoznanja predstavite na matematikom razumljiv način.

1.1 Pravilo ekstenzionalnosti

Zamisel, da je množica natančno določena s svojimi elementi, izrazimo z matematičnim zakonom, ki mu pravimo ***pravilo ekstenzionalnosti***:

Pravilo 1.1 (Ekstenzionalnost množic)**.** Množici sta enaki, če vsebujeta iste elemente.

Kaj pravzaprav pomeni, da je to »*pravilo*«, »*matematični zakon*« ali »*načelo*«? So ga razglasili v parlamentu, je to zakon narave, ali morda dogma, ki jo je razglasil profesor na predavanjih? Bodo tisti, ki pravila ekstenzionalnosti ne spoštujejo, deležni lešnikove masti? Ne. Matematični zakoni so *dogovori*, nekakšna pravila matematične igre. Skozi čas so se uveljavila tista, ki so bila uporabna v naravoslovju in tehniki, ali pa so v njih matematiki prepoznali notranjo lepoto in lastno uporabno vrednost.

V matematiki je izbor besed, s katerimi poimenujemo pojme, hkrati pomemben in nebistven. S povsem človeškega stališča je pomembno, da izbiramo besede, katerih predhodni vsakdanji pomen nakazuje matematični pomen. Hkrati je izbor besed nebistven, saj strukturo, lastnosti in povezave med matematičnimi objekti določajo izključno dogovorjeni matematični zakoni in ne raba besed izven polja matematike. Če bi se dogovorili, da namesto besed ‘množica’ in ‘element’ govorimo ‘zbor’ in ‘član’, ali celo ‘morje’ in ‘riba’, se matematična vsebina teorije morja ne bi čisto nič spremenila. Čeprav se to sliši zabavno, ne gre izzivati svojih stanovskih kolegic in kolegov.

1.2 Končne množice

Vrnimo se k našim množicam. Pravilo ekstenzionalnosti nam pove, da lahko množico podamo tako, da natančno opredelimo njene elemente. A to ne pomeni, da množica obstaja, brž ko jo lahko natančno opredelimo! Ta pot vodi v protislovje, ki ga je odkril Bertrand Russell[1] na začetku 20. stoletja in ga bomo obravnavali v razdelku **??**. Iz zagate so se matematiki rešili s previdno izbranimi pravili, ki določajo dopustne konstrukcije množic.

Posebej preprosta konstrukcija združi končen nabor matematičnih objektov v množico. Na primer, če so a, b in c matematični objekti, potem lahko tvorimo množico

$$\{a, b, c\}$$

katere elementi so natanko a, b in c. To pomeni, da za vsak matematični objekt x velja

$$x \in \{a, b, c\}, \text{ če in samo če } x = a \text{ ali } x = b \text{ ali } x = c.$$

Fraza »*če in samo če*« pomeni:

1. če $x = a$ ali $x = b$ ali $x = c$, potem $x \in \{a, b, c\}$ in
2. če $x \in \{a, b, c\}$, potem $x = a$ ali $x = b$ ali $x = c$.

Prva trditev zagotavlja $1{+}1 \in \{1, 2, 3\}$, ker velja vsaj ena od možnosti: $1{+}1 = 1$ ali $1 + 1 = 2$ ali $1 + 1 = 3$. Iz druge trditve sledi, da $5 \in \{1, 2, 3\}$ ne velja, ker ne velja nobena od možnosti: $5 = 1$ ali $5 = 2$ ali $5 = 3$.

Poskusimo zapisati splošno pravilo, ki zajema zgornje primere.

Pravilo 1.2. Za poljuben končen nabor objektov $a, b, \ldots, z$ je $\{a, b, \ldots, z\}$ množica, katere elementi so natanko objekti $a, b, \ldots, z$.

Za trenutek ustavimo tok misli in opozorimo, da zapis s tropičjem '…' ni dovolj natančen, saj dopušča dvoumnosti. Denimo, so elementi množice

$$\{3, 5, 7, \ldots, 31\},$$

liha števila med 3 in 31, ali samo praštevila? Kljub temu tak zapis uporabljamo, ker v praksi bralec večinoma pravilno ugane, kaj je bilo mišljeno, saj imamo ljudje zelo podobne sposobnosti prepoznavanja vzorcev. Z matematičnega vidika pa to ni dopustno, ker lahko tropičje *vedno* razumemo na več načinov.

[1] Bertrand Arthur William Russell (1872–1970), angleški filozof, logik in matematik.

Pa tu še ni konec težav z zapisom pravila 1.2. Ali smemo tvoriti množico, ki ima več elementov, kot je črk abecede? Ali bi bilo pravilo še vedno isto, če bi namesto $a, b, \ldots, z$ zapisali $a, b, \ldots, j$? Ali smemo tvoriti množico z nič elementi? Če namreč vstavimo nič elementov, se pravilo glasi »*Za vse objekte je* $\{\}$ *množica, katere elementi so natanko objekti*«, kar bi učiteljica slovenščine prečrtala z rdečo. Iz nesrečnega tropičja se res ne vidi, kaj je in kaj ni dovoljeno. Iz zagate se bomo izvili malo kasneje, ko bomo pravilo končnih množic nadomestili s tremi bolj preprostimi, ki imajo skupaj enakovreden učinek.

Preverimo, ali ima pravilo ekstenzionalnosti vsaj pričakovani učinek. Če res zagotavlja, da vrstni red in število pojavitev elementov v množici ni pomembno, bi moralo slediti $\{1, 2\} = \{2, 1, 1\}$. Pa je to res?

Trditev 1.3. *Množici* $\{1, 2\}$ *in* $\{2, 1, 1\}$ *sta enaki.*

Dokaz. Dokaz, ki ga bomo zapisali, je izjemno podroben in ga v praksi ne bi zapisali, saj je z njegovim branjem več dela, kot če bi ga poustvarili sami. Ker pa želimo pokazati, da tudi najbolj trivialna dejstva lahko dokažemo, ga zapišimo. Izhajati smemo izključno iz naslednjih dejstev:

- pravilo ekstenzionalnosti,
- $x \in \{1, 2\}$, če in samo če $x = 1$ ali $x = 2$,
- $x \in \{2, 1, 1\}$, če in samo če $x = 2$ ali $x = 1$ ali $x = 1$.

Uporabimo pravilo ekstenzionalnosti na $\{1, 2\}$ in $\{2, 1, 1\}$, kar pomeni, da moramo preveriti, ali imata iste elemente. To naredimo v dveh korakih:

1. Za vsak element $\{1, 2\}$ dokažemo, da je element $\{2, 1, 1\}$.
   Pa naj bo $x \in \{1, 2\}$. Iz definicije množice $\{1, 2\}$ sledi, da je $x = 1$ ali $x = 2$. Obravnavamo dva primera:
   (a) Primer $x = 1$: iz $x = 1$ sledi, da je $x = 2$ ali $x = 1$ ali $x = 1$, zato je $x \in \{2, 1, 1\}$.
   (b) Primer $x = 2$: iz $x = 2$ sledi, da je $x = 2$ ali $x = 1$ ali $x = 1$, zato je $x \in \{2, 1, 1\}$.
2. Za vsak element $\{2, 1, 1\}$ dokažemo, da je element $\{1, 2\}$.
   Ta korak je zelo podoben prvemu, zato bi ga skoraj vsak matematik »*prepustil bralcu za vajo*«, a tokrat se bomo pomujali in ga zapisali. Naj bo $x \in \{2, 1, 1\}$. Iz definicije množice $\{2, 1, 1\}$ sledi, da je $x = 2$ ali $x = 1$ ali $x = 1$. Obravnavamo tri primere:

(a) Primer $x = 2$: iz $x = 2$ sledi, da je $x = 1$ ali $x = 2$, zato je $x \in \{1, 2\}$.
(b) Primer $x = 1$: iz $x = 1$ sledi, da je $x = 1$ ali $x = 2$, zato je $x \in \{1, 2\}$.
(c) Primer $x = 1$: iz $x = 1$ sledi, da je $x = 1$ ali $x = 2$, zato je $x \in \{1, 2\}$.

Dokaz je končan. □

Mimogrede, kvadratek označuje konec dokaza. Imenuje se tudi *halmoš* po Paulu Halmosu,[2] ki ga je popularizíral. Nekateri avtorji pišejo tudi QED, kar je okrajšava za »*quod erat demonstrandum*«, študentska krilatica pa trdi, da je to okrajšava za »*quite easily done*«.

Še enkrat se pojavi dvom o uporabi pravila 1.2. Nikjer ne piše, da smemo pri naštevanju isti element večkrat ponoviti. Je sploh dovoljeno ponavljati elemente končne množice in pisati $\{2, 1, 1\}$? V vsakdanjem življenju je vsaj nenavadno, da stvari po nepotrebnem ponavljamo. V matematiki razumemo besedilo dobesedno. Ker v pravilu 1.2 piše »*za **vse** objekte*«, imamo povsem proste roke. Povedano z drugimi besedami, množico $\{2, 1, 1\}$ smemo tvoriti, ker nikjer ne piše, da moramo našteti različne elemente.

Nesrečno tropičje v pravilu 1.2 povzroča dovolj dvomov, da bi ga bilo dobro odpraviti. To dosežemo s tremi nadomestnimi pravili, ki imajo skupaj enak učinek kot prvotno pravilo.

Pravilo 1.4. ***Prazna množica*** $\emptyset$ je množica, ki nima elementov.

Pravilo 1.5. Za vsak x in y je ***(neurejeni) par*** ali ***(neurejeni) dvojec*** $\{x, y\}$ množica, katere elementa sta natanko x in y.

Pravilo 1.6. ***Unija*** $A \cup B$ množic A in B je množica, ki ima za elemente natanko vse objekte, ki so element A ali element B (lahko tudi obeh).

V pravilu 1.5 smo besedo »*neurejeni*« zapisali v oklepaju, kar pomeni, da jo običajno opustimo in rečemo samo »*dvojec*«. Se pravi, da »*neurejeni dvojec*« in »*dvojec*« pomenita isto. V primeru nejasnosti raje uporabimo daljšo obliko.

Prvo pravilo pojasni, da lahko tvorimo množico brez elementov. Poleg oznake $\emptyset$ se za prazno množico uporablja tudi zapis $\{\,\}$.

Drugo pravilo pove, kako lahko tvorimo množico z dvema elementoma, pa tudi z enim. Spomnimo se, pravila je treba brati dobesedno: za x in y

[2] Paul Halmos (1916–2006), ameriški matematik madžarskega rodu.

bi lahko vzeli dvakrat isti objekt z in tvorili množico $\{z, z\}$, ki ima natanko elementa z in z. To je pravzaprav množica z enim samim elementom z, zato ji pravimo tudi ***enojec*** in jo zapišemo $\{z\}$.

Tretje pravilo nam omogoča, da tvorimo večje množice. Denimo, množico z elementi a, b, c lahko tvorimo kot unijo

$$\{a, b\} \cup \{c\}\,.$$

To ni edini način, enako množico lahko dobimo na več načinov:

$$(\{a\} \cup \{b\}) \cup \{c\} \quad \text{ali} \quad \{b\} \cup \{c, a\} \quad \text{ali} \quad \{a, c\} \cup \{b, c\} \quad \text{itn.}$$

Kogar to zabava, lahko dokazuje, da so vse te množice enake.

Priročno je imeti pri roki množico z enim elementom, pri čemer je vseeno, kateri element vsebuje. V ta namen podajmo pravilo, ki zagotavlja tako množico.

Pravilo 1.7. ***Standardni enojec*** $\mathbb{1}$ je množica, katere edini element je $(\,)$.

Morda se zdi nenavadno, da množico označimo s številom, a ta občutek bo hitro izginil, ko bomo računali z množicami. Pravzaprav bi lahko prazno množico označili z nič $\mathbb{0}$ in nekateri matematiki to dejansko počnejo.

Edini element množice $\mathbb{1}$ smo zapisali $(\,)$. To ni tiskarska napaka, ampak načrtna izbira, ki bo pojasnjena v razdelku 2.6. In seveda velja $\mathbb{1} = \{(\,)\}$.

Pravilo 1.7 ni nujno potrebno, saj lahko tvorimo veliko različnih enojcev, začenši z $\{\emptyset\}$, katerega obstoj zagotavljata pravili za prazno množico in dvojec. Da se ne bi vsakič znova ukvarjali z nepotrebnim izbiranjem nekega enojca, smo enega od njih proglasili za prvega med enakimi. S prazno množico nimamo podobnih težav, saj je ena sama.

1.3 Preslikave

Temelj matematike ne tvorijo le množice, ampak tudi drugi matematični pojmi. Prvi izmed njih je ***preslikava***, oziroma s tujko ***funkcija***. V srednji šoli ste že spoznali nekatere preslikave, kot so na primer linearne preslikave, trigonometrijske funkcije, logaritem itd. Nas pa ne bodo zanimale posamezne preslikave, ali posebne lastnosti preslikav, ampak preslikave na splošno.

Vsaka preslikava ima tri sestavne dele: ***domeno*** ali ***začetno množico***, ***kodomeno*** ali ***ciljno množico*** in ***prirejanje***. Domeni se pogosto reče tudi

definicijsko območje. Če govorimo o preslikavi, ki ima domeno X in kodomeno Y, to ponazorimo s puščico med X in Y, takole

$$X \longrightarrow Y$$

Če želimo preslikavo poimenovati, na primer f, zapišemo

$$f : X \longrightarrow Y \qquad \text{ali} \qquad X \xrightarrow{f} Y$$

Pravimo, da je f ***preslikava iz*** X ***v*** Y. Zapis nad puščico je prikladen, kadar imamo opravka z več preslikavami, ki jih predstavimo z diagramom. Na primer,

$$X \longrightarrow Y \xrightarrow{f} Z \xleftarrow{g} W$$

nam pove, da imamo opravka z (neimenovano) preslikavo iz X v Y, s preslikavo f iz Y v Z in s preslikavo g iz W v Z. Diagrami so lahko še precej bolj zapleteni.

Tretji del preslikave je ***prirejanje***, ki določa, kako elemente domene preslikamo v elemente kodomene. Kaj pravzaprav to pomeni? Možnih je več odgovorov. V srednji šoli prirejanje enačimo z matematično formulo, ki tako imenovano 'neodvisno spremenljivko' preslika v vrednost, na primer x slika v $2\sin(x + \pi/4)$. S simboli tak predpis zapišemo

$$x \mapsto 2\sin(x + \pi/4).$$

in preberemo »*x se slika v dvakrat sinus od x plus pi četrtin.*« Matematiki smo natančni, zato ne mešamo uporabe puščic $\to$ in $\mapsto$. Navadna puščica se uporablja pri oznaki domene in kodomene, repata pa v predpisu. V računalništvu besedo 'predpis' razumemo kot 'programska koda' in o preslikavah razmišljajo kar kot o algoritmih.

1.3.1 Identiteta in konstantna preslikava

Dve posebej preprosti zvrsti preslikav sta identiteta in konstantna preslikava. Za vsako množico A je ***identiteta*** na A preslikava

$$\mathrm{id}_A : A \to A$$

ki elementu $x \in A$ priredi x. Za vsaki množici A in B ter $b \in B$ ***konstantna preslikava***

$$\mathrm{k}_b : A \to B$$

priredi vsakemu elementu iz A element b. S funkcijskim predpisom zapišemo identiteto in konstantno preslikavo takole:

$$\begin{aligned} \mathrm{id}_A &: A \to A & \qquad \mathrm{k}_b &: A \to B \\ \mathrm{id}_A &: x \mapsto x & \qquad \mathrm{k}_b &: x \mapsto b. \end{aligned}$$

1.3.2 Kako še lahko podamo prirejanje

V teoriji množic lahko prirejanje med elementi domene X in kodomene Y podamo na kak drug način, ki ga ne moremo neposredno izraziti z matematično formulo. Paziti moramo le, da zadošča pogojema:

- ***celovitost***: vsakemu elementu iz X je prirejen vsaj en element iz Y,
- ***enoličnost***: če sta elementu $x \in X$ prirejena $y \in Y$ in $z \in Y$, potem $y = z$.

Obravnavajmo nekaj zgledov.

Zgled 1.8. Definirajmo preslikavo $f : \mathbb{R} \to \mathbb{R}$, ki elementu $x \in \mathbb{R}$ priredi $y \in \mathbb{R}$ natanko tedaj, ko velja $x = y^3$, ali s formulo:

$$f(x) = y \Leftrightarrow x = y^3.$$

(Pozor, nismo zapisali $y = x^3$!) Na primer, f številu -8 priredi število -2, ker velja $-8 = (-2)^3$. Preslikava f ni nič drugega kot kubični koren, le podali smo jo na nenavaden način.

Zgled 1.9. Kaj pa, če bi definirali $f : \mathbb{R} \to \mathbb{R}$, ki elementu $x \in \mathbb{R}$ priredi $y \in \mathbb{R}$ natanko tedaj, ko velja $x = y^2$? Tako prirejanje ni celovito, saj ni nobenega y, da bi veljalo $-4 = y^2$, pa tudi enolično ni, ker je $4 = 2^2$ in $4 = (-2)^2$.

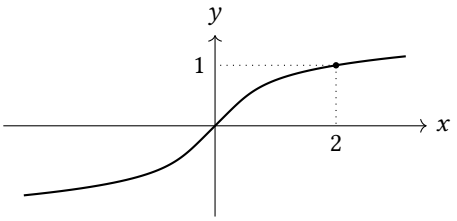
Vaja 1.10. Katera od naslednjih prirejanj določajo preslikavo $f : \mathbb{R} \to \mathbb{Z}$:

1. številu $x \in \mathbb{R}$ priredimo $k \in \mathbb{Z}$ natanko tedaj, ko velja $k \leq x < k + 1$,
2. številu $x \in \mathbb{R}$ priredimo $k \in \mathbb{Z}$ natanko tedaj, ko velja $k < x \leq k + 1$,
3. številu $x \in \mathbb{R}$ priredimo $k \in \mathbb{Z}$ natanko tedaj, ko velja $k < x < k + 1$,
4. številu $x \in \mathbb{R}$ priredimo $k \in \mathbb{Z}$ natanko tedaj, ko velja $k \leq x < k + 2$?

Ali ste katere od teh preslikav že videli in kako jih imenujemo?

Zgled 1.11. Definirajmo preslikavo $f : \mathbb{R} \to \mathbb{R}$ s prirejanjem, ki elementu

$x \in \mathbb{R}$ priredi tisto realno število $y \in \mathbb{R}$ iz kodomene, za katerega velja $y^5 + y - x = 0$. Ali to prirejanje sploh poda preslikavo? Ali je res, da za vsak $x \in \mathbb{R}$ obstaja natanko en $y \in \mathbb{R}$, ki zadošča $y^5 + y - x = 0$? Narišimo množico $\{(x, y) \in \mathbb{R}^2 \mid y^5 + y - x = 0\}$:



Iz slike razberemo, da je prirejanje celovito, ker navpičnica skozi vsak $x \in \mathbb{R}$ seka graf vsaj enkrat. Enolično je, ker ga seka največ enkrat. Torej je f dobro podana preslikava, a slika ni dokaz. Natančnejša utemeljitev bi se glasila: ker je $y^5 + y - x$ polinom lihe stopnje v spremenljivki y, ima vsaj eno ničlo, zato je prirejanje celovito. Ker je $y \mapsto y^5 + y - x$ strogo naraščajoča preslikava, ima največ eno ničlo, zato je prirejanje enolično. (Kako ugotovite, da je preslikava res naraščajoča?)

Preslikavo s *končno* domeno lahko podamo s tabelo, denimo:

$$f : \{1, 2, 3, 5\} \to \mathbb{N}$$

x	$f(x)$
1	10
2	10
3	20
5	10

Tabela elementu v levem stolpcu priredi istoležni element v desnem stolpcu: 1 priredi 10, 2 priredi 10, 3 priredi 20 in 5 priredi 10. Funkcijo lahko predstavimo tudi tako, da naštejemo vsa prirejanja:

$$\begin{aligned} f(1) &:= 10 \qquad \text{ali} \qquad f : 1 \mapsto 10 \\ f(2) &:= 10 \qquad\qquad\quad f : 2 \mapsto 10 \\ f(3) &:= 20 \qquad\qquad\quad f : 3 \mapsto 20 \\ f(5) &:= 10 \qquad\qquad\quad f : 5 \mapsto 10. \end{aligned}$$

To so še vedno le tabele, predstavljene na drugačen način. Tabelarični prikaz lahko uporabimo, kadar je domena f končna množica, katere elemente lahko naštejemo.

Preslikava je lahko določena tudi z opisom računskega postopka, pravimo mu ***algoritem***, s pomočjo katerega izračunamo vrednost preslikave pri danem argumentu. Paziti moramo, da je opis postopka res natančen in nedvoumen, lahko ga kar zapišemo kot program.

1.3.3 Funkcijski predpisi

Predpisu »x *se slika v* $\ldots$«, ki ga zapišemo

$$x \mapsto \cdots$$

pravimo tudi ***funkcijski predpis***. Posvetimo se mu in se ob njem naučimo nekaj natančnosti. Na desni, lahko namesto $\cdots$ zapišemo izraz, v katerem se sme pojaviti simbol x, denimo

$$x \mapsto 1 + x^2.$$

Spremenljivka x nima vnaprej določene vrednosti, pač pa kaže, kam lahko vstavimo elemente domene. Pravimo, da je x ***vezana spremenljivka***, kar pomeni, da je veljavna le v funkcijskem predpisu, nanj je vezana, in da ni pomembno, s katerim simbolom jo označimo. Tako sta funkcijska predpisa

$$x \mapsto 1 + x^2 \qquad \text{in} \qquad a \mapsto 1 + a^2$$

enaka in lahko bi celo pisali $\square \mapsto 1 + \square^2$ ali $\heartsuit \mapsto 1 + \heartsuit^2$.

V funkcijskem predpisu se smejo pojaviti tudi druge spremenljivke, ki jim pravimo ***parametri***. V predpisu

$$x \mapsto a \cdot x + b$$

sta a in b parametra in x vezana spremenljivka. Ni vseeno, katere spremenljivke so vezane in katere parametri:

Predpis	Pomen
$x \mapsto a \cdot x + b$	»*pomnoži z* a *in prištej* b«
$a \mapsto a \cdot x + b$	»*pomnoži z* x *in prištej* b«
$b \mapsto a \cdot x + b$	»*prištej* $a \cdot x$«

V funkcijskem predpisu mora na levi stati en sam simbol, ki na desni kaže, kam je treba vstaviti element iz domene. Tako

$$\sin(x) \mapsto \cos(2x), \qquad 3 + 2 \mapsto 5 \qquad \text{in} \qquad \sin(x) \mapsto 2 \cdot \sin(x)$$

niso veljavni funkcijski predpisi. Kasneje bomo spoznali pogoje, pri katerih je dovoljeno pisati tudi kaj drugega kot golo spremenljivko.

Seveda dopuščamo možnost, da se vezana spremenljivka pojavi enkrat, večkrat ali sploh ne. Funkcijska predpisa

$$x \mapsto 42 \qquad \text{in} \qquad x \mapsto x \cdot \sin(x)$$

sta torej veljavna.

Če želimo preslikavo z danim funkcijskim predpisom poimenovati, na primer f, zapišemo

$$f : x \mapsto 1 + x^2.$$

To preberemo »f *slika* x *v ena plus* x *na kvadrat*«. Običajna sta tudi zapisa

$$f(x) = 1 + x^2 \qquad \text{in} \qquad f(x) := 1 + x^2.$$

Mi se bomo držali zapisa z $:=$, da bomo lahko ločili med definicijo f in trditvijo, da je $f(x)$ enak neki vrednosti.

Zgled 1.12. Z zgledom pojasnimo, zakaj je pametno zapisati definicijo z enim simbolom in enakost z drugim:

> "Naj bo preslikava $f : \mathbb{R} \to \mathbb{R}$ definirana s predpisom $f(x) := 1 + x^2$. Tedaj za vse $x \in \mathbb{R}$ velja $f(x) = (x + 1)^2 - 2x$."

V prvi povedi smo f *definirali*, v drugi pa *trdili*, da velja zapisana enakost.

Funkcijske predpise je podrobno prvi preučeval Alonzo Church,[3] ki je uporabljal zapis

$$\lambda x \,.\, 1 + x^2$$

in teorijo funkcijskih predpisov poimenoval ***λ-račun***. V logiki se je njegov zapis obdržal in se uveljavil tudi v programskih jezikih:

- v Pythonu pišemo `lambda x: 1 + x ** 2`,

[3] Alonzo Church (1903–1995) je bil ameriški matematik in logik, ki je pomembno prispeval k razvoju logike in teoretičnega računalništva. Njegov študent, Dana Stewart Scott, je imel študenta Marka Petkovška in Andreja Bauerja, slednji pa je imel študenta Davorina Lešnika.

- v Haskellu pišemo `\x -> 1 + x ** 2` in
- v OCamlu pišemo `fun x -> 1 + x * x`.

Predvsem v programiranju funkcijskim predpisom pravijo tudi ***anonimne*** ali ***brezimne preslikave***.

Nekateri starejši zapisi funkcijskih predpisov so slabi, a jih ljudje vztrajno uporabljajo. Opozorimo le na en slab zapis, ki povzroča precej preglavic, ne da bi se matematiki tega zares zavedali. Funkcijski predpis mora določati vezano spremenljivko, sicer ne vemo, kako vstaviti vrednosti. Na žalost jo matematiki pogosto izpustijo skupaj in pišejo $1 + x^2$ namesto $x \mapsto 1 + x^2$. Težava je v tem, da se lahko v funkcijskem predpisu pojavi več kot en simbol. Če vam na primer nekdo pove, da ima v mislih funkcijski predpis

$$a \cdot x + b$$

boste zaradi ustaljenih navad v šolskem sistemu vsi mislili, da obravnavamo $x \mapsto a \cdot x + b$. A pravzaprav bi lahko bilo tudi

$$a \mapsto a \cdot x + b \quad \text{ali} \quad b \mapsto a \cdot x + b \quad \text{ali celo} \quad t \mapsto a \cdot x + b.$$

Poudarimo, da je funkcijski predpis le eden od treh sestavnih delov preslikave in zato sam *ne* podaja preslikave. Če ne poznamo domene, ne moremo preveriti, ali je funkcijski predpis celovit. Denimo,

$$x \mapsto \frac{x}{x^2 - 2}$$

ni celovit kot preslikava $\mathbb{R} \to \mathbb{R}$ in je celovit kot preslikava $\mathbb{Q} \to \mathbb{Q}$.

1.3.4 Uporaba in zamenjava

Do sedaj smo se ukvarjali s tem, kako preslikavo podamo, zdaj pa se vprašajmo, kako lahko preslikavo uporabimo. Če je $f : X \to Y$ preslikava iz X v Y in je $x \in X$, potem lahko f ***uporabimo na*** x in dobimo ***vrednost*** preslikave f pri ***argumentu*** x, to je tisti edini element Y, ki ga f priredi x. Vrednost f pri x zapišemo

$$f(x) \qquad \text{ali} \qquad f\,x$$

in preberemo »f *od* x« ali »f *pri* x«. Izraza $f(x)$, oziroma $f\,x$, se imenuje ***aplikacija***. Večinoma se uporablja zapis z oklepaji, a ne vedno: navajeni smo pisati $\ln 2$ in $\sin\alpha$ namesto $\ln(2)$ in $\sin(\alpha)$. Oklepaje izpuščamo tudi v nekaterih programskih jezikih in občasno v algebri.

V analizi je uveljavljen še en zapis za aplikacijo, ki se uporablja za zaporedja. Namreč, zaporedje ni nič drugega kot preslikava $a : \mathbb{N} \to \mathbb{R}$ iz naravnih v realna števila. Aplikacijo $a(n)$, ki označuje n-ti člen zaporedja, ponavadi pišemo a_n, torej argument podpišemo.

Preslikavo lahko uporabimo na argumentu tudi, če je nismo poimenovali. Na primer, preslikavo

$$\begin{aligned} &\mathbb{R} \to \mathbb{R} \\ &x \mapsto 1 + x^2 \end{aligned}$$

uporabimo na argumentu 3:

$$(x \mapsto 1 + x^2)(3).$$

Se vam zdi tak zapis nenavaden? Verjetno, a pomislite, zakaj: ker so vas vzgojili, da je treba vse preslikave poimenovati in se nanje sklicevali z danim imenom.[4] Taka vzgoja vzbuja občutek, da so preslikave bolj imenitne in zastrašujoče kot števila, daljice in drugi matematični objekti. Morda je občutek do neke mere utemeljen za laika, a prav hitro bomo spoznali, da preslikave niso nič posebnega in da lahko z njimi delamo enako kot s števili, vektorji in ostalimi matematičnimi objekti. Računalničarji radi rečejo, da je treba tudi preslikave obravnavati kot enakopravne državljane.

Kako izračunamo vrednost funkcije pri danem argumentu? To je odvisno od tega, kako je podano prirejanje. Če imamo tabelarični prikaz, poiščemo argument v levem stolpcu in pogledamo v pripadajoči desni stolpec. Če je preslikava podana s funkcijskim predpisom, argument vstavimo v predpis. Na primer, če je $f : \mathbb{R} \to \mathbb{R}$ podana s funkcijskim predpisom

$$f(x) := 1 + x^2,$$

potem je vrednost $f(3)$ enaka $1 + 3^2$ – vezano spremenljivko x smo zamenjali s 3. (Seveda je $1 + 3^2$ enako 10, a to je že naslednji korak, ki zahteva dodatno računanje.) Pravimo, da smo simbol x ***zamenjali*** ali ***substituirali*** s 3, oziroma da smo 3 ***vstavili*** v predpis za f namesto x. Preslikavo lahko

[4] Če bi veljalo enako tudi za števila, vam v srednji šoli ne bi pustili pisati kar $3 + 5$, nujno bi bilo poimenovanje $a := 3 + 5$. Tudi trikotnika ne bi smeli narisati, ne da bi mu dali simbolno ime.

uporabimo tudi na kakem bolj zapletenem argumentu, na primer:

$$\begin{aligned} f(3) &= 1 + 3^2, \\ f(2+\sqrt{5}) &= 1 + (2+\sqrt{5})^2, \\ f(y) &= 1 + y^2, \\ f(y+2z^2) &= 1 + (y+2z^2)^2, \\ f(x) &= 1 + x^2. \end{aligned}$$

V vseh primerih smo le zamenjali vezano spremenljivko x z argumentom. Tudi zadnja vrstica je zamenjava, v kateri smo (vezano spremenljivko) x zamenjali z (prosto) spremenljivko x.

Uporabimo lahko tudi funkcijski predpis, pri čemer še vedno velja, da vezano spremenljivko zamenjamo z argumentom. Tako je

$$(x \mapsto 1 + x^2)(3)$$

spet enako $1 + 3^2$. V razdelku 2.3 bomo spoznali še dodatna pravila za vstavljanje izrazov, ki se vrtijo okoli vezanih spremenljivk.

1.3.5 Pravilo ekstenzionalnosti preslikav

Podobno kot za množice tudi za preslikave velja pravilo ekstenzionalnosti, ki pravi, da sta preslikavi enaki, če imata enako domeno in kodomeno ter prirejata argumentom enake vrednosti.

Pravilo 1.13 (Ekstenzionalnost preslikav)**.** Preslikavi sta enaki, če imata enaki domeni in kodomeni ter imata za vse argumente enaki vrednosti.

Natančneje, če sta $f : A \to B$ in $g : C \to D$ preslikavi in velja $A = C$, $B = D$ ter za vsak $x \in A$ velja $f(x) = g(x)$, tedaj velja $f = g$.

Opozorimo na razliko med

$$f(x) = g(x) \qquad \text{in} \qquad f = g.$$

Levi izraz pravi, da sta $f(x)$ in $g(x)$ enaka elementa kodomene, desni pa da sta f in g enaki preslikavi. Na sploh je treba razlikovati med f in $f(x)$, saj to nikakor nista enaka objekta: prvi je preslikava, drugi pa vrednost te preslikave pri x. Verjetno nihče ne bi trdil, da je preslikava cos isto kot $\cos \frac{\pi}{4}$, ali ne? Isti razmislek veleva, da $\cos x$ ni isto kot cos, četudi si mislimo, da je $x \in \mathbb{R}$ neko neznano realno število. Zmeda izhaja iz površnega izražanja,

ko na primer rečemo »$x^2 + \cos x$ *je soda funkcija*«, čeprav bi bilo pravilno »$x \mapsto x^2 + \cos x$ *je soda funkcija*«.

Če dosledno uporabljamo funkcijske predpise, lažje razumemo, da sta cos in $x \mapsto \cos x$ enaki preslikavi, zahvaljujoč pravilu ekstenzionalnosti, obe pa sta različni od $\cos x$, ki sploh ni funkcija, ampak realno število, odvisno od parametra x.

V bran tradicionalnemu zapisu moramo vseeno povedati, da se lahko *dogovorimo* za nekoliko napačen zapis, če to ne povzroča zmede. S tem se izkušeni matematiki izognejo preveč birokratskemu pisanju nebistvenih podrobnosti in lahko bolj učinkovito komunicirajo. A začetnikom priporočamo, da v dobrobit boljšega razumevanja snovi vsaj na začetku študija raje vztrajajo pri doslednem zapisu.

Vrnimo se še k pravilu ekstenzionalnosti preslikav. Ali ni pravzaprav očitno, da sta preslikavi enaki, če imata enaki domeni, kodomeni in vrednosti? Morda res, a to ni razlog, da tega ne bi eksplicitno zapisali. Vsak matematik vam ve povedati kako zgodbo o tem, kako se je v dokazu skrivala napaka ravno tam, kjer je bilo nekaj 'očitno'. Poleg tega pa si lahko predstavljamo razmere, v katerih je smiselno razlikovati med dvema preslikavama, ki imata vedno enake vrednosti, denimo v programiranju, kjer je računska učinkovitost zelo pomembna.

1.3.6 Kompozicija

Kompozicija preslikav je temeljna operacija, ki združi preslikavi $f : A \to B$ in $g : B \to C$ v preslikavo $g \circ f : A \to C$, podano s prirejanjem

$$(g \circ f)(x) := g(f(x)).$$

Zakaj pišemo $g \circ f$ in ne obratno $f \circ g$? Ker si je mnogo lažje zapomniti zgornje računsko pravilo kot pravilo $(f \circ g)(x) = g(f(x))$, ki bi ga dobili, če bi pisali kompozicijo v obratnem vrstnem redu.

Zgled 1.14. Naj bosta $f : \mathbb{R} \to \mathbb{R}$ in $g : \mathbb{R} \to \mathbb{R}$ podani s predpisoma $f(x) := x^2$ in $g(x) := 2x$. Ker se kodomena vsake od njiju ujema z domeno druge, lahko tvorimo obe kompoziciji $g \circ f$ in $f \circ g$:

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) = 2x^2,\\ (f \circ g)(x) &= f(g(x)) = (2x)^2 = 4x^2.\end{aligned}$$

Preslikavi $g \circ f$ in $f \circ g$ sta različni, saj je $(g \circ f)(1) = 2$ in $(f \circ g)(1) = 4$. Kompozicija torej ni komutativna.

Zgled 1.15. Oglejmo si preslikavi $\sin : \mathbb{R} \to [-1,1]$ in $\arcsin : [-1,1] \to \mathbb{R}$. Tudi tu lahko tvorimo obe kompoziciji:

$$\arcsin \circ \sin : \mathbb{R} \to \mathbb{R} \qquad \text{in} \qquad \sin \circ \arcsin : [-1,1] \to [-1,1].$$

Za vsak $y \in [-1,1]$ velja $\sin(\arcsin y) = y$, zato je $\sin \circ \arcsin = \mathrm{id}_{[-1,1]}$. Po drugi strani $\arcsin \circ \sin$ ni identiteta na $\mathbb{R}$, saj je $\arcsin(\sin \pi) = \arcsin 0 = 0 \neq \pi$. Enakost $\arcsin(\sin x) = x$ velja le za $x \in [-\pi/2, \pi/2]$, v splošnem pa je

$$\arcsin(\sin x) = (-1)^m (x - m\pi), \qquad \text{kjer je} \qquad m = \lfloor x/\pi + 1/2 \rfloor.$$

Pri tem $\lfloor t \rfloor$ označuje število t, zaokroženo navzdol, se pravi največje celo število, ki ni večje od t. Narišite graf te funkcije!

Trditev 1.16.

1. *Identiteta je nevtralna za kompozicijo:* $\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A$.
2. *Kompozicija je asociativna:* $(h \circ g) \circ f = h \circ (g \circ f)$.

Dokaz. Trditev je zapisana pomanjkljivo, saj ne piše, kaj so A, B, f in g. Avtorja trditve bi lahko vprašali, kaj je hotel povedati, a je bolje, da poskusimo to razvozlati sami, ker je to odlična vaja iz razumevanja matematičnih besedil.

Takoj vidimo, da je A množica, sicer zapis id_A ne bi bil smiselen, in podobno je tudi B množica. Simboli f, g in h zagotovo označujejo preslikave, saj nastopajo v kompoziciji. Kaj pa njihove domene in kodomene? Preslikava f mora imeti domeno A, sicer ne bi bilo dovoljeno komponirati $f \circ \mathrm{id}_A$, in mora imeti kodomeno B, sicer ne bi bilo dovoljeno komponirati $\mathrm{id}_B \circ f$. Ostaneta še domeni in kodomeni preslikav g in h. Kompozicija $g \circ f$ kaže, da mora biti domena g enaka kodomeni f, torej B. Kompozicija $h \circ g$ pa pove, da je kodomena g enaka domeni h. Če vse to zložimo v diagram, dobimo

$$A \xrightarrow{f} B \xrightarrow{g} ? \xrightarrow{h} ?$$

Trditev moramo razumeti tako, da bo čim bolj splošna in smiselna. Torej bomo za neznani množici vzeli kar poljubni množici C in D:

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$$

Preverimo, ali smo trditev pravilno razumeli. Ko vstavimo podrobnosti, se prvi del glasi: »*Za vse množice A in B ter preslikavo $f : A \to B$ velja*

$\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A$.« Ker je to smiselna izjava, jo dokažimo. Enakost preslikav se dokaže z ekstenzionalnostjo preslikav, torej preverimo, ali imajo $\mathrm{id}_B \circ f$, f in $f \circ \mathrm{id}_A$ enako vrednost za poljuben $x \in A$:

$$\begin{aligned}(\mathrm{id}_B \circ f)(x) &= \mathrm{id}_B(f(x)) = f(x),\\ f(x) &= f(x),\\ (f \circ \mathrm{id}_A)(x) &= f(\mathrm{id}_A(x)) = f(x).\end{aligned}$$

Zapišimo podrobno še drugi del: »Za vse množice A, B, C in D ter preslikave $f : A \to B$, $g : B \to C$ in $h : C \to D$ velja $(h \circ g) \circ f = h \circ (g \circ f)$.« To spet dokažemo tako, da uporabimo levo in desno stran enačbe na poljubnem $x \in A$:

$$\begin{aligned}((h \circ g) \circ f)(x) &= (h \circ g)(f(x)) = h(g(f(x)))\\ (h \circ (g \circ f))(x) &= h((g \circ f)(x)) = h(g(f(x))).\end{aligned}$$ □

1.3.7 Kosoma podano prirejanje

Včasih podamo prirejanje 'po kosih', kar pomeni, da domeno razdelimo na podmnožice in za vsako posebej povemo, kako na njej deluje prirejanje. Zgled, ki ga že poznate iz srednje šole, je preslikava 'absolutna vrednost', ki je definirana po kosih za negativna in nenegativna števila:

$$\begin{aligned}&\mathbb{R} \to \mathbb{R}\\ &x \mapsto \begin{cases} -x & \text{če } x \leq 0,\\ x & \text{če } x \geq 0.\end{cases}\end{aligned}$$

Pravilo preberemo: »*če je $x \leq 0$, mu priredimo vrednost $-x$, in če je $x \geq 0$, mu priredimo vrednost x*«. Domeno $\mathbb{R}$ smo razdelili na množico nepozitivnih števil $\{x \in \mathbb{R} \mid x \leq 0\}$ in množico nenegativnih[5] števil $\{x \in \mathbb{R} \mid x \geq 0\}$. Celovitost tako podanega prirejanja je zagotovljena, če je unija kosov celotna domena, enoličnost pa v primeru, ko se prirejanja skladajo na preseku. V zgornjem zgledu je to res, saj je vsako realno število nepozitivno ali nenegativno, edino hkrati nenegativno in nepozitivno število pa je 0 in to zadošča $-0 = 0$.

Če bi absolutno vrednost definirali s predpisom

$$\begin{aligned}&\mathbb{R} \to \mathbb{R}\\ &x \mapsto \begin{cases} -x & \text{če } x < 0,\\ x & \text{če } x \geq 0,\end{cases}\end{aligned}$$

[5] Preberite pozorno, piše »*ne-negativnih*«!

se kosa ne bi prekrivala in nam ne bi bilo treba preverjati $-0 = 0$.

1.4 Vaje

Vaja 1.17. Kaj veste povedati o množici A, če zanjo velja, da so vsi njeni elementi enaki?

Vaja 1.18. Pravilo ekstenzionalnosti preslikav bi lahko zapisali tudi takole:

> Preslikavi $f : A \to B$ in $g : C \to D$ sta enaki, če velja $A = C$, $B = D$ in za vse $x_1, x_2 \in A$ velja, da iz $x_1 = x_2$ sledi $f(x_1) = g(x_2)$.

Dokažite, da je ta različica enakovredna običajnemu pravilu ekstenzionalnosti.

Vaja 1.19. Definirajmo preslikavo $g : \mathbb{N} \to \mathbb{Z}$ z zahtevo, da naravnemu številu $n \in \mathbb{N}$ priredi tisto celo število $k \in \mathbb{Z}$, za katerega velja $k^2 \leq n < (k+1)^2$. Preverite, da je prirejanje celovito in enolično in podajte čim bolj razumljiv besedni opis preslikave g.

2

Aritmetika množic

Množice lahko ***tvorimo*** ali ***konstruiramo*** iz drugih množic na različne načine. V tem poglavju bomo spoznali tri: zmnožek, vsoto in eksponent. Ostale konstrukcije pridejo na vrsto kasneje, ko bomo že nekaj vedeli o logiki.

Ko opišemo novo konstrukcijo množic, jo moramo natančno opredeliti. Pri tem se naslonimo na pravilo ekstenzionalnosti, ki pove, da je množica opredeljena s svojimi elementi. Če torej želimo določiti elemente neke množice A, to lahko storimo s pogojem oblike »$x \in A$ *natanko tedaj, ko …*«, ali s formulo

$$x \in A \;\Leftrightarrow\; \ldots.$$

Take primere smo že videli:

$$\begin{aligned} x \in \{a, b\} &\;\Leftrightarrow\; x = a \vee x = b, \\ x \in \mathbb{1} &\;\Leftrightarrow\; x = (), \\ x \in A \cup B &\;\Leftrightarrow\; x \in A \vee x \in B, \\ x \in \emptyset &\;\Leftrightarrow\; \bot. \end{aligned}$$

Tudi v nadaljevanju bomo sledili temu receptu in nove konstrukcije množic opisali tako, da bomo natančno opredelili njihove elemente.

2.1 Zmnožek

V srednji šoli ste že spoznali kartezični produkt ali zmnožek, katerega elementi so urejeni pari.

Pravilo 2.1 (Zmnožek množic)**.** Za vsaki množici A in B je $A \times B$ množica, ki se imenuje ***zmnožek*** ali ***kartezični produkt*** A in B. Elementi zmnožka $A \times B$ so natanko vsi urejeni pari (x, y), pri čemer je $x \in A$ in $y \in B$.

Pravilo ne pove nič o urejenih parih, razen da jih tvorimo tako, da elementa $x \in A$ in $y \in B$ združimo v (x, y). Ker smo urejenih parov že navajeni iz srednje šole, ne pomislimo, da bi kaj manjkalo.

Pravilo 2.2 (Enakost urejenih parov)**.** Za vse $x, u \in A$ in $y, v \in B$ velja: če sta urejena para (x, y) in (u, v) enaka, potem $x = u$ in $y = v$.

Pravilo potrebujemo, da lahko definiramo ***projekciji***

$$\mathrm{pr}_1 : A \times B \to A \qquad \text{in} \qquad \mathrm{pr}_2 : A \times B \to B,$$

ki iz urejenega para izluščita njegovi komponenti, se pravi, za vse $x \in A$ in $y \in B$ mora veljati

$$\mathrm{pr}_1(x, y) = x \qquad \text{in} \qquad \mathrm{pr}_2(x, y) = y.$$

Preveriti moramo, da ti dve enačbi podajata enolični in celoviti prirejanji. Ker je vsak element $A \times B$ urejeni par, je celovitost zagotovljena, enoličnost pa sledi iz pravila 2.2: če je neki element $A \times B$ hkrati enak (x, y) in (u, v), tedaj je $x = u$ in $y = v$, zato sta projekciji elementa enolično določeni.

Zgled 2.3. Zakaj tako kompliciramo s tako malenkostjo? Malo zato, ker smo matematiki, predvsem pa zato, ker se učimo, kaj pomeni matematična natančnost. Predstavljajte si, da bi definirali preslikavi $p_1 : \mathbb{N} \to \mathbb{N}$ in $p_2 : \mathbb{N} \to \mathbb{N}$ s predpisoma

$$p_1(m + n) = m \qquad \text{in} \qquad p_2(m + n) = n.$$

Definicija je podobna definiciji projekcij, le da smo urejeni par nadomestili z vsoto. Preslikavi p_1 in p_2 *nista* dobro definirani, ker lahko nekatera naravna števila zapišemo kot vsoto na več različnih načinov, kar pokvari enoličnost:

$$p_1(5) = p_1(3 + 2) = 3 \qquad \text{in} \qquad p_1(5) = p_1(4 + 1) = 4.$$

Pravilo 2.2 pove, da se to z urejenimi pari ne more zgoditi.

Kadar imamo opravka z več zmnožki, na primer $A \times B$ in $C \times D$, bi lahko prišlo do zmede glede projekcij, saj ne bi vedeli, ali pr_1 označuje prvo projekcijo $A \times B \to A$ ali $C \times D \to C$. Takrat simbole opremimo še z dodatnimi oznakami množic, da razločimo projekciji $\mathrm{pr}_1^{A,B} : A \times B \to A$ in $\mathrm{pr}_1^{C,D} : C \times D \to C$, in podobno za pr_2.

Pravili 2.1 in 2.2 omogočata prikladen način za podajanje preslikave, katere domena je zmnožek. Povedali smo, da mora v funkcijskem predpisu na levi stati en sam simbol, na primer:

$$\begin{aligned} \mathbb{R} \times \mathbb{R} &\to \mathbb{R} \\ p &\mapsto \mathrm{pr}_1(p) + \mathrm{pr}_2(p)^2 \cdot \mathrm{pr}_1(p). \end{aligned}$$

Ta zapis je precej nepregleden. Ker urejeni par natanko določa svoji komponenti, lahko zapišemo bolj pregledno:

$$\begin{aligned} \mathbb{R} \times \mathbb{R} &\to \mathbb{R} \\ (x, y) &\mapsto x + y^2 \cdot x. \end{aligned}$$

Če bi funkcijo poimenovali, denimo f, bi dobili običajni zapis:

$$\begin{aligned} f &: \mathbb{R} \times \mathbb{R} \to \mathbb{R} \\ f(x, y) &:= x + y^2 \cdot x. \end{aligned}$$

Za tako preslikavo pravimo, da je 'funkcija dveh spremenljivk', ker si mislimo, da smo podali argumenta x in y ločeno drug od drugega. A lahko bi rekli tudi, da je to funkcija ene spremenljivke, ki jo uporabimo na urejenem paru:

$$\begin{aligned} f &: \mathbb{R} \times \mathbb{R} \to \mathbb{R} \\ f(p) &:= \mathrm{pr}_1(p) + \mathrm{pr}_2(p)^2 \cdot \mathrm{pr}_1(p). \end{aligned}$$

Poleg zmnožka dveh množic bi lahko tvorili tudi zmnožek treh ali več množic. Pravila bi bila podobna kot za zmnožek dveh množic, le da bi namesto urejenih parov tvorili ***urejene večterice***. Na primer, elementi zmnožka $A \times B \times C$ treh množic so urejene trojice (x, y, z), pri čemer je $x \in A$, $y \in B$ in $z \in C$.

2.2 Vsota

Spoznali smo že unijo $A \cup B$ množic A in B, ki vsebuje tiste elemente, ki so v A ali v B. Če imata A in B skupne elemente, bodo ti v uniji seveda nastopili samo enkrat. V skrajnem primeru dobimo $A \cup A = A$. Včasih pa želimo združiti množici tako, da ne pride do prekrivanja. Taka konstrukcija je ***vsota*** $A + B$ množic A in B. Prekrivanje preprečimo tako, da elemente, ki jih je prispevala A, označimo z eno oznako, tiste, ki jih je prispevala B, pa z drugo.

Pravilo 2.4 (Vsota množic)**.** Za vsaki množici A in B je $A + B$ množica, ki se imenuje ***vsota*** ali ***koprodukt*** množic A in B. Njeni elementi so natanko:

1. $\mathsf{in}_1(a)$ za vsak $a \in A$,
2. $\mathsf{in}_2(b)$ za vsak $b \in B$.

Za vse $a, a' \in A$ in $b, b' \in B$ velja: če $\mathsf{in}_1(a) = \mathsf{in}_1(a')$, potem $a = a'$; če $\mathsf{in}_2(b) = \mathsf{in}_2(b')$, potem $b = b'$; ter $\mathsf{in}_1(a) \neq \mathsf{in}_2(b)$.

Tokrat smo z enim pravilom pojasnili, kaj so elementi vsote in tudi kdaj so med seboj enaki. Simboloma in_1 in in_2 pravimo ***injekciji***. Nanju lahko gledamo tudi kot na preslikavi

$$\mathsf{in}_1 : A \to A + B \qquad \text{in} \qquad \mathsf{in}_2 : B \to A + B.$$

Kadar imamo opravka z več vsotami, na primer $A + B$ in $C + D$, bi lahko prišlo do zmede glede oznak. Takrat injekcije opremimo še z dodatnimi oznakami množic, da razločimo injekciji $\mathsf{in}_1^{A,B} : A \to A + B$ in $\mathsf{in}_1^{C,D} : C \to C + D$, in podobno za in_2.

Zgled 2.5. $\{a, b, c\} + \{a, d, e\} = \{\mathsf{in}_1(a), \mathsf{in}_1(b), \mathsf{in}_1(c), \mathsf{in}_2(a), \mathsf{in}_2(d), \mathsf{in}_2(e)\}$.

Kako definiramo preslikavo $A + B \to C$? Ker je vsak element domene $A + B$ bodisi $\mathsf{in}_1(x)$ za neki $x \in A$ bodisi $\mathsf{in}_2(y)$ za neki $y \in B$, *obravnavamo oba primera* tako, da zapišemo *večdelni* funkcijski predpis:

$$\begin{aligned} \mathsf{in}_1(x) &\mapsto \cdots, \\ \mathsf{in}_2(y) &\mapsto \cdots. \end{aligned}$$

Na desni strani prvega pravila smemo uporabiti x, na desni strani drugega

pa y. Če želimo preslikavo poimenovati, zapišemo

$$\begin{aligned} f &: A + B \to C, \\ f(\mathsf{in}_1(x)) &:= \cdots \\ f(\mathsf{in}_2(y)) &:= \cdots. \end{aligned}$$

Zgled 2.6. Predpis

$$\begin{aligned} f &: \{1,2\} + \{2,3\} \to \mathbb{N}, \\ f(\mathsf{in}_1(x)) &:= x^2 \\ f(\mathsf{in}_2(y)) &:= 6/y \end{aligned}$$

enakovredno predstavimo s tabelo

u	$f(u)$
$\mathsf{in}_1(1)$	1
$\mathsf{in}_1(2)$	4
$\mathsf{in}_2(2)$	3
$\mathsf{in}_2(3)$	2

Vsi ti zapisi res določajo celovito in enolično prirejanje, saj nam pravilo za vsoto zagotavlja, da vedno obvelja natanko en primer. Na sploh lahko podamo funkcijski zapis z več primeri, če le pazimo, da obravnavamo vse možnosti, in da se le-te ne prekrivajo. Na primer, predpis

$$\begin{aligned} &(A + B) \times C \to B + A \\ &(\mathsf{in}_1^{A,B}(a), c) \mapsto \mathsf{in}_2^{B,A}(a) \\ &(\mathsf{in}_2^{A,B}(b), c) \mapsto \mathsf{in}_1^{B,A}(b) \end{aligned}$$

je celovit in enoličen, medtem ko predpis

$$\begin{aligned} &(A \times A) + B \to A \\ &\mathsf{in}_1(a_1, a_2) \mapsto a_2 \end{aligned}$$

ni veljaven, ker ni celovit, saj manjka primer $\mathsf{in}_2(b) \mapsto \cdots$.

Poleg vsote dveh množic bi lahko tvorili vsoto treh ali več množic. Pravila bi bila podobna, le da bi imeli več injekcij in več primerov.

2.3 Eksponent

Tretja osnovna konstrukcija je eksponentna množica.

Pravilo 2.7 (Eksponentna množica)**.** Za vsaki množici A in B je B^A množica, ki se imenuje ***eksponent*** ali ***eksponentna množica***. Elementi eksponenta B^A so natanko vse preslikave iz A v B.

Potemtakem je zapis $f : A \to B$ enakovreden zapisu $f \in B^A$. V razdelku 1.3 smo preslikave že podrobno obravnavali, zato nam ni treba pojasnjevati, kdaj sta preslikavi enaki in kaj vse lahko počnemo z elementi eksponenta B^A.

Zgled 2.8.

$$\begin{aligned}\{a,b,c\}^{\{1,2\}} := \{&(1 \mapsto a, 2 \mapsto a), (1 \mapsto a, 2 \mapsto b), (1 \mapsto a, 2 \mapsto c),\\ &(1 \mapsto b, 2 \mapsto a), (1 \mapsto b, 2 \mapsto b), (1 \mapsto b, 2 \mapsto c),\\ &(1 \mapsto c, 2 \mapsto a), (1 \mapsto c, 2 \mapsto b), (1 \mapsto c, 2 \mapsto c)\}.\end{aligned}$$

Ali znate sami razbrati, kako smo podali preslikave?

2.4 Preslikave višjega reda

Preslikavo, ki sprejme kot argument preslikavo, imenujemo ***funkcional*** ali ***preslikava višjega reda***. Znan primer je določeni integral, ki kot argumente sprejme realni števili $a, b \in \mathbb{R}$ in integrabilno funkcijo $f \in \mathbb{R}^{\mathbb{R}}$ ter izračuna ploščino pod f na intervalu $[a, b]$. Še en primer je operacija lim, ki sprejme konvergentno zaporedje $a \in \mathbb{R}^{\mathbb{N}}$ in izračuna njegovo limito.

V razdelku 1.3.6 smo že srečali funkcional, namreč kompozicijo preslikav. Zapišimo jo še enkrat tako, da nastopi operacija $\circ$ kot preslikava:

$$\begin{aligned}\circ &: C^B \times B^A \to C^A,\\ \circ &: (g, f) \mapsto (x \mapsto g(f(x))).\end{aligned}$$

Res, lahko si mislimo, da $\circ$ sprejme urejeni par preslikav (g, f) in izračuna njun kompozitum, ki ga pišemo $g \circ f$ namesto $\circ(g, f)$. Tu smo kompozicijo zapisali z *gnezdenim* funkcijskim predpisom, ki argumentu (g, f) priredi preslikavo, podano s predpisom $x \mapsto g(f(x))$. V splošnem je gnezdeni funkcijski predpis

oblike

$$\begin{aligned} A &\mapsto C^B \\ a &\mapsto (b \mapsto \cdots), \end{aligned}$$

kjer se lahko v $\cdots$ pojavita a in b. Na tak zapis se je treba navaditi, a je zelo prikladen, še posebej v funkcijskem programiranju. Čeprav v matematiki ni pogost, se mu ne bomo izogibali.

Primer gnezdenega funkcijskega predpisa je preslikava k iz razdelka 1.3.1, ki tvori konstantno preslikavo. Spomnimo se, če sta A in B množici ter $b \in B$, definiramo konstantno preslikavo

$$\begin{aligned} \mathrm{k}_b &: A \to B \\ \mathrm{k}_b &: a \mapsto b. \end{aligned}$$

Pravzaprav imamo opravka s preslikavo, ki sprejme $b \in B$ ter tvori konstantno preslikavo:

$$\begin{aligned} \mathrm{k} &: B \to B^A \\ \mathrm{k} &: b \mapsto (a \mapsto b). \end{aligned}$$

Uporabili smo gnezdeni funkcijski predpis.

Pri računanju s funkcionali včasih obravnavamo več funkcijskih predpisov hkrati. Če za vse uporabimo isto vezano spremenljivko, se lahko hitro zmedemo. Na primer, kompozitum preslikav

$$\begin{aligned} &\mathbb{R} \to \mathbb{R} \\ &x \mapsto x^2 - 4 \end{aligned} \quad \text{in} \quad \begin{aligned} &\mathbb{R} \to \mathbb{R} \\ &x \mapsto 2 - x \end{aligned}$$

bi lahko izračunali takole:

$$\begin{aligned} (x \mapsto x^2 - 4) \circ (x \mapsto 2 - x) &= (x \mapsto (x \mapsto x^2 - 4)((x \mapsto 2 - x)x)) \\ &= (x \mapsto (x \mapsto x^2 - 4)(2 - x)) \\ &= (x \mapsto (2 - x)^2 - 4) \\ &= (x \mapsto x^2 - 4x). \end{aligned}$$

Tu imamo tri različne x-e, saj vsak nastopa kot vezana spremenljivka v svojem

funkcijskem predpisu. Ločimo jih z barvami:

$$\begin{aligned}(x \mapsto x^2 - 4) \circ (x \mapsto 2 - x) &= (x \mapsto (x \mapsto x^2 - 4)((x \mapsto 2 - x)x)) \\ &= (x \mapsto (x \mapsto x^2 - 4)(2 - x)) \\ &= (x \mapsto (2 - x)^2 - 4) \\ &= (x \mapsto x^2 - 4x).\end{aligned}$$

Še posebej nejasen je drugi računski korak, ko imamo opravka s tremi barvami hkrati. Spomnimo se, da lahko vezane spremenljivke vedno preimenujemo in da lahko namesto barv preprosto uporabimo tri različne spremenljivke. Kompozicijo

$$\begin{array}{ll} \mathbb{R} \to \mathbb{R} & \\ y \mapsto y^2 - 4 & \end{array} \quad \text{in} \quad \begin{array}{ll} \mathbb{R} \to \mathbb{R} & \\ z \mapsto 2 - z & \end{array}$$

izračunamo še tretjič, tokrat bolj pregledno:

$$\begin{aligned}(y \mapsto y^2 - 4) \circ (z \mapsto 2 - z) &= (x \mapsto (y \mapsto y^2 - 4)((z \mapsto 2 - z)x)) \\ &= (x \mapsto (y \mapsto y^2 - 4)(2 - x)) \\ &= (x \mapsto (2 - x)^2 - 4) \\ &= (x \mapsto x^2 - 4x).\end{aligned}$$

Da ne bo prihajalo do zapletov z vezanimi spremenljivkami, se dogovorimo: *kadar imamo opravka z več vezanimi spremenljivkami, jih po potrebi preimenujemo tako, da so med seboj različne.*

2.5 Izomorfizem množic

Ko otrok prvič spozna pojem števila, je ta zanimiv sam po sebi. Z vnemo šteje do sto in se rad pogovarja o tem, koliko je en milijon. Sčasoma se radovednost osredotoči na aritmetične operacije in, če ima mladenič ali mladenka v sebi matematično žilico, na *zakonitosti* števil: množenje z 1 nima učinka, vrstni red seštevanja ni pomemben itd. Ali tudi operacijam na množicah, ki smo jih spoznali do sedaj, vladajo kakšne podobne zakonitosti?

Za števili a in b velja $a \cdot b = b \cdot a$. Nekaj podobnega velja tudi za množici A in B in njuna zmnožka $A \times B$ in $B \times A$. V splošnem sicer nista enaka, a sta v nekem smislu enakovredna, ker lahko par $(x, y) \in A \times B$ pretvorimo v par $(y, x) \in B \times A$ in obratno. Ta razmislek vodi do pojma izomorfizma.

Definicija 2.9. Množici A in B sta ***izomorfni*** in pišemo $A \cong B$, kadar obstajata preslikavi

$$f : A \to B \qquad \text{in} \qquad g : B \to A,$$

za kateri velja

$$g \circ f = \mathrm{id}_A \qquad \text{in} \qquad f \circ g = \mathrm{id}_B.$$

Pravimo, da je f ***izomorfizem*** med A in B in da je g ***inverz*** ali ***obrat*** f.

Preverimo, da velja $A \times B \cong B \times A$ za poljubni množici A in B. To storimo tako, da zapišemo preslikavi med zmnožkoma in preverimo, da tvorita izomorfizem:[1]

$$\begin{aligned} f &: A \times B \to B \times A & \qquad g &: B \times A \to A \times B \\ f &: (x, y) \mapsto (y, x) & \qquad g &: (v, u) \mapsto (u, v). \end{aligned}$$

Treba je preveriti, da velja $g \circ f = \mathrm{id}_{A\times B}$ in $f \circ g = \mathrm{id}_{B\times A}$. To naredimo z uporabo ekstenzionalnosti preslikav, ki pravi da $g \circ f = \mathrm{id}_{A\times B}$ velja, če velja $(g \circ f)(a, b) = \mathrm{id}_{A\times B}(a, b)$ za vse $a \in A$ in $b \in B$, in podobno za $f \circ g$. Obravnavajmo torej poljubna $a \in A$ in $b \in B$ in izračunajmo:

$$(g \circ f)(a, b) = g(f(a, b)) = g(b, a) = (a, b).$$

Na podoben način preverimo $f \circ g = \mathrm{id}_{B\times A}$.

Zgled 2.10. Primere izmorfizmov poznamo že iz srednje šole. Naj bo $\mathbb{R}_{>0}$ množica vseh pozitivnih realnih števil. Tedaj logaritem in eksponentna funkcija,

$$\log : \mathbb{R}_{>0} \to \mathbb{R} \qquad \text{in} \qquad \exp : \mathbb{R} \to \mathbb{R}_{>0}$$

tvorita izomorfizem, saj za vsak $x \in \mathbb{R}$ velja $\log(\exp x) = x$ in za vsak $y \in \mathbb{R}_{>0}$ velja $\exp(\log y) = y$.

Še več, eksponentna funkcija seštevanje pretvori v množenje, $\exp 0 = 1$ in $\exp(x + y) = \exp x \cdot \exp y$, zato ni le izomorfizem množic, ampak tudi izomorfizem *grup* $(\mathbb{R}, +, 0)$ in $(\mathbb{R}_{>0}, \cdot, 1)$.

[1] Držimo se pravila, da nikoli ne uporabimo iste vezane spremenljivke dvakrat, zato pravilo za f zapišemo z x in y in pravilo za g z v in u. Marsikdo bi oba funkcijska predpisa zapisal z x in y, torej $f : (x, y) \mapsto (y, x)$ in $g : (y, x) \mapsto (x, y)$. To zmede nekatere študente, ker mislijo, da »*sta x v definiciji f in v definiciji g ista, prav tako tudi y*«, karkoli že naj bi to pomenilo. Poudarimo še enkrat: vezana spremenljivka v funkcijskem predpisu nima nikakršne zveze z nobeno drugo pojavitvijo iste spremenljivke kje drugje.

Opazko o izomorfizmu grup smo podtaknili namenoma kot priložnost za nasvet. Če ne veste, kaj je grupa in izomorfizem grup, nikar ne obupavajte. Vsak matematik se v svojem delu nenehno srečuje z neznanimi pojmi. Znameniti profesor France Križanič[2] je v enega od svojih učbenikov zapisal, da naj tisti, ki mu je branje dokazov odveč, ravna tako kot Du Fu:[3]

> Ko berem knjige,
> z vinom se krepčam
> in znak preskočim,
> če ga ne poznam.

Morda bi veljalo odkorakati v knjižnico in ugotoviti, kaj vse je še napisal profesor Križanič.

Dokažimo nekaj osnovnih lastnosti izomorfnosti in izomorfizmov. Tokrat ne bomo zapisali podrobnih dokazov. Za vajo jih dopolnite do tolikšnih podrobnosti, da boste sami sebe prepričali, da trditve držijo.

Trditev 2.11. *Če je $f : A \to B$ izomorfizem med množicama A in B ter sta preslikavi $g : B \to A$ in $h : B \to A$ obe obrata f, potem je $g = h$.*

Dokaz. Ker je g obrat f, velja

$$g \circ f = \mathrm{id}_A \qquad \text{in} \qquad f \circ g = \mathrm{id}_B,$$

in ker je h obrat f, velja

$$h \circ f = \mathrm{id}_A \qquad \text{in} \qquad f \circ h = \mathrm{id}_B.$$

Dokazati moramo, da iz teh štirih predpostavk sledi $g = h$, kar storimo z naslednjim računom:

$$\begin{aligned}
g &= \mathrm{id}_A \circ g && \text{(kompozicija z } \mathrm{id}_A \text{ nima učinka)} \\
&= (h \circ f) \circ g && \text{(predpostavka } h \circ f = \mathrm{id}_A) \\
&= h \circ (f \circ g) && \text{(kompozicija je asociativna)} \\
&= h \circ \mathrm{id}_B && \text{(predpostavka } f \circ g = \mathrm{id}_B) \\
&= h. && \text{(kompozicija z } \mathrm{id}_B \text{ nima učinka)}
\end{aligned}$$

□

[2] France Križanič (1928–2002), slovenski matematik

[3] Du Fu (712–770), kitajski pesnik

Če je $f : A \to B$ izomorfizem, potem ima natanko en obrat, ki ga označimo f^{-1}. Če f ni izomorfizem, zapis f^{-1} ni veljaven izraz.

Oznaka za obrat je nekoliko nerodna, ker tudi obratno vrednost števila $x \in \mathbb{R}$ pišemo x^{-1}. Torej moramo paziti: če je $f : \mathbb{R} \to \mathbb{R}$ izomorfizem in $x \in \mathbb{R}$, je $(f(x))^{-1}$ obrat števila $f(x)$, medtem ko je $f^{-1}(x)$ število, ki ga dobimo, ko obrat preslikave f uporabimo na x. Sami premislite, kaj je $(f^{-1}(x))^{-1}$.

Trditev 2.12. *Za vse izomorfizme $f : A \to B$ in $g : B \to C$ velja*

$$(f^{-1})^{-1} = f \qquad \text{in} \qquad (g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Dokaz. Dokaz prepuščamo za vajo. Pozor, v desni enakosti se je zamenjal vrstni red f in g! Nadalje opazimo še to: zapisali smo $(f^{-1})^{-1}$ in $(g \circ f)^{-1}$, ne da bi predhodno preverili, ali sta f^{-1} in $g \circ f$ izomorfizma. Torej morate v dokazu najprej preveriti, da sta f^{-1} in $g \circ f$ izomorfizma, če sta f in g izomorfizma. □

Trditev 2.13. *Za vse množice A, B in C velja:*

1. $A \cong A$,
2. *če* $A \cong B$, *potem* $B \cong A$,
3. *če* $A \cong B$ *in* $B \cong C$, *potem* $A \cong C$.

Dokaz.

1. id_A je izomorfizem iz A v A, ki je sam svoj obrat,
2. če je $f : A \to B$ izomorfizem iz A v B, potem je f^{-1} izomorfizem iz B v A in f,
3. če je $f : A \to B$ izomorfizem iz A v B in $g : B \to C$ izomorfizem iz B v C, potem je $g \circ f$ izomorfizem iz A v C. □

2.6 Aritmetika množic

Kot že veste, seštevanje, množenje in potenciranje števil zadoščajo naslednjim aritmetičnim zakonom:

$$\begin{aligned} a+0 &= a & a\cdot 1 &= a \\ a+b &= b+a & a\cdot b &= b\cdot a \\ a+(b+c) &= (a+b)+c & a\cdot(b\cdot c) &= (a\cdot b)\cdot c \\ 0\cdot a &= 0 & 1^a &= 1 \\ (a+b)\cdot c &= a\cdot c + b\cdot c & (a\cdot b)^c &= a^c\cdot b^c \\ a^0 &= 1 & a^1 &= a \\ a^{b+c} &= a^b\cdot a^c & a^{b\cdot c} &= (a^b)^c \end{aligned}$$

$$0^a = 0 \quad \text{če } a \neq 0.$$

Že prej smo opazili, da je zakon $a\cdot b = b\cdot a$ podoben izomorfizmu $A\times B \cong B\times A$. Kaj pa ostali zakoni?

Izrek 2.14. *Za vse množice A, B in C velja:*

$$\begin{aligned} A+\emptyset &\cong A & A\times\mathbb{1} &\cong A \\ A+B &\cong B+A & A\times B &\cong B\times A \\ A+(B+C) &\cong (A+B)+C & A\times(B\times C) &\cong (A\times B)\times C \\ \emptyset\times A &\cong \emptyset & \mathbb{1}^A &\cong \mathbb{1} \\ (A+B)\times C &\cong A\times C + B\times C & (A\times B)^C &\cong A^C\times B^C \\ A^\emptyset &\cong \mathbb{1} & A^\mathbb{1} &\cong A \\ A^{B+C} &\cong A^B\times A^C & A^{B\times C} &\cong (A^B)^C \end{aligned}$$

$$\emptyset^A \cong \emptyset \quad \textit{če } A \neq \emptyset.$$

Izrek ni sam sebi namen, ampak je v njem nauk: *z množicami lahko računamo*, tako kot s števili. Preostanek razdelka je posvečen dokazu izreka.

2.6.1 Asociativnost

Za ogrevanje dokažimo asociativnost zmnožkov, $A\times(B\times C)\cong(A\times B)\times C$. Splošni element $A\times(B\times C)$ je urejeni par oblike $(x,(y,z))$, kjer je $x\in A$, $y\in B$ in $z\in C$, medtem ko je splošni element $(A\times B)\times C$ oblike $((u,v),w)$,

kjer je $u \in A$, $v \in B$ in $w \in C$. Izomorfizmov ni težko zapisati:

$$\begin{aligned} f &: A \times (B \times C) \to (A \times B) \times C & \qquad g &: (A \times B) \times C \to A \times (B \times C) \\ f &: (x, (y, z)) \mapsto ((x, y), z) & \qquad g &: ((u, v), w) \mapsto (u, (v, w)). \end{aligned}$$

Preverimo, da je g obrat f. Za vse $x \in A$, $y \in B$ in $z \in C$ velja:

$$g(f(x, (y, z))) = g((x, y), z) = (x, (y, z))$$

in za vse $u \in A$, $v \in B$ in $w \in C$ velja

$$f(g((u, v), w)) = f(u, (v, w)) = ((u, v), w).$$

Tudi asociativnost vsote, $A + (B + C) \cong (A + B) + C$, ni nič bolj zapletena, le da imamo opravka z injekcijami in obravnavanjem primerov. Najprej zapišimo izomorfizma s popolnoma natančnim zapisom, kjer vse injekcije opremimo z oznakami množic:

$$\begin{aligned} f &: A + (B + C) \to (A + B) + C \\ f &: \mathsf{in}_1^{A,B+C}(x) \mapsto \mathsf{in}_1^{A+B,C}(\mathsf{in}_1^{A,B}(x)) \\ f &: \mathsf{in}_2^{A,B+C}(\mathsf{in}_1^{B,C}(y)) \mapsto \mathsf{in}_1^{A+B,C}(\mathsf{in}_2^{A,B}(y)) \\ f &: \mathsf{in}_2^{A,B+C}(\mathsf{in}_2^{B,C}(z)) \mapsto \mathsf{in}_2^{A+B,C}(z) \end{aligned}$$

$$\begin{aligned} g &: (A + B) + C \to A + (B + C) \\ g &: \mathsf{in}_1^{A+B,C}(\mathsf{in}_1^{A,B}(u)) \mapsto \mathsf{in}_1^{A,B+C}(u) \\ g &: \mathsf{in}_1^{A+B,C}(\mathsf{in}_2^{A,B}(v)) \mapsto \mathsf{in}_2^{A,B+C}(\mathsf{in}_1^{B,C}(v)) \\ g &: \mathsf{in}_2^{A+B,C}(w) \mapsto \mathsf{in}_2^{A,B+C}(\mathsf{in}_2^{B,C}(w)) \end{aligned}$$

Isti zapis brez oznak množic je precej bolj čitljiv:

$$\begin{aligned} f &: A + (B + C) \to (A + B) + C & \qquad g &: (A + B) + C \to A + (B + C) \\ f &: \mathsf{in}_1(x) \mapsto \mathsf{in}_1(\mathsf{in}_1(x)) & \qquad g &: \mathsf{in}_1(\mathsf{in}_1(u)) \mapsto \mathsf{in}_1(u) \\ f &: \mathsf{in}_2(\mathsf{in}_1(y)) \mapsto \mathsf{in}_1(\mathsf{in}_2(y)) & \qquad g &: \mathsf{in}_1(\mathsf{in}_2(v)) \mapsto \mathsf{in}_2(\mathsf{in}_1(v)) \\ f &: \mathsf{in}_2(\mathsf{in}_2(z)) \mapsto \mathsf{in}_2(z) & \qquad g &: \mathsf{in}_2(w) \mapsto \mathsf{in}_2(\mathsf{in}_2(w)) \end{aligned}$$

Ali vidite, zakaj matematiki cenimo kratek in pregleden zapis? Preveč podrobnosti lahko zakrije bistvo ideje. Preverjanje, da je g obrat f, prepustimo tistim, ki radi veliko pišejo.

2.6.2 Preslikave in enojec

Preslikavi

$$\begin{aligned} f &: A \times \mathbb{1} \to A & \qquad g &: A \to A \times \mathbb{1} \\ f &: (x, u) \mapsto x & \qquad g &: y \mapsto (y, ( )) \end{aligned}$$

tvorita izomorfizem $A \times \mathbb{1} \cong A$, saj za vsak $a \in A$ in $t \in \mathbb{1}$ velja, upoštevaje da so vsi elementi $\mathbb{1}$ enaki $( )$,

$$g(f(a,t)) = g(a) = (a, ( )) = (a,t) \qquad \text{in} \qquad f(g(a)) = f(a, ( )) = a.$$

Lahko bi rekli, da je $\mathbb{1}$ nevtralni element za zmnožek *do izomorfizma natančno*, s čimer povemo, da ne velja *enakost* $A \times \mathbb{1} = A$, ampak le *izomorfizem* $A \times \mathbb{1} \cong A$. Na tem mestu lahko tudi pojasnimo nenavadni zapis edinega elementa $\mathbb{1}$. Elementi zmnožka dveh množic so urejene dvojice, zmnožka treh množic urejene trojice itd. Zmnožek nič množic je nevtralni element za množenje, torej so njegovi elementi urejene ničterice, oziroma urejena ničterica $( )$, ker je ena sama.

Izomorfizma $A^{\mathbb{1}} \cong A$ ni težko zapisati:

$$\begin{aligned} f &: A^{\mathbb{1}} \to A & \qquad g &: A \to A^{\mathbb{1}} \\ f &: h \mapsto h(( )) & \qquad g &: x \mapsto (y \mapsto x) \end{aligned}$$

Preverimo, da je g inverz f. Za vsak $x \in A$ velja

$$f(g(x)) = f(y \mapsto x) = x,$$

zato je $f \circ g = \mathrm{id}_A$. Za vsak $h \in A^{\mathbb{1}}$ velja

$$g(f(h)) = g(h(( ))) = (y \mapsto h(( ))).$$

Ali sta h in $y \mapsto h(( ))$ enaki preslikavi? Kot vsakič, uporabimo ekstenzionalnost preslikav, le da je tokrat še posebej preprosta: preslikavi z domeno $\mathbb{1}$ sta enaki, če imata enako vrednost pri argumentu $( )$, saj je to edini element $\mathbb{1}$. Torej je $h = (y \mapsto h(( )))$, saj velja

$$(y \mapsto h(( )))(( )) = h(( )).$$

Izomorfnost A in $A^{\mathbb{1}}$ pravzaprav pove nekaj zanimivega: preslikave $\mathbb{1} \to A$ lahko obravnavamo kot elemente A in obratno.

2.6.3 Preslikave in prazna množica

Lotimo se izomorfizmov, v katere je vpletena prazna množica. Tu se ne moremo več zanašati le na prirojen občutek za logiko, saj s prazno množico nimamo vsakdanjih izkušenj, oziroma jo obravnavamo kot posebnost. Kako bi odgovorili na vprašanje, ali so vsi elementi prazne množice praštevila? Pravilni odgovor je 'da'. In hkrati so vsi elementi prazne množice sestavljena števila. Zakaj je to res, bomo bolje razumeli kasneje, ko bomo podrobno obravnavali pravila sklepanja. Zaenkrat si zapomnimo, da je pravilna vsaka izjava »*za vse elemente prazne množice velja …*«. Pravimo, da je taka izjava *na prazno izpolnjena.*

Začnimo z vprašanjem, ali lahko tvorimo kako preslikavo $\emptyset \to A$. Najprej ugotovimo, da so vse preslikave $\emptyset \to A$ enake. Res, za $f, g : \emptyset \to A$ velja $f = g$ natanko tedaj, ko za vse $x \in \emptyset$ velja $f(x) = g(x)$. A ravnokar smo povedali, da je vsaka izjava oblike »*za vse* $x \in \emptyset$ *…*« veljavna. Pa imamo kako preslikavo $\emptyset \to A$? Odgovor je pritrdilen, če lahko podamo kako celovito in enolično prirejanje med elementi $\emptyset$ in A. Ker sta celovitost in enoličnost spet izjavi oblike »*za vse* $x \in \emptyset$ *…*«, sta na prazno izpolnjena, zato bo zadoščalo kakršnokoli prirejanje, denimo: nobenemu elementu ne priredimo nobenega elementa. S tem smo utemeljili naslednjo trditev.

Trditev 2.15. *Za vsako množico A obstaja natanko ena preslikava $\emptyset \to A$.*

Edini preslikavi $\emptyset \to A$ pravimo ***prazna preslikava***. S tem smo utemeljili $A^{\emptyset} \cong \mathbb{1}$, saj izomorfizem prazni preslikavi priredi $()$, njegov obrat pa priredi $()$ prazno preslikavo.

2.6.4 Izomorfizmi in eksponenti

Nazadnje se posvetimo še zakonu $A^{B\times C} \cong (A^B)^C$. Preverimo, da preslikavi[4]

$$\Lambda : A^{B\times C} \to (A^B)^C \qquad \Theta : (A^B)^C \to A^{B\times C}$$
$$\Lambda : f \mapsto (c \mapsto (b \mapsto f(b,c))) \qquad \Theta : g \mapsto ((b,c) \mapsto g(c)(b))$$

[4]Saj ste se že naučili grške črke, ali ne?

tvorita izomorfizem. Za vse $f \in A^{B\times C}$, $x \in B$ in $y \in C$ velja

$$\begin{aligned}\Theta(\Lambda(f))(x,y) &= ((b,c) \mapsto \Lambda(f)(c)(b))(x,y)\\ &= \Lambda(f)(y)(x)\\ &= (c \mapsto (b \mapsto f(b,c)))(y)(x)\\ &= (b \mapsto f(b,y))(x)\\ &= f(x,y),\end{aligned}$$

zato je $\Theta(\Lambda(f)) = f$. Prav tako za vse $g \in (A^B)^C$ in $x \in B$ in $y \in C$ velja

$$\begin{aligned}\Lambda(\Theta(g))(y)(x) &= (c \mapsto (b \mapsto \Theta(g)(b,c)))(y)(x)\\ &= (b \mapsto \Theta(g)(b,y))(x)\\ &= \Theta(g)(x,y)\\ &= ((b,c) \mapsto g(c)(b))(x,y)\\ &= g(y)(x)\end{aligned}$$

in zato $\Lambda(\Theta(g)) = g$. Preslikavi $\Lambda(f)$ pravimo ***transpozicija*** preslikave f, in prav tako preslikavi $\Theta(g)$ pravimo transpozicija preslikave g.

Izomorfizem $A^{B\times C} \cong (A^B)^C$ je zanimiv, ker pove, da lahko preslikavo dveh argumentov vedno prevedemo na preslikavo enega argumenta. Natančneje, če je $f : B \times C \to A$ preslikava dveh argumentov, je njena transpozicija $\Lambda(f) : C \to A^B$ preslikava enega argumenta, njena vrednost pa je preslikava, ki pričakuje še en argument. To dejstvo se s pridom izkorišča v funkcijskem programiranju: namesto, da bi definirali preslikavo $f : B\times C \to A$, ki sprejme urejeni par (b,c) in vrne vrednost $f(b,c)$, raje definiramo enakovredno preslikavo $\tilde{f} : B \to C \to A$, ki sprejme b in vrne preslikavo $\tilde{f}(b)$, ta pa sprejme še c in vrne vrednost $\tilde{f}(b)(c)$.

2.7 Vaje

Vaja 2.16. Zapišite pravila za zmnožek treh množic. Nato premislite še, kako bi podali pravila za zmnožek n množic, kjer je n naravno število. Seveda ne velja uporaba tropičja '...'!

Vaja 2.17. Naštejte vse elemente množice $\mathbb{1} + \mathbb{1} + \mathbb{1}$.

Vaja 2.18. Podajte primer izomorfizma $f : \mathbb{R} \to \mathbb{R}$ in števila $x \in \mathbb{R}$, da velja $f^{-1}(x) = (f(x))^{-1}$. Nato podajte še primer, ko velja $f^{-1}(x) \neq (f(x))^{-1}$.

Vaja 2.19. Ozrimo se še enkrat na dokaz trditve 2.11. Ali smo uporabili vse štiri predpostavke? Zapišite bolj splošno trditev, se pravi tako, ki navede samo tiste predpostavke, ki jih res potrebujemo v dokazu.

Vaja 2.20. Pogosto rečemo, da sta seštevanje in odštevanje obratni operaciji. Strogo vzeto ti dve operaciji nista inverza druga drugi, saj sta obe preslikavi $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$. V kakšnem smislu točno sta seštevanje in odštevanje obratni, tj. kateri dve preslikavi sta pravzaprav inverza druga drugi?

Vaja 2.21. Preveri tiste izomorfnosti iz izreka 2.14, ki jih v razdelku 2.6 nismo utemeljili.

3

Simbolni zapis

Tako kot vsaka stroka ima tudi matematika svoj strokovni jezik, ki obsega matematične simbole in izraze ter svojevrsten način izražanja. Matematiki stremimo k popolni natančnosti in nedvoumnosti matematične misli. To je seveda le ideal, ki se mu bolj ali manj približamo, dejanska matematična besedila pa pišemo ljudje za ljudi, zato ni nič nenavadnega, da so prežeta s tradicijo in nepisanimi družbenimi dogovori, ki matematiko oddaljijo od formalnega ideala, a jo tudi naredijo humano. V pomoč se v tem poglavju posvetimo samo formi matematičnega izražanja.

Matematično komuniciranje je raznoliko, saj je namenjeno različnim publikam in zato posredovano na različne načine. Tako v raziskovalnem matematičnem članku ne bomo našli pojasnil in izračunov, ki jih profesor matematike zahteva od svojih študentov. In verjetno ni dveh matematikov, ki bi uporabljala povsem usklajen matematični zapis in izrazoslovje. Kljub temu je matematični jezik skupen vsem matematikom in v večji meri poenoten. Nesporazume, ki nastopijo zaradi različnih navad, pa lahko rešimo s pogovorom. Vsi izkušeni matematiki vedo, da vedo zelo malo in zato vprašajo, ko česa ne vedo. To naj bo torej nasvet za to poglavje: vprašajte in če ne dobite odgovora, vprašajte še enkrat.

3.1 Pisave in simboli

Matematična abeceda vsebuje precej več simbolov kot zgolj običajne črke in številke. Nekatere že poznamo, na primer $=$, $<$, $+$, $\emptyset$, $\cup$, $\cap$, $\int$ in tako naprej, precej jih bomo še spoznali. Poleg tega matematiki uporabljamo različne pisave, kot je prikazano v tabeli 3.1. Na tabli in v zvezku sicer težko ločimo med pokončno, odebeljeno in ležečo pisavo, zato nabor pisav omejimo. V tiskanem besedilu se vedno držimo nekaterih pravil glede izbire pisav. Tako posamezne črke a, b, c, ..., x, y, z pišemo v ležeči pisavi, imena elementarnih funkcij pa pokončno: sin, cos, log, ... Naglasnih znakov, kot so na primer šumniki, običajno ne uporabljamo. Včasih z uporabo znakov nakažemo povezavo med dvema objektoma: f je funkcija in F njen integral, $\mathscr{A}$ je linearna preslikava in A njej pripadajoča matrika itd.

Pisava	Črke
pokončna	ABCDEFGHIJKLMNOPQRSTUVWXYZ
odebeljena	**ABCDEFGHIJKLMNOPQRSTUVWXYZ**
ležeča	*ABCDEFGHIJKLMNOPQRSTUVWXYZ*
kaligrafska	$\mathscr{ABCDEFGHIJKLMNOPQRSTUVWXYZ}$
frakturna	$\mathfrak{ABCDEFGHIJKLMNOPQRSTUVWXYZ}$
dvopoudarjena	$\mathbb{ABCDEFGHIJKLMNOPQRSTUVWXYZ}$

Tabela 3.1: Pisave

Črke lahko dodatno opremimo s črticami, vijugami, vektorskimi znaki, strešicami in podobno:

$$a \quad a' \quad \dot{a} \quad \bar{a} \quad \vec{a} \quad \tilde{a} \quad \hat{a} \quad \check{a}.$$

Uporabimo lahko tudi ***podpis*** ali ***nadpis***, ki je lahko črka, številka ali kak drug simbol, na primer

$$a_i \quad a^i \quad a_1 \quad a_\star \quad a^\dagger.$$

Podpisu in nadpisu pogovorno pravimo tudi ***indeks*** in ***eksponent***, a to ni najbolj posrečena raba, ker se indeks lahko pojavi tudi v nadpisu ali kje drugje, eksponent pa lahko pomeni tudi število, s katerim potenciramo.

Kljub temu obilju črk in oznak posežemo še po drugih abecedah, še posebej grški, zato se jo čim prej naučite! Grške črke skupaj z njihovo izgovorjavo najdete v tabeli 3.2. Prostoročni zapis grških črk se boste naučili v razredu.

Grška črka		**Izgovorjava**	
velika	*mala*	*v slovenščini*	*v grščini*
Α	α	alfa	alfa
Β	β	beta	vita
Γ	γ	gama	ɣama
Δ	δ	delta	delta
Ε	ϵ, ε	epsilon	epsilon
Ζ	ζ	zeta	zita
Η	η	eta	ita
Θ	θ, ϑ	θeta	θita
Ι	ι	jota	jota
Κ	κ	kapa	kapa
Λ	λ	lambda	lamda
Μ	μ	mi	mi
Ν	ν	ni	ni
Ξ	ξ	ksi	ksi
Ο	o	omikron	omikron
Π	π, ϖ	pi	pi
Ρ	ρ, ϱ	ro	ro
Σ	σ, ς	sigma	siɣma
Τ	τ	tau̯	taf
Υ	υ	ipsilon	ipsilon
Φ	ϕ, φ	fi	fi
Χ	χ	hi	χi
Ψ	ψ	psi	psi
Ω	ω	omega	omeɣa

Izgovorjava: u̯ je ustnični u (kot v besedi ‘pav’); ɣ je cerkljanski ‘g’ (nekaj med ‘g’ in ‘h’ — vprašajte sošolce s tega območja); θ je angleški nezveneči ‘th’ (kot v besedi ‘thing’); χ je nemški ‘ch’ (kot v besedi ‘ich’).

Tabela 3.2: Grška abeceda

Pa tudi to še ni dovolj! V teoriji množic uporabljamo še hebrejske črke alef א, bet ב in gimel ג.

In zakaj pravzaprav potrebujemo tako veliko število črk? Verjetno zato, ker je v matematiki krajši zapis bolj učinkovit, saj zasede manj prostora na papirju, pa še hitreje ga zapišemo in preberemo. Računalničarji imajo drugačne navade, saj pri njih velja, da naj se uporabljajo opisna imena, ki razkrijejo pomen: kjer bi matematik in fizik uporabila m in a, bi računalničar zapisal `masa_delca` in `pospesek`.

3.2 Izrazi

Matematično besedilo je mešanica naravnega jezika in simbolnega zapisa. Delom besedila, ki so napisani s simboli, pravimo ***simbolni izrazi*** ali krajše kar ***izrazi***. Vsi ste jih že videli, denimo

$$(3+4)\cdot 6 \qquad \int_0^1 \frac{x}{1+x^2}\,dx \qquad ax^2+bx+c=0 \qquad x>0 \vee x\leq 0$$

Ste se kdaj vprašali, zakaj pravzaprav pišemo ulomke z vodoravno črto, integral z znakom $\int$, zakaj ima množenje prednost pred seštevanjem in zakaj seštevamo od leve proti desni, čeprav bi lahko tudi v drugi smeri? Odgovor je vedno isti: to so splošno sprejete navade, ki so se izoblikovale v razvoju matematike. To niso matematične resnice, ampak *dogovori* med ljudmi, ki se jih držimo zato, ker so se izkazali za smiselne. Na primer, integralski znak $\int$ je Leibniz[1] izpeljal iz črke S, ker je na integral gledal kot na določene vrste vsoto (latinsko 'summa').

Z vidika vsebine raznolikost matematičnega zapisa ni potrebna, saj bi lahko vse izraze pisali na isti način. Namesto simbolov, kot so $+$, $-$ in $\sqrt{}$, bi lahko uporabljali besede `plus`, `minus`, `sqrt` in jih zapisovali kot preslikave. Tak zapis je preprost in enoten, saj se nam ni treba ukvarjati s predponami, medponami in priponami ter z levim in desnim združevanjem. Uporablja se v računalništvu, a kdo bi želel na tablo namesto $3+\sqrt{5-4}$ zapisati `plus(3, sqrt(minus(5, 4)))`?

Ni vsako zaporedje znakov pravilen izraz. Denimo, $3+)x\cdot 4$ ni pravilen izraz, ker ima narobe postavljen zaklepaj. Izraz je ***pravilno formiran*** ali ***sintaktično pravilen***, če ustreza pravilom, ki določajo, kako postavljamo

[1] Gottfried Wilhelm von Leibniz (1646–1716) je bil nemški filozof, matematik, fizik, pravnik, zgodovinar, jezikoslovec, knjižničar in diplomat lužiškosrbskega porekla.

oklepaje, vejice, pike, kako uporabljamo razne posebne simbole ($+$, $\vee$, $\int$) itd. Natančna ***sintaktična pravila*** za pisanje matematičnih izrazov so precej zapletena, ker je matematični zapis raznovrsten in se je razvijal skozi zgodovino. Mnoga že poznate (»*vsak oklepaj mora imeti ustrezni zaklepaj*«, »*piše se $a + b$ in ne $ab+$*«), zato jih ne bomo podrobno obravnavali – to je delo za računalničarje, ki želijo taka pravila implementirati. Posvetimo se raje pravilom in dogovorom za zapis izrazov, ki jih pogosto srečamo v matematiki.

Predpone, medpone, pripone Nekatere operacije in relacije pišemo kot ***medpone*** ali ***infiksne operacije***, tako da simbol operacije stoji med obema operandoma, na primer

$$x + y \qquad x - y \qquad x \times y \qquad x \oplus y \qquad x \leq y \qquad x \simeq y$$

Kadar zapišemo operator za operand, pravimo, da je zapis ***pripona*** ali ***postfiksna operacija***, na primer

$$x! \qquad x\uparrow$$

Zapis operatorja je ***predpona*** ali ***prefiksna operacija***, če stoji pred operandom, na primer

$$-x \qquad \neg x \qquad \Box x \qquad \downarrow x$$

Poleg teh poznamo tudi druge zapise:

$$x^y \qquad \frac{x}{y} \qquad \sqrt{x} \qquad \langle x, y \rangle.$$

Skrajni primer je zapis množenja brez simbola, ko namesto $x \cdot y$ zapišemo kar $x\,y$.

Podpisi in nadpisi Argumente operacije ali funkcije včasih zapišemo v podpis ali nadpis. Na primer, če je $a : \mathbb{N} \to \mathbb{R}$ zaporedje, pogosto zapišemo i-ti člen s podpisom a_i. Primer nadpisa je n-ti odvod funkcije f, ki ga zapišemo $f^{(n)}$.

Prednost in združevanje Nekatere operacije imajo ***prednost*** ali ***prioriteto***, ki pove, katera operacija pride prej na vrsto, kadar ni oklepajev: potenciranje ima prednost pred množenjem in množenje pred seštevanjem. Operacija lahko tudi ***združuje*** ali ***asociira*** levo ali desno. Na primer, seštevanje $+$ združuje levo, zato je $5 + 2 + 1$ enako $(5 + 2) + 1$. Pri seštevanju to

sicer ni pomembno, pri odštevanju pa moramo upoštevati združevanje na levo: $5-2-1$ je enako $(5-2)-1$ in ne $5-(2-1)$. Potenciranje združuje na desno, saj 2^{3^4} pomeni $2^{(3^4)}$. Nekatere operacije ne združujejo in v takih primerih moramo uporabiti oklepaje.

Povejmo še to: nič ni narobe, če zapišemo več oklepajev, kot je to nujno potrebno. Izraza $3 \cdot 4 + 5$ in $(((3) \cdot 4) + 5)$ sta enakovredna. Prava mera oklepajev izboljša razumljivost simbolnega zapisa.

Implicitni argumenti, privzete vrednosti in preobteževanje Argumente operacije lahko opustimo in od bralca pričakujemo, da bo pravilno uganil, kaj smo mislili. Pravimo, da so to ***implicitni argumenti***. Primer implicitnih argumentov smo že videli, ko smo zapisali prvo in drugo projekcijo

$$\mathsf{pr}_1 : A \times B \to A, \qquad \mathsf{pr}_2 : A \times B \to B.$$

Če bi bili zelo natančni, bi morali pri projekcijah zapisati tudi množici A in B:

$$\mathsf{pr}_1^{A,B} : A \times B \to A, \qquad \mathsf{pr}_2^{A,B} : A \times B \to B.$$

Pravimo, da sta A in B implicitna argumenta, kar pomeni, da ju opustimo, če to ne povzroča zmede.

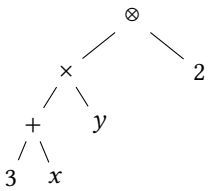
Vaja 3.1. Ali ima kompozicija preslikav $\circ$ implicitne argumente? Katere?

Argument operacije ima lahko ***privzeto vrednost***. Na primer, logaritem x z osnovo b zapišemo $\log_b x$. Če opustimo b, se razume, da je mišljen desetiški logaritem, $\log x = \log_{10} x$. Pravimo, da je privzeta vrednost osnove $b = 10$.

Vaja 3.2. Ali poznaš še kako drugo operacijo s privzeto vrednostjo?

Simbol lahko tudi ***preobtežimo***, da ima več pomenov, nato pa od bralca pričakujemo, da bo uganil, katerega smo mislili. Na primer, $+$ uporabljamo za seštevanje naravnih števil, seštevanje celih števil, seštevanje racionalnih števil, seštevanje realnih števil, seštevanje kompleksnih števil, seštevanje vektorjev, seštevanje matrik, itd. S preobteževanjem ne gre pretiravati, ker lahko pripelje do zmede. Običajno z istim simbolom označimo različne operacije, ki imajo kaj skupnega. Tako $+$ praviloma uporabljamo za operacijo, ki je komutativna, asociativna in ima nevtralni element.

Izrazi predstavljajo drevesa Izrazi so zaporedja znakov, ki jih pišemo z leve na desno. Ponekod na svetu bi jih pisali z desne na levo ali navpično. Izrazi so le *predstavitve* tako imenovanih ***sintaktičnih dreves***. Izraz $((3 + x) \times y) \otimes 2$ predstavlja sintaktično drevo



O sintaktičnih drevesih ne bomo govorili, le zapomnimo si, da se uporabljajo v programiranju za predstavitev izrazov in da so uporabna, ko simbolni zapis obravnavamo matematično s prijemi iz algebre.

3.3 Slike in diagrami

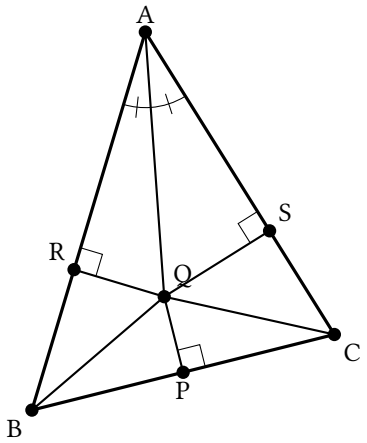
Matematiki uporabljamo tudi diagrame in slike, slednje predvsem v geometriji in analizi. Z njimi lahko razjasnimo pojme in si pomagamo pri predstavi zapletenih pojmov in konstrukcij, zato so nepogrešljivo orodje. To še posebej velja za poučevanje matematike. Pri uporabi slik moramo biti pazljivi, ker nas lahko zavedejo. V poduk naj bo naslednji 'izrek'.

Izrek 3.3 (neveljaven)**.** *Vsi trikotniki so enakokraki.*

Neveljaven dokaz. Naj bo $\triangle ABC$ poljuben trikotnik, glej sliko 3.1. Naj bo P središče stranice BC ter Q presečišče simetrale kota $\angle BAC$ in simetrale stranice BC. Naj bo R pravokotna projekcija točke Q na stranico AB in S pravokotna projekcija točke Q na stranico AC. Trikotnik $\triangle BCQ$ je enakokrak z vrhom Q, zato velja $BQ \cong CQ$. Trikotnika $\triangle AQR$ in $\triangle AQS$ sta skladna, ker imata skupno stranico in kota ob njej, nasprotna kota pa sta oba prava, torej velja $AR \cong AS$ in $QR \cong QS$. Sklepamo, da sta tudi trikotnika $\triangle BQR$ in $\triangle CQS$ skladna, saj sta pravokotna trikotnika s skladno kateto in skladno hipotenuzo. Potemtakem sta skladni še preostali kateti, $RB \cong SC$, od koder izračunamo

$$AB \cong AR + RB \cong AS + SC \cong AC.$$

Trikotnik $\triangle ABC$ je res enakokrak. □



Slika 3.1: trikotnik $\triangle ABC$

Vaja 3.4. Poišči napako v dokazu izreka 3.3.

3.4 Logične formule

Matematična izjava je besedilo, ki izraža kako matematično dejstvo. Primeri matematičnih izjav:

- $2 + 2 = 5$.
- »*Točke P, Q in R so kolinearne.*«
- »*Enačba* $x^2 + 1 = 0$ *ima tri realne rešitve.*«
- $a > 5$.
- $\phi \vee \psi \Rightarrow (\neg\phi \Rightarrow \psi)$.

Izjava je lahko resnična, neresnična ali pa je njena resničnost *odvisna* od vrednosti parametrov, ki nastopajo v njej:

- Izjava »*Vsa realna števila so večja od* 3.« je neresnična.
- Izjava »*Nekatera realna števila so večja od* 3.« je resnična.
- Resničnost izjave »*Število* x *je večje od* 3.« je odvisna od vrednosti x.

Matematične izjave običajno pišemo kombinirano v naravnem in simbolnem jeziku, saj so tako najlažje razumljive ljudem. Če situacija to zahteva, izjavo zapišemo *samo* z matematičnimi simboli. Tako zapisani izjavi pravimo

logična formula ali ***logični izraz***. Osnovni gradniki logičnih formul so ***logične operacije*** iz tabele 3.3 in delimo jih na tri sklope:

- ***konstanti*** $\bot$ in $\top$,
- ***vezniki*** $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\neg$ in $\veebar$,
- ***kvantifikatorja*** $\forall$ in $\exists$.

Opozorimo na nekatere posebnosti matematičnega izražanja. V matematiki ločimo med dvema vrstama disjunkcije:

- disjunkcija $\phi \vee \psi$ je ***inkluzivna***: velja ϕ ali ψ, lahko tudi oba.
- ***ekskluzivna*** disjunkcija $\phi \veebar \psi$: velja ϕ ali ψ, vendar *ne* oba.

Bodite pozorni na to razliko, saj lahko v vsakdanji rabi »*ali*« označuje inkluzivno ali ekskluzivno disjunkcijo.

Vaja 3.5. Ko vas vprašajo »*Želiš kavo ali čaj?*«, odgovorite z »*da*«.

V implikaciji $\phi \Rightarrow \psi$ imenujemo ϕ ***antecedent*** ali ***predpostavka*** in ψ ***konsekvent*** ali ***posledica***. Izmed vseh veznikov implikacija povzroča največ težav, saj jo uporabljamo zelo ohlapno. Če mati sinu reče

»*Če ne pospraviš sobe, potem ti ne spečem palačink,*«

bo sin razočaran, ko bo pospravil sobo, mama pa ne bo spekla palačink. A če bi sin študiral matematiko, bi vedel, da mama ni povedala nič o tem, kaj bo storila, če sobo pospravi. Če bi mama rekla:

»*Če pospraviš sobo, potem ti spečem palačinke,*«

bi to bila drugačna obljuba, ki bi mamo zavezala k peki palačink v primeru, da sin pospravi sobo. Mama svoje obljube ne bi prelomila tudi v primeru, ko bi spekla palačinke, a sin sobe ne bi pospravil; se pa velja vprašati, ali gre lenobo nagrajevati s palačinkami. Če označimo »*sin pospravi sobo*« s ϕ in »*mama speče palačinke*« s ψ, zgornji izjavi zapišemo simbolno z

$$\neg\phi \Rightarrow \neg\psi \qquad \text{in} \qquad \phi \Rightarrow \psi.$$

Ti izjavi nista ekvivalentni.

Ekvivalenca $\phi \Leftrightarrow \psi$ je okrajšava za $(\phi \Rightarrow \psi) \wedge (\psi \Rightarrow \phi)$. Pozor, v vsakdanjem pogovoru ekvivalenco in implikacijo pogosto pomešamo, celo v matematičnih besedilih! Definicija

Operacija	Zapis	Izgovorjava
resnica	$\top$	»*resnica*« »*je res*« »*pravilno*«
neresnica	$\bot$	»*neresnica*« »*ni res*« »*nepravilno*«
konjunkcija	$\phi \wedge \psi$	»ϕ *in* ψ«
disjunkcija	$\phi \vee \psi$	»ϕ *ali* ψ«
implikacija	$\phi \Rightarrow \psi$	»*če* ϕ*, potem* ψ« »*iz* ϕ *sledi* ψ« »ϕ*, samo če* ψ« »ψ *sledi iz* ϕ« »ϕ *je zadosten pogoj za* ψ« »ψ *je potreben pogoj za* ϕ«
ekvivalenca	$\phi \Leftrightarrow \psi$	»ϕ*, če in samo če* ψ« »ϕ *natanko tedaj, ko* ψ«
negacija	$\neg\phi$	»*ne* ϕ« »*ni res, da* ϕ« »*ne velja* ϕ«
ekskluzivna disjunkcija	$\phi \veebar \psi$ $\phi \oplus \psi$	»*bodisi* ϕ *bodisi* ψ«
univerzalni kvantifikator	$\forall x \in S \,.\, \phi$	»*za vse* x *iz* S *velja* ϕ« »ϕ *za vse* x *iz* S«
eksistenčni kvantifikator	$\exists x \in S \,.\, \phi$	»*obstaja* x *iz* S*, da* ϕ« »*za neki* x *iz* S *velja* ϕ« »ϕ *za neki* x *iz* S«

Tabela 3.3: Logični konstanti, vezniki in kvantifikatorja

»*Število se imenuje* **sodo**, *če je deljivo z dva.*«

je zapisana kot implikacija, a jo je treba razumeti kot ekvivalenco:

»*Število se imenuje* **sodo**, *če in samo če je deljivo z dva.*«

Res, implikacija bi dopuščala možnost, da se tudi število 3 imenuje sodo.

V uporabi so nekatere ustaljene okrajšave:

Okrajšava	Pomen
$\exists x, y \in S \,.\, \phi$	$\exists x \in S \,.\, (\exists y \in S \,.\, \phi)$
$\forall x \in S, y \in T \,.\, \phi$	$\forall x \in S \,.\, (\forall y \in T \,.\, \phi)$
$\phi \Leftrightarrow \psi \Leftrightarrow \rho \Leftrightarrow \sigma$	$(\phi \Leftrightarrow \psi) \wedge (\psi \Leftrightarrow \rho) \wedge (\rho \Leftrightarrow \sigma)$
$a = b = c = d$	$a = b \wedge b = c \wedge c = d$
$a \leq b < c \leq d$	$a \leq b \wedge b < c \wedge c \leq d$

Srečamo tudi okrajšave, ki jih odsvetujemo. V nizu neenakosti naj gredo vse primerjave v isto smer. Torej ne pišemo $a \leq b < c \geq d$, ker se zlahka zmotimo in mislimo, da velja $a \geq d$. To bi morali zapisati ločeno kot $a \leq b < c$ in $c \geq d$. Prav tako ne nizamo relacije $\neq$, saj premnogi iz $a \neq b \neq c$ napačno sklepajo $a \neq c$, čeprav $\neq$ *ni* tranzitivna relacija. Zapis $a = b \neq c = d$ je v redu, saj en sam $\neq$ ne povzroči težav.

Dogovorimo se za prioriteto logičnih operacij:

- negacija $\neg$ ima prednost pred
- konjunkcijo $\wedge$, ki ima prednost pred
- disjunkcijo $\vee$, ki ima prednost pred
- implikacijo $\Rightarrow$, ki ima prednost pred
- kvantifikatorjema $\forall$ in $\exists$.

Na primer:

$$\begin{aligned}
\neg\phi \vee \psi \quad &\text{pomeni} \quad (\neg\phi) \vee \psi, \\
\neg\neg\phi \Rightarrow \phi \quad &\text{pomeni} \quad (\neg(\neg\phi)) \Rightarrow \phi, \\
\phi \vee \psi \wedge \rho \quad &\text{pomeni} \quad \phi \vee (\psi \wedge \rho), \\
\phi \wedge \psi \Rightarrow \phi \vee \psi \quad &\text{pomeni} \quad (\phi \wedge \psi) \Rightarrow (\phi \vee \psi).
\end{aligned}$$

Kvantifikatorja vedno zajameta čim daljšo izjavo:

$$\begin{aligned}
&\forall x \in S\,.\,\phi \Rightarrow \psi && \text{pomeni} && \forall x \in S\,.\,(\phi \Rightarrow \psi),\\
&\forall x \in S\,.\,\phi \Rightarrow \psi && \textit{ne}\ \text{pomeni} && (\forall x \in S\,.\,\phi) \Rightarrow \psi,\\
&\exists x \in S\,.\,\phi \wedge \psi && \text{pomeni} && \exists x \in S\,.\,(\phi \wedge \psi),\\
&\forall x \in A\,.\,\phi \wedge \exists y \in B\,.\,\psi && \text{pomeni} && \forall x \in A\,.\,(\phi \wedge (\exists y \in B\,.\,\psi)),\\
&\forall x \in A\,.\,\phi \wedge \exists y \in B\,.\,\psi && \textit{ne}\ \text{pomeni} && (\forall x \in A\,.\,\phi) \wedge (\exists y \in B\,.\,\psi),\\
&\forall x \in S\,.\,\phi \Rightarrow \forall y \in T\,.\,\psi && \text{pomeni} && \forall x \in S\,.\,(\phi \Rightarrow \forall y \in T\,.\,\psi),\\
&\forall x \in S\,.\,\phi \Rightarrow \forall y \in T\,.\,\psi && \textit{ne}\ \text{pomeni} && (\forall x \in S\,.\,\phi) \Rightarrow (\forall y \in T\,.\,\psi).
\end{aligned}$$

Dalje, konjunkcija in disjunkcija združujeta levo:

$$\begin{aligned}
&\phi \wedge \psi \wedge \rho && \text{pomeni} && (\phi \wedge \psi) \wedge \rho,\\
&\phi \vee \psi \vee \rho && \text{pomeni} && (\phi \vee \psi) \vee \rho.
\end{aligned}$$

Za disjunkcijo in konjunkcijo sicer ni pomembno, kako postavimo oklepaje, ker sta si obe možnosti ekvivalentni, vendar je prav, da natančno določimo, katera od njiju je mišljena. Implikacija združuje desno:

$$\phi \Rightarrow \psi \Rightarrow \rho \qquad \text{pomeni} \qquad \phi \Rightarrow (\psi \Rightarrow \rho).$$

Tu *ni* vseeno, kako postavimo oklepaje, saj $\phi \Rightarrow (\psi \Rightarrow \rho)$ in $(\phi \Rightarrow \psi) \Rightarrow \rho$ v splošnem nista ekvivalentna.

Zgled 3.6. Naj bosta $x, y \in \mathbb{R}$. Izjava $x \leq y \Rightarrow (y \leq x \Rightarrow x = y)$ je veljavna za vse vrednosti x in y, izjava $(x \leq y \Rightarrow y \leq x) \Rightarrow x = y$ pa velja natanko tedaj, ko je $x \leq y$.

Vendar pozor! Kadar vidite niz implikacij

$$\phi \Rightarrow \psi \Rightarrow \rho \Rightarrow \sigma$$

le-ta pogosto označuje konjunkcijo implikacij

$$(\phi \Rightarrow \psi) \wedge (\psi \Rightarrow \rho) \wedge (\rho \Rightarrow \sigma),$$

podobno kot $a \leq b \leq c \leq d$ označuje konjunkcijo neenakosti. Tako pišemo, čeprav je formalno nepravilno, ker želimo nakazati zaporedje sklepov »*iz* ϕ *sledi* ψ *in nato iz* ψ *sledi* ρ *in nato iz* ρ *sledi* σ«. Običajno vsak sklep

zapišemo v svojo vrstico. Recimo, za nenegativni števili x in y bi takole zapisali utemeljitev neenakosti med aritmetično in geometrijsko sredino:

$$\begin{aligned}
(x-y)^2 \geq 0 &\Rightarrow x^2 - 2xy + y^2 \geq 0 && \text{(zmnožimo)}\\
&\Rightarrow x^2 + 2xy + y^2 \geq 4xy && \text{(prištejemo } 4xy\text{)}\\
&\Rightarrow (x+y)^2 \geq 4xy && \text{(razstavimo)}\\
&\Rightarrow \frac{(x+y)^2}{4} \geq xy && \text{(delimo s 4)}\\
&\Rightarrow \frac{x+y}{2} \geq \sqrt{xy}. && \text{(korenimo)}
\end{aligned}$$

Če res želite izraziti gnezdeno implikacijo, je bolje uporabiti oklepaje in zapisati $\phi \Rightarrow (\psi \Rightarrow \rho)$.

Logična kvantifikatorja V zapisih $\forall x \in S\,.\,\phi$ in $\exists x \in S\,.\,\phi$ je S množica, razred[2] ali tip spremenljivke x. V praksi se uporablja več inačic zapisa za kvantifikatorje, kot so:

$$\forall(x\,:\,S),\,\phi \qquad\qquad \forall x \in S\,:\,\phi \qquad\qquad (\forall x \in S)\phi.$$

Podobne zapise najdemo tudi za eksistenčni kvantifikator. Srečamo tudi zapis

$$\phi \quad \forall x \in S,$$

ki pa ga odsvetujemo, ker je nepregleden in nepraktičen, ko imamo opravka z več gnezdenimi kvantifikatorji. Poleg tega uvede vezano spremenljivko x v formuli ϕ šele potem, ko smo že prebrali ϕ.

Kvantifikator $\exists x \in S\,.\,\phi$ pravi, da obstaja *vsaj en* x, lahko jih je tudi več. Na primer, $\exists x \in \mathbb{R}\,.\,x^2 = 4$ je resnična izjava, saj obstajata dve števili, katerih kvadrat je 4. V razdelku 3.7 bomo zapisali »*obstaja natanko en*« s pomočjo $\exists$ in $\forall$.

Poznamo tudi ***neomejena kvantifikatorja***

$$\forall x\,.\,\phi \qquad \text{in} \qquad \exists x\,.\,\phi,$$

ki se uporabljata, kadar je vnaprej znana množica S, po kateri teče spremenljivka x. V matematičnem besedilu je običajno razvidna iz spremnega besedila, včasih pa se zanesemo na ustaljene navade: n je naravno ali celo število, x realno, f je funkcija ipd.

[2] V poglavju **??** bomo spoznali razliko med množicami in razredi, zaenkrat si S predstavljamo kot množico.

Zgled 3.7. Naj bo $f : \mathbb{N} \to \{0, 1\}$ preslikava. V formuli

$$(\forall n \,.\, f(n) = 0) \vee (\exists n \,.\, f(n) = 1)$$

se pojavita neomejena kvantifikatorja. Sklepamo, da je n naravno število, saj se v formuli pojavi izraz $f(n)$, ki je smiselen le, če je $n \in \mathbb{N}$. Torej bi natančneje zapisali

$$(\forall n \in \mathbb{N} \,.\, f(n) = 0) \vee (\exists n \in \mathbb{N} \,.\, f(n) = 1).$$

Ta zapis je res bolj natančen, a verjetno se lahko strinjamo, da ni bistveno bolj pregleden od prvotnega.

3.5 Kako beremo in pišemo simbolni zapis

Izjave, zapisane v simbolni obliki, ni težko prebrati. Na primer,

$$\forall x, y \in \mathbb{R} \,.\, x^2 = 4 \wedge y^2 = 4 \Rightarrow x = y,$$

preberemo:

> »*Za vse realne x in y, če je x^2 enako 4 in y^2 enako 4, potem je x enako y.*«

Več izkušenj pa je potrebnih, da golo branje nadgradimo z razumevanjem matematičnega pomena. Ali razumete, da zgornja izjava pravi

> »*Število 4 ima največ en realen kvadratni koren.*«

pa tudi

> »*Enačba $x^2 = 4$ ima največ eno realno rešitev.*«

Prehod iz golega branja formule do njenega razumevanja zahteva čas in vajo. Tudi prevod v obratno smer, iz matematične misli v simbolno obliko, ni preprost, zato povejmo, kako prevedemo nekatere standardne fraze.

»ϕ ***je zadosten pogoj za*** ψ« Zadošča dokazati ϕ zato, da dokažemo ψ, v simbolni obliki $\phi \Rightarrow \psi$.

»ϕ ***je potreben pogoj za*** ψ« Izjava ψ ne more veljati, ne da bi veljal ϕ. Z drugimi besedami, če velja ψ, potem velja tudi ϕ, kar se v simbolni obliki zapiše $\psi \Rightarrow \phi$.

»ϕ ***je zadosten in potreben pogoj za*** ψ« To je kombinacija prejšnjih dveh primerov, ki trdi, da iz ϕ sledi ψ in iz ψ sledi ϕ, kar pa je ekvivalenca: $\phi \Leftrightarrow \psi$.

»***Naslednje izjave so ekvivalentne:*** ϕ***,*** ψ***,*** ρ ***in*** σ***.***« To pomeni, da sta vsaki dve izmed danih izjav ekvivalentni, se pravi

$$(\phi \Leftrightarrow \psi) \wedge (\phi \Leftrightarrow \rho) \wedge (\phi \Leftrightarrow \sigma) \wedge (\psi \Leftrightarrow \rho) \wedge (\psi \Leftrightarrow \sigma) \wedge (\rho \Leftrightarrow \sigma).$$

Ker je ekvivalenca tranzitivna relacija, ni treba obravnavati vseh kombinacij, zadostujejo že tri, ki dane izjave povežejo med seboj:

$$(\phi \Leftrightarrow \psi) \wedge (\psi \Leftrightarrow \rho) \wedge (\rho \Leftrightarrow \sigma).$$

To pišemo krajše

$$\phi \Leftrightarrow \psi \Leftrightarrow \rho \Leftrightarrow \sigma,$$

čeprav je formalno gledano tak zapis nepravilen. Tako zaporedje ekvivalenc običajno dokažemo s ciklom implikacij

$$\phi \Rightarrow \psi, \qquad \psi \Rightarrow \rho, \qquad \rho \Rightarrow \sigma, \qquad \sigma \Rightarrow \phi.$$

»***Za vsak*** x ***iz*** S***, za katerega velja*** ϕ***, velja tudi*** ψ« To lahko preberemo tudi kot »*za vsak* x *iz* S*, če zanj velja* ϕ*, potem velja* ψ«, kar je v simbolni obliki

$$\forall x \in S \,.\, \phi \Rightarrow \psi.$$

Tudi izjave oblike »*vsi* ϕ*-ji so* ψ*-ji*« so te oblike, denimo »*vsa od dva večja praštevila so liha*« zapišemo

$$\forall n \in \mathbb{N} \,.\, (n > 2 \wedge \text{»}n \text{ je praštevilo«}) \Rightarrow \text{»}n \text{ je lih«}.$$

»***Enačba*** $f(x) = g(x)$ ***nima realne rešitve***« To lahko povemo takole: ni res, da obstaja $x \in \mathbb{R}$, za katerega bi veljalo $f(x) = g(x)$. S simboli zapišemo

$$\neg \exists x \in \mathbb{R} \,.\, f(x) = g(x).$$

Opozoriti velja, da iz same enačbe ne moremo vedno sklepati, kaj je neznanka. V enačbi $ax^2 + bx + c = 0$ bi za neznanko lahko načeloma imeli katerokoli od štirih spremenljivk a, b, c in x, ali pa kar vse. Večina matematikov bi sicer uganila, da je najverjetneje neznanka x, vendar se v splošnem ne moremo zanašati na običaje in uganjevanje, ampak moramo točno povedati, kateri simboli so *neznanke* in kateri *parametri*.

Kombinacije kvantifikatorjev Pozor, vrstnega reda kvantifikatorjev ne smemo mešati:

- $\forall x \in \mathbb{R} \,.\, \exists y \in \mathbb{R} \,.\, x < y$ pomeni »*vsako realno število je manjše od nekega realnega števila*« (kar je res),
- $\exists x \in \mathbb{R} \,.\, \forall y \in \mathbb{R} \,.\, x < y$ pomeni »*obstaja najmanjše realno število*« (kar ni res).

To dejstvo bomo utrjevali na vajah. Zapomnite si, da morate biti tudi pri ostalih predmetih posebej pozorni na vrstni red »za vsak« in »obstaja«. Je profesorica pri analizi rekla »*za vsak* $\epsilon > 0$ *obstaja tak* $\delta > 0$*, da …*« ali je rekla »*obstaja tak* $\delta > 0$*, da za vsak* $\epsilon > 0$ *…*«? Če boste zamešali ti dve izjavi na ustnem izpitu iz analize, boste imeli pokvarjen dan ali pa cele počitnice!

Kvantifikator z dodatnim pogojem Pogosto kvantifikacijo kombiniramo z dodatnim pogojem, na primer:

- »*Obstaja* liho *naravno število, ki ni deljivo s 7.*«
- »*Vsako* sodo *naravno število je deljivo s 3.*«

V prvem primeru je dodatni pogoj izražen z besedico »*liho*« in v drugem s »*sodo*«. Kako zapišemo take izjave s formulo in kam vtaknemo dodatni pogoj? Izjavi pretvorimo po korakih:

- »*Obstaja liho naravno število, ki ni deljivo s 7.*«
- »*Obstaja naravno število, ki je liho in ki ni deljivo s 7.*«
- »*Obstaja* x *iz* $\mathbb{N}$*, da je* x *lih in* x *ni deljiv s 7.*«
- $\exists x \in \mathbb{N} \,.\, $»$x$ *je lih*« $\wedge$ »x *ni deljiv s 7*«
- $\exists x \in \mathbb{N} \,.\, (\exists y \in \mathbb{N} \,.\, x = 2y + 1) \wedge \neg(\exists z \in \mathbb{N} \,.\, x = 7z)$

In še druga izjava:

- »*Vsako sodo naravno število je deljivo s 3.*«
- »*Vsako naravno število, ki je sodo, je deljivo s 3.*«
- »*Za vsako naravno število velja, da če je sodo, potem je deljivo s 3.*«
- »*Za vsak* x *iz* $\mathbb{N}$ *velja, če je* x *sod, potem je* x *deljiv s* 3.«
- $\forall x \in \mathbb{N} \,.\, $»$x$ *je sod*« $\Rightarrow$ »x *je deljiv s 3*«
- $\forall x \in \mathbb{N} \,.\, (\exists y \in \mathbb{N} \,.\, x = 2y) \Rightarrow (\exists z \in \mathbb{N} \,.\, x = 3z)$

Zapomnimo si, da ***dodatni pogoj pri*** $\exists$ ***izrazimo z veznikom*** $\wedge$ in ***dodatni pogoj pri*** $\forall$ ***z veznikom*** $\Rightarrow$:

Izjava	Formula
»*Za vsak $x \in A$, ki zadošča $\phi(x)$, velja $\psi(x)$*«	$\forall x \in A \,.\, (\phi(x) \Rightarrow \psi(x))$
»*Obstaja $x \in A$, ki zadošča $\phi(x)$, in zanj velja $\psi(x)$*«	$\exists x \in A \,.\, (\phi(x) \wedge \psi(x))$

Vaja 3.8. Ugotovi, kakšen je matematični pomen naslednjih izjav:

- $\forall x \in \mathbb{R} \,.\, x \leq 0 \Rightarrow \exists y \in \mathbb{R} \,.\, y^2 = x$,
- $\forall x \in \mathbb{R} \,.\, x \leq 0 \wedge \exists y \in \mathbb{R} \,.\, y^2 = x$,
- $\exists x \in \mathbb{R} \,.\, x \leq 0 \wedge x^2 = -1$,
- $\exists x \in \mathbb{R} \,.\, x \leq 0 \Rightarrow x^2 = -1$.

Najprej ugotovi, kako je treba postaviti oklepaje, da so formule berljive.

Včasih lahko izjavo zapišemo s formulo na več načinov. Na primer, izjavo

»*Za vsako pozitivno realno število x velja $\phi(x)$.*«

bi lahko zapisali kot:

- $\forall x \in \mathbb{R}_{>0} \,.\, \phi(x)$,
- $\forall x \in \{y \in \mathbb{R} \mid y > 0\} \,.\, \phi(x)$,
- $\forall x \in \mathbb{R} \,.\, x > 0 \Rightarrow \phi(x)$,
- $\forall x > 0 \,.\, \phi(x)$.

Pri prvem smo uporabili zapis $\mathbb{R}_{>0}$, ki označuje množico vseh pozitivnih realnih števil. Pri drugem smo se znebili $\mathbb{R}_{>0}$, vendar je zapis bolj nepregleden. Pri tretjem smo predstavili pozitivnost kot dodatni pogoj. Četrti način je najbolj berljiv in se pogosto uporablja, a nam ne pove, ali je x realno, celo ali racionalno število.

Od nekega člena naprej in neskončno mnogo členov Pri zaporedjih pogosto srečamo dve frazi, ki ju zapišemo s kombinacijo kvantifikatorjev. Naj bo $a : \mathbb{N} \to \mathbb{R}$ zaporedje in $\phi(x)$ izjava o realnem številu x. Izjavo

»*Od nekega člena naprej vsi členi zaporedja a zadoščajo ϕ.*«

zapišemo

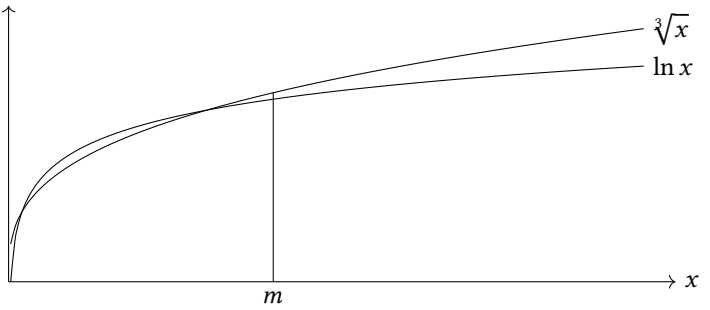
$$\exists m \in \mathbb{N} \,.\, \forall n \geq m \,.\, \phi(a_n),$$

ali brez okrajšave

$$\exists m \in \mathbb{N} \,.\, \forall n \in \mathbb{N} \,.\, n \geq m \Rightarrow \phi(a_n).$$

Členi pred a_m morda ne zadoščajo ϕ, vendar jih je končno mnogo, zato pravimo tudi, da »*skoraj vsi členi zaporedja a zadoščajo* ϕ«.

Zgled 3.9. Primerjajmo zaporedji $\sqrt[3]{n}$ in $\ln n$, katerih grafa sta prikazana na sliki 3.2. Pri majhnih n je včasih večji kubični koren, včasih logaritem, od



Slika 3.2: Grafa funkcij $\sqrt[3]{x}$ in $\ln x$

nekega člena naprej pa je kubični koren vedno večji:

$$\exists m \in \mathbb{N} \,.\, \forall n \geq m \,.\, \sqrt[3]{n} > \ln n.$$

Poiščite primeren m in dokažite, da neenakost res velja za vse $n \geq m$.

Izjavo

»*Neskončno mnogo členov zaporedja a zadošča* ϕ.«

zapišemo

$$\forall m \in \mathbb{N} \,.\, \exists n \geq m \,.\, \phi(a_n),$$

ali brez okrajšav

$$\forall m \in \mathbb{N} \,.\, \exists n \in \mathbb{N} \,.\, n \geq m \wedge \phi(a_n),$$

Formulo preberemo tudi »*a zadošča* ϕ *neskončnokrat*«.

Zgled 3.10. Zaporedje $a_n := (-1/2)^n$ ima neskončno mnogo pozitivnih členov:

$$\forall m \in \mathbb{N} \,.\, \exists n \geq m \,.\, (-1/2)^n > 0.$$

Res, za dani m vzamemo $n := 2m$, saj je $2m \geq m$ in $(-1/2)^{2m} = 1/4^m > 0$. Prav tako ima neskončno mnogo negativnih členov, saj za dani m vzamemo $n := 2m + 1$.

Pozor: člene štejemo po indeksih, ne po vrednostih. Konstantno zaporedje $a_n := 42$ ima neskončno mnogo pozitivnih členov, čeprav imajo vsi isto vrednost.

Če od nekega člena naprej vsi členi zaporedja a zadoščajo ϕ, potem neskončno mnogo členov zaporedja a zadošča ϕ. Res, če $\phi(a_n)$ velja za vse $n \geq m_0$, za dani m vzamemo $n := m + m_0$, saj je $n \geq m$ in $n \geq m_0$. Obratno ne velja: zaporedje $a_n := (-1/2)^n$ iz prejšnjega zgleda ima neskončno mnogo pozitivnih členov, ni pa res, da so od nekega člena naprej vsi njegovi členi pozitivni.

Frazi sta povezani tudi z negacijo. V poglavju 4 bomo videli, kako negacijo »porinemo« v izjavo, in ugotovili, da velja

$$\neg(\exists m \in \mathbb{N} \,.\, \forall n \geq m \,.\, \phi(a_n)) \iff \forall m \in \mathbb{N} \,.\, \exists n \geq m \,.\, \neg\phi(a_n).$$

Z besedami: ni res, da od nekega člena naprej vsi členi zaporedja a zadoščajo ϕ, natanko tedaj, ko neskončno mnogo členov zaporedja a ne zadošča ϕ. Pri zaporedju $a_n := (-1/2)^n$ to pomeni, da niso od nekega člena naprej vsi členi pozitivni, ker ima neskončno mnogo negativnih členov.

3.6 Definicije

Preden v matematičnem besedilu uporabimo simbol ali spremenljivko, ga moramo *vpeljati*. To pomeni, da moramo pojasniti, kakšen je pomen simbola. Poznamo dva osnovna načina za vpeljavo novih simbolov:

- Nov simbol s lahko ***definiramo*** kot okrajšavo za neki drugi izraz ali logično formulo.
- Nov simbol s je (vezana ali prosta) ***spremenljivka***, ki predstavlja neki (neznan, poljuben, nedoločen) element dane množice A.

V obeh primerih dodamo simbol s v ***kontekst***, se pravi v spisek znanih simbolov, o čemer bomo povedali več v poglavju 4. Če smo simbol uvedli le začasno, moramo podati njegovo območje veljavnosti, na primer trenutno poglavje ali trenutni dokaz.

Definicija kot okrajšava Definicija je v prvi vrsti **okrajšava** za neki izraz. Z njo uvedemo nov simbol s in mu pripišemo neko vrednost. Simbol s je enak vrednosti, ki smo mu jo pripisali. Simbolni zapis za definicijo je

$$s := \ldots$$

Na primer, v besedilu bi lahko napisali »*Naj bo* $s := \log_2 7 + \pi/6$.« S tem smo v kontekst dodali simbol s in predpostavko $s = \log_2 7 + \pi/6$. V matematičnih besedilih boste zasledili tudi naslednje načine za definicijo:

- $s = \log_2 7 + \pi/6$ (namesto $:=$ uporabimo $=$)
- $s \equiv \log_2 7 + \pi/6$ (namesto $:=$ uporabimo $\equiv$)
- $s \triangleq \log_2 7 + \pi/6$ (namesto $:=$ uporabimo $\triangleq$)

Kadar definiramo simbol tako, da mu priredimo funkcijski predpis, recimo

$$f := (x \mapsto x^2 + 7)$$

to raje zapišemo kot

$$f(x) := x^2 + 7.$$

Poglejmo še, kako definiramo okrajšave za logične formule. Denimo, da želimo s $\phi(x)$ označiti izjavo $\exists y \in \mathbb{R} \,.\, y^2 = x + 1$. Glede na zgornji dogovor zapišemo

$$\phi := (x \mapsto (\exists y \in \mathbb{R} \,.\, y^2 = x + 1))$$

ali

$$\phi(x) := (\exists y \in \mathbb{R} \,.\, y^2 = x + 1).$$

Vendar takega zapisa v praksi ne boste videli. Dosti bolj pogost je zapis

$$\phi(x) \quad :\Leftrightarrow \quad \exists y \in \mathbb{R} \,.\, y^2 = x + 1$$

ali pa kar $\phi(x) \Leftrightarrow \exists y \in \mathbb{R} \,.\, y^2 = x + 1$.

Definicije novih matematičnih pojmov Kaj pa definicije novih pojmov, ki jih srečujete pri predavanjih, denimo naslednji pojem iz analize:

Definicija 3.11. Zaporedje števil $a : \mathbb{N} \to \mathbb{R}$ je **neomejeno**, če za vsak $x \in \mathbb{R}$ obstaja $i \in \mathbb{N}$, da je $|a_i| > x$.

S stališča simbolnega zapisa je to le uvedba novega simbola neomejeno:

$$\text{neomejeno}(a) := (\forall x \in \mathbb{R} \,.\, \exists i \in \mathbb{N} \,.\, |a_i| > x).$$

Seveda bistvo take definicije ni le krajši zapis, ampak predvsem uporabna vrednost pojma »neomejeno zaporedje«.

3.7 Enolični obstoj

S kvantifikatorjema $\forall$ in $\exists$ lahko izrazimo tudi druge kvantifikatorje. Na primer, »*obstajata vsaj dva elementa x in y iz A, ki izpolnjujeta pogoj ϕ*«, zapišemo

$$\exists x \in A \,.\, \exists y \in A \,.\, x \neq y \wedge \phi(x) \wedge \phi(y).$$

Pozor, formula

$$\exists x \in A \,.\, \exists y \in A \,.\, \phi(x) \wedge \phi(y)$$

dopušča možnost $x = y$ in je ekvivalentna $\exists z \in A \,.\, \phi(z)$.

Vaja 3.12. Katere od formul izražajo dejstvo, da ima funkcija $f : \mathbb{R} \to \mathbb{R}$ vsaj dve različni ničli:

- $\exists x \in \mathbb{R} \,.\, \exists y \in \mathbb{R} \,.\, f(x) = 0 \wedge f(y) = 0$.
- $(\exists x \in \mathbb{R} \,.\, f(x) = 0) \wedge (\exists y \in \mathbb{R} \,.\, f(y) = 0)$.
- $\exists x \in \mathbb{R} \,.\, \exists y \in \mathbb{R} \,.\, x \neq y \Rightarrow f(x) = 0 \wedge f(y) = 0$.
- $\exists x \in \mathbb{R} \,.\, \exists y \in \mathbb{R} \,.\, x \neq y \wedge f(x) = 0 \wedge f(y) = 0$.

Pogosto želimo izraziti »*obstaja natanko en x iz A, da velja $\phi(x)$*«, kar naredimo takole:

$$(\exists x \in A \,.\, \phi(x)) \wedge (\forall y, z \in A \,.\, \phi(y) \wedge \phi(z) \Rightarrow y = z) \tag{3.1}$$

ali ekvivalentno

$$\exists x \in A \,.\, (\phi(x) \wedge \forall y \in A \,.\, \phi(y) \Rightarrow x = y). \tag{3.2}$$

Formulo (3.1) razdelimo na dva dela:

- $\exists x \in A \,.\, \phi(x)$ pove, da obstaja *vsaj en* želeni x.
- $\forall y, z \in A \,.\, \phi(y) \wedge \phi(z) \Rightarrow y = z$ pove, da sta vsaka dva elementa, ki zadoščata ϕ, enaka; se pravi, da obstaja *največ en* želeni x.

Formulo (3.2) preberemo takole: obstaja $x \in A$, ki zadošča $\phi(x)$, in vsak element, ki zadošča ϕ, je enak x.

Za formulo (3.1) uporabljamo okrajšavo

$$\exists! x \in A \,.\, \phi(x),$$

ki jo beremo »*obstaja natanko en x iz A, da velja $\phi(x)$*«. Uporablja se tudi zapis $\exists^1 x \in A \,.\, \phi(x)$.

3.8 Enolični opis

Če dokažemo, da obstaja natanko en $x \in A$, ki zadošča pogoju $\phi(x)$, potem se lahko nanj smiselno sklicujemo s »*tisti x iz A, ki zadošča $\phi(x)$*«, na primer:

- »*tisto realno število x, za katero je $x^3 = 2$*« (namreč kubični koren iz 2),
- »*tista množica S, ki nima nobenega elementa*« (namreč prazna množica).

Ni pa vsak tovrstni zapis veljaven:

- »*tisto racionalno število x, za katero je $x^2 = 2$*« (takega števila ni),
- »*tisto realno število x, za katero je $x^2 = 2$*« (sta dve taki števili),
- »*tista množica S, ki ima natanko en element*« (takih množic je več).

Za opredelitev matematičnih objektov z enoličnim opisom uvedimo simbolni zapis. Če dokažemo

$$\exists! x \in A \,.\, \phi(x)$$

potem lahko pišemo

$$\iota x \in A \,.\, \phi(x),$$

in beremo »*tisti $x \in A$, za katerega velja $\phi(x)$*«. Velja

$$\phi(\iota x \in A \,.\, \phi(x)).$$

Spremenljivka x je *vezana* v $\iota x \in A \,.\, \phi(x)$.

Zgled 3.13. Denimo, da še ne bi poznali simbola $\sqrt{}$ za kvadratne korene. Tedaj bi lahko kvadratni koren iz 2 zapisali kot

$$\iota x \in \mathbb{R} \,.\, (x > 0 \wedge x^2 = 2)$$

Še več, preslikavo $\sqrt{} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ lahko definiramo takole:

$$\sqrt{} : x \mapsto (\iota y \in \mathbb{R} \,.\, (y \geq 0 \wedge y^2 = x)).$$

Vaja 3.14. Zapišite »limita zaporedja $a : \mathbb{N} \to \mathbb{R}$« z operatorjem ι, pod predpostavko, da je a konvergentno zaporedje. Najprej povejte z besedami »limita zaporedja a je tisti $x \in \mathbb{R}$, ki ...«, nato pa zapišite še v obliki $\iota x \in \mathbb{R} \,.\, \ldots$.

3.9 Vaje

Vaja 3.15. Zapiši $a = b \neq c = d$ brez okrajšav.

Vaja 3.16. Je »*n je sod in* $n > 2$« potreben ali zadosten pogoj za »*n ni praštevilo*«?

Vaja 3.17. Podaj konkretne primere izjav ϕ, ψ in ρ, iz katerih je razvidno, da izjava $(\phi \Leftrightarrow \psi) \wedge (\psi \Leftrightarrow \rho)$ *ni* ekvivalentna niti $(\phi \Leftrightarrow \psi) \Leftrightarrow \rho$ niti $\phi \Leftrightarrow (\psi \Leftrightarrow \rho)$.

Vaja 3.18. V simbolni obliki zapiši »*n je lih*« in »*n je praštevilo*«. Namig: n je lih, kadar obstaja naravno število k, za katerega velja $n = 2k + 1$, in n je praštevilo, kadar je $n > 1$ in n *ni* zmnožek dveh naravnih števil, ki sta obe večji od 1.

Vaja 3.19. Zapiši v simbolni obliki: Sistem enačb

$$a_1 x + b_1 y = c_1,$$
$$a_2 x + b_2 y = c_2$$

nima pozitivnih realnih rešitev x, y.

Vaja 3.20. Zapiši v simbolni obliki:

1. »*Enačba* $f(x) = g(x)$ *ima največ eno realno rešitev.*«
2. »*Enačba* $f(x) = g(x)$ *ima več kot eno realno rešitev.*«
3. »*Enačba* $f(x) = g(x)$ *ima natanko dve realni rešitvi.*«

4

Dokazi

V srednji šoli se dijaki pri matematiki učijo, *kako* se kaj izračuna. Na univerzi imajo študentje matematike pred seboj zahtevnejšo nalogo: poleg *kako* morajo vedeti tudi *zakaj*. Od njih se pričakuje, da bodo računske postopke znali tudi utemeljiti, ne pa samo slediti pravilom, ki jih je predpisal učitelj. Razumeti morajo dokaze znamenitih izrekov in sami poiskati dokaze preprostih izjav. Da bi se lažje spopadli s temi novimi nalogami, bomo prvi del predmeta Logika in množice posvetili matematični infrastrukturi: izjavam, pravilom sklepanja in dokazom. Učili se bomo, kako pišemo dokaze, kako jih analiziramo in kako jih sami poiščemo.

4.1 Kaj je matematični dokaz?

Osrednji pojem matematične aktivnosti je *dokaz*. Namen dokaza je s pomočjo točno določenih in vnaprej dogovorjenih *pravil sklepanja* utemeljiti neko matematično *izjavo*. Načeloma mora dokaz vsebovati vse podrobnosti in natanko opisati posamezne korake sklepanja, ki vodijo do želene matematične izjave. Ker bi bili taki dokazi zelo dolgi in bi vsebovali nezanimive podrobnosti, matematiki običajno predstavijo samo oris ali glavno zamisel dokaza. Izkušenemu matematiku to zadošča, saj zna oris sam dopolniti do pravega

dokaza. Matematik začetnik seveda potrebuje več podrobnosti. Poglejmo si primer.

Izrek 4.1. *Za vsako celo število n je $n^3 - n$ deljivo s 3.*

Izkušeni matematik je ta izrek že videl, še sam ne ve kolikokrat, zato bi le pripomnil, da je število $n^3 - n$ zmnožek treh zaporednih celih števil. Tak namig bi starejšemu študentu matematike zadoščal, da bi sestavil dokaz:

> *Dokaz.* Ker je $n^3 - n = (n-1) \cdot n \cdot (n+1)$, je $n^3 - n$ zmnožek treh zaporednih celih števil, od katerih je eno deljivo s 3, torej je tudi $n^3 - n$ deljivo s 3. □

Čeprav bi bila večina matematikov s tem dokazom zadovoljna, bi morali za popoln dokaz preveriti še nekaj podrobnosti:

- Ali velja $n^3 - n = (n-1) \cdot n \cdot (n+1)$?
- Ali je izmed treh zaporednih celih števil eno deljivo s 3?
- Ali je zmnožek treh števil deljiv s 3, če je eno od njih deljivo s 3?

S srednješolskim znanjem algebre ugotovimo, da je odgovor na prvo vprašanje pritrdilen. Tudi odgovora na drugo in tretje vprašanje sta očitno pritrdilna, mar ne? To pa ne pomeni, da ju ni treba dokazati. Nasprotno, zgodovina matematike nas uči, da moramo prav »očitne« izjave še posebej skrbno preveriti. V idealnem primeru bi bil dokaz zapisan tako, da bi lahko njegovo pravilnost preverili mehansko, z računalnikom.[1]

Če dokaz izreka 4.1 zapišemo preveč podrobno, postane dolgočasen in nerazumljiv:

> *Dokaz.* Naj bo n poljubno celo število. Tedaj velja
>
> $$\begin{aligned} n^3 - n &= n \cdot n^2 - n \cdot 1 \\ &= n \cdot (n^2 - 1) \\ &= n \cdot ((n+1) \cdot (n-1)) \\ &= n \cdot ((n-1) \cdot (n+1)) \\ &= (n \cdot (n-1)) \cdot (n+1) \\ &= (n-1) \cdot n \cdot (n+1). \end{aligned}$$

[1] Kogar to zanima, se lahko nauči uporabljati kak dokazovalni pomočnik, v zadnjem času hitro napreduje Lean.

Vidimo, da je $n^3 - n$ zmnožek treh zaporednih celih števil. Dokažimo, da je eno od njih deljivo s 3. Število n lahko enolično zapišemo kot $n = 3k + r$, kjer je k celo število in $r = 0$, $r = 1$ ali $r = 2$. Obravnavajmo tri primere:

- če je $r = 0$, je $n = 3k$, zato je n deljiv s 3,
- če je $r = 1$, je $n-1 = (3k+1)-1 = 3k+(1-1) = 3k+0 = 3k$, zato je $n - 1$ deljiv s 3,
- če je $r = 2$, je $n + 1 = (3k + 2) + 1 = 3k + (2 + 1) = 3k + 3 = 3k + 3 \cdot 1 = 3(k + 1)$, zato je $n + 1$ deljiv s 3.

Vemo torej, da je $n - 1$, n ali $n + 1$ deljiv s 3. Obravnavamo tri primere:

- Če je $n - 1$ deljiv s 3, tedaj obstaja celo število k, da je $n-1 = 3k$. V tem primeru je $(n-1)n(n+1) = (3k)n(n+1) = 3(kn(n + 1))$, zato je $(n - 1)n(n + 1)$ deljivo s 3.
- Če je n deljiv s 3, tedaj obstaja celo število k, da je $n = 3k$. V tem primeru je $(n - 1)n(n + 1) = (n - 1)(3k)(n + 1) = (3k)(n-1)(n+1) = 3(k(n-1)(n+1))$, zato je $(n-1)n(n+1)$ deljivo s 3.
- Če je $n + 1$ deljiv s 3, tedaj obstaja celo število k, da je $n + 1 = 3k$. V tem primeru je $(n - 1)n(n + 1) = (n - 1)n(3k) = (n - 1)(3k)n = (3k)(n - 1)n = 3(k(n - 1)n)$, zato je $(n - 1)n(n + 1)$ deljivo s 3.

V vsakem primeru je $(n-1)n(n+1)$ deljivo s 3. Ker smo dokazali, da je $n^3 - n = (n - 1)n(n + 1)$, je tudi $n^3 - n$ deljivo s 3. □

Tovrstni dokazi so res le sami sebi namen. Dober dokaz poleg gole resnice bralcu na razumljiv način posreduje tudi matematične ideje, na katerih sloni dokaz. Ta socialna komponenta dokaza je izrazito odvisna ne le od pisca, ampak tudi od bralca, ki mu je dokaz namenjen.

4.2 Struktura dokaza

Matematiki v sklopu svojih aktivnosti *konstruiramo* matematične objekte:

- v geometriji konstruiramo trikotnike z ravnilom in šestilom,

- računamo števke števila π, s čimer konstruiramo njegove približke,
- ko rešujemo enačbo, konstruiramo število, ki ji zadošča,
- konstruiramo elemente množice, na primer $(2, \mathsf{in}_1(3)) \in \mathbb{N} \times (\mathbb{Z} + \mathbb{Z})$.

Tudi na dokaze lahko gledamo kot na konstrukcije, ki jih gradimo s pomočjo *pravil sklepanja*. Le-ta povedo, kakšna so »pravila igre« v dokazovanju, ne pa tudi, kako dobro igrati igro dokazovanja. Pri tem predmetu bomo spoznali pravila in podali nekaj namigov, kako konstruirati osnovne dokaze, pri ostalih predmetih pa boste videli »žive dokaze«, ki imajo manj tehničnih podrobnosti in se bolj osredotočajo na komuniciranje idej.

Dokaz ima ugnezdeno strukturo: sestoji iz poddokazov, ki sestoje iz nadaljnjih poddokazov itn., ki se zaključijo z osnovnimi koraki. Ta struktura iz običajnega besedila ni razvidna, a je prisotna. Za zgled vzemimo naslednji izrek.

Izrek 4.2. *Za vse izjave p, q, r velja $(p \vee q) \wedge r \Rightarrow (p \wedge r) \vee (q \wedge r)$.*

Dokaz. Predpostavimo $p \vee q$ in r. Če velja p, potem sledi $p \wedge r$ ter od tod $(p \wedge r) \vee (q \wedge r)$. Če pa velja q, sledi $q \wedge r$ ter spet $(p \wedge r) \vee (q \wedge r)$. □

Zgornji dokaz z dodanimi podrobnostmi in označeno ugnezdeno strukturo je prikazan na sliki 4.1. Zamik vrstice pove, kako globoko v dokazu stojimo: vrstici, ki postavi cilj, sledi njen dokaz eno stopnjo globlje. S škatlo obdamo tisti del dokaza, pri katerem iz zamikov samih ne bi bilo razvidno, kje se konča. Zunanja škatla najprej vpelje spremenljivke p, q in r, nato pove, kaj bomo dokazali, temu pa sledi dokaz. Vrstice so oštevilčene, da se lahko nanje sklicujemo. Notranji škatli sta obravnavi dveh primerov.

Ko pišemo ali beremo dokaz, moramo v vsakem trenutku poznati

- **cilj**: kaj trenutno dokazujemo in
- **kontekst**: katere spremenljivke, predpostavke in že dokazana dejstva imamo na voljo.

Na primer, v vrstici (6) iz dokaza na sliki 4.1 je cilj $(p \wedge r) \vee (q \wedge r)$, veljavne so spremenljivke p, q in r, na voljo imamo predpostavko (2), dokazali pa smo že dejstvi (4) in (5). Ko napravimo korak v dokazu, mora biti utemeljen z enim od pravil sklepanja. Dokaz je popoln, ko smo utemeljili vse poddokaze. V nadaljevanju spoznajmo pravila sklepanja in druge korake, ki tvorijo dokaz.

1 Dokažimo $(p \vee q) \wedge r \Rightarrow (p \wedge r) \vee (q \wedge r)$:
2 Predpostavimo $(p \vee q) \wedge r$.
3 Dokažimo $(p \wedge r) \vee (q \wedge r)$:
4 Zaradi (2) velja $p \vee q$.
5 Zaradi (2) velja r.
6 Uporabimo (4) in obravnavamo dva primera:
7 Predpostavimo p.
8 Dokažimo $(p \wedge r) \vee (q \wedge r)$:
9 Dokažimo levi disjunkt $p \wedge r$:
10 • p velja zaradi (7),
11 • r velja zaradi (5).
12 Predpostavimo q.
13 Dokažimo $(p \wedge r) \vee (q \wedge r)$:
14 Dokažimo desni disjunkt $q \wedge r$:
15 • q velja zaradi (12),
16 • r velja zaradi (5).

Slika 4.1: Dokaz izreka 4.2

Vpeljava spremenljivke Nekatera pravila sklepanja zahtevajo, da v dokazu ***vpeljemo spremenljivko***. To storimo tako, da jo naznanimo skupaj z njeno domeno:

»*Naj bo* $x \in A$.«

S tem postane x veljavna spremenljivka, ki jo smemo uporabljati. O njej vemo le to, da je element množice A, ne vemo pa, kateri element – pravimo, da je x ***prosta spremenljivka***. V matematičnih besedilih boste zasledili tudi naslednje fraze, ki uvedejo prosto spremenljivko:

- »*Naj bo* $x \in A$ *poljuben.*«
- »*Fiksirajmo* $x \in A$.«
- »*Izberimo* $x \in A$.«

Pozor: besedi »fiksirajmo« in »izberimo« bi dali komu misliti, da si lahko izbere točno določen element po lastni volji, a si je bolje predstavljati, da je x »neznan« ali »nedoločen«.

Spremenljivka ima območje veljavnosti, ki je omejeno s poddokazom, v katerem jo vpeljemo.

Zgled 4.3. V dokazu na sliki 4.1 vpeljemo spremenljivke p, q in r v vrstici (**??**). Veljavne so v celotnem dokazu.

Pozor: spremenljivk ne vpeljemo kar tako, ampak le takrat, ko uporabimo pravilo sklepanja, ki to zahteva.

Vpeljava predpostavke Nekatera pravila sklepanja zahtevajo, da ***vpeljemo predpostavko*** ϕ (ali ***hipotezo***), se pravi, da se pretvarjamo, da izjava ϕ velja. V takem primeru zapišemo:

»*Predpostavimo* ϕ.«

Včasih vpeljemo predpostavko tudi s »*če velja* ϕ«.

Predpostavka ima svoje območje veljavnosti, ki je omejeno s poddokazom, v katerem jo vpeljemo.

Zgled 4.4. V dokazu na sliki 4.1 v vrstici (2) predpostavimo $(p \vee q) \wedge r$, območje veljavnosti je do konca dokaza. V vrstici (7) predpostavimo p, območje veljavnosti pa je prva notranja škatla. V vrstici (12) predpostavimo q, območje veljavnosti pa je druga notranja škatla.

Kadar se skličemo na že znano izjavo ali na predpostavko, pravimo, da smo jo ***uporabili***.

Zgled 4.5. V dokazu na sliki 4.1 smo predpostavko (2) uporabili v vrsticah (4) in (5). V vrsticah (10) in (11) smo uporabili predpostavko (7) in dejstvo (5). V vrsticah (15) in (16) smo uporabili predpostavko (12) in dejstvo (5).

Pozor: predpostavk ne vpeljemo kar tako, ampak le takrat, ko uporabimo pravilo sklepanja, ki to zahteva.

Okrajšava V dokazu smemo kadarkoli ***vpeljati okrajšavo***, na primer:

»*Naj bo* $\varphi := \frac{1+\sqrt{5}}{2}$.«

V nadaljevanju dokaza smemo uporabljati φ in dejstvo, da je enak $(1 + \sqrt{5})/2$.

Vaja 4.6. Ali je v zvezi z $(1 + \sqrt{5})/2$ kaj posebnega?

Izpeljava dejstva V dokazu smemo kadarkoli ***izpeljati dejstvo***, kar pomeni, da utemeljimo neko izjavo, ki jo nameravamo kasneje uporabiti. Če je utemeljitev dejstva ϕ kratka, zapišemo:

»*Zaradi … velja* ϕ.«

Če utemeljitev zahteva celoten poddokaz, ga podamo:

Velja ϕ:
⋯ ⟨dokaz ϕ⟩ ⋯

Zgled 4.7. V dokazu na sliki 4.1 nismo vpeljali nobene okrajšave, smo pa v vrsticah (4) in (5) izpeljali dejstvi $p \vee q$ in r. Dejstvo (4) smo uporabili v vrstici (6), dejstvo (5) pa v vrsticah (11) in (16).

Posvetimo se še pravilom sklepanja, ki jih delimo na:

- pravila sklepanja za logične operacije:
  - pravila vpeljave, s katerimi dokazujemo izjave,
  - pravila uporabe, s katerimi uporabljamo predpostavke in dejstva;
- pravila sklepanja za enakost;
- pravilo o izključenem tretjem in dokaz s protislovjem.

4.3 Pravila vpeljave in uporabe

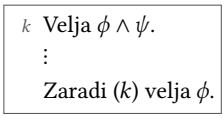
Vsaka logična operacija ima svoja pravila vpeljave in uporabe, s katerimi dokazujemo še nedokazane izjave in uporabljamo že dokazane izjave.

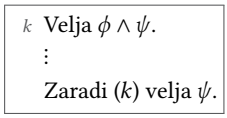
Konjunkcija Konjunkcijo $\phi \wedge \psi$ dokažemo tako, da posebej dokažemo ϕ in posebej ψ. Pravilo vpeljave torej predstavimo takole:

Dokažimo $\phi \wedge \psi$:
Dokažimo ϕ:
⋯ ⟨dokaz ϕ⟩ ⋯
Dokažimo ψ:
⋯ ⟨dokaz ψ⟩ ⋯

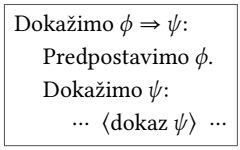
Kaj pa, če že vemo, da velja $\phi \wedge \psi$? Tedaj lahko izpeljemo ϕ in izpeljemo ψ,

zato imamo dve pravili uporabe:

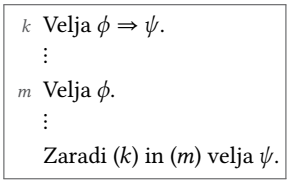




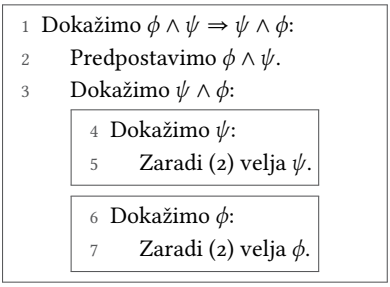
Implikacija Implikacijo $\phi \Rightarrow \psi$ dokažemo tako, da predpostavimo ϕ in dokažemo ψ. Pravilo vpeljave torej predstavimo takole:



Če vemo, da velja $\phi \Rightarrow \psi$, in vemo, da velja ϕ, lahko izpeljemo ψ. Pravilo uporabe za implikacijo, ki se imenuje tudi ***modus ponens***, se torej glasi:

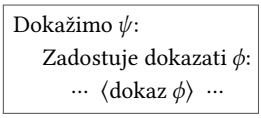


Zgled 4.8. Naj bosta ϕ in ψ izjavi. Takole dokažemo, da iz $\phi \wedge \psi$ sledi $\psi \wedge \phi$:



Celoten dokaz je vpeljava implikacije. V vrsticah (3)–(7) vidimo vpeljavo konjunkcije, v vrsticah (5) in (7) pa uporabo konjunkcije.

V dokazih boste videli frazo »*zadostuje dokazati*«:



To je pravzaprav uporaba implikacije $\phi \Rightarrow \psi$, ki pa jo je pisec zamolčal, ker meni, da je očitna. Bolj podrobno bi zapisali:

Dokažimo ψ:
  Ker velja $\phi \Rightarrow \psi$, zadostuje dokazati ϕ:
    $\cdots$ ⟨dokaz ϕ⟩ $\cdots$

Še vedno od bralca pričakujemo, da bo vedel, zakaj velja $\phi \Rightarrow \psi$. Običajno je to splošno znana implikacija, ki je nima smisla vedno znova ponavljati.

Disjunkcija Disjunkcijo $\phi \vee \psi$ dokažemo tako, da dokažemo enega od disjunktov, zato imamo dve pravili vpeljave:

Dokažimo $\phi \vee \psi$:
  Dokažimo levi disjunkt ϕ:
    $\cdots$ ⟨dokaz ϕ⟩ $\cdots$

Dokažimo $\phi \vee \psi$:
  Dokažimo desni disjunkt ψ:
    $\cdots$ ⟨dokaz ψ⟩ $\cdots$

Če vemo, da velja $\phi \vee \psi$, ne vemo pa, kateri od disjunktov velja, obravnavamo dva primera:

k Velja $\phi \vee \psi$.
⋮
Dokažimo ρ:
  Uporabimo (k) in obravnavamo dva primera:
    Predpostavimo ϕ.
    Dokažimo ρ:
      $\cdots$ ⟨dokaz ρ⟩ $\cdots$
    Predpostavimo ψ.
    Dokažimo ρ:
      $\cdots$ ⟨dokaz ρ⟩ $\cdots$

V prvem primeru smo izpeljali cilj pod predpostavko, da velja levi disjunkt ϕ, v drugem pa pod predpostavko, da velja desni disjunkt ψ.

Zgled 4.9. Obravnavajmo nekoliko bolj zapleten dokaz:

1 Dokažimo $((p \Rightarrow r) \wedge (q \Rightarrow r)) \Rightarrow (p \vee q \Rightarrow r)$:
2 Predpostavimo $(p \Rightarrow r) \wedge (q \Rightarrow r)$.
3 Dokažimo $p \vee q \Rightarrow r$:
4 Predpostavimo $p \vee q$.
5 Dokažimo r:
6 Uporabimo (4) in obravnavamo dva primera:
7 Predpostavimo p.
8 Dokažimo r:
9 Zaradi (2) velja $p \Rightarrow r$.
10 Zaradi (9) in (7) velja r.
11 Predpostavimo q.
12 Dokažimo r:
13 Zaradi (2) velja $q \Rightarrow r$.
14 Zaradi (13) in (11) velja r.

Celoten dokaz je vpeljava implikacije. V vrsticah (3)–(14) vidimo še eno vpeljavo implikacije, v vrsticah (6)–(14) pa uporabo disjunkcije. V vrsticah (9) in (13) vidimo uporabo konjunkcije, v vrsticah (10) in (14) pa uporabo implikacije.

Resnica Resnice $\top$ ni treba dokazovati, zapišemo »očitno«:

Dokažimo $\top$:
Očitno.

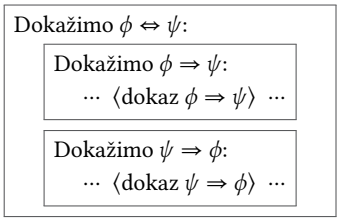
Običajno $\top$ nastopi kot cilj, ko prvotni cilj poenostavimo v ekvivalentno obliko in dobimo $\top$. Na primer, cilj $12^2 + 12^2 < 17^2$ lahko z računanjem prevedemo v ekvivalentno izjavo $288 < 289$, ki je ekvivalentna $\top$. S tem je dokaz zaključen, saj $\top$ ni treba dokazati.

Pravila uporabe za resnico ni.

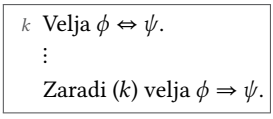
Neresnica Neresnica $\bot$ nima pravila vpeljave. (To ne pomeni, da $\bot$ ni možno dokazati, saj lahko sledi iz protislovnih predpostavk.) Pravilo uporabe za $\bot$ pravi, da iz neresnice sledi karkoli:

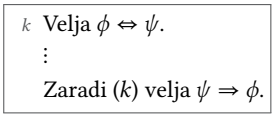
k Velja $\bot$.
$\vdots$
Zaradi (k) velja ρ.

Ekvivalenca Ekvivalenco $\phi \Leftrightarrow \psi$ dokažemo tako, da posebej dokažemo obe implikaciji:

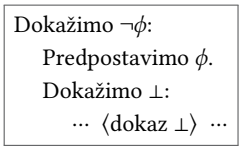


Ekvivalenco uporabimo tako, da izpeljemo eno od implikacij:



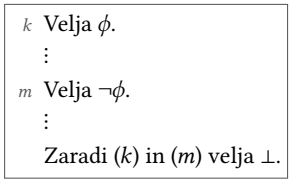


Negacija Negacijo $\neg\phi$ dokažemo tako, da predpostavimo ϕ in dokažemo $\bot$:



Namesto »dokazujemo neresnico $\bot$«, običajno rečemo »iščemo protislovje«.

Pravilo uporabe za negacijo pravi, da iz ϕ in $\neg\phi$ sledi neresnica:



Namesto »dokazali smo neresnico« rečemo »izpeljali smo protislovje«.

Zgled 4.10. Dokažimo, da iz protislovja sledi karkoli. Natančneje, iz p in $\neg p$

sledi poljubna izjava q:

```
1 Dokažimo p ∧ ¬p ⇒ q:
2   Predpostavimo p ∧ ¬p.
3   Dokažimo q:
4     Zaradi (2) velja p.
5     Zaradi (2) velja ¬p.
6     Zaradi (4) in (5) velja ⊥.
7     Zaradi (6) velja q.
```

Celoten dokaz je vpeljava implikacije. V vrsticah (4) in (5) smo uporabili konjunkcijo, v vrstici (6) negacijo, v vrstici (7) pa neresnico.

Zgled 4.11. Dokažimo, da iz p sledi $\neg\neg p$:

```
1 Dokažimo p ⇒ ¬¬p:
2   Predpostavimo p.
3   Dokažimo ¬¬p:
4     Predpostavimo ¬p.
5     Dokažimo ⊥:
6       Zaradi (2) in (4) velja ⊥.
```

Celoten dokaz je vpeljava implikacije. V vrsticah (3)–(6) vidimo vpeljavo negacije, v vrstici (6) pa uporabo negacije.

Univerzalni kvantifikator Izjavo $\forall x \in A \,.\, \phi(x)$ dokažemo tako, da vpeljemo spremenljivko $x \in A$ in dokažemo $\phi(x)$:

```
Dokažimo ∀x ∈ A . φ(x):
  Naj bo x ∈ A.
  Dokažimo φ(x):
    ⋯ ⟨dokaz φ(x)⟩ ⋯
```

Pozor: spremenljivka x mora biti *sveža*, se pravi, da na tem mestu v dokazu ni veljavna. Če je x že veljavna, izberemo svežo spremenljivko y in izjavo $\forall x \in A \,.\, \phi(x)$ najprej zapišemo kot $\forall y \in A \,.\, \phi(y)$.

Če vemo, da velja $\forall x \in A \,.\, \phi(x)$, in vemo, da je $\langle \text{izraz} \rangle \in A$, lahko

izpeljemo $\phi(\langle \text{izraz} \rangle)$:

k Velja $\forall x \in A \,.\, \phi(x)$.
⋮
m Velja $\langle \text{izraz} \rangle \in A$.
⋮
Zaradi (k) in (m) velja $\phi(\langle \text{izraz} \rangle)$.

Zgled 4.12. Sedaj lahko dokažemo, da izjava $\forall x \in \emptyset \,.\, \phi(x)$ velja, upoštevaje dejstvo, da za vsak x velja $\neg(x \in \emptyset)$:

1 Dokažimo $\forall x \in \emptyset \,.\, \phi(x)$:
2 Naj bo $x \in \emptyset$.
3 Dokažimo $\phi(x)$:
4 Velja $\neg(x \in \emptyset)$.
5 Zaradi (2) in (4) velja $\bot$.
6 Zaradi (5) velja $\phi(x)$.

Celoten dokaz je vpeljava univerzalnega kvantifikatorja. V vrstici (5) smo uporabili negacijo, v vrstici (6) pa neresnico.

Eksistenčni kvantifikator Izjavo $\exists x \in A \,.\, \phi(x)$ dokažemo tako, da podamo element množice A, ki zadošča ϕ:

Dokažimo $\exists x \in A \,.\, \phi(x)$:
 Podamo $x := \langle \text{izraz} \rangle$.
  Dokažimo $\langle \text{izraz} \rangle \in A$:
  ⋯ ⟨dokaz $\langle \text{izraz} \rangle \in A$⟩ ⋯
  Dokažimo $\phi(\langle \text{izraz} \rangle)$:
  ⋯ ⟨dokaz $\phi(\langle \text{izraz} \rangle)$⟩ ⋯

Opomba: $\langle \text{izraz} \rangle$ sme vsebovati vse proste spremenljivke, ki so trenutno na voljo (x *ni* na voljo).

Če vemo, da velja $\exists x \in A \,.\, \phi(x)$, smemo vpeljati spremenljivko $x \in A$, za katero velja $\phi(x)$:

k Velja $\exists x \in A \,.\, \phi(x)$.
⋮
Zaradi (k) imamo $x \in A$ in $\phi(x)$.

Pozor: spremenljivka x mora biti sveža, se pravi, da na tem mestu v dokazu

ni veljavna. Če je x že veljavna, izberemo svežo spremenljivko y in izjavo $\exists x \in A \,.\, \phi(x)$ najprej zapišemo kot $\exists y \in A \,.\, \phi(y)$.

Zgled 4.13. Dokažimo še, da velja $\neg\exists x \in \emptyset \,.\, \phi(x)$, upoštevaje dejstvo, da za vsak x velja $\neg(x \in \emptyset)$:

```
1 Dokažimo ¬∃x ∈ ∅ . φ(x):
2     Predpostavimo ∃x ∈ ∅ . φ(x).
3     Dokažimo ⊥:
4         Zaradi (2) imamo x ∈ ∅ in φ(x).
5         Zaradi (4) velja x ∈ ∅.
6         Velja ¬(x ∈ ∅).
7         Zaradi (5) in (6) velja ⊥.
```

Celoten dokaz je vpeljava negacije. V vrstici (4) smo uporabili eksistenčni kvantifikator, v vrstici (5) konjunkcijo, v vrstici (7) pa negacijo.

4.4 Enakost in ekvivalenca

Pravila za enakost se glasijo:

- ***refleksivnost***: $a = a$,
- ***simetričnost***: če $a = b$, potem $b = a$,
- ***tranzitivnost***: če $a = b$ in $b = c$, potem $a = c$,
- ***pravilo zamenjave***: če $a = b$ in $\phi(a)$, potem $\phi(b)$.

Zaenkrat enakosti ne bomo posvečali posebne pozornosti, saj jo v praksi študenti dobro obvladajo.

Zgled 4.14. Pravilo za simetričnost enakosti sledi iz refleksivnosti in pravila zamenjave. Predpostavimo, da velja $a = b$, in obravnavajmo izjavo $\phi(x) := (x = a)$. Zaradi refleksivnosti velja $\phi(a)$, torej po pravilu zamenjave velja $\phi(b)$, kar je enako $b = a$.

Vaja 4.15. Ali tudi tranzitivnost enakosti sledi iz refleksivnosti in pravila zamenjave?

Pravila za logično ekvivalenco so podobna pravilom za enakost:

- ***refleksivnost***: $\phi \Leftrightarrow \phi$,

- ***simetričnost***: če $\phi \Leftrightarrow \psi$, potem $\psi \Leftrightarrow \phi$,
- ***tranzitivnost***: če $\phi \Leftrightarrow \psi$ in $\psi \Leftrightarrow \xi$, potem $\phi \Leftrightarrow \xi$,
- ***pravilo zamenjave***: če $\phi \Leftrightarrow \psi$, smemo ϕ nadomestiti s ψ.

Zadnje pravilo dovoljuje, da lahko izjave poenostavljamo in predelujemo, če le pazimo, da ne kršimo logične ekvivalence.

Vaja 4.16. S pravili sklepanja za ekvivalenco dokažite refleksivnost, simetričnost in tranzitivnost ekvivalence. Kako bi dokazali pravilo zamenjave? Upoštevajte, da smemo zamenjati izjavo z njej ekvivalentno kjerkoli, tudi znotraj druge izjave.

Reševanje enačb V osnovni in srednji šoli nas učijo, da smemo na obeh straneh enačbe prišteti ali odšteti poljuben izraz, pomnožiti ali deliti smemo s poljubnim neničelnim izrazom, ipd. Od kod izhajajo ta pravila? In kaj pomeni, da smo enačbo »rešili«? Rešitev enačbe

$$x^2 - 5x + 6 = 0$$

običajno zapišemo takole:

$$x_1 = 2, \qquad x_2 = 3.$$

Kako naj to razumemo s stališča matematične logike? Treba je pojasniti dvoje: kaj pomenita x_1 in x_2, saj v prvotni enačbi nastopa spremenljivka x, ter kako naj razumemo vejico med izjavama $x_1 = 2$ in $x_2 = 3$. Z indeksoma 1 in 2 štejemo rešitve enačbe in sta v resnici nepotrebna,[2] na kar kaže tudi dejstvo, da pišemo $x = \ldots$ in ne $x_1 = \ldots$, kadar je rešitev ena sama. Torej bi lahko rešitev zapisali kot

$$x = 2, \quad x = 3.$$

Sedaj pa je tudi jasno, da bi namesto vejice morala stati disjunkcija, se pravi

$$x = 2 \vee x = 3.$$

Začetna enačba in tako zapisana rešitev sta logično ekvivalentni:

$$x^2 - 5x + 6 = 0 \iff x = 2 \vee x = 3.$$

Povzemimo: reševanje enačbe je postopek, s katerim dano enačbo $f(x) = g(x)$ prevedemo v njeno *logično ekvivalentno* obliko $x = a_1 \vee x = a_2 \vee \cdots \vee x = a_n$, iz katere so neposredno razvidne rešitve enačbe.

[2] Kako pa bi zapisali rešitve enačbe $x_1^2 - 5x_1 + 6 = 0$?

Pravila za reševanje enačb torej niso nič drugega kot recepti, s pomočjo katerih enačbo predelamo v njeno *ekvivalentno* obliko, ki je korak bližje končni obliki, v kateri bi radi zapisali rešitev. To pojasnjuje srednješolska pravila za reševanje enačb. Na primer, za realna števila $a, b, c \in \mathbb{R}$ vedno velja

$$a = b \Rightarrow c \cdot a = c \cdot b,$$

medtem ko obratna implikacija

$$c \cdot a = c \cdot b \Rightarrow a = b$$

za splošne a in b velja le v primeru, ko je $c \neq 0$. Ker pri reševanju enačb potrebujemo implikacijo v obe smeri, srednješolce učimo, da smejo enačbo množiti samo z od nič različnimi števili.

Vaja 4.17. Ali smemo obe strani enačbe kvadrirati?

Vaja 4.18. Denimo, da v postopku reševanja enačbe pomotoma naredimo korak, ki ni ekvivalenca, ampak le implikacija:

$$\begin{aligned} f_1(x) &= g_1(x) \Leftrightarrow \\ &\vdots \\ f_k(x) &= g_k(x) \Rightarrow \qquad \text{(napačen korak)} \\ f_{k+1}(x) &= g_{k+1}(x) \Leftrightarrow \\ &\vdots \\ x = a_1 \vee \cdots \vee x &= a_n \end{aligned}$$

Smo dobili preveč ali premalo rešitev prvotne enačbe?

4.5 Pravilo o izključenem tretjem

Pravilo o izključenem tretjem se glasi:

$$\text{»}\textit{Za vsako izjavo } \phi \textit{ velja } \phi \vee \neg\phi.\text{«}$$

Se pravi, da je vsaka izjava bodisi resnična bodisi neresnična. Torej ni »tretje možnosti« za resničnostno vrednost izjave ϕ, od koder izhaja ime pravila.

Pravilo o izključenem tretjem omogoča *posredne* dokaze izjav, od katerih je najbolj znano ***dokazovanje s protislovjem***:

Dokažimo ϕ s protislovjem:
  Predpostavimo $\neg\phi$.
  Dokažimo $\bot$:
    $\cdots$ ⟨dokaz $\bot$⟩ $\cdots$

Dokaz s protislovjem sloni na dejstvu, da lahko dokažemo $\neg\neg\phi \Rightarrow \phi$, vendar pri tem potrebujemo pravilo o izključenem tretjem:

1 Dokažimo $\neg\neg\phi \Rightarrow \phi$:
2 Predpostavimo $\neg\neg\phi$.
3 Dokažimo ϕ:
4 Ker velja $\phi \vee \neg\phi$, obravnavamo dva primera:
5 Predpostavimo ϕ.
6 Dokažimo ϕ:
7 Zaradi (5) velja ϕ.
8 Predpostavimo $\neg\phi$.
9 Dokažimo ϕ:
10 Zaradi (8) in (2) velja $\bot$.
11 Zaradi (10) velja ϕ.

Velja tudi obrat: pravilo o izključenem tretjem lahko izpeljemo z dokazom s protislovjem:

1 Dokažimo $\phi \vee \neg\phi$ s protislovjem:
2 Predpostavimo $\neg(\phi \vee \neg\phi)$.
3 Dokažimo $\bot$:
4 Velja $\phi \vee \neg\phi$:
5 Dokažimo desni disjunkt $\neg\phi$:
6 Predpostavimo ϕ.
7 Dokažimo $\bot$:
8 Zaradi (6) velja $\phi \vee \neg\phi$.
9 Zaradi (8) in (2) velja $\bot$.
10 Zaradi (4) in (2) velja $\bot$.

Pravilo o izključenem tretjem omogoča še nekatere druge načine dokazovanja izjav. Najprej, implikacijo $\phi \Rightarrow \psi$ smemo zamenjati s ***kontrapozicijo***

$\neg\psi \Rightarrow \neg\phi$, saj sta ekvivalentni. V eno smer dokaz ekvivalence poteka takole:

```
1 Dokažimo (φ ⇒ ψ) ⇒ (¬ψ ⇒ ¬φ):
2     Predpostavimo φ ⇒ ψ.
3     Dokažimo ¬ψ ⇒ ¬φ:
4         Predpostavimo ¬ψ.
5         Dokažimo ¬φ:
6             Predpostavimo φ.
7             Dokažimo ⊥:
8                 Zaradi (2) in (6) velja ψ.
9                 Zaradi (8) in (4) velja ⊥.
```

V drugo smer potrebujemo dokaz s protislovjem:

```
1 Dokažimo (¬ψ ⇒ ¬φ) ⇒ (φ ⇒ ψ):
2     Predpostavimo ¬ψ ⇒ ¬φ.
3     Dokažimo φ ⇒ ψ:
4         Predpostavimo φ.
5         Dokažimo ψ s protislovjem:
6             Predpostavimo ¬ψ.
7             Dokažimo ⊥:
8                 Zaradi (2) in (6) velja ¬φ.
9                 Zaradi (4) in (8) velja ⊥.
```

Dalje, disjunkcijo $\phi \vee \psi$ smemo zamenjati z implikacijo $\neg\phi \Rightarrow \psi$. Ekvivalenco $(\phi \vee \psi) \Leftrightarrow (\neg\phi \Rightarrow \psi)$ v eno smer dokažemo takole:

```
1  Dokažimo (φ ∨ ψ) ⇒ (¬φ ⇒ ψ):
2      Predpostavimo φ ∨ ψ.
3      Dokažimo ¬φ ⇒ ψ:
4          Predpostavimo ¬φ.
5          Dokažimo ψ:
6              Uporabimo (2) in obravnavamo dva primera:
7                  Predpostavimo φ.
8                  Dokažimo ψ:
9                      Zaradi (7) in (4) velja ⊥.
10                     Zaradi (9) velja ψ.
11                 Predpostavimo ψ.
12                 Dokažimo ψ:
13                     Zaradi (11) velja ψ.
```

V drugo smer potrebujemo pravilo o izključenem tretjem:

1 Dokažimo $(\neg\phi \Rightarrow \psi) \Rightarrow (\phi \vee \psi)$:
2 Predpostavimo $\neg\phi \Rightarrow \psi$.
3 Dokažimo $\phi \vee \psi$:
4 Ker velja $\phi \vee \neg\phi$, obravnavamo dva primera:
5 Predpostavimo ϕ.
6 Dokažimo $\phi \vee \psi$:
7 Dokažimo levi disjunkt ϕ:
8 Zaradi (5) velja ϕ.
9 Predpostavimo $\neg\phi$.
10 Dokažimo $\phi \vee \psi$:
11 Dokažimo desni disjunkt ψ:
12 Zaradi (2) in (9) velja ψ.

Pravilo o izključenem tretjem je koristno tudi za poenostavljanje negacij s pomočjo naslednjih ekvivalenc, ki povedo, kako $\neg$ »porinemo« v izjavo:

$$\begin{aligned}
\neg(\phi \wedge \psi) &\iff \neg\phi \vee \neg\psi \\
\neg(\phi \vee \psi) &\iff \neg\phi \wedge \neg\psi \\
\neg(\phi \Rightarrow \psi) &\iff \phi \wedge \neg\psi \\
\neg(\neg\phi) &\iff \phi \\
\neg(\forall x \in S\,.\,\phi(x)) &\iff \exists x \in S\,.\,\neg\phi(x) \\
\neg(\exists x \in S\,.\,\phi(x)) &\iff \forall x \in S\,.\,\neg\phi(x)
\end{aligned}$$

Dokažimo le predzadnjo ekvivalenco, ostale pa prepustimo za vajo (zadnja ekvivalenca velja brez uporabe izključenega tretjega). V eno smer dokaz poteka takole:

1 Dokažimo $(\exists x \in S\,.\,\neg\phi(x)) \Rightarrow \neg(\forall x \in S\,.\,\phi(x))$:
2 Predpostavimo $\exists x \in S\,.\,\neg\phi(x)$.
3 Dokažimo $\neg(\forall x \in S\,.\,\phi(x))$:
4 Predpostavimo $\forall x \in S\,.\,\phi(x)$.
5 Dokažimo $\bot$:
6 Zaradi (2) imamo $x \in S$ in $\neg\phi(x)$.
7 Zaradi (6) velja $x \in S$.
8 Zaradi (6) velja $\neg\phi(x)$.
9 Zaradi (4) in (7) velja $\phi(x)$.
10 Zaradi (9) in (8) velja $\bot$.

V drugo smer potrebujemo dokaz s protislovjem:

1 Dokažimo $\neg(\forall x \in S\,.\,\phi(x)) \Rightarrow \exists x \in S\,.\,\neg\phi(x)$:
2 Predpostavimo $\neg(\forall x \in S\,.\,\phi(x))$.
3 Dokažimo $\exists x \in S\,.\,\neg\phi(x)$ s protislovjem:
4 Predpostavimo $\neg(\exists x \in S\,.\,\neg\phi(x))$.
5 Dokažimo $\bot$:
6 Velja $\forall x \in S\,.\,\phi(x)$:
7 Naj bo $x \in S$.
8 Dokažimo $\phi(x)$ s protislovjem:
9 Predpostavimo $\neg\phi(x)$.
10 Dokažimo $\bot$:
11 Zaradi (7) in (9) velja $\exists x \in S\,.\,\neg\phi(x)$.
12 Zaradi (11) in (4) velja $\bot$.
13 Zaradi (6) in (2) velja $\bot$.

Posrednih načinov dokazovanja, ki smo jih predstavili tu, se poslužujemo le, ko neposredni dokaz ni možen ali pa je zapleten, saj nam ne povedo prav veliko o dokazani izjavi. Na primer, v neposrednem dokazu izjave $\exists x \in A\,.\,\phi(x)$ podamo element $a \in A$, ki zadošča $\phi(a)$, s posrednim dokazom ekvivalentne izjave $\neg\forall x \in A\,.\,\neg\phi(x)$ pa samo dokažemo, da ni možno, da tak element ne bi obstajal.

Zgled 4.19. Pokažimo, kako zgoraj navedene ekvivalence uporabimo, ko dokazujemo negacijo izjave. Denimo, da bi radi ovrgli izjavo

»*Vsako zaporedje pozitivnih realnih števil ima limito* 0.«

Najprej jo zapišemo v simbolni obliki in pred njo postavimo negacijo, saj izjavo ovržemo tako, da dokažemo njeno negacijo:

$$\neg\forall a \in \mathbb{R}^{\mathbb{N}}\,.\,(a_n)_n \text{ pozitivno zaporedje} \Rightarrow 0 \text{ je limita zaporedja } (a_n)_n. \quad (4.1)$$

Zgornja pravila za računanje negacije nam povedo, da se $\neg\forall$ spremeni v $\exists\neg$ in da se nato implikacija oblike $\phi \Rightarrow \psi$ spremeni v $\phi \wedge \neg\psi$. Tako dobimo ekvivalentno obliko (4.1):

$$\exists a \in \mathbb{R}^{\mathbb{N}}\,.\,(a_n)_n \text{ pozitivno zaporedje} \wedge \neg(0 \text{ je limita zaporedja } (a_n)_n).$$

To preberemo z besedami:

»*Obstaja tako zaporedje* $(a_n)_n$*, da je* $(a_n)_n$ *zaporedje pozitivnih števil in da* 0 *ni limita zaporedja* $(a_n)_n$.«

Če se še malo potrudimo, preberemo bolj razumljivo:

> »*Obstaja tako zaporedje pozitivnih realnih števil, da* 0 *ni njegova limita.*«

S tem še nismo končali, saj je »*Število* 0 *ni limita zaporedja* $(a_n)_n$« negacija izjave »0 *je limita zaporedja* $(a_n)_n$«, kar v simbolni obliki zapišemo

$$\neg\forall\epsilon > 0\,.\,\exists m \in \mathbb{N}\,.\,\forall n \geq m\,.\,|a_n - 0| < \epsilon. \tag{4.2}$$

Z zgornjimi pravili za negiranje operacijo $\neg$ postopoma »porivamo« navznoter:

$$\begin{aligned}
\neg\forall\epsilon > 0\,.\,\exists m \in \mathbb{N}\,.\,\forall n \geq m\,.\,|a_n - 0| < \epsilon &\iff\\
\exists\epsilon > 0\,.\,\neg\exists m \in \mathbb{N}\,.\,\forall n \geq m\,.\,|a_n - 0| < \epsilon &\iff\\
\exists\epsilon > 0\,.\,\forall m \in \mathbb{N}\,.\,\neg\forall n \geq m\,.\,|a_n - 0| < \epsilon &\iff\\
\exists\epsilon > 0\,.\,\forall m \in \mathbb{N}\,.\,\exists n \geq m\,.\,\neg(|a_n - 0| < \epsilon) &\iff\\
\exists\epsilon > 0\,.\,\forall m \in \mathbb{N}\,.\,\exists n \geq m\,.\,|a_n - 0| \geq \epsilon &\iff\\
\exists\epsilon > 0\,.\,\forall m \in \mathbb{N}\,.\,\exists n \geq m\,.\,|a_n| \geq \epsilon &\iff\\
\exists\epsilon > 0\,.\,\forall m \in \mathbb{N}\,.\,\exists n \geq m\,.\,a_n \geq \epsilon.
\end{aligned}$$

Ugotovili smo, da iščemo zaporedje $(a_n)_n$ pozitivnih števil, ki zadošča

> »*Obstaja tak* $\epsilon > 0$*, da za vsak* $m \in \mathbb{N}$ *obstaja* $n \geq m$*, da je* $a_n \geq \epsilon$.«

Kako najdemo zaporedje, ki zadošča temu pogoju? Poskusimo kar naivno: vstavimo neko konkretno vrednost za ϵ, na primer 42:

> »*Za vsak* $m \in \mathbb{N}$ *obstaja* $n \geq m$*, da je* $a_n \geq 42$.«

Potrebujemo zaporedje z neskončno mnogo členi, ki so vsaj 42, na primer $a_n := 43$. Res, če je $m \in \mathbb{N}$ poljuben, lahko vzamemo kar $n = m$, saj velja $a_n = a_m = 43 > 42 = \epsilon$.

Povzemimo odgovor: ni res, da ima vsako zaporedje pozitivnih realnih števil limito 0, saj zaporedje $a_n := 43$ nima limite 0.

4.6 Brez izgube za splošnost

Poglavje zaključimo še s tehniko dokazovanja, ki jo boste srečali v praksi in ki od bralca zahteva malo več znanja kot osnovna pravila sklepanja.

Fraza »*brez izgube za splošnost …*« nakazuje, da dokaz obravnava le poseben primer, iz katerega sledi cilj, oziroma je preostanek dokaza zelo podoben posebnemu primeru. Bralec mora sam razbrati, zakaj je tako. Podajmo primer.

Trditev 4.20. *Za vsa cela števila a, b in c je $|a-b|+|b-c|+|c-a|$ sodo število.*

Dokaz. Brez izgube za splošnost smemo predpostaviti $a \geq b \geq c$. Tedaj velja

$$|a-b|+|b-c|+|c-a| = (a-b)+(b-c)-(c-a) = 2(a-c),$$

kar je sodo število. □

Zakaj je avtor dokaza predpostavil, da velja $a \geq b \geq c$? S frazo »*brez izgube za splošnost*« nam sporoča, da ni treba obravnavati vseh šestih primerov

$$\begin{array}{lll} a \geq b \geq c, & a \geq c \geq b, & b \geq a \geq c, \\ b \geq c \geq a, & c \geq a \geq b, & c \geq b \geq a, \end{array}$$

ker lahko vsakega od njih prevedemo na $a \geq b \geq c$. In res, ker števila a, b in c v izrazu $|a-b|+|b-c|+|c-a|$ nastopajo *simetrično*, se vrednost izraza ne spremeni, če jih premešamo. Denimo, ko zamenjamo a in b, dobimo $|b-a|+|a-c|+|c-b|$, kar je enako prvotnemu izrazu $|a-b|+|b-c|+|c-a|$. Števila torej uredimo po padajočem vrstnem redu $a \geq b \geq c$ in obravnavamo le en primer.

5

Boolova algebra

V tem poglavju bomo izjavam priredili resničnostne vrednosti in jih prikazali z resničnostnimi tabelami. Dokazali bomo, da so izjave, ki jih sestavimo iz izjavnih simbolov in logičnih veznikov, dokazljive natanko tedaj, ko so tavtologije, in da lahko vsako resničnostno tabelo dobimo kot tabelo neke izjave. Na koncu bomo zbrali pravila Boolove algebre, s katerimi izjave poenostavljamo z računanjem.

5.1 Izjavni in predikatni račun

V nadaljevanju bomo potrebovali natančno opredelitev formul, ki jih obravnavamo. Naj bo $\mathbb{2} := \{\bot, \top\}$. ***Izjavne spremenljivke*** ali ***izjavni simboli*** so spremenljivke, ki zavzamejo vrednosti v $\mathbb{2}$. ***Izjavna formula*** je formula, ki jo sestavimo iz izjavnih simbolov, iz $\top$ in $\bot$ ter iz logičnih veznikov $\neg$, $\wedge$, $\vee$, $\Rightarrow$ in $\Leftrightarrow$. Na primer, $\neg p \vee q$ je izjavna formula z izjavnima simboloma p in q. Z izjavnimi formulami se ukvarja ***izjavni račun***. Formule, v katerih nastopajo tudi kvantifikatorji in spremenljivke z vrednostmi v poljubnih množicah, so predmet ***predikatnega računa***. Taka je na primer formula $\forall x \in \mathbb{N} \,.\, \exists y \in \mathbb{N} \,.\, x < y$.

Izjavna formula $\phi(p_1, \ldots, p_n)$ z izjavnimi simboli $p_1, \ldots, p_n$ določa presli-

kavo

$$2 \times \cdots \times 2 \to 2$$

s predpisom

$$(p_1, \ldots, p_n) \mapsto \phi(p_1, \ldots, p_n).$$

Preslikava priredi vrednostim $b_1, \ldots, b_n \in 2$ vrednost $\top$, če je izjava $\phi(b_1, \ldots, b_n)$ resnična, in vrednost $\bot$, če je neresnična. Preslikavi, ki slika iz produkta $2 \times \cdots \times 2$ v 2, pravimo ***Boolova preslikava***.

Zgled 5.1. Izjavna formula

$$(p \vee q) \wedge \neg r \tag{5.1}$$

z izjavnimi simboli p, q in r določa Boolovo preslikavo

$$\begin{aligned} 2 \times 2 \times 2 &\to 2 \\ (p, q, r) &\mapsto (p \vee q) \wedge \neg r. \end{aligned} \tag{5.2}$$

Nikar ne mislite, da sta (5.1) in (5.2) ista reč! Prva je izjava in druga preslikava.

5.2 Resničnostne tabele

Vsaka izjava lahko priredimo ***resničnostno vrednost***. Če izjava velja, je njena resničnostna vrednost resnica $\top$, če pa izjava ne velja, je njena resničnostna vrednost neresnice $\bot$.

Zgled 5.2. Resničnostna vrednost izjave $e^\pi < \pi^e$ je $\bot$. Resničnostna vrednost izjave[1] $1782^{12} + 1841^{12} = 1922^{12}$ je $\bot$.

Zgled 5.3. Kadar izjava vsebuje spremenljivke (pravimo jim tudi ***parametri***), je njena resničnostna vrednost *odvisna* od parametrov. Na primer, če sta $x, y \in \mathbb{N}$ spremenljivki, je resničnostna vrednost izjave $2x < y + 3$ odvisna od x in y, kar lahko prikažemo z ***resničnostno tabelo***:

[1] Enačba se pojavi v risani seriji *Simpsonovi* kot »protiprimer« za veliki Fermatov izrek.

y \ x	0	1	2	3	4	5	6	⋯
0	$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	⋯
1	$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	⋯
2	$\top$	$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$	⋯
3	$\top$	$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$	⋯
4	$\top$	$\top$	$\top$	$\top$	$\bot$	$\bot$	$\bot$	⋯
5	$\top$	$\top$	$\top$	$\top$	$\bot$	$\bot$	$\bot$	⋯
6	$\top$	$\top$	$\top$	$\top$	$\top$	$\bot$	$\bot$	⋯
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

Zgled 5.4. Bolj uporabne so končne resničnostne tabele, v katerih parametri zavzemajo vrednosti iz končne množice. Na primer, resničnostna tabela izjavne formule $\neg p \vee q$ je

p	q	$\neg p \vee q$
$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\top$	$\top$	$\top$

Boolovo preslikavo lahko prikažemo z resničnostno tabelo.

Vaja 5.5. Koliko vrstic ima resničnostna tabela izjavne formule z n izjavnimi simboli?

5.3 Tavtologije

Izjava je ***tavtologija***, če je njena resničnostna vrednost $\top$ ne glede na vrednosti parametrov.

Zgled 5.6. Formula $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$ je tavtologija, kar razberemo iz njene resničnostne tabele:

p	q	r	$((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$
$\bot$	$\bot$	$\bot$	$\top$
$\bot$	$\bot$	$\top$	$\top$
$\bot$	$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top$
$\top$	$\bot$	$\top$	$\top$
$\top$	$\top$	$\bot$	$\top$
$\top$	$\top$	$\top$	$\top$

V desnemstolpcu so vse vrednosti enake $\top$, zato je formula resnična ne glede na vrednosti p, q in r.

Zgled 5.7. Formula $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow r)$ ni tavtologija, kar pokaže njena resničnostna tabela:

p	q	r	$(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow r)$
$\bot$	$\bot$	$\bot$	$\bot$
$\bot$	$\bot$	$\top$	$\top$
$\bot$	$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top$
$\top$	$\bot$	$\top$	$\top$
$\top$	$\top$	$\bot$	$\top$
$\top$	$\top$	$\top$	$\top$

V prvi in tretji vrstici ima formula vrednost $\bot$. Formuli $p \Rightarrow (q \Rightarrow r)$ in $(p \Rightarrow q) \Rightarrow r$ torej nista ekvivalentni, se pravi, da implikacija ni asociativna.

Dejstvo, da je izjava resnična lahko torej utemeljimo na dva načina: z dokazom ali z resničnostno tabelo. Naslednji izrek pove, kakšen je odnos med njima.

Izrek 5.8. *Izjavna formula je tavtologija natanko tedaj, ko ima dokaz.*

Dokaz. Dokaz najdete v [Pri92]. □

Pozor: Izrek velja v izjavnem računu, v predikatnem računu pa *ne* velja. Lahko se namreč zgodi, da ima formula predikatnega računa neskončno

resničnostno tabelo, v kateri so vse resničnostne vrednosti $\top$, a formula nima dokaza.

5.4 Disjunktivna in konjunktivna oblika

Vsaka formula v izjavnem računu ima resničnostno tabelo. Ali lahko vsako tabelo dobimo kot resničnostno tabelo neke formule? Na primer, ali obstaja formula, katere resničnostna tabela se glasi

p	q	?
$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\top$
$\top$	$\bot$	$\top$
$\top$	$\top$	$\bot$

Odgovor je pritrdilen. Podajmo dva načina, kako tako izjavo izračunamo iz tabele.

5.4.1 Disjunktivna oblika

Za vsako vrstico v tabeli, ki ima vrednost $\top$, zapišemo konjunkcijo simbolov in njihovih negacij, pri čemer negiramo tiste simbole, ki imajo v dani vrstici vrednost $\bot$. Na primer, v zgornji tabeli imata druga in tretja vrstica vrednost $\top$, zanju zapišemo konjunkciji:

- 2. vrstica: $\neg p \wedge q$,
- 3. vrstica: $p \wedge \neg q$.

Nato tvorimo disjunkcijo tako dobljenih konjunkcij:

$$(\neg p \wedge q) \vee (p \wedge \neg q).$$

Dobljena formula ima želeno resničnostno tabelo.

5.4.2 Konjunktivna oblika

Za vsako vrstico v tabeli, ki ima vrednost $\bot$, zapišemo disjunkcijo simbolov in njihovih negacij, pri čemer negiramo tiste simbole, ki imajo v dani vrstici vrednost $\top$. Na primer, v zgornji tabeli imata prva in četrta vrstica vrednost $\bot$, zanju zapišemo disjunkciji:

- 1. vrstica: $p \vee q$,

- 4. vrstica: $\neg p \vee \neg q$.

Nato tvorimo konjunkcijo tako dobljenih disjunkcij:

$$(p \vee q) \wedge (\neg p \vee \neg q).$$

Zgornjo tabelo bi lahko dobili tudi kot resničnostno tabelo formule $p \Leftrightarrow q$.

Zgled 5.9. Poiščimo izjavno formulo, ki je resnična natanko tedaj, ko sta resnični vsaj dve od izjav p, q in r. Njena resničnostna tabela je

p	q	r	?
$\bot$	$\bot$	$\bot$	$\bot$
$\bot$	$\bot$	$\top$	$\bot$
$\bot$	$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\bot$
$\top$	$\bot$	$\top$	$\top$
$\top$	$\top$	$\bot$	$\top$
$\top$	$\top$	$\top$	$\top$

Vrednost $\top$ imajo četrta, šesta, sedma in osma vrstica, zato je disjunktivna oblika

$$(\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge q \wedge r).$$

Vrednost $\bot$ imajo prva, druga, tretja in peta vrstica, zato je konjunktivna oblika

$$(p \vee q \vee r) \wedge (p \vee q \vee \neg r) \wedge (p \vee \neg q \vee r) \wedge (\neg p \vee q \vee r).$$

Obe obliki sta daljši od ekvivalentne formule $(p \wedge q) \vee (p \wedge r) \vee (q \wedge r)$.

5.4.3 Polni nabori

Polni nabor je tak izbor veznikov, s katerim lahko dobimo vsako resničnostno tabelo. Ker, lahko vsako resničnostno tabelo dobimo z uporabo veznikov $\neg$, $\vee$ in $\wedge$, tvorijo $\neg, \vee, \wedge$ polni nabor. Lahko bi ga še zmanjšali na $\neg, \wedge$, saj lahko $p \vee q$ izrazimo kot $\neg(\neg p \wedge \neg q)$.

Zgled 5.10. Nabor $\wedge, \vee$ *ni* poln, saj ne moremo dobiti resničnostne tabele

p	?
$\bot$	$\top$
$\top$	$\bot$

Res, če iz p, $\wedge$ in $\vee$ sestavimo poljubno formulo $\phi(p)$, na primer $(p \wedge (p \vee p)) \wedge p$, bo ta ekvivalentna p in bo zato veljalo $\phi(\top) = \top$, zgornja tabela pa zahteva $\phi(\top) = \bot$.

5.5 Boolova algebra

Ekvivalentni izjavi imata enake resničnostne vrednosti, torej lahko ekvivalenco $\Leftrightarrow$ obravnavamo kar kot enakost, saj to tudi je, kar se tiče resničnostnih vrednosti. Zato lahko namesto $p \Leftrightarrow q$ pišemo tudi $p = q$, če imamo v mislih le resničnostne vrednosti.

Opomba 5.11. Ekvivalentni izjavi imata lahko različna *pomena.* Na primer, $\forall x, y \in \mathbb{R}\,.\, x + y = y + x$ in $\forall \alpha \in \mathbb{R}\,.\, \sin(2\alpha) = 2 \cdot \cos\alpha \cdot \sin\alpha$ sta ekvivalentni, saj sta obe resnični, a ne moremo reči, da je njun pomen enak. (Predstavljajte si, da bi vas v srednji šoli profesorica matematike vprašala adicijski izrek za sin, vi pa bi odgovorili »*vrstni red seštevanja realnih števil ne vpliva na vrednost vsote*«.)

Za logične veznike veljajo ***algebrajska pravila***, se pravi enačbe, kakršne poznamo v algebri. Ta pravila lahko uporabljamo kot računska pravila, s katerimi lahko izjavo poenostavimo v ekvivalentno obliko. Pogosto je tako računanje bolj prikladno kot dokazovanje. Spodaj našteta pravila lahko preverimo tako, da zapišemo resničnostne tabele izjav in jih primerjamo.

Pravilom, ki veljajo za logične veznike, pravimo ***Boolova algebra***. Razdelimo jih po sklopih.

Pravila za konjunkcijo:

$$
\begin{aligned}
(p \wedge q) \wedge r &= p \wedge (q \wedge r) && \text{(asociativnost } \wedge\text{)} \\
p \wedge q &= q \wedge p && \text{(komutativnost } \wedge\text{)} \\
p \wedge p &= p && \text{(idempotentnost } \wedge\text{)} \\
\top \wedge p &= p && (\top \text{ je nevtralen za } \wedge) \\
\bot \wedge p &= \bot && (\bot \text{ absorbira } \wedge)
\end{aligned}
$$

Pravila za disjunkcijo:

$$(p \vee q) \vee r = p \vee (q \vee r) \qquad \text{(asociativnost } \vee\text{)}$$
$$p \vee q = q \vee p \qquad \text{(komutativnost } \vee\text{)}$$
$$p \vee p = p \qquad \text{(idempotentnost } \vee\text{)}$$
$$\bot \vee p = p \qquad (\bot \text{ je nevtralen za } \vee)$$
$$\top \vee p = \top \qquad (\top \text{ absorbira } \vee)$$

Pravila za implikacijo:

$$(p \Rightarrow q) = (\neg q \Rightarrow \neg p) \qquad \text{(kontrapozicija)}$$
$$(p \Rightarrow q) = \neg p \vee q$$
$$(\bot \Rightarrow q) = \top$$
$$(\top \Rightarrow q) = q$$
$$(p \Rightarrow \bot) = \neg p$$
$$(p \Rightarrow \top) = \top$$
$$(p \Rightarrow p) = \top$$
$$((p \wedge q) \Rightarrow r) = (p \Rightarrow (q \Rightarrow r))$$
$$((p \vee q) \Rightarrow r) = (p \Rightarrow r) \wedge (q \Rightarrow r)$$
$$(p \Rightarrow (q \wedge r)) = (p \Rightarrow q) \wedge (p \Rightarrow r)$$

Pravila za ekvivalenco:

$$(p \Leftrightarrow q) = (p \Rightarrow q) \wedge (q \Rightarrow p)$$
$$(p \Leftrightarrow \top) = p$$
$$(p \Leftrightarrow \bot) = \neg p$$

Kombinirana pravila:

$$\neg(p \wedge q) = \neg p \vee \neg q \qquad \text{(De Morganovo pravilo za } \wedge\text{)}$$
$$\neg(p \vee q) = \neg p \wedge \neg q \qquad \text{(De Morganovo pravilo za } \vee\text{)}$$
$$\neg(p \Rightarrow q) = p \wedge \neg q$$
$$p \wedge (p \vee q) = p \qquad \text{(absorpcijsko pravilo za } \wedge\text{)}$$
$$p \vee (p \wedge q) = p \qquad \text{(absorpcijsko pravilo za } \vee\text{)}$$
$$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r) \qquad \text{(distributivnost } \wedge\text{)}$$
$$p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r) \qquad \text{(distributivnost } \vee\text{)}$$

Pravila za negacijo:

$$\begin{aligned} \neg\top &= \bot \\ \neg\bot &= \top \\ \neg\neg p &= p && \text{(negacija je involucija)} \\ p \vee \neg p &= \top && \text{(pravilo o izključenem tretjem)} \\ p \wedge \neg p &= \bot \end{aligned}$$

V tabeli 5.1 za pregled navajamo še nekaj pravil za kvantifikatorje. Tokrat uporabimo $\iff$ namesto $=$, ker je to bolj običajno. Te ekvivalence je treba preveriti tako, da jih dokažemo.

Zgled 5.12. Pokažimo z računanjem, da je naslednja izjava resnična:

$$\big(\forall x \in A\,.\,\phi(x) \Rightarrow \psi(x)\big) \wedge \big(\forall x \in A\,.\,\phi(x)\big) \Rightarrow \forall x \in A\,.\,\psi(x).$$

Običajno bi tovrstno izjavo dokazali s pravili sklepanja, tu pa bomo raje ponazorili, kako se uporablja pravila Boolove algebra in pravila iz tabele 5.1. Vsi trije kvantifikatorji vežejo spremenljivko x. Da jih ne bi zamešali, vezane spremenljivke preimenujemo:

$$\big(\forall x \in A\,.\,\phi(x) \Rightarrow \psi(x)\big) \wedge \big(\forall y \in A\,.\,\phi(y)\big) \Rightarrow \forall z \in A\,.\,\psi(z).$$

Tudi v nadaljevanju bo vsak novi kvantifikator vezal svojo spremenljivko. Pravila iz tabele uporabljamo ne glede na imena vezanih spremenljivk. Sedaj

$$
\begin{aligned}
(\forall x \in \emptyset \,.\, \phi(x)) &\iff \top \\
(\exists x \in \emptyset \,.\, \phi(x)) &\iff \bot \\
(\forall x \in \{a\} \,.\, \phi(x)) &\iff \phi(a) \\
(\exists x \in \{a\} \,.\, \phi(x)) &\iff \phi(a) \\
(\neg \forall x \in A \,.\, \phi(x)) &\iff \exists x \in A \,.\, \neg \phi(x) \\
(\neg \exists x \in A \,.\, \phi(x)) &\iff \forall x \in A \,.\, \neg \phi(x) \\
(\psi \Rightarrow \forall x \in A \,.\, \phi(x)) &\iff \forall x \in A \,.\, (\psi \Rightarrow \phi(x)) \\
(\psi \vee \forall x \in A \,.\, \phi(x)) &\iff \forall x \in A \,.\, (\psi \vee \phi(x)) \\
(\psi \wedge \exists x \in A \,.\, \phi(x)) &\iff \exists x \in A \,.\, (\psi \wedge \phi(x)) \\
(\exists x \in A \,.\, \phi(x)) \Rightarrow \psi &\iff \forall x \in A \,.\, (\phi(x) \Rightarrow \psi) \\
(\forall x \in A \,.\, \phi(x) \wedge \psi(x)) &\iff (\forall y \in A \,.\, \phi(y)) \wedge (\forall z \in A \,.\, \psi(z)) \\
(\exists x \in A \,.\, \phi(x) \vee \psi(x)) &\iff (\exists y \in A \,.\, \phi(y)) \vee (\exists z \in A \,.\, \psi(z)) \\
(\forall x \in A \,.\, \forall y \in B \,.\, \phi(x, y)) &\iff \forall y \in B \,.\, \forall x \in A \,.\, \phi(x, y) \\
(\exists x \in A \,.\, \exists y \in B \,.\, \phi(x, y)) &\iff \exists y \in B \,.\, \exists x \in A \,.\, \phi(x, y) \\
(\forall u \in A \times B \,.\, \phi(u)) &\iff \forall x \in A \,.\, \forall y \in B \,.\, \phi(x, y) \\
(\exists u \in A \times B \,.\, \phi(u)) &\iff \exists x \in A \,.\, \exists y \in B \,.\, \phi(x, y) \\
(\forall u \in A + B \,.\, \phi(u)) &\iff (\forall x \in A \,.\, \phi(\mathsf{in}_1(x))) \wedge (\forall y \in B \,.\, \phi(\mathsf{in}_2(y))) \\
(\forall u \in A \cup B \,.\, \phi(u)) &\iff (\forall x \in A \,.\, \phi(x)) \wedge (\forall y \in B \,.\, \phi(y)) \\
(\exists u \in A + B \,.\, \phi(u)) &\iff (\exists x \in A \,.\, \phi(\mathsf{in}_1(x))) \vee (\exists y \in B \,.\, \phi(\mathsf{in}_2(y))) \\
(\exists u \in A \cup B \,.\, \phi(u)) &\iff (\exists x \in A \,.\, \phi(x)) \vee (\exists y \in B \,.\, \phi(y)) \\
(\forall u \in \{x \in A \mid \psi(x)\} \,.\, \phi(u)) &\iff \forall x \in A \,.\, (\psi(x) \Rightarrow \phi(x)) \\
(\exists u \in \{x \in A \mid \psi(x)\} \,.\, \phi(u)) &\iff \exists x \in A \,.\, (\psi(x) \wedge \phi(x))
\end{aligned}
$$

Tabela 5.1: Pravila za kvantifikatorje. V pravilih, v katerih nastopa ψ brez argumenta, spremenljivka x v ψ ne nastopa.

računamo, pri čemer je vsaka vrstica ekvivalentna naslednji:

$$
\begin{aligned}
& \big(\forall x \in A\,.\,\phi(x) \Rightarrow \psi(x)\big) \wedge \big(\forall y \in A\,.\,\phi(y)\big) \Rightarrow \forall z \in A\,.\,\psi(z) \\
\iff\ & \Big(\forall u \in A\,.\,\big(\phi(u) \Rightarrow \psi(u)\big) \wedge \phi(u)\Big) \Rightarrow \forall z \in A\,.\,\psi(z) \\
\iff\ & \Big(\forall u \in A\,.\,\big(\neg\phi(u) \vee \psi(u)\big) \wedge \phi(u)\Big) \Rightarrow \forall z \in A\,.\,\psi(z) \\
\iff\ & \Big(\forall u \in A\,.\,\phi(u) \wedge \big(\neg\phi(u) \vee \psi(u)\big)\Big) \Rightarrow \forall z \in A\,.\,\psi(z) \\
\iff\ & \Big(\forall u \in A\,.\,\big(\phi(u) \wedge \neg\phi(u)\big) \vee \big(\phi(u) \wedge \psi(u)\big)\Big) \Rightarrow \forall z \in A\,.\,\psi(z) \\
\iff\ & \Big(\forall u \in A\,.\,\bot \vee \big(\phi(u) \wedge \psi(u)\big)\Big) \Rightarrow \forall z \in A\,.\,\psi(z) \\
\iff\ & \big(\forall u \in A\,.\,\phi(u) \wedge \psi(u)\big) \Rightarrow \forall z \in A\,.\,\psi(z) \\
\iff\ & \big(\forall v \in A\,.\,\phi(v)\big) \wedge \big(\forall w \in A\,.\,\psi(w)\big) \Rightarrow \forall z \in A\,.\,\psi(z) \\
\iff\ & \big(\forall v \in A\,.\,\phi(v)\big) \Rightarrow \Big(\big(\forall w \in A\,.\,\psi(w)\big) \Rightarrow \forall z \in A\,.\,\psi(z)\Big) \\
\iff\ & \big(\forall v \in A\,.\,\phi(v)\big) \Rightarrow \Big(\big(\forall z \in A\,.\,\psi(z)\big) \Rightarrow \forall z \in A\,.\,\psi(z)\Big) \\
\iff\ & \big(\forall v \in A\,.\,\phi(v)\big) \Rightarrow \top \\
\iff\ & \top.
\end{aligned}
$$

Ugotovite, katero pravilo smo uporabili v vsakem od računskih korakov.

Zgled 5.13. Tako imenovani *»paradoks« pivca* pravi, da v vsaki neprazni gostilni sedi gost, za katerega velja: če pije on, pijejo vsi gostje. To ni pravi paradoks, le na prvi pogled presenetljivo dejstvo, ki ga zlahka utemeljimo: če pijejo vsi gostje, ustreza katerikoli gost, sicer pa izberemo gosta, ki ne pije.

Sedaj pa izjavo dokažimo še formalno z računanjem. Naj bo A množica gostov in $\phi(x)$ izjava »*gost x pije*«. Predpostavko, da je gostilna neprazna, zapišemo kot $\exists z \in A\,.\,\top$, zato se paradoks pivca v simbolni obliki glasi

$$(\exists z \in A\,.\,\top) \Rightarrow \exists x \in A\,.\,(\phi(x) \Rightarrow \forall y \in A\,.\,\phi(y)).$$

Označimo $\rho := \forall y \in A\,.\,\phi(y)$ in $\sigma := \exists z \in A\,.\,\top$, torej lahko izjavo zapišemo krajše $\sigma \Rightarrow \exists x \in A\,.\,\phi(x) \Rightarrow \rho$. Izjavo preoblikujemo v ekvivalentno izjavo $\top$

takole:

$$
\begin{aligned}
& \sigma \Rightarrow \exists x \in A \,.\, (\phi(x) \Rightarrow \rho) \\
\iff\ & \sigma \Rightarrow \exists x \in A \,.\, (\neg\phi(x) \vee \rho) \\
\iff\ & \sigma \Rightarrow \big(\exists v \in A \,.\, \neg\phi(v)\big) \vee \exists w \in A \,.\, \rho \\
\iff\ & \sigma \Rightarrow \big(\exists v \in A \,.\, \neg\phi(v)\big) \vee (\exists w \in A \,.\, \top \wedge \rho) \\
\iff\ & \sigma \Rightarrow \big(\exists v \in A \,.\, \neg\phi(v)\big) \vee (\exists w \in A \,.\, \rho \wedge \top) \\
\iff\ & \sigma \Rightarrow \big(\exists v \in A \,.\, \neg\phi(v)\big) \vee (\rho \wedge \exists w \in A \,.\, \top) \\
\iff\ & \sigma \Rightarrow \big(\exists v \in A \,.\, \neg\phi(v)\big) \vee (\rho \wedge \sigma) \\
\iff\ & \sigma \Rightarrow \big(\neg\forall v \in A \,.\, \phi(v)\big) \vee (\rho \wedge \sigma) \\
\iff\ & \sigma \Rightarrow \neg\rho \vee (\rho \wedge \sigma) \\
\iff\ & \neg\sigma \vee \big(\neg\rho \vee (\rho \wedge \sigma)\big) \\
\iff\ & (\neg\sigma \vee \neg\rho) \vee (\rho \wedge \sigma) \\
\iff\ & \neg(\sigma \wedge \rho) \vee (\rho \wedge \sigma) \\
\iff\ & \neg(\rho \wedge \sigma) \vee (\rho \wedge \sigma) \\
\iff\ & (\rho \wedge \sigma) \vee \neg(\rho \wedge \sigma) \\
\iff\ & \top.
\end{aligned}
$$

Ugotovite, katero pravilo smo uporabili v vsakem od računskih korakov.

Literatura

[Pri92] Niko Prijatelj. *Osnove matematične logike, 1. del.* DMFA Založništvo, 1992.