Logika in Množice

Zapiski predavanj
(delovna verzija)

Primož Šparl

Ljubljana, januar 2015

Kazalo

Poglavje 1

Osnove matematične logike

Predstavimo na kratko snov, ki jo bomo obravnavali pri tem predmetu. Kot pove že naslov predmeta, se bomo ukvarjali z (matematično) logiko in množicami. Kaj pa to pomeni?

S čim se v matematiki sploh ukvarjamo? Marsikdo bo najbrž dejal, da je matematika predvsem računanje, premetavanje števil in reševanje enačb. A to so samo aplikacije, ki jih je omogočila bogata matematična teorija. Bistvo matematike je v odkrivanju novih spoznanj (tako imenovanih trditev in izrekov), do katerih lahko pridemo iz aksiomov, definicij in že znanih rezultatov z logičnim sklepanjem. Da bi se torej lahko lotili "prave matematike", se je treba najprej naučiti pravil logičnega sklepanja. To bo osrednja tema tega poglavja.

Preden se sploh lotimo česa takega, priporočimo bralcu nasvet kako se lotiti reševanja matematičnih nalog in problemov. Dobro se je držati naslednjih treh korakov:

1. korak: Problem je treba najprej razumeti.
O čem sploh govori trditev, ki bi jo naj dokazali ali ovrgli? Najprej je torej treba poznati pomen vseh besed, ki nastopajo v trditvi. Kakšno strukturo ima trditev? Je enostavna ali sestavljena izjava? Kaj so predpostavke in kaj naj bi dokazali? Moramo pokazati, da imajo neko lastnost vse reči, o katerih trenutno govorimo, ali je dovolj konstruirati en sam konkreten primer?

2. korak: Kako bomo problem rešili?
Sedaj, ko dobro razumemo, kaj so predpostavke in kaj naloga od nas zahteva, moramo ugotoviti, kako bomo zadevo izpeljali. Ko imamo enkrat problem "v glavi", je morda pravi čas, da zopet preletimo predavanja in vaje. Ali smo že kdaj videli kak podoben primer? Na vajah? Na predavanjih? V kaki knjigi? Če je temu tako, skušajmo uporabiti ideje, ki so pripeljale do rešitve sorodnih primerov.

3. korak: Problem dejansko rešimo, rešitev zapišemo v zgledni obliki in jo preverimo.
Ko smo enkrat naredili načrt, kako priti do rešitve, ga je treba le še izvesti. Pri tem pa moramo ves razmislek znati tudi zapisati v taki obliki, da bo lahko kdorkoli, ki pozna osnovne pojme iz obravnavane snovi, na podlagi zapisanega rekonstruiral rešitev. Na koncu rešitev še enkrat natančno preštudiramo. Preverimo vsak korak v sklepanju.

Zgoraj opisana metoda bi morala načeloma vedno delovati. Da pa v praksi zadeva res deluje, se je treba dogovoriti še za nekaj osnovnih stvari. Najprej se je treba dogovoriti za *jezik*, ki ga bomo pri ukvarjanju z matematiko uporabljali. Če želimo v tem jeziku brati in pisati stavke (ki predstavljajo neke izjave), moramo poznati njegovo *sintakso*. Tako napisane stavke je seveda potrebno tudi razumeti - poznati moramo torej pomen besed in besednih zvez, to je, poznati je treba *semantiko* jezika. Šele tedaj, ko zapisane stavke v izbranem jeziku razumemo, se lahko začnemo spraševati o *pravilnosti* oziroma *nepravilnosti* pripadajočih izjav. A to ni naloga matematične logike. Njena naloga je, da izjave analizira (temu pravimo *logična analiza*) in na ta način "pridela" izjave, ki logično sledijo iz omenjenih začetnih izjav ali so jim celo enakovredne. Na ta način namreč dane izjave bolje razumemo in se zato lažje odločamo o njihovi pravilnosti oziroma nepravilnosti.

Zgled: Oglejmo si izjavo: "Če velja, da v primeru, ko je deset sodo število, ne obstaja več kot deset praštevil, potem je deset sodo število in ne obstaja več kot deset praštevil."

Ali znamo presoditi o njeni resničnosti? Najbrž težko. A s pomočjo logične analize se da ugotoviti, da je zgornja izjava enakovredna izjavi "Deset je sodo število." No, da je ta izjava resnična, pa seveda vemo. ▲

Zgled: Oglejmo si še en podoben primer. Vsi se najbrž strinjamo, da je za vsako naravno število n izjava "Če je n^2 liho število, je tudi n liho število." pravilna. Če pa bi nekdo od nas zahteval dokaz njene pravilnosti, bi imel najbrž marsikdo težave. No, naloga je precej lažja, če najprej ugotovimo, da je omenjena izjava enakovredna izjavi "Če je n sodo število, je tudi število n^2 sodo." ▲

1.1 Izjave in izjavne povezave

Najprej se moramo dogovoriti, da izhajamo iz predpostavke, da je vsaka izjava, o kateri bomo govorili, bodisi *pravilna* (oziroma *resnična*) ali pa *nepravilna* (oziroma *neresnična*). Dejstvo, da je izjava p resnična, bomo

praviloma označevali s $p \sim 1$, da je neresnična pa s $p \sim 0$. Dogovorimo se najprej za osnovne gradnike izjavnega računa.

Definicija. Izjava, ki se je ne da razbiti na več krajših izjav, katerih vsaka zase ima pomen, je *enostavna izjava*. Izjava, ki ni enostavna, je *sestavljena*.

Zgled: Tako je na primer izjava "Matematična logika je bav bav." enostavna, saj se je ne da razbiti na več manjših smiselnih enot. Po drugi strani je izjava "Če se matematične logike lotimo na pravi način, ni noben bav bav." sestavljena, saj sestoji iz izjav "Matematične logike se lotimo na pravi način." in "Matematična logika ni noben bav bav." ▲

V nadaljevanju bomo izjave praviloma označevali z malimi črkami p, q, r, s, itd.

Na kakšen način torej sestavljene izjave sestavljamo iz enostavnih? Tako, da enostavne izjave med seboj povežemo z *logičnimi vezniki*. Mi se bomo osredotočili na najpomembnejših pet, to so *negacija*, *logični in*, *logični ali*, *implikacija* in *ekvivalenca*. Vsak logični veznik mora imeti lastnost, da je pri vsaki možni vrednosti (pravilna ali nepravilna) vstopnih izjav vrednost pripadajoče sestavljene izjave natanko določena.

Za vsako sestavljeno izjavo lahko sestavimo njeno tako imenovano resničnostno tabelo.

Definicija. Naj bo p izjava, ki je sestavljena iz enostavnih izjav $p_1, p_2, \ldots, p_k$. Tedaj je *resničnostna tabela* za izjavo p tabela, v kateri je za vsak možen nabor vrednosti enostavnih izjav $p_1, p_2, \ldots, p_k$ zapisana vrednost izjave p pri teh vrednostih enostavnih izjav $p_1, p_2, \ldots, p_k$.

Vpeljimo sedaj zgoraj omenjene logične veznike, zraven pa si oglejmo še pripadajoče resničnostne tabele.

Definicija (Negacija)**.** Naj bo p poljubna izjava. Izjava *ne* p, kar s simboli označimo $\neg p$, je izjava, ki je resnična, če je izjava p neresnična in je neresnična, če je izjava p resnična.

Z resničnostno tabelo torej pomen veznika negacije ponazorimo takole:

p	$\neg p$
0	1
1	0

Definicija (Konjunkcija)**.** Naj bosta p in q poljubni izjavi. Izjava p *in* q, s simboli $p \wedge q$, je izjava, ki je resnična, ko sta tako izjava p kot izjava q resnični, in je neresnična v vseh drugih primerih.

Z resničnostno tabelo torej pomen veznika konjunkcije ponazorimo takole:

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

Definicija (Disjunkcija)**.** Naj bosta p in q poljubni izjavi. Izjava p *ali* q, s simboli $p \vee q$, je izjava, ki je neresnična, ko sta tako izjava p kot izjava q neresnični, in je resnična v vseh drugih primerih.

Z resničnostno tabelo torej pomen veznika disjunkcije ponazorimo takole:

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

Pozor! Paziti je treba na razliko med pogovornim jezikom in formalnim matematičnim jezikom. V pogovornem jeziku namreč z besedico ali pogosto mislimo na ekskluzivni ali.

Definicija (Implikacija)**.** Naj bosta p in q poljubni izjavi. Izjava *če* p *potem* q, ali tudi *iz* p *sledi* q, kar zapišemo kot $p \Rightarrow q$, je izjava, ki je neresnična, ko je izjava p resnična, izjava q pa neresnična, in je resnična v vseh drugih primerih.

Z resničnostno tabelo torej pomen veznika implikacije ponazorimo takole:

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Pozor! Tudi tukaj se pomen v pogovornem jeziku razlikuje od matematičnega, saj v pogovornem jeziku "Če boš priden, dobiš nagrado." ponavadi v resnici pomeni "Če boš priden, dobiš nagrado, sicer pa ne."

Definicija. Denimo, da sta p in q taki izjavi, da je izjava $p \Rightarrow q$ pravilna. Tedaj pravimo, da je izjava p *zadosten pogoj* za izjavo q, izjava q pa *potreben pogoj* za izjavo p.

Zakaj uporabljamo tako terminologijo, je precej očitno. Če je namreč izjava $p \Rightarrow q$ pravilna, iz resničnostne tabele za implikacijo razberemo, da so možne samo naslednje tri situacije: $p \sim 0$ in $q \sim 0$, $p \sim 0$ in $q \sim 1$ ali pa $p \sim 1$ in $q \sim 1$. Če torej dodatno vemo še to, da je $p \sim 1$, mora zagotovo veljati $q \sim 1$. Dejstvo, da je p resnična izjava, je torej zadostna informacija za ugotovitev, da je tudi q resnična izjava. Podoben premislek utemelji tudi pojem "potreben pogoj".

Definicija (Ekvivalenca)**.** Naj bosta p in q poljubni izjavi. Izjava p *natanko tedaj, ko* q, oziroma p *če in samo če* q, kar zapišemo kot $p \iff q$, je izjava, ki je resnična, ko sta izjavi p in q bodisi obe resnični bodisi obe neresnični, in je neresnična v obeh preostalih primerih.

Z resničnostno tabelo torej pomen veznika ekvivalence ponazorimo takole:

p	q	$p \iff q$
0	0	1
0	1	0
1	0	0
1	1	1

Na tem mestu velja povedati, da so p, q, $p \wedge q$, $p \Rightarrow (q \vee (\neg r))$, itd. le tako imenovane *izjavne forme*, ne pa izjave. A mi bomo malce površni in bomo tudi izjavnim formam rekli kar izjave.

Kadar izjave sestavljamo v vedno bolj zapletene izjave, lahko dobljeni izraz zaradi prevelikega števila oklepajev postane težko berljiv, kot na primer v izjavi $(((p \Rightarrow q) \Rightarrow r) \iff (((\neg p) \wedge r) \Rightarrow p))$. Zato sklenemo sledeči dogovor glede moči vezave posameznih veznikov.

Dogovor: Izmed zgornjih petih logičnih veznikov si po moči vezave, od najmočnejšega do najšibkejšega, sledijo $\neg$, $\wedge$, $\vee$, $\Rightarrow$ in $\iff$. To torej pomeni, da ima negacija prednost pred vsemi drugimi vezniki, konjunkcija pred vsemi razen negacije, itd. Poleg tega pravila pa velja še, da izraze vedno asociiramo z leve proti desni, kar pomeni, da pri veznikih enake moči vrednost izjave izračunavamo z leve proti desni.

V zgornji izjavi torej lahko izpustimo prav vse oklepaje, saj je po tem dogovoru to ravno izjava $p \Rightarrow q \Rightarrow r \iff \neg p \wedge r \Rightarrow p$. Seveda pa se včasih oklepajem ne moremo povsem izogniti. Na primer, izjava $p \Rightarrow q \Rightarrow r$ ima pri vrednostih $p \sim q \sim r \sim 0$ vrednost 0, izjava $p \Rightarrow (q \Rightarrow r)$ pa ima pri istih vrednostih izjav p, q in r vrednost 1.

Kako za neko sestavljeno izjavo sestavimo njeno resničnostno tabelo? Ena izmed možnosti je ta, da najprej določimo vrstni red vezave logičnih veznikov, nato pa tabelo izpolnjujemo po stolpcih v tem vrstnem redu.

Ko za neko sestavljeno izjavo sestavimo resničnostno tabelo, se lahko zgodi ena izmed naslednjih treh možnosti: v *resničnostnem stolpcu*, to je stolpcu, v katerem so zapisane vrednosti pripadajoče sestavljene izjave glede na vrednosti enostavnih izjav, ki to izjavo sestavljajo, so same enice, same ničle, ali pa je nekaj ničel in nekaj enic. Te tri "tipe" izjav posebej poimenujmo.

Definicija. Sestavljena izjava, ki je resnična ne glede na vrednosti enostavnih izjav, ki jo sestavljajo, je *tautologija* ali *resnica*. Sestavljena izjava, ki je neresnična ne glede na vrednosti enostavnih izjav, ki jo sestavljajo, je *protislovje* ali *laž*. Sestavljena izjava, ki ni ne resnica ne laž, je *faktična* izjava.

Zakaj ime faktična izjava? Zato, ker nam za takšno izjavo informacija o njeni resničnosti oziroma neresničnosti nekaj pove o vrednostih enostavnih izjav, ki jo sestavljajo. Na primer, če vemo, da je izjava "Če je f injektivna funkcija, ima globalni maksimum v točki $x = 3$." neresnična, potem vemo, da je f res injektivna funkcija, ki pa nima globalnega maksimuma v točki $x = 3$. To je namreč edina možnost, pri kateri je ta sestavljena izjava neresnična.

Naloga 1.1. Zapišite resničnostno tabelo za sestavljene izjave $p \wedge (q \Rightarrow \neg p)$, $p \vee (q \iff r) \wedge q$ in $\neg(p \Rightarrow q) \vee (q \Rightarrow p)$.

Naloga 1.2. Denimo, da ste prebivalec otoka vitezov (ki vedno govorijo resnico) in oprod (ki vedno lažejo) in da ste oproda. Vaš prijatelj (ki ve, da ste vi oproda), je pred naslednjo nalogo: iz košare mora izbrati enega izmed treh ključev (bel, rdeč in moder) in z njim odkleniti ena izmed treh vrat (kovinska, plastična in lesena). Če mu uspe odkleniti vrata, dobi nagrado. Le en ključ odklene sploh kakšna vrata, pa še to samo ena. Vi ste nekako izvedeli, da je to bel ključ, ki odklene lesena vrata. Na voljo imate samo en trdilni stavek, ki mu ga lahko poveste. Ali mu lahko z vašo izjavo posredujete dovolj informacij, da bo z gotovostjo vedel kako priti do nagrade? Kaj pa če vaš prijatelj ne ve, da ste vi oproda, poleg tega pa bi moral prijatelj najprej izbrati škatlo (rumeno, oranžno ali vijolično), od katerih bi bili dve prazni, v eni pa bi bili omenjeni trije ključi? Če veste katera škatla je prava, ali bi mu tedaj lahko z enim trdilnim stavkom pomagali do nagrade?

Naloga 1.3. Na otoku vitezov in oprod srečamo dva domačina, Janeza in Tončko. Ko ju ogovorimo, nam povesta naslednje.

Janez: "Midva s Tončko sva poročena in sva oba istega stanu."
Tončka: "Kje pa, nisva poročena in niti istega stanu nisva!"

Ali lahko na podlagi tega kaj sklepamo o njunem stanu in o tem ali sta poročena ali ne?

Naloga 1.4. Vrnimo se še malce na otok vitezov in oprod. Tokrat srečamo Bonifacija, Francija in Majdo. Tole nam povedo:

Bonifacij: "Jutri bo na našem otoku velika zabava, na katero lahko pridejo le vitezi in tujci."
Majda: "Naš Franci je vitez, Bonifacij pa oproda."
Franci: "Veš kaj Majda, če sem jaz vitez, si oproda ti!"

Ali bo torej jutri res zabava za viteze in tujce?

1.2 Ekvivalenca izjav

Kot smo povedali že uvodoma, je ena izmed glavnih nalog matematične logike analiza izjav. Dani izjavi je treba poiskati izjave, ki so ji "enakovredne" oziroma "ekvivalentne". Na ta način izjavo "prevedemo" v enakovredno obliko, ki pa nam nemalokrat omogoči, da lažje presodimo o resničnosti oziroma neresničnosti dane izjave. Opredelimo sedaj pojem ekvivalence izjav.

Definicija. Izjavi p in q sta *enakovredni* oziroma *ekvivalentni*, če je izjava $p \iff q$ tautologija. V tem primeru to dejstvo označimo s $p \sim q$.

Če smo malce površni, bi torej lahko rekli, da sta izjavi p in q ekvivalentni, če imata v resničnostni tabeli enaka stolpca. Oglejmo si zgled.

Zgled: Premislimo, če sta izjavi "Če je $\mathcal{B}$ linearno neodvisna množica, ki je hkrati še ogrodje prostora V, je $\mathcal{B}$ baza prostora V." in "Množica $\mathcal{B}$ je linearno odvisna, ali ni ogrodje prostora V, ali pa je baza prostora V." ekvivalentni. V ta namen označimo vse tri enostavne izjave, ki nastopajo v danih dveh izjavah:

$p \equiv$ "$\mathcal{B}$ je linearno neodvisna množica."
$q \equiv$ "$\mathcal{B}$ je ogrodje prostora V."
$r \equiv$ "$\mathcal{B}$ je baza prostora V."

Zgornji izjavi sta tedaj $p \wedge q \Rightarrow r$ in $\neg p \vee \neg q \vee r$. Sedaj lahko izpolnimo

resničnostno tabelo za pripadajočo ekvivalenco:

p	q	r	$p \wedge q \Rightarrow r$		$\iff$	$\neg p \vee \neg q \vee r$
0	0	0	0	1	**1**	1
0	0	1	0	1	**1**	1
0	1	0	0	1	**1**	1
0	1	1	0	1	**1**	1
1	0	0	0	1	**1**	1
1	0	1	0	1	**1**	1
1	1	0	1	0	**1**	0
1	1	1	1	1	**1**	1

Pripadajoča ekvivalneca je torej tautologija in zato sta izjavi $p \wedge q \Rightarrow r$ in $\neg p \vee \neg q \vee r$ ekvivalentni. ▲

Zakaj smo zgoraj rekli "površni"? Dve izjavi, ki sta si sicer ekvivalentni, sta lahko, vsaj načeloma, sestavljeni iz različno mnogo enostavnih izjav. To pa pomeni, da pripadajoča resničnostna stolpca sploh nista enakih dolžin in ju je zato nemogoče primerjati. Na primer, lahko se je prepričati, da je izjava $p \wedge (p \vee q)$ ekvivalentna izjavi p. A prva ima resničnostno tabelo s štirimi vrsticami, druga pa resničnostno tabelo z dvema vrsticama.

Spomnimo se priporočila, kaj naj bi bil prvi korak pri reševanju matematičnih problemov? Problem je treba najprej razumeti. No, zdaj najbrž že vidimo vlogo matematične logike. Dani izjavi je treba poiskati čimveč ekvivalentnih izjav, da bomo problem bolje razumeli in ga nato znali rešiti. Kako pa to storimo? Zaenkrat znamo namreč le preveriti, če sta dve dani izjavi ekvivalentni ali ne. To je namreč povsem preprosto. Zapišemo resničnostno tabelo za ekvivalenco obeh izjav in preverimo, če je pripadajoča izjava tautologija. A mi izjave, ki naj bi bila naši dani izjavi ekvivalentna, seveda še ne poznamo. Zato je treba poznati čimveč splošnih ekvivalenc med izjavami (izjavnimi formami), da lahko z uporabo le-teh iz naše izjave pridelamo njej ekvivalentne izjave. Nekaj najbolj pomembnih je zbranih v naslednjem izreku.

Izrek 1.1. *Naj bodo p, q, r poljubne izjave. Tedaj veljajo naslednje ekvivalence:*

1. $p \wedge 1 \sim p,\ p \vee 1 \sim 1,\ p \wedge 0 \sim 0$ *in* $p \vee 0 \sim p$
2. $p \wedge \neg p \sim 0$ *in* $p \vee \neg p \sim 1$
3. $p \sim \neg(\neg p)$
4. $p \wedge p \sim p$ *in* $p \vee p \sim p$ IDEMPOTENTNOST

5. $p \wedge q \sim q \wedge p$ *in* $p \vee q \sim q \vee p$ KOMUTATIVNOST
6. $(p \wedge q) \wedge r \sim p \wedge (q \wedge r)$ *in* $(p \vee q) \vee r \sim p \vee (q \vee r)$ ASOCIATIVNOST
7. $p \wedge (q \vee r) \sim (p \wedge q) \vee (p \wedge r)$ *in* $p \vee (q \wedge r) \sim (p \vee q) \wedge (p \vee r)$ DISTRIBUTIVNOST
8. $\neg(p \wedge q) \sim \neg p \vee \neg q$ *in* $\neg(p \vee q) \sim \neg p \wedge \neg q$ DEMORGANOVA ZAKONA
9. $p \wedge (p \vee q) \sim p$ *in* $p \vee (p \wedge q) \sim p$ ABSORBCIJA
10. $p \Rightarrow q \sim \neg p \vee q$ *in* $\neg(p \Rightarrow q) \sim p \wedge \neg q$
11. $p \Rightarrow q \sim \neg q \Rightarrow \neg p$
12. $p \iff q \sim (p \Rightarrow q) \wedge (q \Rightarrow p)$ *in* $\neg(p \iff q) \sim p \iff \neg q$

DOKAZ: Točka 1 sledi neposredno iz definicij logičnih veznikov konjunkcije in disjunkcije. Ostale ekvivalence bo bralec dokazal sam s pomočjo pripadajočih resničnostnih tabel. Seveda pa tega ni treba narediti za prav vse podane ekvivalence. Ko smo neko ekvivalenco enkrat dokazali, jo seveda lahko uporabimo pri dokazu drugih. Na primer, ko dokažemo idempotentnost, distributivnost in absorbcijo $p \wedge (p \vee q) \sim p$, sledi $p \vee (p \wedge q) \sim (p \vee p) \wedge (p \vee q) \sim p \wedge (p \vee q) \sim p$. Podobno se lahko ekvivalenca pod številko 11 potem, ko smo dokazali že vse prejšnje ekvivalence, dokaže takole: $p \Rightarrow q \sim \neg p \vee q \sim q \vee \neg p \sim \neg\neg q \vee \neg p \sim \neg q \Rightarrow \neg p$. □

Oglejmo si na tem mestu nekaj zgledov, ki ponazarjajo pravkar povedano.

ZGLED: Naj bo n neko izbrano naravno število. Oglejmo si še enkrat izjavo "Če je n^2 liho število, je tudi n liho število." in poskušajmo dokazati, da je pravilna. Če s p označimo izjavo "n^2 je liho število." in s q izjavo "n je liho število.", potem želimo v resnici pokazati, da je izjava $p \Rightarrow q$ resnična. Po zgornjem izreku je ta izjava ekvivalentna izjavi $\neg q \Rightarrow \neg p$. No, resničnost te izjave je lažje dokazati. Iz definicije logičnega veznika implikacije namreč sledi, da je edina možnost, pri kateri ta izjava ne bi bila resnična, ta, da je $\neg q \sim 1$ in $\neg p \sim 0$. Pa denimo, da velja $\neg q \sim 1$, kar v resnici pomeni, da je n sodo število. Tedaj obstaja naravno število n_0, da je $n = 2n_0$. Potem pa je $n^2 = (2n_0)^2 = 4n_0^2 = 2(2n_0^2)$, kar je prav tako sodo število. To pa pomeni, da izjava p ni resnična, torej je resnična izjava $\neg p$. Tako smo res pokazali, da je izjava $\neg q \Rightarrow \neg p$ resnična, s tem pa je seveda resnična tudi izjava "Če je n^2 liho število, je tudi n liho število.". ▲

Ustavimo se pri zgornjem zgledu še za trenutek. Kaj smo sploh pokazali? Da je n liho število? Da je n^2 liho število? Seveda nič od tega. Smo pa

pokazali, da je n liho število, če je le n^2 liho število. Z drugimi besedami, pokazali smo, da je lihost števila n^2 zadosten pogoj za lihost števila n. Ali še drugače, lihost števila n je potreben pogoj za lihost števila n^2.

ZGLED: Naj bo n zopet neko izbrano naravno število. Kako pa je z resničnostjo trditve "Število n je liho natanko tedaj, ko je n^2 liho število." Če uporabimo oznake prejšnjega zgleda, lahko našo trditev sedaj zapišemo kot $q \iff p$. Po izreku 1.1 je ta izjava ekvivalentna izjavi $(q \Rightarrow p) \wedge (p \Rightarrow q)$. Ker je ta izjava konjunkcija, je seveda pravilna natanko tedaj, ko sta obe izjavi, ki jo sestavljata, pravilni. Da je izjava $p \Rightarrow q$ pravilna, že vemo. Kako pa je s pravilnostjo izjave $q \Rightarrow p$? No, če je izjava q resnična, je $n = 2n_0 - 1$ za neko naravno število n_0. Tedaj pa je $n^2 = (2n_0 - 1)^2 = 4n_0^2 - 4n_0 + 1 = 2(2n_0^2 - 2n_0 + 1) - 1$, kar je seveda zopet liho število. Izjava p je torej v tem primeru resnična in tako je resnična tudi izjava $q \Rightarrow p$. Izjava "Število n je liho natanko tedaj, ko je n^2 liho število." je torej pravilna izjava. Bralca vabimo naj razmisli o vprašanju: "Smo mar zdaj dokazali, da je n liho število?" Povejmo še, da smo torej pravkar dokazali, da je lihost števila n *potreben in zadosten pogoj* za lihost števila n^2. ▲

Pomudimo se sedaj še pri naslednjem vprašanju. Denimo, da imamo dano naravno število n in da imamo dan stolpec dolžine 2^n, sestavljen iz samih ničel in enic. Ali tedaj obstaja izjava, sestavljena iz n enostavnih izjav, katere resničnostni stolpec je ravno dani stolpec? Razrešimo najprej naslednjo posebno obliko tega vprašanja. Denimo, da iščemo sestavljeno izjavo q, ki je sestavljena iz enostavnih izjav $p_1, p_2, \ldots, p_n$ in ki je pri natanko enem naboru vrednosti enostavnih izjav p_i (recimo mu *izbrani nabor*) resnična, pri vseh ostalih pa neresnična. Ker je konjunkcija izjav resnična natanko tedaj, ko je vsaka izmed nastopajočih izjav resnična, lahko torej za q vzamemo konjunkcijo vseh tistih izjav p_i, ki so pri izbranem naboru resnične in negacij vseh tistih izjav p_j, ki so pri izbranem naboru neresnične. Vsaki taki konjunkciji rečemo *osnovna konjunkcija* izjav $p_1, p_2, \ldots, p_n$. No, sedaj je na dlani tudi odgovor na začetno vprašanje kako dobiti izjavo, ki je pri vsakem izmed v naprej predpisanih naborov izjav $p_1, p_2, \ldots, p_n$ resnična, pri ostalih naborih pa neresnična. Vzamemo disjunkcijo vseh zgoraj opisanih osnovnih konjunkcij. Edini izmed 2^{2^n} možnih stolpcev, pri katerem ta metoda ne deluje, je stolpec samih ničel. A taka izjava je protislovje (ki jo označimo z 0) in se jo lahko recimo dobi že kot $p \wedge \neg p$. To pomeni, da smo pravkar dokazali spodnji izrek 1.2. (Predno ga navedemo, si oglejmo še definicijo pojma izbrana disjunktivna oblika.)

Definicija. Denimo, da je q sestavljena izjava, ki je sestavljena iz enostavnih izjav $p_1, p_2, \ldots, p_n$. Če je q zapisana kot disjunkcija samih osnovnih

konjunkcij izjav $p_1, p_2, \ldots, p_n$, pravimo, da je q zapisana v *izbrani* oziroma *normalni disjunktivni obliki*.

Izrek 1.2. *Vsako izjavo, ki ni protislovje, lahko zapišemo v izbrani disjunktivni obliki.*

DOKAZ: Denimo, da imamo izjavo q, ki je odvisna od n enostavnih izjav in ni protislovje. Zapišemo resničnostno tabelo za izjavo q, nato pa dobljenemu stolpcu v resničnostni tabeli priredimo izjavo v izbrani disjunktivni obliki z enako resničnostno tabelo. Po zgornjem premisleku to lahko naredimo (in to na en sam način, do vrstnega reda osnovnih konjunkcij natančno). Da sta izjava q in tako dobljena izjava ekvivalentni, je seveda očitno. □

Da vse skupaj še malce bolj razjasnimo, si oglejmo konkreten zgled.

ZGLED: Poiščimo izjavo q, ki je odvisna od enostavnih izjav p_1, p_2 in p_3 in ima naslednjo resničnostno tabelo:

p_1	p_2	p_3	q
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Izjava q ima v prvi vrstici vrednost 1, zato je treba vzeti pripadajočo osnovno konjunkcijo $\neg p_1 \wedge \neg p_2 \wedge \neg p_3$. Osnovna konjunkcija, ki ustreza peti vrstici je $p_1 \wedge \neg p_2 \wedge \neg p_3$, osnovna konjunkcija, ki ustreza zadnji vrstici pa $p_1 \wedge p_2 \wedge p_3$. Izjava q je torej ekvivalentna izjavi

$$(\neg p_1 \wedge \neg p_2 \wedge \neg p_3) \vee (p_1 \wedge \neg p_2 \wedge \neg p_3) \vee (p_1 \wedge p_2 \wedge p_3) \sim$$
$$\neg p_1 \wedge \neg p_2 \wedge \neg p_3 \ \vee \ p_1 \wedge \neg p_2 \wedge \neg p_3 \ \vee \ p_1 \wedge p_2 \wedge p_3.$$

▲

Jasno je, da ima vsaka izjava natanko en zapis v izbrani disjunktivni obliki (do vrstnega reda osnovnih konjunkcij in vrstenga reda izjav p_i v posamezni osnovni konjunkciji natančno). To pomeni, da lahko ekvivalenco izjav študiramo tudi s pomočjo zapisa v izbrani disjunktivni obliki. Vsaki

izmed danih izjav poiščemo njej ekvivalentno izjavo v izbrani disjunktivni obliki in ju primerjamo.

Za konec tega razdelka si oglejmo še naslednji poučen zgled uporabe izreka 1.2.

ZGLED: Denimo, da ste se znašli na otoku vitezov in oprod. Kot tujec seveda niste preveč priljubljeni, saj domačini nikdar ne vedo ali je to, kar trenutno izjavljate, resnica ali laž. V resnici ste jim postali že tako moteči, da so sklenili, da se vas odkrižajo. Izbira, kako bo do tega prišlo, pa je na srečo (odvisno od tega, kako dobri ste v logiki) v vaših rokah. Domačini vas namreč skupaj s silakom, za katerega pa ne veste ali je oproda ali vitez, napotijo po poti, ki je uhojena skozi pragozd. Na nekem mestu se pot razcepi. Ena izmed poti vodi do obale, na kateri čaka vaš čoln, druga pa vodi do jase, na kateri mrgoli strupenih kač. Vaš stražar kot domačin seveda ve, katera pot vodi do obale. Na razpotju lahko silaku zastavite eno samo vprašanje. Kaj boste vprašali, da boste lahko iz odgovora razbrali, katera pot vodi do obale?

Izjava, katere resničnost nas zanima, je recimo "Leva pot vodi do obale." (označimo jo s p). Seveda pa stražarja ne moremo kar vprašati "Ali leva pot vodi do obale?", saj ne vemo ali je vitez ali oproda. Pomembna je torej tudi resničnost izjave "Vi ste oproda." (označimo jo s q). Ali lahko iz p in q sestavimo izjavo, ki nas bo odrešila? Poizkusimo poiskati izjavo r, ki bo imela to lastnost, da bomo na vprašanje o njeni resničnosti, ne glede na stan našega stražarja, dobili odgovor "da" natanko tedaj, ko leva pot vodi do obale. Kakšno vrednost torej mora imeti izjava r, če sta p in q obe neresnični? Ker v tem primeru na svobodo vodi desna pot, mora biti odgovor, ki ga bomo dobili "ne". Ker v tem primeru naš sogovornik ni oproda, govori resnico, torej mora biti izjava r, po pravilnosti katere ga bomo vprašali, neresnična. Če sta p in q obe nepravilni, mora biti torej tudi izjava r nepravilna. Kaj pa, če je p nepravilna, q pa pravilna? Ker tudi v tem primeru do obale vodi desna pot, mora ogovorjeni odgovoriti z "ne". A ta je sedaj oproda, torej laže, kar pomeni, da mora biti izjava, po pravilnosti katere ga sprašujemo, resnična. Podobno dobimo vrednosti za r še pri ostalih dve možnostih. Dobimo

p	q	r
0	0	0
0	1	1
1	0	1
1	1	0

Katera je torej izjava r, ki jo iščemo? Lahko se spomnimo, da je zgornja tabela ravno "negacija" resničnostne tabele za izjavo $p \iff q$. Tako bi ugotovili, da lahko za r vzamemo kar izjavo $\neg(p \iff q)$, ki je po izreku 1.1

ekvivalentna izjavi $p \iff \neg q$. No, izjavo r bi lahko zapisali tudi v izbrani disjunktivni obliki, to je, $r \sim \neg p \wedge q \ \vee \ p \wedge \neg q$. Tudi od tod bi z uporabo ekvivalenc izreka 1.1 prišli do izjave $p \iff \neg q$. Eno izmed vprašanj, ki nam pomaga do rešitve, je torej: "Ali je res, da leva pot vodi do obale natanko tedaj, ko ste vi vitez?" ▲

Naloga 1.5. V naslednjih sestavljenih izjavah prepoznajte enostavne izjave, ki jih sestavljajo, nato te enostavne izjave označite s simboli (p, q, r, itd.), pripadajočo sestavljeno izjavo zapišite v jeziku matematične logike in dobljeno izjavo čimbolj poenostavite (z uporabo ekvivalenc med izjavami). Dobljeno poenostavljeno izjavo nato zapišite z besedami. (Pozor! Tu se ne ukvarjamo s pomenom konkretnih izjav, zato tudi nočemo trditi, da je to, kar izjave povedo, nujno vedno res!)

- "Če sta Ana in Jakob oba viteza, je vsaj eden izmed njiju oproda."
- "Če množica $\mathcal{B}$ ni baza vektorskega prostora V, je $\mathcal{B}$ ogrodje za V natanko tedaj, ko velja, da je $\mathcal{B}$ baza ali ogordje za V."
- "Če je zaporedje **a** konvergentno, potem iz dejstva, da je omejeno, sledi, da je konvergentno in ima stekališče."
- "Če ni res, da Floki grize, ko je jezen, potem je Floki jezen in grize."

Naloga 1.6. Pokažite, da bi lahko shajali samo z logičnima veznikoma negacije in disjunkcije, to je, da lahko vsaki izjavi najdemo ekvivalentno izjavo, v kateri nastopata samo negacija in disjunkcija. Nato izjavi $p \Rightarrow q \iff \neg r$ poiščite ekvivalentno izjavo, ki vsebuje le negacije in disjunkcije.

Naloga 1.7. Naj bo n neko naravno število. S pomočjo logičnih ekvivalenc iz izreka 1.1 prevedite izjavo "Če je n liho število, število $\sqrt{2n}$ ni celo število." v ekvivalentno obliko, ki vam bo omogočila dokaz resničnosti te izjave.

Naloga 1.8. Na otoku vitezov in oprod srečate tri domačine, Francija, Janeza in Jožeta. Ali lahko enemu izmed njih zastavite vprašanje, na katerega bo odgovoril pritrdilno natanko tedaj, ko so vsi trije istega stanu?

1.3 Logične implikacije in sklepanje

V prejšnjem razdelku smo se ukvarjali z vprašanjem, kdaj sta dve izjavi ekvivalentni, torej kdaj v resnici nosita isto informacijo, in kako dani izjavi poiščemo čimveč ekvivalentnih izjav. Včasih pa se zgodi, da ekvivalentne izjave, ki bi nam ustrezala, enostavno ne znamo najti, ali pa nas zanima zgolj naslednje: če vemo, da je neka dana izjava resnična, katere izjave so

potem tudi zagotovo resnične? V takih primerih torej iščemo izjave, ki iz dane izjave, ali množice izjav, "logično sledijo". Opredelimo ta pojem bolj natančno.

Definicija. Naj bosta p in q izjavi. Pravimo, da je izjava q *logična posledica* izjave p, če je izjava $p \Rightarrow q$ tautologija. V tem primeru pravimo, da je $p \Rightarrow q$ *logična implikacija*.

Oglejmo si zgled.

Zgled: Pokažimo, da je izjava $q \Rightarrow p$ logična posledica izjave p. V ta namen se je potrebno prepričati, da je izjava $p \Rightarrow (q \Rightarrow p)$ tautologija. To lahko dosežemo preko pripadajoče resničnostne tabele. Še bolj eleganten način je ta, da s pomočjo ekvivalenc izreka 1.1 pokažemo, da velja

$$p \Rightarrow (q \Rightarrow p) \sim \neg p \vee (\neg q \vee p) \sim \neg p \vee p \vee \neg q \sim 1 \vee \neg q \sim 1.$$

▲

Zakaj so logične implikacije pomembne? Premislimo, kaj pomeni dejstvo, da je izjava q logična posledica izjave p. To seveda ne pomeni, da je izjava q vedno resnična. Po definiciji logičnega veznika implikacije namreč vrednost izjave q v primeru, ko je p neresnična izjava, ne vpliva na resničnost sestavljene izjave $p \Rightarrow q$. Dejstvo, da je izjava q logična posledica izjave p, pomeni, da je izjava q resnična pri vsakem naboru enostavnih izjav, ki sestavljajo izjavi p in q, pri katerem je resnična izjava p. Logične implikacije nam torej povedo kdaj smemo iz pravilnosti neke izjave *sklepati* na pravilnost neke druge izjave. Na ta način torej logične implikacije podajajo pravila *logičnega sklepanja*. V tem pa v resnici tiči bistvo matematike. V idealnem svetu bi bil namreč matematik sposoben dani izjavi poiskati vse mogoče ekvivalentne izjave ali vsaj razumeti, kako naj bi take izjave izgledale. V resnici pa tega žal nismo sposobni. Zato smo se prisiljeni zadovoljiti že s tem, da pokažemo, da so neke izjave logične posledice drugih. Na ta način lahko bogato matematično teorijo uporabimo tudi pri reševanju povsem konkretnih problemov.

Omeniti velja tudi naslednje. V bogati zgodovini matematike je bilo vpeljanih že ogromno različnih pojmov in teorij, med katerimi običajno, vsaj na videz, ni prav nobene zveze. In vendar vedno znova odkrivamo povezave med njimi. Nemalokrat se je na primer zgodilo, da so matematiki po temeljitem študiju neke nove teorije odkrili, da gre v resnici za pojme, ki so bili vpeljani, seveda s povsem drugimi imeni in na povsem drug način, že pred desetletji. Na ta način se rezultati različnih teorij dopolnjujejo, hkrati pa pripomorejo tudi k bolj "čisti" teoriji, kar je v današnji poplavi novih rezultatov vsekakor

dobrodošlo. Tako imamo danes zelo elegantne in kratke dokaze mnogih klasičnih rezultatov, katerih prvi dokazi so bili tako tehnično zahtevni in dolgi, da so bili praktično neberljivi.

Zgolj kot zanimivost omenimo eno izmed najdlje odprtih domnev v teoriji števil, katere formulacija je povsem preprosta in razumljiva slehernemu človeku, odgovor na njeno resničnost pa je očitno tako zapleten in zahteva tolikšno mero logičnega sklepanja, da ga v več kot 260 letih ni našel še nihče. In to kljub dejstvu, da so domnevo skušali rešiti največji umi zadnjih stoletij. Gre za tako imenovano Goldbachovo domnevo iz leta 1742. Ta pravi, da je vsako sodo število, ki je večje od 2, moč zapisati kot vsoto dveh (ne nujno različnih) praštevil. Čeprav ta problem buri matematične duhove že toliko časa, še do danes nihče ni uspel dokazati niti da je ta izjava pravilna, niti da je nepravilna. S pomočjo računalnikov je bilo na primer preverjeno, da je izjava pravilna za vsa naravna števila do vključno 10^{18}, a to seveda za dokončni odgovor ne pomeni praktično nič. Kdor bi o tej zadevi želel izvedeti kaj več, si lahko na primer ogleda knjigo Apostolosa Doxiadisa z naslovom "Stric Petros in Goldbachova domneva". Glavni junak knjige in njegova zgodba sta sicer plod pisateljeve domišljije, a bralec se bo ob branju seznanil z nekaterimi zanimivimi dejstvi iz zgodovine teorije števil.

V času študija na PeF se seveda ne bomo ukvarjali s tako težkimi vprašanji. Pa vendar se tudi takrat, ko se spopadamo s precej lažjimi nalogami, v resnici skoraj vedno sprašujemo, ali je neka izjava logična posledica neke druge izjave (ali večih izjav) ali ne. Zato je zelo pomembno, da se naučimo nekaj osnovnih prijemov pri takšnem sklepanju. Oglejmo si nekaj najpomembnejših logičnih implikacij.

Izrek 1.3. *Naj bodo p, q in r poljubne izjave. Tedaj veljajo naslednje logične implikacije:*

$p \wedge q$	$\Rightarrow$	p	Poenostavitev
$p \wedge (p \Rightarrow q)$	$\Rightarrow$	q	Modus ponens
$\neg q \wedge (p \Rightarrow q)$	$\Rightarrow$	$\neg p$	Modus tollens
$\neg p \wedge (p \vee q)$	$\Rightarrow$	q	Disjunktivni silogizem
$(p \Rightarrow q) \wedge (q \Rightarrow r)$	$\Rightarrow$	$(p \Rightarrow r)$	Hipotetični silogizem
p	$\Rightarrow$	$p \vee q$	Pridružitev

Dokaz: Komentar z zgornjega zgleda je na mestu tudi tukaj. Seveda lahko vse te implikacije dokažemo preprosto tako, da sestavimo pripadajoče resničnostne tabele. Dokazov pa se lahko lotimo tudi s pomočjo izreka 1.1.

Na primer,

$$p \wedge (p \Rightarrow q) \Rightarrow q \sim \neg(p \wedge (\neg p \vee q)) \vee q \sim (\neg p \vee (p \wedge \neg q)) \vee q \sim (1 \wedge (\neg p \vee \neg q)) \vee q \sim \neg p \vee \neg q \vee q \sim \neg p \vee 1 \sim 1,$$

s čimer smo dokazali veljavnost logične implikacije Modus ponens. Dokaze preostalih logičnih implikacij prepuščamo bralcu. □

Včasih govorimo o tem, da je neka izjava logična posledica množice nekih izjav (oziroma *predpostavk*). V tem primeru v resnici govorimo o tem, da je ta naša izjava logična posledica konjunkcije vseh omenjenih izjav. Kako preveriti, če je sklep, da je dana izjava res logična posledica predpostavk, pravilen? Lahko seveda formiramo pripadajočo implikacijo konjunkcije vseh predpostavk in izjave, ki naj bi iz njih logično sledila, in preverimo, če je dobljena izjava tautologija. A če v vseh teh izjavah nastopa veliko število enostavnih izjav, je tak pristop preveč zamuden. Že pri šestih enostavnih izjavah moramo namreč izpolniti resničnostno tabelo s 64 vrsticami.

Razmišljamo lahko takole. Če je izjava p logična posledica predpostavk $p_1, p_2, \ldots, p_n$ in je izjava q logična posledica predpostavk $p_1, p_2, \ldots, p_n$ in p, je seveda q tudi logična posledica predpostavk $p_1, p_2, \ldots, p_n$ (bralca vabimo, da to dokaže). To pomeni, da lahko dejstvo, da je neka izjava logična posledica danih predpostavk, dokažemo "po korakih". Vsako izjavo, ki jo dobimo kot logično posledico predpostavk, lahko priključimo k množici predpostavk.

Na tem dejstvu temelji vsak matematičen dokaz. Iz predpostavk izpeljujemo nove in nove logične posledice, dokler ne pridemo do tiste, ki je naš cilj. Da bomo sklepanje, ki ga je pri tem treba opraviti, zapisali v strnjeni in berljivi obliki, sklenimo naslednji dogovor o "pravilih za pisanje formalnega dokaza":

- Vsak korak premisleka zapišemo v novo vrstico, vrstice pa številčimo.
- V začetne vrstice zapišemo vse predpostavke, dejstvo, da so to predpostavke pa označimo tako, da k vrsticam dopišemo besedico "predp".
- Včasih je kako izjavo bolje prepisati v ekvivalentno obliko. Kadar storimo to, v vrstico, kamor zapišemo ekvivalentno izjavo, dopišemo znak $\sim$ in dodamo številko vrstice, v kateri se nahaja originalna izjava.
- Če se v nekem koraku sklepanja opremo na eno izmed logičnih implikacij izreka 1.3, navedemo katero (Po, MP, MT, DS, HS, Pr) in v oklepaju dodamo številke vrstic pripadajočih izjav, ki pri tem nastopajo v vlogi izjav p, q in r.

- Seveda je pri takem logičnem sklepanju vsaka vrstica, ki jo na ta način dobimo, logična posledica predpostavk, torej je logična posledica tudi vsaka konjunkcija tako dobljenih izjav. Kadar torej več izjav že dobljenih vrstic povežemo s konjunkcijo, rečemo, da smo pripadajoče izjave *združili*, to dejstvo pa v našem zapisu označimo z Zd skupaj s pripadajočimi številkami.

Opisana pravila bomo najbolje razumeli, če si jih ogledamo na konkretnem zgledu.

Zgled: Denimo, da so resnične naslednje izjave:

"Če grem na avtobus, zamudim v službo."
"Grem na avtobus ali na vlak."
"Če zamudim v službo, nimam časa za kosilo."
"Če grem na vlak, preberem časnik."
"Imam čas za kosilo."

Ali je sklep, da bom potemtakem prebral časnik, pravilen? Napravimo premislek najprej "opisno". Ker imam čas za kosilo, po pravilu Modus tollens ne zamudim v službo. Po vnovični uporabi pravila Modus tollens torej v službo ne grem z avtobusom. Po pravilu disjunktivnega silogizma torej grem na vlak. Po pravilu modus ponens pa to pomeni, da preberem časnik. Torej je sklep, da preberem časnik, pravilen.

Poiščimo še formalen dokaz pravilnosti zgornjega sklepa, to je, pokažimo, da je izjava "Prebral bom časnik" logična posledica predpostavk. Očitno v sklepanju nastopajo naslednje enostavne izjave:

$a \equiv$ "Grem na avtobus."
$v \equiv$ "Grem na vlak."
$z \equiv$ "Zamudim službo."
$k \equiv$ "Imam čas za kosilo."
$c \equiv$ "Preberem časnik."

Da je zgornji sklep pravilen, lahko torej z upoštevanjem zgornjega dogov-

ora formalno dokažemo takole:

1.	$a \Rightarrow z$	$predp$
2.	$a \vee v$	$predp$
3.	$z \Rightarrow \neg k$	$predp$
4.	$v \Rightarrow c$	$predp$
5.	k	$predp$
6.	$\neg\neg k$	~ 5
7.	$\neg z$	$MT(3,6)$
8.	$\neg a$	$MT(1,7)$
9.	v	$DS(2,8)$
10.	c	$MP(4,9)$

Kot smo omenili že zgoraj, bi lahko veljavnost sklepa, da je izjava c logična posledica predpostavk, pokazali tudi tako, da bi zapisali resničnostno tabelo za izjavo $(a \Rightarrow z) \wedge (a \vee v) \wedge (z \Rightarrow \neg k) \wedge (v \Rightarrow c) \wedge k \Rightarrow c$ in se s tem prepričali, da gre za tautologijo. A pripadajoča resničnostna tabela bi imela 32 vrstic, kar bi zagotovo vzelo bistveno več časa kot zgornji postopek. ▲

Zgled: Denimo, da so resnične trditve: "Če grem z vlakom, potem iz dejstva, da zjutraj popijem čaj, sledi, da ne grem z avtom." "Grem z avtom ali vlakom." "Če grem v posteljo pozno, zjutraj ne popijem čaja."

Ali je tedaj sklep, da v primeru, ko popijem čaj, grem z vlakom, pravilen? Kaj hitro ugotovimo, da pravilnosti sklepa ne moremo dokazati. Pokažimo, da sklep ni pravilen. To dosežemo tako, da poiščemo take vrednosti enostavnih izjav, ki nastopajo v zgornjih sestavljenih izjavah, da bodo vse predpostavke resnične, izjava "Če popijem čaj, grem na vlak." pa bo neresnična. Če naj bo to res, mora veljati, da ne grem na vlak, grem z avtom, zjutraj popijem čaj in ne grem pozno v posteljo. Hitro se prepričamo, da so v tem primeru vse predpostavke res resnične, izjava "Če popijem čaj, grem na vlak." pa ni resnična. ▲

Da dokažemo, da nek sklep ni pravilen, je torej dovolj najti take vrednosti enostavnih izjav, ki sestavljajo predpostavke in "zaključek", da so vse predpostavke pravilne, izjava, ki naj bi iz njih sledila, pa ne.

Zgled: Oglejmo si še malce manj trivialen (pravilen) sklep in zapišimo formalen dokaz njegove pravilnosti. Denimo, da so resnične izjave: $v \Rightarrow p$, $t \vee s$, $p \wedge q \Rightarrow r \vee s$, $t \vee u \Rightarrow v \wedge z$, $\neg s$ in $\neg q \Rightarrow (z \Rightarrow s)$. Ali smemo od tod

sklepati, da je tedaj resnična izjava r?

1.	$v \Rightarrow p$	$predp$
2.	$t \vee s$	$predp$
3.	$p \wedge q \Rightarrow r \vee s$	$predp$
4.	$t \vee u \Rightarrow v \wedge z$	$predp$
5.	$\neg s$	$predp$
6.	$\neg q \Rightarrow (z \Rightarrow s)$	$predp$
7.	t	$DS(2,5)$
8.	$t \vee u$	$Pr(7)$
9.	$v \wedge z$	$MP(4,8)$
10.	v	$Po(9)$
11.	p	$MP(1,10)$
12.	z	$Po(9)$
13.	$z \wedge \neg s$	$Zd(5,12)$
14.	$\neg(\neg z \vee s)$	~ 13
15.	$\neg(z \Rightarrow s)$	~ 14
16.	$\neg\neg q$	$MT(6,15)$
17.	q	~ 16
18.	$p \wedge q$	$Zd(11,17)$
19.	$r \vee s$	$MP(3,18)$
20.	r	$DS(5,19)$

▲

Naloga 1.9. Vaš prijatelj Janko se zelo navdušuje nad delom nekega precej svojevrstnega slikarja. Na vseh svojih slikah uporablja le modro, rdečo in zeleno barvo. No, da je stvar še toliko bolj nenavadna ima hkrati še naslednje "muhe". Če na sliki uporabi modro in rdečo, uporabi tudi zeleno. Če uporabi rdečo ali zeleno, uporabi tudi modro. Na isti sliki nikoli ne uporabi tako modre kot zelene. Vedno uporabi vsaj eno izmed modre in rdeče. Lahko na podlagi tega vašemu prijatelju Janku kaj poveste o tem, kakšne barve bodo na njegovi novi sliki, ki jo namerava kupiti?

Naloga 1.10. V vsakem izmed spodnjih primerov so podane izjave p, q in r. Če vam nekdo pove, da sta izjavi p in q resnični, ali smete kaj sklepati o resničnosti izjave r?

1. primer:
$p \equiv$ "Če bo jutri deževalo, grem v službo z avtobusom."
$q \equiv$ "Jutri grem v službo s kolesom."
$r \equiv$ "Jutri ne bo deževalo."

2. primer: Naj bosta a in b realni števili.
$p \equiv$ "Če je $a > 10$, je $b < 3/2$."
$q \equiv$ "$b = 1$."
$r \equiv$ "$a > 10$."

3. primer: Naj bosta zopet a in b realni števili.
$p \equiv$ "Če je $a < b$, je $a^2 < b^2$."
$q \equiv$ "$b < a$."
$r \equiv$ "$b^2 < a^2$."

4. primer: Naj bodo a, b in c realna števila.
$p \equiv$ "Če je $b > a$ in $b > 0$, je $b > c$."
$q \equiv$ "$b \leq c$."
$r \equiv$ "$b \leq a$ ali $b \leq 0$."

Naloga 1.11. Denimo, da so resnične predpostavke $p \vee (q \Rightarrow \neg r)$, q, $t \iff p$, $s \wedge \neg p \Rightarrow r \vee t$ in $t \Rightarrow \neg q$. Ali smemo tedaj sklepati, da je izjava s neresnična?

1.4 Kvantifikatorji

O množicah bomo bolj natančno govorili v drugem poglavju. Zaenkrat se zadovoljimo z dogovorom, da je *množica* zbirka nekih reči. Množice bomo praviloma označevali z velikimi latinskimi črkami, na primer, A, B, C, itd. Rečem, ki sestavljajo dano množico, rečemo *elementi* te množice. Da je reč a element množice A, označimo z $a \in A$.

Definicija. Naj bo A neka množica, $\mathcal{L}$ pa neka lastnost. Pravimo, da je lastnost $\mathcal{L}$ *smiselna* za elemente množice A, če za vsak $a \in A$ velja bodisi, da to lastnost ima, bodisi da te lastnosti nima, to je, če lahko za vsak $a \in A$ sodimo o resničnosti izjave, da ima a lastnost $\mathcal{L}$.

Naj bo sedaj $\mathcal{L}$ neka smiselna lastnost za elemente množice A. Tedaj izjavo "a ima lastnost $\mathcal{L}$" krajše zapišemo z $L(a)$ (izjavo "a nima lastnosti $\mathcal{L}$" pa seveda z $\neg L(a)$). "Funkciji" L pravimo *(enomestni) predikat* na množici A. Kot vidimo torej enomestni predikati na nek način ustrezajo lastnostim. Zato smo včasih malce površni in kar predikatu L rečemo lastnost.

Ko želimo podati določene izjave, ki govore o elementih množice A, se lahko dogovorimo, da se do nadaljnjega vse izjave nanašajo na elemente množice A. To dosežemo z dogovorom, da je množica A *domena pogovora*. Včasih želimo povedati, da imajo dano lastnost (recimo L) *vsi* elementi iz naše domene pogovora, spet drugič pa želimo povedati, da ima to lastnost

vsaj en element domene pogovora. S tem nekaj povemo o *kvantiteti* elementov, ki imajo dano lastnost, zato pripadajoča znaka, ki ju uporabljamo za zapise takih izjav, imenujemo *kvantifikatorja*.

Definicija. Naj bo A domena pogovora in naj bo L enomestni predikat, ki predstavlja neko smiselno lastnost $\mathcal{L}$ za elemente domene pogovora A. Tedaj izjavo "Vsi elementi domene pogovora imajo lastnost $\mathcal{L}$." v jeziku matematične logike zapišemo kot $\forall a : L(a)$. Znak $\forall$ imenujemo *univerzalni kvantifikator*. Izjavo "Nekateri elementi domene pogovora imajo lastnost $\mathcal{L}$." v jeziku matematične logike zapišemo kot $\exists a : L(a)$. Kvantifikator $\exists$ je *eksistenčni kvantifikator*.

Če se ne dogovorimo za domeno pogovora, bi zgornji izjavi zapisali kot $\forall a \in A : L(a)$, oziroma $\exists a \in A : L(a)$.

Zgled: Dogovorimo se, da je domena pogovora množica vseh naravnih števil. V jeziku matematične logike zapišimo izjavi "Nekatera praštevila so dvomestna." in "Niso vsa dvomestna števila praštevila." Očitno je govora o naslednjih dveh lastnostih, ki sta smiselni za naravna števila:

$P(x) \equiv$ "x je praštevilo."
$D(x) \equiv$ "x je dvomestno število."

Prva izjava očitno govori o obstoju, zato tukaj uporabimo eksistenčni kvantifikator. O eksistenci česa pa govori ta izjava? O eksistenci naravnega števila, ki je praštevilo in to še dvomestno povrhu. Jasno je torej, da je prva izjava $\exists x : (P(x) \wedge D(x))$. No, druga izjava pravi, da ni res, da so vsa dvomestna (naravna) števila praštevila. Pa zapišimo najprej izjavo "Vsa dvomestna števila so praštevila." Tu gre seveda za univerzalni kvantifikator. Vendar pa izjava ne pove, da so vsa naravna števila praštevila, temveč le, da so takšna tista, ki so dvomestna. Povedano še drugače, ta izjava pove, da če je neko naravno število dvomestno, je praštevilo. Gre torej za implikacijo. Izjava "Vsa dvomestna števila so praštevila." ima torej zapis $\forall x : (D(x) \Rightarrow P(x))$, naša prvotna izjava pa je tedaj $\neg(\forall x : (D(x) \Rightarrow P(x)))$. ▲

Seveda pa ne poznamo samo izjav, ki bi govorile o lastnostih nekih reči. Včasih govorimo tudi o tem, v kakšni zvezi ali *relaciji* sta dva (ali trije, štirje, ...) elementi neke množice. V tem primeru govorimo pač o *večmestnih predikatih*. Na primer, na množici vseh učencev nekega razreda lahko vpeljemo dvomestni predikat V, kjer je $V(x, y)$ izjava "x je večji od y".

Preden si ogledamo naslednji zgled, opozorimo še na naslednje. Kvantifikatorja torej uporabljamo zato, da povemo za koliko elementov domene pogovora velja izjava, ki sledi (kvantifikatorju). A ker take izjave lahko govore

tudi o relacijah med raznimi elementi domene pogovora, je treba pri vsakem kvantifikatorju povedati, na katero "spremenljivko" v izjavi, ki sledi, se ta kvantifikator nanaša. Zato moramo za kvantifikator vedno napisati spremenljivko, na primer $\forall a$ ali $\exists b$, itd. Da pa se izognemo težavi, ko bi nam pri daljših in bolj zapletenih izjavah začelo zmanjkovati črk za spremenljivke, se dogovorimo, da ima vsak kvantifikator "moč delovanja" le na najkrajši možni smisleni izjavi, ki mu sledi. V resnici smo ta dogovor upoštevali že v zgornjem zgledu.

Zgled: Spomnimo se zopet zgornjega zgleda, ki je govoril o tem, da je v primeru, ko je n^2 liho število, tudi n liho število. Ker tam nismo nič določili kakšno naj bo naravno število n, smo torej govorili o vseh naravnih številih. Našo trditev bi torej na hitro (brez določitve domene pogovora in vpeljave predikatov) lahko zapisali takole:

$$\forall n \in \mathbb{N} : (n^2 \text{ liho } \Rightarrow n \text{ liho}),$$

oziroma, če uporabimo nekaj standardnih oznak:

$$\forall n \in \mathbb{N} : (2 \nmid n^2 \ \Rightarrow 2 \nmid n).$$

▲

Zgled: Zapišimo (v jeziku matematične logike) izjavo "Vsaka eksponentna realna funkcija raste hitreje od kake polinomske realne funkcije."
Najprej se dogovorimo za domeno pogovora. Očitno lahko vzamemo, da je $\mathcal{D} = \{f : \mathbb{R} \to \mathbb{R}\}$ kar množica vseh realnih funkcij. Potrebujemo tudi nekaj predikatov:

$E(f) \equiv$ "f je eksponentna funkcija."
$P(f) \equiv$ "f je polinomska funkcija."
$H(f, g) \equiv$ "f raste hitreje kot g."

Naša trditev se torej glasi:

$$\forall f : (E(f) \Rightarrow \exists g : (P(g) \wedge H(f, g))).$$

▲

Zgled: Zapišimo v jeziku matematične logike še trditev iz Goldbachove domneve. V tem primeru se je smiselno dogovoriti, da so domena pogovora vsa naravna števila. Potrebujemo naslednje predikate:

$S(n) \equiv$ "n je sodo število."
$D(n) \equiv$ "Število n je večje od 2."

$P(n) \equiv$ "n je praštevilo."
$V(n, r, s) \equiv$ "n je vsota števil r in s."

Trditev Goldbachove domneve lahko sedaj zapišemo takole:

$$\forall n \,:\, (S(n) \wedge D(n) \Rightarrow \exists p \,:\, (P(p) \wedge \exists q \,:\, (P(q) \wedge V(n, p, q)))).$$

Ta zapis je seveda zelo nestandarden in malce težko berljiv. Najprej opazimo, da lahko oba eksistenčna kvantifikatorja združimo, nato pa se dogovorimo še, da namesto $\exists p \exists q$ pišemo kar $\exists p, q$. Glede na to, da imamo za skoraj vse zgornje predikate že vpeljane standardne oznake, lahko tako zgornjo izjavo preoblikujemo v bolj "všečno" obliko takole:

$$\forall n \,:\, (2 \mid n \wedge n > 2 \Rightarrow \exists p, q \,:\, (P(p) \wedge P(q) \wedge n = p + q)).$$

▲

Ugotovili smo že, da je pri razumevanju izjav zelo pomembno, da znamo dani izjavi poiskati čimveč ekvivalentnih izjav. Tudi pri izjavah, v katerih nastopajo kvantifikatorji, imamo dve zelo pomembni ekvivalenci:

$$\neg\forall x \,:\, L(x) \sim \exists x \,:\, \neg L(x)$$
$$\neg\exists x \,:\, L(x) \sim \forall x \,:\, \neg L(x)$$

Zakaj sta ti dve ekvivalenci tako zelo pomembni. Recimo, da se moramo odločiti o resničnosti trditve, da imajo vsi elementi neke množice A lastnost L in se nam zdi, da to ne drži. Kako naj to dokažemo? Zgornja ekvivalenca nam pove, da je to sila preprosto. Vse kar je treba storiti je, da poiščemo en sam element množice A, ki lastnosti L nima.

Zgled: Da pokažemo, da izjava "Za vsa cela števila z velja $z^2 > 0$." ni resnična, je dovolj videti, da 0^2 ni večje od 0. S tem smo namreč našli celo število z, ki lastnosti $z^2 > z$ nima. ▲

Recimo, da imamo dano domeno pogovora $\mathcal{D}$. Kako tedaj dokažemo pravilnost izjave $\exists x \,:\, L(x)$? Preprosto. Treba je najti *konkreten* element množice $\mathcal{D}$, ki ima lastnost L. Na primer, pravilnost trditve "Nekatera praštevila so večja od 1 000." lahko dokažemo tako, da se prepričamo, da je 1 009 praštevilo (dovolj je videti, da ni deljivo z nobenim izmed praštevil $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$). Kako pa dokažemo, da je pravilna izjava $\forall x \,:\, L(x)$. No, če je množica $\mathcal{D}$ "dovolj majhna", se lahko pač za vsak njen element posebej prepričamo, da lastnost L ima. Sicer pa je potrebno narediti premislek, ki pokaže, da takoj, ko je $x \in \mathcal{D}$, velja $L(x)$. Tukaj je torej

potrebno delati s splošnim elementom množice $\mathcal{D}$. Na primer, prav nič nam ne pomaga, da je računalnik preveril, da Goldbachovi domnevi zadoščajo vsa soda števila med 4 in 10^{18}. Pa ne zato, ker računalniku ne bi zaupali. Dokler namreč ne napravimo premisleka, ki je neodvisen od konkretne vrednosti sodega naravnega števila, nismo naredili praktično nič.

Bralec si bo ob pravkar povedanem morda mislil, da pretiravamo, češ, če je izjava pravilna za vsa naravna števila do 10^{18}, bo pa že splošno resnična. A zgodovina je že postregla s primeri, ki nazorno kažejo na to, da bi bil lahko tak zaključek napačen. Leta 1919 je György Pólya, madžarsko-ameriški matematik, postavil naslednjo domnevo: če za poljubno izbrano naravno število $n \geq 2$ za vsako izmed števil $m \leq n$ preverimo ali ima v praštevilski faktorizaciji liho ali sodo mnogo praštevilskih faktorjev (šteto z večkratnostjo), je takih z liho mnogo faktorji vsaj polovica. Dolga leta ni bilo znano kako je z resničnostjo te domneve. Potem pa je leta 1958 Haselgrove pokazal, da domneva ne velja. Kasneje se je izkazalo, da je najmanjši protiprimer število 906 150 257.

Zgornji primer Pólyajeve domneve nas torej uči, da smemo neko izjavo vzeti za resnično šele takrat, ko jo v celoti (teoretično) dokažemo. Zgled takšnega premisleka je bil recimo naš dokaz, da za vsako naravno število n velja, da je v primeru, ko je n^2 liho število, liho tudi število n.

Opozorimo za konec še na naslednje. Ko kvantifikatorje gnezdimo, je pri uporabi enakih kvantifikatorjev vrstni red nepomemben. Tako je, na primer, $\forall x \forall y : P(x, y) \sim \forall y \forall x : P(x, y)$. To pa ne velja več, če uporabljamo različne kvantifikatorje, v kar nas prepriča naslednji zgled.

Zgled: Naj bodo domena našega pogovora naravna števila. Oglejmo si relacijo $M(x, y)$, ki naj pomeni $x^2 < y$.

Tedaj izjava $\forall x \exists y : M(x, y)$ pravi, da za vsako naravno število x lahko najdemo naravno število y, ki je večje od kvadrata števila x. Ta izjava je seveda pravilna, saj lahko za y vzamemo kar x^2+1. No, izjava $\exists y \forall x : M(x, y)$ pove nekaj povsem drugega. Ta pravi, da obstaja naravno število y, ki je večje od kvadrata kateregakoli naravnega števila, kar seveda ni res. Če je namreč $x = y$, potem seveda ni res $x^2 < y$.

V čem je bila torej bistvena razlika? V "prvi varianti" je moral za vsak x obstajati y, ki je "bil dober" za x. Ta y je torej lahko odvisen od x. Povsem drugače je v "drugi varianti", kjer bi morali najti nek (fiksen) y, ki bi bil "dober" za vse x. ▲

Naloga 1.12. Denimo, da so domena pogovora realna števila. Naslednje izjave zapišite v jeziku matematične logike s predikati:

- Za vsako celo število x obstaja celo število y, da velja $x = 3y$.

- Za vsako celo število y obstaja celo število x, da velja $x = 3y$.
- Za vsako celo število x in vsako celo število y velja $x = 3y$.
- Obstaja tako celo število x, da za neko celo število y velja $x = 3y$.

Sedaj vsako izmed zgornjih izjav zanikajte in dobljeno prepišite v slovenski jezik.

Naloga 1.13. Spodnji dve izjavi zapišite s predikati in ju zanikajte:

- Za vsak $\varepsilon > 0$ obstaja $\delta > 0$, da za vsako realno število x, ki se od 1 razlikuje za manj kot δ, velja, da se x^2 od 1 razlikuje za manj kot ε.
- Za vsako realno število M obstaja realno število x_0, da je $f(x) > M$ za vse $x \geq x_0$.

Naloga 1.14. Naslednjo izjavo o celih številih ter njeno negacijo zapišite v slovenskem jeziku.

$$\forall z \,:\, (\neg(\exists y \,:\, z = 13y) \Rightarrow \exists y \,:\, z = 2y)\,.$$

1.5 Metode dokazovanja

V prejšnjih dveh razdelkih smo se naučili, kako naj bi dokazovali veljavnost ali neveljavnost logičnih sklepanj. A včasih samo z omenjenimi prijemi ne uspemo. Zato si bomo v tem razdelku ogledali še tri metode dokazovanja, ki jih, poleg že omenjenih pravil iz izreka 1.3, najbolj pogosto uporabljamo. Prvo izmed njih imenujemo *pogojni sklep*, drugo *dokaz s protislovjem*, tretjo pa *analiza primerov*.

Oglejmo si najprej metodo *pogojnega sklepa*, ki temelji na naslednji trditvi.

Trditev 1.4. *Naj bodo $p_1, p_2, \ldots, p_n$, ter p in q poljubne izjave. Tedaj je izjava q logična posledica izjav $p_1, p_2, \ldots, p_n$ in p natanko tedaj, ko je izjava $p \Rightarrow q$ logična posledica izjav $p_1, p_2, \ldots, p_n$.*

Dokaz: Označimo konjunkcijo $p_1 \wedge p_2 \wedge \cdots \wedge p_n$ z r. Dokazujemo torej, da je izjava $r \wedge p \Rightarrow q$ tautologija natanko tedaj, ko je izjava $r \Rightarrow (p \Rightarrow q)$ tautologija. Po izreku 1.1 je

$$r \Rightarrow (p \Rightarrow q) \sim \neg r \vee (\neg p \vee q) \sim (\neg r \vee \neg p) \vee q \sim \neg(r \wedge p) \vee q \sim r \wedge p \Rightarrow q,$$

torej sta izjavi $r \wedge p \Rightarrow q$ in $r \Rightarrow (p \Rightarrow q)$ ekvivalentni. Seveda od tod takoj sledi, da je ena tautologija natanko tedaj, ko je tautologija tudi druga. □

Zgornja trditev torej pove naslednje. Če želimo dokazati, da je izjava oblike $p \Rightarrow q$ logična posledica predpostavk $p_1, p_2, \ldots, p_n$, lahko to dokažemo

tako, da predpostavkam dodamo še "novo predpostavko" p in nato s pravili logičnega sklepanja pokažemo, da je izjava q logična posledica predpostavk $p_1, p_2, \ldots, p_n, p$. Pravimo, da v takem primeru delamo *pogojni sklep*.

Sklenimo še dogovor kako pri zapisu formalnega dokaza pravilnosti sklepa označimo dejstvo, da delamo pogojni sklep. Denimo, da želimo pokazati veljavnost izjave $p \Rightarrow q$. V vrstici, kjer pričnemo s pogojnim sklepom, torej kjer predpostavkam dodamo *predpostavko pogojnega sklepa*, v našem primeru p, vrstice začnemo številčiti v "naslednjem nivoju" (na primer, če je bila zadnja vrstica označena s 5, bomo to vrstico označili s 6.1, če je bila prejšnja vrstica označena s 3.7, bo nova 3.8.1, itd.), zraven pa dopišemo "predp PS". Potem sledeče vrstice številčimo znotraj tega nivoja, dokler se pogojni sklep ne zaključi (v našem primeru, ko pokažemo pravilnost izjave q). Potem se vrnemo v prejšnji nivo in zapišemo izjavo, ki smo jo dokazali s pogojnim sklepom (v našem primeru $p \Rightarrow q$), zraven dopišemo PS in v oklepajih začetno in končno vrstico pogojnega sklepa. Oglejmo si vse skupaj na zgledu.

Zgled: Pokažimo, da lahko iz pravilnosti predpostavk $(p \Rightarrow q) \Rightarrow s$, $t \Rightarrow \neg r$ in $p \wedge \neg t \Rightarrow q$ sklepamo na pravilnost izjave $r \Rightarrow s$. Bralec bo opazil, da v dokazu delamo pogojni sklep znotraj pogojnega sklepa.

1.	$(p \Rightarrow q) \Rightarrow s$	$predp$
2.	$t \Rightarrow \neg r$	$predp$
3.	$p \wedge \neg t \Rightarrow q$	$predp$
4.1.	r	$predp\ PS$
4.2.	$\neg\neg r$	~ 4.1
4.3.	$\neg t$	$MT(2, 4.2)$
4.4.1.	p	$predp\ PS$
4.4.2.	$p \wedge \neg t$	$Zd(4.3, 4.4.1)$
4.4.3.	q	$MP(3, 4.4.2)$
4.4.	$p \Rightarrow q$	$PS(4.4.1 - 4.4.3)$
4.5.	s	$MP(1, 4.4)$
4.	$r \Rightarrow s$	$PS(4.1 - 4.5)$

▲

Naslednja metoda dokaza je *dokaz s protislovjem*, ki temelji na naslednji trditvi.

Trditev 1.5. *Naj bodo $p_1, p_2, \ldots, p_n$ in q poljubne izjave. Tedaj je izjava q logična posledica izjav $p_1, p_2, \ldots, p_n$ natanko tedaj, ko je protislovje logična posledica izjav $p_1, p_2, \ldots, p_n$ in $\neg q$.*

DOKAZ: Označimo z r konjunkcijo $p_1 \wedge p_2 \wedge \cdots \wedge p_n$. Kdaj je protislovje logična posledica izjav $p_1, p_2, \ldots, p_n$ in $\neg q$? Natanko tedaj, ko je izjava $r \wedge \neg q \Rightarrow 0$ tautologija. Trditev tedaj sledi zaradi

$$r \wedge \neg q \Rightarrow 0 \sim \neg(r \wedge \neg q) \vee 0 \sim \neg r \vee q \sim r \Rightarrow q.$$

□

Po zgornji trditvi torej lahko to, da je q logična posledica predpostavk $p_1, p_2, \ldots, p_n$, dokažemo s tem, da iz predpostavk $p_1, p_2, \ldots, p_n$ in $\neg q$ logično izpeljemo protislovje. Kadar se poslužujemo te metode dokaza, pravimo, da delamo *dokaz s protislovjem*. V formalnem zapisu pravilnosti sklepa dokaz s protislovjem označimo podobno kot pogojni sklep. Ko dodamo "predpostavko" $\neg q$, začnemo vrstice številčiti v novem nivoju, dopišemo "predp RA", ko pridemo do protislovja, pa se vrnemo na prejšnji nivo, na katerem zapišemo izjavo, katere pravilnost smo s tem dokazali. Zraven dopišemo RA, v oklepaje pa damo začetno in končno vrstico dokaza s protislovjem. (Oznaka RA prihaja iz latinskega imena za dokaz s protislovjem, namreč "Reductio ad absurdum".)

ZGLED: Dokažimo pravilnost sklepa iz prejšnjega zgleda še z uporabo dokaza s protislovjem.

1.	$(p \Rightarrow q) \Rightarrow s$	*predp*
2.	$t \Rightarrow \neg r$	*predp*
3.	$p \wedge \neg t \Rightarrow q$	*predp*
4.1.	$\neg(r \Rightarrow s)$	*predp RA*
4.2.	$\neg\neg r \wedge \neg s$	~ 4.1
4.3.	$\neg\neg r$	$Po(4.2)$
4.4.	$\neg t$	$MT(2, 4.3)$
4.5.	$\neg s$	$Po(4.2)$
4.6.	$\neg(p \Rightarrow q)$	$MT(1, 4.5)$
4.7.	$p \wedge \neg q$	~ 4.6
4.8.	p	$Po(4.7)$
4.9.	$p \wedge \neg t$	$Zd(4.4, 4.8)$
4.10.	q	$MP(3, 4.9)$
4.11.	$\neg q$	$Po(4.7)$
4.12.	$q \wedge \neg q$	$Zd(4.10, 4.11)$
4.13.	0	~ 4.12
4.	$r \Rightarrow s$	$RA(4.1 - 4.13)$

▲

Dokaz s protislovjem je ena izmed najpogosteje uporabljenih metod pri dokazovanju v matematiki. Oglejmo si dva klasična izreka, ki ju je moč na najbolj eleganten način dokazati ravno z metodo dokaza s protislovjem.

ZGLED: Pri analizi običajno dokažemo, da $\sqrt{2}$ ni racionalno število. Dokaz je za naše potrebe zelo poučen, zato si ga bomo natančno ogledali. (Morda velja omeniti, da so podoben dokaz poznali že Pitagorejci (500 p. n. š).)

Kako naj torej dokažemo, da neko realno število ni racionalno število? Kaj hitro ugotovimo, da nimamo prav nobene ideje, kako bi se tega lotili direktno. Zato poizkusimo z dokazom s protislovjem. Pa denimo, da $\sqrt{2}$ je racionalno število. V tem primeru torej obstajata neničelni tuji si celi števili m in n, da je $\sqrt{2} = \frac{m}{n}$. Tedaj pa je $2 = \frac{m^2}{n^2}$ in ker je $n \neq 0$, od tod dobimo $2n^2 = m^2$. Ker je levo število sodo, mora biti torej tudi m^2 sodo število. Ugotovili smo že, da je za neničelno celo število z število z^2 liho natanko tedaj, ko je liho že število z. Torej lahko sklepamo, da mora biti število m sodo, to je, $m = 2m_0$ za neko celo število m_0. Vstavimo v našo enačbo, pa dobimo $2n^2 = 4m_0^2$ in tako je $n^2 = 2m_0^2$ tudi sodo število. Kot prej lahko od tod zaključimo, da je tudi število n sodo, to je, $n = 2n_0$ za neko celo število n_0. A števili m in n sta si tuji, po drugi strani pa sta obe deljivi z 2, kar je vsekakor nemogoče. To protislovje nam pove, da $\sqrt{2}$ torej res ni racionalno število. ▲

ZGLED: Oglejmo si še enega izmed klasičnih rezultatov, ki se ga najlažje dokaže z metodo dokaza s protislovjem. Dokazali bomo izrek, ki ga je poznal že Evklid (300 p. n. š).

Izrek, ki je znan tudi kot Evklidov izrek, pravi: "Obstaja neskončno mnogo praštevil." No, da bi se lotili dokaza, je treba najprej poznati definicijo praštevila in razumeti kaj naj bi pomenilo dejstvo, da je nekih reči neskončno mnogo. Zaenkrat se zadovoljimo kar z "definicijo", da ima množica A neskončno mnogo elementov, če za vsak $n \in \mathbb{N}$ velja, da ima A več kot n elementov (pri čemer se zopet zanašamo na to, da bralec nekako intuitivno razume kaj pomeni to, da ima neka množica več kot n elementov).

Kako naj torej dokažemo, da je praštevil neskončno mnogo? Lahko bi skušali skonstruirati neskončno mnogo praštevil. A kako to storiti? Kmalu ugotovimo, da ta pot ne bo obrodila sadov in tako se dokaz s protislovjem ponuja kar sam. Pa denimo, da obstaja le končno mnogo različnih praštevil in označimo njihovo število z n. Vsa praštevila sedaj uredimo po velikosti in jih po vrsti označimo s $p_1, p_2, \ldots, p_n$. Kaj lahko tedaj povemo o številu $p = p_1 p_2 \cdots p_n + 1$? Ker je največje praštevilo število p_n in očitno velja $p > p_n$, število p ne more biti praštevilo. Tedaj pa mora biti deljivo z vsaj enim izmed praštevil p_i, $i \in \{1, \ldots, n\}$. A ker p_i deli število $p_1 p_2 \cdots p_n$, mora potemtakem deliti tudi število 1, kar pa je seveda nemogoče. To protislovje nam torej pove, da je praštevil res neskončno mnogo. ▲

Posvetimo se nazadnje še dokazovanju po metodi *analize primerov*, ki

temelji na naslednji trditvi.

Trditev 1.6. *Naj bodo $p_1, p_2, \ldots, p_n$, ter p, q in r poljubne izjave. Tedaj je izjava r logična posledica izjav $p_1, p_2, \ldots, p_n$ in izjave $p \vee q$ natanko tedaj, ko je r logična posledica izjav $p_1, p_2, \ldots, p_n, p$ in hkrati logična posledica izjav $p_1, p_2, \ldots, p_n, q$.*

Dokaz: Označimo z s konjunkcijo $p_1 \wedge p_2 \wedge \cdots \wedge p_n$. Pokazati želimo, da je $s \wedge (p \vee q) \Rightarrow r$ tautologija natanko tedaj, ko sta tautologiji $s \wedge p \Rightarrow r$ in $s \wedge q \Rightarrow r$. Ker je slednje res natanko tedaj, ko je tautologija izjava $(s \wedge p \Rightarrow r) \wedge (s \wedge q \Rightarrow r)$, trditev sledi iz ekvivalence

$$\begin{gathered}(s \wedge p \Rightarrow r) \wedge (s \wedge q \Rightarrow r) \sim \big(\neg(s \wedge p) \vee r\big) \wedge \big(\neg(s \wedge q) \vee r\big) \sim \\ \big(\neg(s \wedge p) \wedge \neg(s \wedge q)\big) \vee r \sim \big((\neg s \vee \neg p) \wedge (\neg s \vee \neg q)\big) \vee r \sim \\ \big(\neg s \vee (\neg p \wedge \neg q)\big) \vee r \sim \big(\neg s \vee \neg(p \vee q)\big) \vee r \sim \\ \neg\big(s \wedge (p \vee q)\big) \vee r \sim s \wedge (p \vee q) \Rightarrow r.\end{gathered}$$

□

Zgornja trditev torej pove, da lahko analizo primerov uporabimo takrat, ko je ena izmed predpostavk oblike $p \vee q$, to je, ko je ena izmed predpostavk lahko "izpolnjena na več načinov". Tokrat formalni dokaz zapišemo tako, da posebej naredimo dokaz, pri katerem kot predpostavko vzamemo izjavo p in posebej dokaz, pri katerem kot predpostavko vzamemo izjavo q.

Zgled: Pokažimo, da lahko iz pravilnosti predpostavk $p \vee t$, $r \Rightarrow \neg p$, $t \Rightarrow s$, $r \vee q$ in $s \iff q$ sklepamo na pravilnost izjave s. Seveda lahko pravilnost tega sklepa dokažemo tudi z metodo dokaza s protislovjem (bralca vabimo, da zapiše ustrezen dokaz), a mi bomo ubrali drugo pot. Pokazati želimo, da je s logična posledica predpostavk. Ker je ena izmed predpostavk izjava $r \vee q$, napravimo naslednjo analizo primerov. Pokažimo najprej, da je s logična posledica predpostavk, kjer namesto izjave $r \vee q$ vzamemo izjavo r.

1.	$p \vee t$	$predp$
2.	$r \Rightarrow \neg p$	$predp$
3.	$t \Rightarrow s$	$predp$
4.	r	$predp$
5.	$s \iff q$	$predp$
6.	$\neg p$	$MP(2,4)$
7.	t	$DS(1,6)$
8.	s	$MP(3,7)$

Pokažimo sedaj še, da je s logična posledica predpostavk, kjer namesto izjave $r \vee q$ vzamemo izjavo q.

1.	$p \vee t$	$predp$
2.	$r \Rightarrow \neg p$	$predp$
3.	$t \Rightarrow s$	$predp$
4.	q	$predp$
5.	$s \iff q$	$predp$
6.	$(s \Rightarrow q) \wedge (q \Rightarrow s)$	~ 5
7.	$q \Rightarrow s$	$Po(6)$
8.	s	$MP(4,7)$

S tem je pravilnost celotnega sklepa po analizi primerov dokazana. ▲

Oglejmo si dokaz z analizo primerov še na primeru konkretne trditve.

Zgled: Pokažimo, da za poljubni realni števili x in y velja $|xy| = |x||y|$. Dokazujemo torej, da je resnična izjava $\forall x, y \in \mathbb{R} : |xy| = |x||y|$. Ker moramo veljavnost trditve $|xy| = |x||y|$ dokazati za poljuben par realnih števil x in y, moramo torej enakost dokazati neodvisno od konkretne vrednosti števil x in y.

Najprej natančno razdelajmo, kaj problem od nas sploh zahteva. V ta namen je treba najprej natančno opredeliti oznako $|x|$. Že iz srednje šole vemo, da velja

$$|x| = \begin{cases} x & ; \quad x \geq 0 \\ -x & ; \quad x < 0. \end{cases}$$

Najprej se omejimo na primer, ko je vsaj eden izmed x in y enak 0 (bralec bo opazil, da delamo analizo primerov - bodisi je vsaj eno izmed števil enako 0 ali pa to ni res). V tem primeru je tudi njegova absolutna vrednost enaka 0 in tako je res $|xy| = |0| = 0 = |x||y|$. Od slej lahko torej privzamemo, da sta x in y neničelna. Ker je torej vrednost $|x|$ odvisna od predznaka števila x, vrednost $|y|$ pa od predznaka števila y, se zdi smiselno ločiti štiri različne primere (zopet delamo analizo primerov).

1. primer: $x > 0$ in $y > 0$.
V tem primeru je torej $|x| = x$ in $|y| = y$. Ker je seveda $xy > 0$, tako dobimo $|xy| = xy = |x||y|$.

2. primer: $x > 0$ in $y < 0$.
Tedaj je $xy < 0$ in tako je $|xy| = -(xy) = x(-y) = |x||y|$.

3. primer: $x < 0$ in $y > 0$.
Tudi v tem primeru velja $xy < 0$ in tako je $|xy| = -(xy) = (-x)y = |x||y|$.

4. primer: $x < 0$ in $y < 0$.
Tedaj je $xy > 0$ in tako je $|xy| = xy = (-x)(-y) = |x||y|$.

V vsakem primeru torej res velja $|xy| = |x||y|$. ▲

Preden zaključimo poglavje o matematični logiki se še enkrat vrnimo na vprašanje, kako dokažemo, da izjava, ki vsebuje kvantifikator, ni pravilna. Pomagamo si z ekvivalencama iz prejšnjega razdelka. Če želimo dokazati, da izjava $\forall x : L(x)$ ni resnična, je, vsaj načeloma, stvar sila preprosta. V tem primeru je treba zgolj skonstruirati *protiprimer*, to je, najti moramo nek x iz domene pogovora, ki lastnosti L nima. Kaj pa če želimo pokazati, da ni resnična izjava $\exists x : L(x)$? To lahko dokažemo s premislekom, da za vsak x iz domene pogovora velja, da lastnosti L nima. A takšen premislek je mnogokrat težko najti. Pogosto se zato izkaže, da je v takem primeru primeren pristop dokaz s protislovjem. Predpostavimo, da x z lastnostjo L obstaja, nato pa iz tega izpeljemo protislovje. Oglejmo si zgled.

Zgled: Vsi najbrž "vemo" kako je z resničnostjo trditve "Obstaja naravno število N, ki je večje od vseh drugih naravnih števil." Skušajmo to, da je ta trditev neresnična, dokazati.

Seveda nam tokrat en sam primer (ali več) prav nič ne pomaga. Če namreč rečemo, da ta N ne more biti 10, ker je $11 > 10$, 11 pa je naravno število, je to sicer čisto res. A s tem smo zgolj dokazali, da za N ne moremo izbrati števila 10. Ker pa ima množica $\mathbb{N}$ neskončno mnogo elementov, nam je še vedno ostalo neskončno mnogo kandidatov za N. Uporabimo raje metodo dokaza s protislovjem. Privzemimo, da tak N obstaja in pokažimo, da lahko iz tega izpeljemo logični nesmisel. To ni težko. Ker je namreč N naravno število, je tudi $N+1$ naravno število. Po definiciji števila N, bi tedaj moralo veljati $N > N + 1$, kar pa seveda ni res, saj bi to pomenilo $0 > 1$. To protislovje nam pove, da torej N ne more obstajati, kar smo tudi trdili. ▲

Naloga 1.15. Pokažite, da je za vsako liho naravno število n število $n^2 + 4n + 3$ deljivo s 4. Ali je res celo, da je za lih n število $n^2 + 4n + 3$ vedno deljivo z 8? Je morda celo vedno deljivo s 16?

Naloga 1.16. Pokažite, da je vsako celo število bodisi liho bodisi sodo. Kakšno metodo dokaza ste uporabili?

Naloga 1.17. Ali za vsako realno število x velja $\sin^2 x \leq |\sin x|$?

Poglavje 2

Teorija množic

O množicah se govori že v osnovni šoli. Vse od tlej običajno množice dojemamo kot skupek nekih reči. Govorimo recimo o množici jabolk v zaboju, o množici vseh učencev neke osnovno šole ali pa o množici vseh hrastovih dreves v nekem gozdu. Na samem začetku množice predstavljamo tako, da v krog ali elipso narišemo objekte, ki naj bi bili elementi te množice. Seveda kaj hitro ugotovimo, da vseh množic ne moremo predstaviti na ta način. Čeprav se namreč najbrž vsi strinjamo, da je množica vseh hrastovih dreves na Rožniku zares množica, je okrog teh hrastov nemogoče narisati tako elipso, da bodo v njej samo ta hrastova drevesa in nič drugega. Množico vseh hrastovih dreves na Rožniku si torej predstavljamo abstraktno - odmislimo vsa ostala drevesa, podrast, živali, poti in podobno, kar ostane, pa je potem ta množica, ki jo iščemo. Če bralca ta argument ni prepričal, naj si skuša predstavljati, kako bi predstavil množico vseh praštevil, za katero tudi najbrž vsi priznavamo, da obstaja. Na podlagi teh primerov se torej zdi, da dokaj dobro razumemo kaj naj bi pomenil pojem množice. Potemtakem bi morali znati ta pojem natančno definirati. Kot pa bomo kmalu videli, temu ni tako. Izkaže se namreč, da pojma množice sploh ne smemo definirati, če želimo zgraditi neprotislovno teorijo.

Oglejmo si kakšne težave si nakopljemo, če skušamo pojem množice definirati. Oče teorije množic, nemški matematik Georg Cantor (1845 – 1918), je naredil prav to napako. Po njegovi "definiciji", naj bi bila množica "skupnost različnih določenih reči iz našega nazornega ali miselnega sveta, ki jo imamo za celoto." To je nekako v skladu s tem, kar smo na konkretnih primerih opažali zgoraj. Težava pa je ta, da bi po tej definiciji obstajala tudi množica vseh množic, kar pa nas pripelje v tako imenovani Russelov paradoks (1902). (Bertrand A. W. Russel, 1872–1970, je bil britanski filozof, matematik in zgodovinar.)

Russelov paradoks: Denimo, da bi obstajala množica A vseh množic, to je množica, katere elementi so sploh vse množice. Sedaj pa naj bo B tista njena podmnožica, ki sestoji ravno iz vseh množic (torej elementov množice A), ki ne vsebujejo same sebe. No, sedaj si zastavimo usodno vprašanje: "Ali množica B vsebuje samo sebe?" Če B samo sebe vsebuje, potem po definiciji množice B ne sme vsebovati same sebe. Po drugi strani pa, če B ne vsebuje same sebe, mora biti po definiciji množice B vendarle vsebovana sama v sebi, saj B vsebuje ravno vse množice s to lastnostjo. Kakorkoli stvar obrnemo, množica B je vsebovana sama v sebi natanko tedaj, ko ni vsebovana sama v sebi, kar je seveda protislovje. Kaj je torej narobe? Izvirni greh je bil v tem, da smo privzeli obstoj množice vseh množic, ki potemtakem ne more obstajati.

Zato se v sodobni teoriji množic pojma množice sploh ne definira, temveč privzamemo nekaj osnovnih aksiomov teorije množic, ki govore o tem kdaj sta dve množici enaki, kaj lahko z množicami počnemo, kako iz že obstoječih množic tvorimo nove, itd. Vso nadaljnjo teorijo potem izpeljemo iz teh nekaj osnovnih aksiomov. Seveda skušamo aksiome postaviti tako, da se dobljena teorija čimbolj ujema z našo intuicijo in predstavo o tem, kaj naj bi se z množicami smelo početi. Izkaže se, da lahko na ta način praktično vse pojme v matematiki zgradimo na osnovi množic. Kot bomo videli, relacije, prav tako pa tudi funkcije, niso nič drugega kot množice. Celo naravna števila so le neke posebne množice, podobno pa seveda potem velja še za cela, racionalna, realna in kompleksna števila.

2.1 Pripadnost in pojem enakosti množic

Najpomembnejši koncept v teoriji množic je *pripadnost*. Ker pa ne bomo definirali niti pojma množice, tudi pojma pripadnosti ne moremo definirati, temveč ga privzamemo kot nek osnovni, nedefiniran, pojem. Vse kar se je treba dogovoriti je, da za vsako reč velja, da neki dani množici bodisi pripada ali pa ne. Situacija je podobna tisti v elementarni geometriji, kjer ne definiramo pojmov točka in premica, niti ne definiramo pojma incidence, to je, ne definiramo kaj pomeni to, da neka točka leži na neki premici. Pomembno je le to, da za vsako dano točko in vsako dano premico velja, da ta točka bodisi leži ali pa ne leži na tej premici.

Dejstvo, da element a pripada množici A, bomo zapisali kot $a \in A$ (da a ne pripada A pa kot $a \notin A$). Naš prvi aksiom govori o povezavi med pojmom vsebovanosti in enakostjo množic. Po naši intuitivni predstavi pojma množice je množica natanko določena s svojimi elementi. Kot smo omenili, skušamo

aksiome teorije množic postaviti tako, da se dobljena teorija kar se da ujema z intuitivno predstavo. Naš prvi aksiom zato postavimo tako, da pove natanko to, da je množica povsem določena s svojimi elementi.

Aksiom o ekstenzionalnosti: Za poljubni množici A in B velja, da je $A = B$ natanko tedaj, ko imata A in B natanko iste elemente, to je

$$A = B \iff (\forall x \in A : x \in B) \wedge (\forall x \in B : x \in A).$$

Kdor se z abstraktno matematiko srečuje prvič, si bo ob tem aksiomu zagotovo mislil, da je povsem nepotreben. V resnici pa ta aksiom vpeljuje pojem enakosti množic. S tem aksiomom namreč sklepamo dogovor o tem, kaj natančno opredeli neko množico. Po tem dogovoru torej takoj, ko ugotovimo, da imata "dve" množici natanko iste elemente, sklenemo, da gre v resnici za eno in isto množico. Da vse skupaj vendarle ni povsem odveč, bo bralca najbrž prepričal tudi naslednji zgled.

Zgled: Čeprav na podlagi tega prvega aksioma sploh še ne vemo, ali sploh obstaja kakšna množica, za potrebe tega zgleda privzemimo, da obstajajo množice $A = \{1, 2, 3\}$, $B = \{n \in \mathbb{N} : 1 \leq n \leq 3\}$ in $C = \{n \in \mathbb{N} : n \geq 3 \Rightarrow n^3 \leq 30\}$. Hitro se prepričamo, da vse tri množice sestojijo iz natanko istih treh elementov. Po aksiomu o ekstenzionalnosti torej velja $A = B = C$, kar iz samega opisa množic ni povsem jasno razvidno. Aksiom o ekstenzionalnosti torej zagotavlja, da je povsem vseeno na kakšen način povemo, kateri elementi pripadajo dani množici. Pomembno je le kateri elementi to so. ▲

Še nekaj velja izpostaviti. Prav nič nismo govorili o tem, kakšne reči dopuščamo kot elemente množic. Elementi množic so potemtakem lahko tudi množice, pa množice množic, itd. Kot smo omenili že zgoraj, so na primer tudi naravna števila le množica množic.

Naloga 2.1. Množici $A = \{n \in \mathbb{N} : (n > 5 \Rightarrow n^2 < 20)\}$ in $B = \{z \in \mathbb{C} : (z^4 = |z| \iff z^2 \neq |z|)\}$ zapišite eksplicitno, to je, naštejte vse njune elemente.

2.2 Podmnožice in aksiom o paru

Kaj lahko z množicami počnemo? Kako iz znanih množic zgradimo nove? Odgovore na ta in podobna vprašanja bomo dobili, ko podamo še nekaj naslednjih aksiomov. V tem razdelku si bomo ogledali dva izmed njih.

Prvi govori o tem, da lahko iz neke dane množice "poberemo" vse elemente, ki imajo neko smiselno lastnost za elemente te množice, pa dobimo (novo) množico. Preden ga podamo, vpeljimo pojem podmnožice.

Definicija. Naj bosta A in B množici. Pravimo, da je A *podmnožica* množice B, če je vsak element množice A hkrati tudi element množice B. To dejstvo označimo z $A \subseteq B$. Če želimo posebej poudariti, da je A podmnožica množice B, vendar A in B nista enaki, pišemo $A \subsetneq B$ in rečemo, da je A *prava podmnožica* množice B.

V jeziku matematične logike bi torej definicijo inkluzije lahko zapisali takole: $A \subseteq B \iff \forall x \in A : x \in B$.

Neposredno iz definicij in aksioma o ekstenzionalnosti dobimo naslednjo trditev, ki jo že dobro poznamo iz naše intuitivne predstave o množicah.

Trditev 2.1. *Naj bodo A, B in C poljubne množice. Tedaj velja:*

1. $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$.
2. $A = B \iff A \subseteq B \wedge B \subseteq A$.

Druga točka te trditve je pravzaprav natanko aksiom o ekstenzionalnosti, podan preko pojma inkluzije. Kljub temu gre za zelo pomembno zadevo, ki si jo velja dobro zapomniti. Skoraj vsako enakost dveh konkretnih množic namreč dokažemo tako, da dokažemo vsako izmed obeh inkluzij.

Podajmo sedaj napovedani aksiom o podmnožici.

Aksiom o podmnožici: Naj bo A neka množica in naj bo L neka smiselna lastnost za elemente množice A. Tedaj obstaja množica, katere elementi so natanko tisti elementi množice A, ki imajo lastnost L.

Velja spomniti, da je lastnost L za elemente množice A smiselna, če za vsak $a \in A$ velja, da lastnost L bodisi ima ali pa je nima. Tako "množica vseh duhovitih Slovenk" ni množica. Nimamo namreč vsi iste predstave o tem, kdaj je nekdo duhovit in kdaj ne.

Po aksiomu o ekstenzionalnosti je seveda z množico A in lastnostjo L množica, o kateri govori aksiom o podmnožici, natanko določena. Označimo jo z $\{x \in A : L(x)\}$ (včasih se uporablja tudi oznaka $\{x \in A \mid L(x)\}$). Zgodi se tudi, da uporabljamo še malce drugačen zapis. Tako lahko na primer množico vseh sodih celih števil podamo kot $S = \{n \in \mathbb{Z} \mid \exists m \in \mathbb{Z} : n = 2m\}$, lahko pa tudi kot $S = \{2z : z \in \mathbb{Z}\}$.

Spomnimo se sedaj razmisleka iz Russelovega paradoksa. S podobnim argumentom lahko torej zaradi aksioma o podmnožici pokažemo, da za vsako

množico obstaja neka množica, ki ni njen element. Posledično nobena množica ne more vsebovati (kot elemente) vseh množic.

Pokazati, da je neka množica podmnožica druge, je naloga, ki jo v matematiki srečujemo na vsakem koraku. Razmislimo kako kaj takega dokažemo. Po definiciji bo torej množica A podmnožica množice B, če uspemo pokazati, da je *vsak* element množice A vsebovan v množici B. Če je množica A "dovolj majhna", lahko seveda za vsak njen konkreten element posebej preverimo, če pripada množici B ali ne. Sicer pa je treba ubrati drugo pot. Pri takem dokazovanju prav nič ne zaležejo konkretni primeri. Premislek je treba narediti v splošnem.

Zgled: Naj bo $A = \{2n - 1 \mid n \in \mathbb{Z}\}$ množica vseh lihih celih števil in naj bo $B = \{(2n-1)^3 \mid n \in \mathbb{Z}\}$ množica vseh kubov lihih celih števil. Pokažimo, da velja $B \subseteq A$. Da dobimo občutek kaj se sploh dogaja, si je seveda priporočljivo ogledati nekaj elementov množice B. Tako so elementi množice B, na primer, števila $(2-1)^3 = 1$, pa $(8-1)^3 = 343$, itd. Števili, ki smo ju dobili (torej 1 in 343), sta res lihi. A to seveda še ni dokaz, da velja $B \subseteq A$. Da bi to dokazali, je treba vzeti poljuben element množice B, torej poljuben $m \in B$, in pokazati, da je tedaj m vsebovan v množici A. Po definiciji množice B torej obstaja $n \in \mathbb{Z}$, da je $m = (2n-1)^3$. Tedaj pa je $m = 8n^3 - 6n^2 + 12n - 1 = 2(4n^3 - 3n^2 + 6n) - 1$, kar je res liho število, saj je $4n^3 - 3n^2 + 6n \in \mathbb{Z}$. Tako je res $m \in A$. Ker je bil m poljuben element množice B, smo s tem dokazali, da velja $B \subseteq A$. ▲

Definicija. Množica, ki ne premore nobenega elementa, se imenuje *prazna množica*. Označimo jo s $\{\}$ oziroma $\emptyset$.

Po aksiomu o ekstenzionalnosti je seveda prazna množica ena sama, zato lahko upravičeno uporabljamo zgornjo oznako. Pokažimo sedaj, da je prazna množica podmnožica vsake množice.

Trditev 2.2. *Naj bo A poljubna množica. Potem je $\emptyset \subseteq A$.*

Dokaz: Po definiciji pojma podmnožice je torej treba pokazati, da velja $\forall x \in \emptyset : x \in A$. Da bi to dokazali je torej zopet treba vzeti poljuben $x \in \emptyset$ in pokazati, da je x element množice A. A ker prazna množica po definiciji ne premore nobenega elementa, primernega elementa x sploh ni moč vzeti, zato je ta trditev "na prazno" izpolnjena. □

Zaenkrat seveda ne vemo niti tega ali sploh obstaja kaka množica. Konec koncev nismo dokazali niti obstoja prazne množice. Eden izmed kasnejših aksiomov zagotavlja, da obstaja vsaj ena (neskončna) množica, zato odslej

privzemimo, da obstaja vsaj ena množica. Obstoj prazne množice potem takoj sledi. Če je namreč A poljubna množica (kot smo se dogovorili, vsaj ena obstaja), je po aksiomu o podmnožici tudi $B = \{x \in A : x \neq x\}$ množica. Ker B očitno ne more vsebovati nobenega elementa, saj je izjava $x \neq x$ vedno neresnična, je B prazna množica.

Sedaj pa je že čas, da se vprašamo kako skonstruiramo še kakšne bolj bogate množice. Nek napredek nam zagotavlja že naslednji aksiom.

Aksiom o paru: Naj bosta A in B poljubni množici. Tedaj obstaja množica, katere edina elementa sta A in B.

Po aksiomu o ekstenzionalnosti je seveda taka množica ena sama. Označimo jo z $\{A, B\}$. Tu velja omeniti, da nekateri avtorji namesto zgornjega aksioma vzamejo aksiom, ki pravi, da za poljubni dve reči x in y obstaja množica, katere edina elementa sta x in y. A kot smo že povedali, je moč teorijo zgraditi tako, da je vsak matematični objekt zgrajen na pojmu množice. Potemtakem lahko besedico *reč* nadomestimo kar z besedico *množica*.

Kaj smo s tem pridobili? Zaenkrat poznamo le prazno množico $\emptyset$. Če v aksiomu o paru za A in B vzamemo to množico, ugotovimo, da obstaja množica $\{\emptyset, \emptyset\}$. Po aksiomu o ekstenzionalnosti je to seveda kar množica $\{\emptyset\}$. Pozor, slednja ni enaka prazni množici $\emptyset$. Ena je brez elementov, druga pa ne, torej po aksiomu o ekstenzionalnosti ne moreta biti enaki. Nadaljujemo, pa ugotovimo, da obstaja tudi množica $\{\emptyset, \{\emptyset\}\}$. Seveda lahko zgodbo peljemo naprej, a na ta način bomo ves čas operirali samo z množicami z največ dvema elementoma. To pa seveda ni zadovoljivo. Zato potrebujemo nove aksiome, ki bodo omogočili konstrukcijo bolj bogatih množic.

Naloga 2.2. Iz definicije pojma podmnožice izluščite trditev, ki pove kdaj množica A ni podmnožica množice B.

Naloga 2.3. Zapišite trditev, ki pove kdaj množica A ni prava podmnožica množice B.

Naloga 2.4. Naj bo $A = \{a, b\}$ neka množica z dvema elementoma. Pokažite, da tedaj obstaja množica $\{a\}$. Vsaki taki množici, torej množici z enim samim elementom, pravimo *singleton*.

Naloga 2.5. Ali lahko samo z doslej sprejetimi aksiomi (in privzetkom, da obstaja vsaj ena množica) pokažemo, da obstaja množica $\{\{\{\emptyset\}\}\}$?

Naloga 2.6. Pokažite, da obstajata vsaj dve različni množici z enim elementom.

2.3 Unija in presek dveh množic

Kot smo videli v prejšnjem razdelku, doslej sprejeti aksiomi ne omogočajo konstrukcij "bogatih množic", torej množic z veliko elementi. Doslej smo namreč uspeli skonstruirati le množice brez elementov, množice z enim elementom in pa take z dvema. A po našem intuitivnem prepričanju obstajajo še precej bolj bogate množice, na primer množica vseh naravnih števil ali pa množica vseh celih števil med 0 in 100. Če naj bo torej aksiomatska teorija množic res kar se da skladna z našimi predstavami o množicah, morajo aksiomi zagotoviti tudi obstoj takšnih množic.

Prvi korak na poti k bolj bogatim množicam je pojem *unije* množic.

Definicija. Naj bosta A in B poljubni množici. Tedaj je njuna *unija*, ki jo označimo z $A \cup B$, množica, ki sestoji iz vseh elementov, ki pripadajo vsaj eni izmed obeh množic. Podobno je *presek* množic A in B, ki ga označimo z $A \cap B$, množica vseh tistih elementov, ki pripadajo obema množicama. Če je $A \cap B$ prazna množica, pravimo, da sta množici A in B *disjunktni*.

Kako pa je z obstojem množic $A \cup B$ in $A \cap B$? Ali znamo za poljubni množici A in B zagotoviti obstoj njune unije in preseka? Denimo najprej da sta A in B podmnožici neke množice C. Tedaj lahko zapišemo

$$A \cup B = \{x \in C : (x \in A \vee x \in B)\}$$
$$\text{in}$$
$$A \cap B = \{x \in C : (x \in A \wedge x \in B)\}.$$

Po aksiomu o podmnožici torej v tem primeru unija $A \cup B$ in presek $A \cap B$ obstajata. Iz zgornjega tudi razberemo, da je unija množic v zelo tesni povezavi z logičnim veznikom disjunkcije, presek množic pa v zelo tesni povezavi z logičnim veznikom konjunkcije. Kot bomo videli spodaj (izrek 2.4), ima to dejstvo daljnosežne posledice.

Kaj pa v splošnem, ko imamo dani samo množici A in B in ne vemo ali sta tidve množici podmnožici neke skupne množice? Da presek $A \cap B$ obstaja tudi v tem splošnem primeru, ni težko videti.

Trditev 2.3. *Naj bosta A in B poljubni množici. Tedaj njun presek $A \cap B$ obstaja.*

Dokaz: Presek $A \cap B$ je po definiciji množica vseh elementov x, ki pripadajo tako A kot B. Povedano drugače, $A \cap B$ je množica vseh elementov iz A, ki imajo to lastnost, da pripadajo B, to je $A \cap B = \{a \in A : a \in B\}$. Izjava $a \in B$ seveda definira smiselno lastnost za elemente množice A in zato množica $A \cap B$ obstaja po aksiomu o podmnožici. □

Obstoja unije ne moremo zagotoviti tako zlahka. Pravzaprav se izkaže, da obstoja unije z doslej sprejetimi aksiomi ni mogoče zagotoviti. Zato potrebujemo nov aksiom.

Aksiom o uniji: Naj bosta A in B poljubni množici. Tedaj obstaja množica, katere elementi so natanko tisti elementi, ki pripadajo vsaj eni izmed množic A in B, to je, obstaja njuna unija $A \cup B$.

Oglejmo si dva zgleda.

Zgled: Naj bo $A = \{n \in \mathbb{N} : 2|n\}$ in $B = \{n \in \mathbb{N} : 3|n\}$. Lahko se je prepričati, da za naravno število n velja $2|n \wedge 3|n \iff 6|n$, torej je $A \cap B = \{n \in \mathbb{N} : (2|n \wedge 3|n)\} = \{n \in \mathbb{N} : 6|n\}$. Presek množic A in B je torej množica vseh naravnih števil, ki so deljiva s 6. Podobno je $A \cup B = \{n \in \mathbb{N} : (2|n \vee 3|n)\}$, to je, $A \cup B$ je množica vseh tistih naravnih števil, ki so deljiva z 2 ali 3. ▲

Zgled: Naj bo A poljubna množica. Po aksiomu o paru tedaj obstaja množica $\{A, A\} = \{A\}$. Po aksiomu o uniji pa tedaj obstaja tudi množica $A \cup \{A\}$. Če za A vzamemo kar prazno množico $\emptyset$, dobimo množico $\emptyset \cup \{\emptyset\} = \{\emptyset\}$. Če zadevo ponovimo s to novo množico, dobimo množico $\{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$. Nadaljujemo, pa dobimo množico $\{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$. Po še enem koraku dobimo množico

$$\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}.$$

Kot vidimo, postajajo zadeve na ta način zelo nepregledne. Opazimo pa, da ima nastala množica v vsakem koraku en element več kot prejšnja. Namen tega zgleda ni bil pokazati, da lahko konstruiramo "čudne" množice, temveč da lahko že ob predpostavki obstoja prazne množice z uporabo doslej sprejetih aksiomov dokažemo obstoj množice z enim elementom, z dvema elementoma, s tremi elementi, itd. Izkaže se, da lahko na ta način konstruiramo množico, ki zadošča Peanovim aksiomom. Na ta način torej lahko konstruiramo "množico naravnih števil" (ki pa vsaj na prvi pogled izgleda precej čudno - zato narekovaji). ▲

Vpeljimo še pojem razlike in komplementa množic.

Definicija. Naj bosta A in B poljubni množici. Tedaj je *razlika* množic A in B, ki jo označimo z $A \setminus B$, množica vseh tistih elementov množice A, ki niso vsebovani v množici B. Ko obravnavamo samo množice, ki so podmnožice neke *univerzalne* množice U, razliko $U \setminus A$ označimo z A^C in govorimo o

komplementu množice A (glede na U). *Simetrična razlika* množic A in B, ki jo označimo z $A\Delta B$, je množica vseh tistih elementov, ki so bodisi vsebovani v A, pa niso vsebovani v B, bodisi so vsebovani v B, pa niso vsebovani v A.

Tudi za obstoj množice $A \setminus B$ seveda ne potrebujemo novega aksioma, saj gre za podmnožico množice A, torej $A \setminus B = \{x \in A : x \notin B\}$, ki obstaja po aksiomu o podmnožici. Jasno je seveda tudi, da je $A\Delta B = (A \setminus B) \cup (B \setminus A)$, torej sedaj, ko imamo aksiom o uniji, tudi za obstoj simetrične razlike ne potrebujemo novega aksioma.

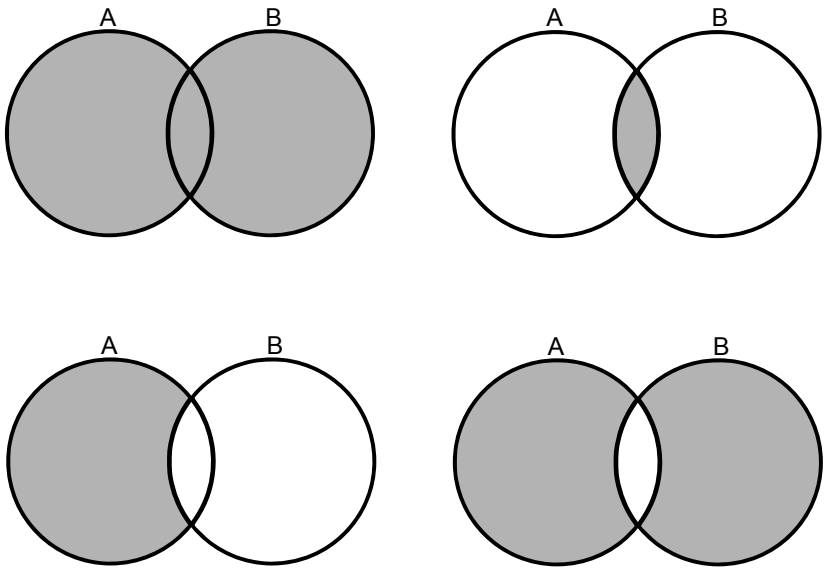
Ko obravnavamo odnose med množicami, nam je lahko v veliko pomoč predstavitev množic s tako imenovanimi Vennovimi diagrami. (John Venn, 1834 – 1923, je bil britanski logik, ki je "svoje diagrame" vpeljal okrog leta 1880.) To storimo tako, da vsako množico, ki v tej obravnavi nastopa, predstavimo kot neko območje v ravnini (recimo krog ali elipso) in to na tak način, da so na dobljeni sliki predstavljeni vsi možni preseki med množicami. Na primer, če obravnavamo množici A in B, je treba pripadajoča kroga narisati tako, da dobimo območje, ki predstavlja presek $A \cap B$, pa območji, ki predstavljata razliki $A \setminus B$ in $B \setminus A$ in tudi območje, ki predstavlja elemente, ki ne pripadajo niti A niti B. Na sliki 2.1 spodaj so prikazani Vennovi diagrami, ki ponazarjajo unijo, presek, razliko in simetrično razliko dveh množic. Takšne predstavitve so smiselne za situacije, v katerih nastopajo do največ štiri množice. Sicer je namreč pripadajočo sliko že zelo težko narisati (pri petih množicah bi recimo morali prikazati kar 32 "območij").

Opozoriti velja še naslednje. Vennovi diagrami nikdar ne morejo služiti kot rigorozen dokaz neke trditve. So le v pomoč za lažje razumevanje problema oziroma konkretne situacije.

Spomnimo se izreka 1.1 iz razdelka 1.2, ki je dal celo vrsto ekvivalenc med izjavnimi formami. Glede na to, da operacije unije, preseka in razlike množic temeljijo na logičnih veznikih negacije, disjunkcije in konjunkcije, naslednji izrek ni presentljiv.

Izrek 2.4. *Naj bodo A, B in C poljubne podmnožice univerzalne množice U. Tedaj so resnične vse naslednje izjave:*

1. $\emptyset \subseteq A$ *in* $A \subseteq A$.
2. $(A^C)^C = A$, $A \cap A^C = \emptyset$ *in* $A \cup A^C = U$.
3. $A \cup \emptyset = A$ *in* $A \cap \emptyset = \emptyset$.
4. $A \cup A = A$ *in* $A \cap A = A$.
5. $A \cup B = B \cup A$ *in* $A \cap B = B \cap A$.
6. $(A \cup B) \cup C = A \cup (B \cup C)$ *in* $(A \cap B) \cap C = A \cap (B \cap C)$.



Slika 2.1: Ponazoritev množic $A \cup B$, $A \cap B$, $A \setminus B$ in $A \Delta B$ z Vennovimi diagrami.

7. $A \subseteq A \cup B$ *in* $A \cap B \subseteq A$.
8. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *in* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
9. $(A \cup B)^C = A^C \cap B^C$ *in* $(A \cap B)^C = A^C \cup B^C$.
10. $A \setminus B = A \cap B^C$.
11. $A \cup B = A$ *natanko tedaj, ko je* $B \subseteq A$.
12. $A \cap B = B$ *natanko tedaj, ko je* $B \subseteq A$.
13. $A \subseteq B$ *natanko tedaj, ko je* $B^C \subseteq A^C$.

Dokaz: Enakosti bo bralec zlahka dokazal s pomočjo izreka 1.1. Seveda pa jih lahko dokaže tudi brez uporabe tega izreka. Oglejmo si na primer, kako lahko dokažemo enega izmed distributivnostnih zakonov. Izberimo recimo prvega: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. Kot smo omenili, enakost dveh množic običajno pokažemo v dveh korakih.

Pokažimo najprej, da velja $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ in v ta namen izberimo poljuben $x \in A \cap (B \cup C)$. Tedaj je $x \in A$ in $x \in B \cup C$, kar med drugim pomeni, da je $x \in B$ ali $x \in C$. Če je $x \in B$, je $x \in A \cap B$, če pa je $x \in C$, je $x \in A \cap C$. V vsakem primeru je torej $x \in (A \cap B) \cup (A \cap C)$, kot smo želeli. Ker je bil $x \in A \cap (B \cup C)$ poljuben, smo s tem dokazali $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Za dokaz druge vsebovanosti privzemimo sedaj $x \in (A \cap B) \cup (A \cap C)$, kar seveda pomeni, da je $x \in A \cap B$ ali $x \in A \cap C$ (lahko seveda tudi oboje).

No, če je $x \in A \cap B$, je $x \in A$ in $x \in B$, torej je $x \in B \cup C$ in posledično tudi $x \in A \cap (B \cup C)$. Če pa je $x \in A \cap C$, je $x \in A$ in $x \in C$, torej je zopet $x \in B \cup C$ in posledično $x \in A \cap (B \cup C)$. V vsakem primeru je torej $x \in A \cap (B \cup C)$. Ker je bil $x \in (A \cap B) \cup (A \cap C)$ poljuben, smo s tem dokazali še vsebovanost $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$, s čimer pa je dokazana tudi enakost $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Ustavimo se še pri delu izreka, ki ne govori o enakostih. Da velja 1. točka, smo pravzaprav dokazali že v trditvi 2.2, saj vsebovanost $A \subseteq A$ sledi po definiciji. Dokazi zadnjih treh točk izreka so si zelo podobni, zato si oglejmo le dokaz prve izmed teh treh izjav. V tem primeru je naša trditev ekvivalenca dveh izjav. Da dokažemo njeno pravilnost, je torej po izreku 1.1 dovolj pokazati, da sta pravilni obe pripadajoči implikaciji.

Lotimo se najprej "implikacije iz leve na desno". Privzemimo v ta namen, da velja $A \cup B = A$ in pokažimo, da tedaj velja $B \subseteq A$. To bo res, če bo za vsak $x \in B$ veljalo $x \in A$. Pa naj bo $x \in B$ poljuben. Tedaj je seveda $x \in A \cup B$. Ker pa po predpostavki velja $A \cup B = A$, je torej $x \in A$, kot smo želeli. Ker je bil $x \in B$ poljuben, smo torej pokazali, da res velja $B \subseteq A$.

Lotimo se sedaj še "implikacije iz desne na levo". Privzemimo torej, da velja $B \subseteq A$ in pokažimo, da tedaj velja $A \cup B = A$. Da je $A \subseteq A \cup B$ sledi neposredno iz definicije vsebovanosti. Denimo sedaj še, da je $x \in A \cup B$ poljuben in pokažimo, da tedaj velja $x \in A$. Ker je $x \in A \cup B$, je $x \in A$ ali $x \in B$. Če je $x \in A$, seveda ni kaj dokazovati. Denimo torej, da je $x \in B$. Ker po predpostavki velja $B \subseteq A$, je torej tudi v tem primeru $x \in A$, kot smo želeli. Ker je bil $x \in A \cup B$ poljuben, smo s tem dokazali enakost $A \cup B = A$, s tem pa je dokaz končan. □

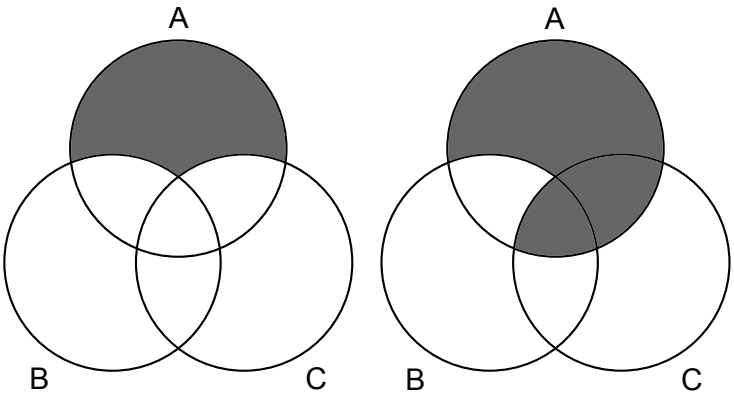
Da si še malce bolj razjasnimo postopek dokazovanja pravilnosti oziroma nepravilnosti izjav, ki govore o zvezah med (splošnimi) množicami, si oglejmo še naslednji zgled.

Zgled: Ali za poljubno trojico množic A, B in C velja $(A \setminus B) \setminus C = A \setminus (B \setminus C)$? Če množici v splošnem nista enaki, ali velja vsaj katera izmed obeh možnih vsebovanosti?

Če si ogledamo pripadajoča Vennova diagrama (slika 2.2), kaj hitro ugotovimo, da enakost v splošnem ne velja. Iz Vennovih diagramov tudi brž ugotovimo, kako naj konstruiramo protiprimer. Poskrbeti moramo le, da bo obstajal nek element, ki bo vsebovan v $A \cap C$. Vzamemo lahko, na primer, $A = \{a\}$, $B = \emptyset$ ter $C = \{a\}$. Tedaj je $(A \setminus B) \setminus C = A \setminus C = \emptyset$ in $A \setminus (B \setminus C) = A \setminus \emptyset = A = \{a\}$.

Kako pa je z vsebovanostjo? Iz Vennovih diagramov razberemo, da najbrž velja $(A \setminus B) \setminus C \subseteq A \setminus (B \setminus C)$. Zapišimo dokaz te trditve. Po definiciji

pojma podmnožice moramo za vsak $x \in (A \setminus B) \setminus C$ pokazati, da pripada množici $A \setminus (B \setminus C)$. Pa naj bo $x \in (A \setminus B) \setminus C$ poljuben. Tedaj je $x \in A \setminus B$ in $x \notin C$. Torej je $x \in A$, $x \notin B$ ter $x \notin C$. Ker torej x ne pripada množici B, ne more pripadati niti množici $B \setminus C$. Ker pa je $x \in A$, torej res velja $x \in A \setminus (B \setminus C)$, kot smo trdili. Ker je bil $x \in (A \setminus B) \setminus C$ poljuben, smo s tem našo trditev dokazali. ▲



Slika 2.2: Vennova diagrama, ki prikazujeta množici $(A \setminus B) \setminus C$ in $A \setminus (B \setminus C)$.

Seveda si lahko pri dokazovanju raznih izjav o (splošnih) množicah pomagamo tudi z izrekom 2.4. Oglejmo si dva zgleda.

ZGLED: Pokažimo, da za poljubne množice A, B in C velja $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$. Enakost seveda lahko dokažemo tako, da se prepričamo, da je vsaka izmed obeh množic vsebovana v drugi. S pomočjo izreka 2.4 pa gre stvar precej hitreje. Naj bo U unija vseh treh množic. Tedaj lahko smiselno govorimo o komplementih. Tako je

$$(A \setminus C) \cap (B \setminus C) = (A \cap C^C) \cap (B \cap C^C) = (A \cap B) \cap C^C = (A \cap B) \setminus C.$$

▲

ZGLED: Pokažimo, da za poljubni množici A in B velja $A \Delta B = (A \cup B) \setminus (A \cap B)$. Po definiciji je $A \Delta B = (A \setminus B) \cup (B \setminus A)$. Tokrat naj bo U unija obeh množic, torej $U = A \cup B$. Po izreku 2.4 torej velja

$$A \Delta B = (A \cap B^C) \cup (B \cap A^C) = (A \cup (B \cap A^C)) \cap (B^C \cup (B \cap A^C)) =$$
$$((A \cup B) \cap U) \cap (U \cap (B^C \cup A^C)) = (A \cup B) \cap (A^C \cup B^C) =$$
$$(A \cup B) \cap (A \cap B)^C = (A \cup B) \setminus (A \cap B).$$

▲

Naloga 2.7. Podane imamo množice $A = \{z \in \mathbb{Z} : 110 \mid z\}$, $B = \{z \in \mathbb{Z} : 22 \mid z\}$ in $C = \{z \in \mathbb{Z} : 10 \mid z\}$. Ali tedaj velja katera izmed enakosti $A = B \cup C$, $A = B \cap C$ ali $C = B \setminus A$?

Naloga 2.8. Naj bo $A = \{x \in \mathbb{R} \,|\, ax^2 + bx + c = 0$ za neke $a, b, c \in \mathbb{Z}$, ki niso vsi enaki $0\}$ in $B = \{x \in \mathbb{R} \,|\, ax^2 + bx + c = 0$ za neke $a, b, c \in \mathbb{Q}$, ki niso vsi enaki $0\}$. Pokažite, da velja $2 \in A$ in $\sqrt{2} \in A$. Ali velja celo $\mathbb{Q} \subseteq A$? Velja morda $A = B$?

Naloga 2.9. Uporabite trditve izreka 2.4, da dokažete naslednjo trditev za poljubne podmnožice A, B in C univerzalne množice U: $C^C \subset B \Rightarrow (A \setminus B) \cup C = C$.

Naloga 2.10. Naj bosta A in B poljubni množici. Pokažite, da sta tedaj množici A in $B \setminus A$ disjunktni, ter da je $A \cup B = A \cup (B \setminus A)$.

Naloga 2.11. Naj bodo A, B in C poljubne množice. Ali tedaj velja $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$? Ali morda velja sklep, da v primeru, ko velja $A \cup B = A \cup C$ velja tudi $B = C$?

Naloga 2.12. Pokažite, da za poljubne množice A, B in C velja $A\Delta(B\Delta C) = (A\Delta B)\Delta C$.

Naloga 2.13. Naj bo U neka univerzalna množica in naj bosta A in B taki njeni podmnožici, da za vsako podmnožico C množice U velja $A \cap C = B \cap C$. Ali smemo od tod sklepati, da velja enakost $A = B$? Kaj pa če za vsako podmnožico C množice U velja $A \cup C = B \cup C$, ali smemo tedaj sklepati na enakost $A = B$?

2.4 Unija in presek družine množic

V prejšnjem razdelku smo spoznali pojem unije in preseka dveh množic. A zdi se, da ni nobene potrebe po omejevanju na zgolj dve množici. Ni namreč težko ugotoviti, kako definirati unijo in presek treh množic. Kako pa je z unijo in presekom poljubne družine množic?

Razmislimo najprej, kako definirati unijo in presek treh množic. Za množice A, B in C se zdi unijo teh treh množic smiselno definirati kot množico vseh elementov, ki so vsebovani v vsaj eni izmed teh treh množic, presek pa kot množico elementov, ki so vsebovani v vseh treh množicah. Dejstvo, da smo tu govorili o treh množicah, očitno nima prav posebej velikega pomena. Bistveno je, da pri uniji zahtevamo, da je element vsebovan v vsaj eni izmed obravnavanih množic, pri preseku pa, da je vsebovan v vseh teh množicah.

No, sedaj pa že lahko podamo definicijo unije in preseka poljubnega nabora množic. Namesto o uniji in preseku množic iz nekega nabora ponavadi raje govorimo o uniji in preseku družine množic.

Definicija. Naj bo I neka neprazna množica (indeksov) in denimo, da imamo za vsak indeks $i \in I$ dano neko množico A_i. Tedaj je *unija* družine množic $\{A_i : i \in I\}$, ki jo označimo z $\bigcup_{i\in I} A_i$, množica, ki sestoji natanko iz tistih elementov, ki so vsebovani v vsaj eni izmed množic A_i. Podobno je *presek* družine $\{A_i : i \in I\}$, ki ga označimo z $\bigcap_{i\in I} A_i$, množica, ki sestoji natanko iz tistih elementov, ki so vsebovani v vsaki izmed množic A_i.

Preden nadaljujemo opozorimo, da kljub temu, da smo indekse označili z i, to ne pomeni, da so to lahko le števila. Indeksna množica I je tako lahko čisto poljubna neprazna množica.

Glede na to, da so v uniji ravno elementi, ki so vsebovani v vsaj eni izmed obravnavanih množic, v preseku pa tisti, ki so vsebovani v vseh teh množicah, je jasno, da lahko v primeru, ko so vse množice A_i podmnožice neke univerzalne množice U, unijo in presek družine $\{A_i : i \in I\}$ zapišemo s pomočjo eksistenčnega in univerzalnega kvantifikatorja kot

$$\bigcup_{i\in I} A_i = \{x \in U : (\exists i \in I : x \in A_i)\} \quad \text{in}$$

$$\bigcap_{i\in I} A_i = \{x \in U : (\forall i \in I : x \in A_i)\}.$$

Spomnimo se, da smo v splošnem za obstoj unije dveh množic potrebovali aksiom o uniji. Kako pa je z obstojem unije in preseka poljubne družine množic? Če gre za družino končno mnogo množic (pojma končnosti sicer še nismo definirali, zato se zaenkrat oprimo kar na našo intuitivno pojmovanje tega pojma), seveda ni težav, saj po aksiomu o ekstenzionalnosti očitno velja, da je na primer unija množic A, B, C in D enaka množici $A \cup (B \cup (C \cup D))$, ki po aksiomu o uniji obstaja. Pri poljubnih družinah pa, vsaj kar se tiče unije, zopet naletimo na težave (za obstoj preseka poljubne družine množic novega aksioma ne potrebujemo, saj je eksistenca zagotovljena po aksiomu o podmnožici). Pravzaprav se izkaže, da z doslej sprejetimi aksiomi njenega obstoja ni moč dokazati. Zato aksiom o uniji posplošimo tako, da bo zagotavljal obstoj unije poljubnih družin množic.

Aksiom o uniji: Naj bo $\{A_i : i \in I\}$ poljubna neprazna družina množic. Tedaj obstaja množica, ki sestoji natanko iz vseh elementov, ki so vsebovani v vsaj eni izmed množic te družine. Povedano drugače, unija $\bigcup_{i\in I} A_i$ obstaja.

Prepričajmo se, da ta aksiom implicira naš prvotni aksiom o uniji, to je, pokažimo, da lahko "stari" aksiom o uniji zares nadomestimo z "novim". Res, če imamo dani množici A in B, po aksiomu o paru obstaja družina $\{A, B\}$, potem pa po (novem) aksiomu o uniji obstaja tudi unija te družine. A po definiciji je to množica, ki sestoji iz elementov, ki so vsebovani v vsaj eni izmed množic A in B, kar pa je ravno definicija množice $A \cup B$, ki potemtakem zares obstaja.

Oglejmo si nekaj zgledov presekov in unij družin množic.

ZGLED: Za vsak $n \in \mathbb{N}$ naj bo $A_n = [0, n]$ zaprt interval v $\mathbb{R}$ s krajišči 0 in n.

Pokažimo, da tedaj velja $\bigcup_{n=1}^{9} A_n = [0, 9]$. Kot običajno enakost množic dokažemo tako, da se prepričamo, da je vsaka izmed obeh množic vsebovana v drugi. Pa naj bo najprej $x \in \bigcup_{n=1}^{9} A_n$. Po definiciji unije obstaja $n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, da je $x \in A_n = [0, n]$. Sledi $0 \leq x \leq n$, ker pa je $n \leq 9$ od tod takoj dobimo še $0 \leq x \leq 9$ in tako $x \in [0, 9]$. Naj bo sedaj še $x \in [0, 9]$. Tedaj je seveda $x \in A_9$, torej je zagotovo tudi $x \in \bigcup_{n=1}^{9} A_n$. S tem je enakost $\bigcup_{n=1}^{9} A_n = [0, 9]$ dokazana. Seveda bi to enakost lahko dokazali tudi s pomočjo izreka 2.4, saj za vsak $n \in \mathbb{N}$ očitno velja $A_n \subseteq A_{n+1}$, torej je $A_n \cup A_{n+1} = A_{n+1}$. Tako je $A_1 \cup A_2 = A_2$. Posledično je $A_1 \cup A_2 \cup A_3 = A_2 \cup A_3 = A_3$. Nadaljujemo, pa ugotovimo, da velja $\bigcup_{n=1}^{9} A_n = A_9 = [0, 9]$.

Podobno se dokaže (bodisi direktno ali pa s pomočjo izreka 2.4), da velja $\bigcap_{n=1}^{9} A_n = [0, 1]$.

Kako pa je z unijo $\bigcup_{n\in\mathbb{N}} A_n$? Hitro pridemo do sklepa, da mora veljati $\bigcup_{n\in\mathbb{N}} A_n = \mathbb{R}^+ \cup \{0\}$. A tokrat zgornjega argumenta, ki temelji na izreku 2.4, ne moremo speljati, saj je množic "preveč". Dokaz je torej treba speljati tako, da se zopet dokažeta obe vsebovanosti. Naj bo torej najprej $x \in \bigcup_{n\in\mathbb{N}} A_n$. Po definiciji unije za nek i velja $x \in A_i$, torej je $0 \leq x \leq i$ in tako očitno velja $x \in \mathbb{R}^+ \cup \{0\}$. Denimo sedaj, da je $x \in \mathbb{R}^+ \cup \{0\}$. Kot smo omenili že v 1. poglavju, so naravna števila navzor neomejena, torej za vsako realno število M obstaja naravno število N, za katerega je $N > M$. Ker je $x \in \mathbb{R}^+ \cup \{0\}$, tako obstaja naravno število n, da je $n > x$. Tedaj pa je seveda $x \in A_n$ in tako $x \in \bigcup_{n\in\mathbb{N}} A_n$. Enakost $\bigcup_{n\in\mathbb{N}} A_n = \mathbb{R}^+ \cup \{0\}$ torej res velja. ▲

ZGLED: Za vsak $n \in \mathbb{N}$ naj bo $A_n = \{\frac{m}{n} : m \in \mathbb{Z}\}$. Čemu je tedaj enaka unija $\bigcup_{n\in\mathbb{N}} A_n$ in čemu presek $\bigcap_{n\in\mathbb{N}} A_n$?

Pokažimo najprej, da velja $\bigcup_{n\in\mathbb{N}} A_n = \mathbb{Q}$. Ker je število $\frac{m}{n}$ za vsaka $n \in \mathbb{N}$ in $m \in \mathbb{Z}$ racionalno število, vsebovanost $\bigcup_{n\in\mathbb{N}} A_n \subseteq \mathbb{Q}$ seveda velja. Za vsak $x \in \bigcup_{n\in\mathbb{N}} A_n$ namreč po definiciji unije obstaja $n \in \mathbb{N}$, da je $x \in A_n$, po definiciji množice A_n pa obstaja $m \in \mathbb{Z}$, da je $x = \frac{m}{n}$ in tako je $x \in \mathbb{Q}$. Naj

bo sedaj še x poljubno racionalno število. Po definiciji racionalnih števil tedaj obstajata celo število m in neničelno celo število n, da je $x = \frac{m}{n}$. Brez škode za splošnost lahko privzamemo, da je $n > 0$, to je, $n \in \mathbb{N}$ (sicer namesto m in n pač vzamemo $-m$ in $-n$). Tedaj pa je $x \in A_n$ in zato tudi $x \in \bigcup_{n\in\mathbb{N}} A_n$, s čimer je dokaz enakosti $\bigcup_{n\in\mathbb{N}} A_n = \mathbb{Q}$ končan.

Pokažimo sedaj še, da velja $\bigcap_{n\in\mathbb{N}} A_n = \mathbb{Z}$. Naj bo v ta namen $q \in \bigcap_{n\in\mathbb{N}} A_n$. Tedaj je seveda $q \in A_1 = \mathbb{Z}$, s čimer smo dokazali vsebovanost $\bigcap_{n\in\mathbb{N}} A_n \subseteq \mathbb{Z}$. Naj bo sedaj $z \in \mathbb{Z}$ poljuben. Za vsak $n \in \mathbb{N}$ je tedaj $z = \frac{nz}{n} \in A_n$, torej je res $z \in \bigcap_{n\in\mathbb{N}} A_n = \mathbb{Z}$, s čimer je enakost $\bigcap_{n\in\mathbb{N}} A_n = \mathbb{Z}$ dokazana. ▲

Spomnimo se izreka 2.4. Med drugim ta izrek pove, da za unijo in presek veljata oba distributivnostna zakona, obenem pa veljata še oba DeMorganova zakona. Kot pokažeta naslednji dve trditvi, posplošitvi teh dveh zakonov veljata tudi kadar obravnavamo unije in preseke poljubnih družin množic.

Trditev 2.5. *Naj bo $\{A_i : i \in I\}$ poljubna neprazna družina množic in naj bo B poljubna množica. Tedaj velja*

$$\left(\bigcup_{i\in I} A_i\right) \cap B = \bigcup_{i\in I}(A_i \cap B) \quad \text{in} \quad \left(\bigcap_{i\in I} A_i\right) \cup B = \bigcap_{i\in I}(A_i \cup B).$$

Dokaz: Pokažimo prvo izmed obeh enakosti, drugo pa bo s povsem podobnim premislekom bralec dokazal sam. Naj bo v ta namen najprej $x \in \left(\bigcup_{i\in I} A_i\right) \cap B$. Tedaj je $x \in \bigcup_{i\in I} A_i$ in $x \in B$. Po definiciji unije tako obstaja $i \in I$, da je $x \in A_i$, od koder sledi $x \in A_i \cap B$. Sledi $x \in \bigcup_{i\in I}(A_i \cap B)$, kot smo želeli. Pa naj bo sedaj še $x \in \bigcup_{i\in I}(A_i \cap B)$. Tedaj obstaja $i \in I$, da je $x \in A_i \cap B$, torej je $x \in A_i$ in $x \in B$. Sledi $x \in \bigcup_{i\in I} A_i$, od koder potem takoj dobimo še $x \in \left(\bigcup_{i\in I} A_i\right) \cap B$. S tem je enakost $\left(\bigcup_{i\in I} A_i\right) \cap B = \bigcup_{i\in I}(A_i \cap B)$ dokazana. □

Trditev 2.6. *Naj bo $\{A_i : i \in I\}$ poljubna neprazna družina podmnožic univerzalne množice U. Tedaj velja*

$$\left(\bigcup_{i\in I} A_i\right)^C = \bigcap_{i\in I} A_i^C \qquad \text{in} \qquad \left(\bigcap_{i\in I} A_i\right)^C = \bigcup_{i\in I} A_i^C.$$

Dokaz: Zopet pokažimo le prvo izmed obeh enakosti. Drugo lahko na podoben način dokaže bralec sam, lahko pa se opre tudi na dejstvo, da za vsako podmnožico A množice U velja $(A^C)^C = A$.

Naj bo torej najprej $x \in \left(\bigcup_{i\in I} A_i\right)^C$. To pomeni, da je $x \in U$ in $x \notin \bigcup_{i\in I} A_i$. Po definiciji je $\bigcup_{i\in I} A_i = \{z \in U : (\exists i \in I : z \in A_i)\}$, torej je izjava $x \notin \bigcup_{i\in I} A_i$ ekvivalentna izjavi $\forall i \in I : x \notin A_i$. Ker je seveda $x \in U$, torej za vsak $i \in I$ velja, da je $x \in A_i^C$, in tako res velja $x \in \bigcap_{i\in I} A_i^C$.

Naj bo sedaj še $x \in \bigcap_{i\in I} A_i^C$. Tedaj za vsak $i \in I$ velja $x \in A_i^C$, torej je izjava $\forall i \in I : x \notin A_i$ pravilna. To pa pomeni, da izjava $\exists i \in I : x \in A_i$ ni pravilna, in tako $x \notin \bigcup_{i\in I} A_i$. Ker seveda velja $x \in U$, smo s tem dokazali $x \in \left(\bigcup_{i\in I} A_i\right)^C$, s čimer je dokaz končan. □

Naloga 2.14. Za vsak $i \in \mathbb{N}$ naj bo $A_i = [i, i+1]$. Določite množici $A = \bigcup_{i\in\mathbb{N}} A_i$ ter $\bigcap_{i\in\mathbb{N}} A_i$. Svoje trditve dokažite.

Naloga 2.15. Naj bo $\mathbb{N}_2 = \mathbb{N} \setminus \{1\}$ in naj bo za vsak $n \in \mathbb{N}_2$ dana množica $A_n = (\frac{1}{n}, \frac{n}{n+1})$. Določite množici $A = \bigcup_{i\in\mathbb{N}_2} A_i$ ter $\bigcap_{i\in\mathbb{N}_2} A_i$. Svoje trditve dokažite.

Naloga 2.16. Naj bo I neka neprazna množica indeksov in naj bo za vsak $i \in I$ dana podmnožica A_i neke univerzalne množice U. Denimo, da za neko dano množico B velja, da je $A_i \subseteq B$ za vse $i \in I$. Pokažite, da tedaj velja $\bigcup_{i\in I} A_i \subseteq B$.

Naloga 2.17. Denimo da sta $\{A_n : n \in \mathbb{N}\}$ in $\{B_n : n \in \mathbb{N}\}$ taki družini množic, da za vsak $n \in \mathbb{N}$ velja $A_n \subseteq B_n$. Ali tedaj velja tudi $\bigcap_{n\in\mathbb{N}} A_n \subseteq \bigcap_{n\in\mathbb{N}} B_n$? Kaj pa če za vsak $n \in \mathbb{N}$ velja $A_n \subsetneq B_n$, ali tedaj velja $\bigcap_{n\in\mathbb{N}} A_n \subsetneq \bigcap_{n\in\mathbb{N}} B_n$?

Naloga 2.18. Naj bosta $\{A_i : i \in I\}$ in $\{B_i : i \in I\}$ poljubni neprazni družini množic. Pokažite, da tedaj velja

$$\left(\bigcap_{i\in I} A_i\right) \cup \left(\bigcap_{i\in I} B_i\right) \subseteq \bigcap_{i\in I} (A_i \cup B_i).$$

Pokažite, da enakost v splošnem ne velja.

2.5 Potenčna množica in kartezični produkt

V prejšnjih razdelkih smo spoznali nekaj načinov, kako iz danih množic konstruiramo nove. V tem razdelku bomo tem dodali še dva nova.

Imejmo dano neko množico A. Po aksiomu o podmnožici za vsako smiselno lastnost elementov množice A obstaja njena podmnožica, ki sestoji iz natanko tistih elementov množice A, ki to lastnost imajo. Na ta način torej lahko iz

dane množice A dobimo celo vrsto novih podmnožic. Po aksiomu o paru za poljubni dve taki podmnožici množice A obstaja množica, katere edina elementa sta ravno ti dve množici. Po aksiomu o uniji lahko take množice podmnožic množice A potem združujemo v večje in večje množice, ki vsebujejo kot elemente vedno več podmnožic množice A. To lahko počnemo toliko časa, dokler ne dobimo množico vseh možnih podmnožic množice A. Tej množici damo posebno ime.

Definicija. Naj bo A množica. Tedaj je njena *potenčna množica* $\mathcal{P}(A)$ množica, ki sestoji iz vseh podmnožic množice A.

Zgled: Naj bo $A = \{a, b\}$. Tedaj je $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$. Poiščimo še potenčno množico množice, ki smo jo pravkar konstruirali. Dobimo

$$\begin{aligned}\mathcal{P}(\mathcal{P}(A)) = \Big\{ & \emptyset, \\ & \{\emptyset\}, \{\{a\}\}, \{\{b\}\}, \{\{a, b\}\}, \\ & \{\emptyset, \{a\}\}, \{\emptyset, \{b\}\}, \{\emptyset, \{a, b\}\}, \{\{a\}, \{b\}\}, \{\{a\}, \{a, b\}\}, \{\{b\}, \{a, b\}\}, \\ & \{\emptyset, \{a\}, \{b\}\}, \{\emptyset, \{a\}, \{a, b\}\}, \{\emptyset, \{b\}, \{a, b\}\}, \{\{a\}, \{b\}, \{a, b\}\}, \\ & \{\emptyset, \{a\}, \{b\}, \{a, b\}\} \Big\}.\end{aligned}$$

▲

Zgled: Glede na to, da smo doslej uspeli zares dokazati le obstoje množic, ki temeljijo na prazni množici, si malce oglejmo še kako je s potenčnimi množicami takih množic. Najprej določimo potenčno množico prazne množice. Seveda je $\mathcal{P}(\emptyset) = \{\emptyset\}$. Dalje, $\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$. Napravimo še en korak. $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$. ▲

Iz zgornjih dveh zgledov razberemo, da se zadeve kaj hitro začno komplicirati v smislu preglednosti dobljene množice. Poleg tega vidimo, da po "velikosti" potenčna množica množice A precej naraste v primerjavi z A. Zato obstoj potenčne množice poljubne množice ni samoumeven. Še več, izkaže se, da obstoja potenčne množice poljubne množice ni mogoče zagotoviti z doslej sprejetimi aksiomi. Zato je treba privzeti nov aksiom.

Aksiom o potenčni množici: Naj bo A poljubna dana množica. Tedaj obstaja množica vseh njenih podmnožic, to je, obstaja potenčna množica množice A.

Oglejmo si sedaj nekaj osnovnih lastnosti potenčnih množic. V zgornjih zgledih je $\emptyset$ vedno element pripadajoče potenčne množice. Da je temu tako, ni slučaj.

Trditev 2.7. *Naj bo A poljubna množica. Tedaj je $\mathcal{P}(A)$ neprazna množica.*

Dokaz: Po trditvi 2.2 velja $\emptyset \subseteq A$, torej potenčna množica $\mathcal{P}(A)$ vsebuje vsaj element $\emptyset$. Posledično je seveda $\mathcal{P}(A)$ neprazna množica. □

Kako je s potenčno množico preseka in unije pokaže naslednja trditev.

Trditev 2.8. *Naj bosta A in B poljubni množici. Tedaj velja*

$$\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B) \quad \text{in} \quad \mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B).$$

Enakost $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$ v splošnem ne velja.

Dokaz: Posvetimo se najprej enakosti $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$. Da dokažemo vsebovanost $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$ naj bo X poljubna podmnožica množice $A \cap B$. Tedaj je seveda X tako podmnožica množice A kot podmnožica množice B in zato je $X \in \mathcal{P}(A)$, ter $X \in \mathcal{P}(B)$. Sledi $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$, kot smo želeli. Da dokažemo še vsebovanost $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$ naj bo sedaj še $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$. Tedaj je $X \in \mathcal{P}(A)$, to je $X \subseteq A$, ter $X \in \mathcal{P}(B)$, to je $X \subseteq B$. Sledi $X \subseteq A \cap B$ in tako $X \in \mathcal{P}(A \cap B)$, kot smo želeli. S tem je enakost $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$ dokazana.

Dokažimo sedaj vsebovanost $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$. Naj bo v ta namen $X \in \mathcal{P}(A) \cup \mathcal{P}(B)$. Tedaj je $X \subseteq A$ ali $X \subseteq B$, torej je $X \subseteq A \cup B$ in tako $X \in \mathcal{P}(A \cup B)$. Da enakost v splošnem ne velja dokaže naslednji konkreten primer. Za $A = \{1\}$ in $B = \{2\}$ je $\mathcal{P}(A \cup B) = \mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$, po drugi strani pa je $\mathcal{P}(A) \cup \mathcal{P}(B) = \{\emptyset, \{1\}\} \cup \{\emptyset, \{2\}\} = \{\emptyset, \{1\}, \{2\}\}$. □

V matematiki pogosto potrebujemo pojem urejenih parov, urejenih trojic, itd. Kot bomo videli, so ti pojmi izrednega pomena, saj na njih temeljijo pojmi kot so relacije, funkcije, itd. Kako na podlagi doslej povedanega vpeljati pojem urejenega para? Intuitivno je *urejeni par* (x, y) par elementov x in y (pri čemer sta x in y lahko enaka), v katerem imamo pojem prvega elementa (x) in drugega elementa (y). To je torej neurejeni par $\{x, y\}$, ki ima zraven tega še podatek o tem, kateri izmed elementov je prvi in kateri drugi. Izkaže se, da je moč ta koncept doseči že z doslej zgrajeno teorijo množic. Urejeni par (x, y) lahko namreč definiramo kot par $\{\{x\}, \{x, y\}\}$. Naslednja trditev pokaže, da se ta definicija ujema z našo intuitivno predstavo o urejenih parih.

Trditev 2.9. *Za poljubna urejena para (a, b) in (c, d) velja, da je $(a, b) = (c, d)$ natanko tedaj, ko je $a = c$ in $b = d$.*

Dokaz: Najprej se prepričajmo, da je urejeni par (x, y) singleton natanko tedaj, ko je $x = y$. Če je $x = y$, je $(x, y) = \{\{x\}, \{x, y\}\} = \{\{x\}, \{x\}\} = \{\{x\}\}$ res singleton. Obratno, če je (x, y) singleton, je $\{x\} = \{x, y\}$, torej je $y \in \{x\}$, kar pa seveda pomeni $x = y$.

Pokažimo sedaj končno, da res velja $(a, b) = (c, d)$ natanko tedaj, ko je $a = c$ in $b = d$. Primer, ko je katerikoli (in zato oba) izmed parov singleton (kar je po pravkar povedanem ekvivalentno temu, da je $a = b$ ali $c = d$), je jasen. Privzemimo torej, da $a \neq b$ in $c \neq d$. Če je $a = c$ in $b = d$, seveda ni kaj dokazovati. Denimo torej, da je $(a, b) = (c, d)$, to je, da velja $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. Ker po predpostavki $a \neq b$ in $c \neq d$, v vsaki izmed obeh množic nastopa natanko po en singleton. Tako mora seveda veljati $\{a\} = \{c\}$, od koder dobimo $a = c$. Sledi še $\{a, b\} = \{c, d\}$ in tako je $b \in \{c, d\}$. A ker je $a \neq b$ in je $a = c$, od tod sledi $b = d$, kot smo trdili. □

Sedaj, ko smo se prepričali, da se naša definicija urejenega para ujema z intuitivnim pojmovanjem tega pojma, lahko "pozabimo" na samo definicijo in uporabljamo le običajno oznako (a, b).

Definicija. Naj bosta A in B poljubni množici. *Kartezični produkt* $A \times B$ množic A in B je množica

$$A \times B = \{(a, b) : a \in A,\ b \in B\},$$

ki sestoji iz vseh urejenih parov, pri katerih prvi element pripada množici A, drugi pa množici B. Množico $A \times A$ včasih krajše označimo kar z A^2.

Kako je z obstojem kartezičnega produkta množic? Ker je vsak urejeni par element potenčne množice $\mathcal{P}(\mathcal{P}(A \cup B))$, ki po aksiomih o uniji in o potenčni množici obstaja, po aksiomu o podmnožici obstaja tudi kartezični produkt $A \times B$, zato za njegov obstoj novega aksioma ne potrebujemo.

Oglejmo si dva zgleda in nekaj osnovnih lastnosti kartezičnih produktov.

Zgled: Naj bo $A = \{1, 2\}$ in $B = \{a, b, c, d\}$. Tedaj je

$$A \times B = \{(1, a), (1, b), (1, c), (1, d), (2, a), (2, b), (2, c), (2, d)\}.$$

Tudi množico vseh dni v prestopnem letu lahko predstavimo kot podmnožico ustreznega kartezičnega produkta. Vzemimo

$$A = \{n \in \mathbb{N} : 1 \leq n \leq 12\} \quad \text{in} \quad B = \{n \in \mathbb{N} : 1 \leq n \leq 31\}.$$

Tedaj lahko množico vseh dni v prestopnem letu predstavimo kot $(A \times B) \setminus C$, kjer je $C = \{(2, 30), (2, 31), (4, 31), (6, 31), (9, 31), (11, 31)\}$. ▲

ZGLED: Kolobar Gaussovih celih števil $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ je podmnožica množice kompleksnih števil, ki sestoji iz vseh števil oblike $a+bi$, kjer je $a, b \in \mathbb{Z}$. Izkaže se, da ima vsako število oblike $a + bi$, kjer sta $a, b \in \mathbb{Z}$, enoličen zapis take oblike (z drugimi besedami, če za $a, b, c, d \in \mathbb{Z}$ velja $a + bi = c + di$, potem je $a = c$ in $b = d$). To pomeni, da lahko množico $\mathbb{Z}[i]$ predstavimo kot kartezični produkt $\mathbb{Z} \times \mathbb{Z}$, kjer urejeni par (a, b) ustreza številu $a + bi$. ▲

Trditev 2.10. *Naj bosta A in B poljubni množici. Tedaj je kartezični produkt $A \times B$ prazna množica natanko tedaj, ko je vsaj ena izmed množic A in B prazna.*

DOKAZ: Resničnost izjave iz trditve pokažimo tako, da dokažemo resničnost naslednje ekvivalentne izjave: kartezični produkt $A \times B$ je neprazen natanko tedaj, ko sta tako A kot B neprazni množici. Denimo najprej, da je $A \times B$ neprazna množica. Tedaj obstaja nek $(a, b) \in A \times B$. Po definiciji je $a \in A$ in $b \in B$, zato nobena izmed množic A in B ni prazna. Denimo sedaj, da niti A niti B ni prazna množica. Tedaj obstaja $a \in A$ in $b \in B$. Sledi, da je $(a, b) \in A \times B$ in tako $A \times B$ ni prazna množica. □

Trditev 2.11. *Naj bodo A, B, C in D poljubne neprazne množice. Tedaj je $A \times B = C \times D$ natanko tedaj, ko je $A = C$ in $B = D$.*

DOKAZ: Če je $A = C$ in $B = D$ seveda očitno velja $A \times B = C \times D$. Naj bo sedaj $A \times B = C \times D$. Pokažimo, da tedaj velja $A = C$, dokaz, da je tudi $B = D$ pa prepustimo bralcu. Naj bo $a \in A$ poljuben. Ker je B neprazna množica, obstaja vsaj en $b \in B$. Tedaj pa je $(a, b) \in A \times B = C \times D$, torej je $a \in C$ (in $b \in D$). Tako je $A \subseteq C$. Povsem analogen dokaz pokaže tudi vsebovanost $C \subseteq A$ (tukaj potrebujemo nepraznost množice D). □

Trditev 2.12. *Naj bodo A, B, C in D poljubne množice. Tedaj velja*

$$(A \times C) \cap (B \times D) = (A \cap B) \times (C \cap D) \quad \text{in}$$

$$(A \times C) \cup (B \times D) \subseteq (A \cup B) \times (C \cup D).$$

Enakost $(A \times C) \cup (B \times D) = (A \cup B) \times (C \cup D)$ v splošnem ne velja.

DOKAZ: Veljavnost prve enakosti lahko utemeljimo z zaporedjem naslednjih ekvivalenc:

$$(x, y) \in (A \times C) \cap (B \times D) \sim (x, y) \in A \times C \wedge (x, y) \in B \times D \sim$$
$$x \in A \wedge y \in C \wedge x \in B \wedge y \in D \sim x \in A \cap B \wedge y \in B \cap D \sim$$
$$(x, y) \in (A \cap B) \times (C \cap D).$$

Pokažimo še vsebovanost $(A\times C)\cup(B\times D)\subseteq(A\cup B)\times(C\cup D)$. Naj bo v ta namen $(x,y)\in(A\times C)\cup(B\times D)$. Tedaj je $(x,y)\in A\times C$ ali $(x,y)\in B\times D$. V prvem primeru je $x\in A$ in $y\in C$, v drugem pa $x\in B$ in $y\in D$. V obeh primerih je torej $x\in A\cup B$ in $y\in C\cup D$, torej je res $(x,y)\in(A\cup B)\times(C\cup D)$, kot smo trdili. Da se prepričamo, da enakost v splošnem ne velja, vzemimo $A=D=\emptyset$ in $B=C=\{1\}$. Tedaj je $(A\times C)\cup(B\times D)=\emptyset\cup\emptyset=\emptyset$ ter $(A\cup B)\times(C\cup D)=\{1\}\times\{1\}=\{(1,1)\}$. □

Naloga 2.19. Poiščite potreben in zadosten pogoj, da za množici A in B velja $\mathcal{P}(A\cup B)=\mathcal{P}(A)\cup\mathcal{P}(B)$.

Naloga 2.20. Koliko elementov ima vsaka izmed potenčnih množic $\mathcal{P}(\{1,2\})$, $\mathcal{P}(\{1,2,3\})$ in $\mathcal{P}(\{1,2,3,4\})$?

Naloga 2.21. Naj bosta A in B poljubni množici. Pokažite, da tedaj velja $A\subseteq B$ natanko tedaj, ko $\mathcal{P}(A)\subseteq\mathcal{P}(B)$.

Naloga 2.22. Naj bo $\{A_i : i\in I\}$ poljubna družina množic. Pokažite, da tedaj velja

$$\mathcal{P}\left(\cap_{i\in I}A_i\right)=\bigcap_{i\in I}\mathcal{P}(A_i).$$

Naloga 2.23. Naj bodo A,B,C in D poljubne množice. Ali tedaj velja

$$(A\setminus B)\times(C\setminus D)=(A\times C)\setminus(B\times D)?$$

Ali velja vsaj katera izmed vsebovanosti?

Naloga 2.24. V ravnini $\mathbb{R}^2$ skicirajte množico $([0,1]\cup[2,3])\times([1,2])$.

Naloga 2.25. Naj bodo A,B,C poljubne množice. Ali tedaj velja enakost $A\times(B\cup C)=(A\times B)\cup(A\times C)$? Kaj pa $A\times(B\cap C)=(A\times B)\cap(A\times C)$?

Naloga 2.26. Naj bo $A=\{1,\{1\},\{1,\{1\}\}\}$. Določite množici $A\times A$ ter $A\cap\mathcal{P}(A)$.

2.6 Relacije in particije

Tako kot urejeni pari in z njimi povezani kartezični produkti so tudi relacije nepogrešljiva sestavina vsake matematične teorije. Med premicami v ravnini imamo recimo relacijo vzporednosti ali pa pravokotnosti. Med števili imamo recimo relacijo "biti manjši", itd. Seveda pa relacije srečujemo tudi v svetu okrog nas. Govorimo recimo o prijateljstvih, o poznanstvih, o velikosti,

itd. Poznamo relacije, ki govore o zvezah med dvemi rečmi, med tremi rečmi, itd. Tukaj se bomo ukvarjali le z relacijami, ki govore o zvezah med dvema rečema, to je, obravnavali bomo tako imenovane *binarne* relacije. V nadaljevanju tega razdelka bomo pridevnik "binarna" izpuščali. Za zapis (binarne) relacije so kot naročeni urejeni pari. Podajmo definicijo.

Definicija. Naj bosta A in B množici. *Relacija iz A v B* je neka množica urejenih parov (a, b), kjer je $a \in A$ in $b \in B$. Relacija je torej neka podmnožica množice $A \times B$. V primeru, ko je $B = A$, govorimo o *relaciji na množici A*.

Relacije običajno označujemo s črkami R, S, T, itd. Dejstvo, da je $(x, y) \in R$ praviloma zapišemo z xRy, kar beremo kot "x je v relaciji R z y." Da x ni v relaciji R z y ponavadi označimo z $x \not R y$. Oglejmo si nekaj zgledov.

Zgled: Na vsako smiselno lastnost elementov neke množice lahko gledamo kot na relacijo. Na primer, če je $A = \{2, 3, 4, 5, 6, 7, 8, 9\}$ in nas zanima lastnost "je praštevilo", lahko to lastnost predstavimo kot relacijo R iz A v B, kjer je $B = \{\mathrm{DA}, \mathrm{NE}\}$ in sicer je

$$R = \{(2, \mathrm{DA}), (3, \mathrm{DA}), (4, \mathrm{NE}), (5, \mathrm{DA}), (6, \mathrm{NE}), (7, \mathrm{DA}), (8, \mathrm{NE}), (9, \mathrm{NE})\}.$$

▲

Zgled: Naj bo A poljubna množica. Na potenčni množici $\mathcal{P}(A)$ že poznamo relacijo vsebovanosti $\subseteq$. Tudi pripadnost elementov podmnožic množice A lahko predstavimo kot relacijo in sicer gre tu za relacijo iz A v $\mathcal{P}(A)$, kjer je $a \in A$ v relaciji z $X \in \mathcal{P}(A)$, če je $a \in X$. ▲

Zgled: Na množici $A = \mathbb{Z} \times \mathbb{Z}$ lahko vpeljemo relacijo R s predpisom $(a, b)R(c, d) \iff ad = bc$. Tako je potem na primer $(1, 2)R(12, 24)$ in $(-2, 3)R(4, -6)$, po drugi strani pa na primer $(1, 1) \not R (2, 1)$. Lahko je tudi videti, da je $(0, 0)$ v relaciji z vsakim elementom $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. ▲

Zgled: Premislimo kako dobiti vse možne relacije na množici $A = \{1, 2\}$. Ker so relacije na A ravno podmnožice kartezičnega produkta $A \times A$, je množica vseh iskanih relacij ravno potenčna množica $\mathcal{P}(A \times A)$. Bralec bo preveril, da na ta način dobimo 16 različnih relacij na A. Najbolj "revna" izmed teh relacij je *prazna relacija* $\emptyset$. Najbolj "bogata" je na drugi strani kar relacija $A \times A$. A ti dve relaciji nista preveč zanimivi. Zanimive so ostale, ki so nekje vmes med obema. ▲

Kot smo videli v zadnjem zgledu, imamo že na množici z le dvema elementoma kar veliko možnih relacij. Bolj bogata kot je množica, več je seveda

možnosti. Na primer, že na množici prvih petih naravnih števil imamo kar 33 554 432 različnih relacij. Zato seveda vseh možnih relacij na dani množici enostavno ni mogoče obravnavati, temveč nas običajno zanimajo le relacije, ki imajo kake posebno lepe lastnosti.

Definicija. Naj bo R relacija na množici A. Pravimo, da je relacija R

- *refleksivna*, če za vsak $x \in A$ velja xRx,
- *irefleksivna*, če za vsak $x \in A$ velja $x \not R x$,
- *simetrična*, če za vsaka $x, y \in A$ velja $xRy \Rightarrow yRx$.
- *asimetrična*, če za vsaka $x, y \in A$ velja $xRy \Rightarrow y \not R x$.
- *antisimetrična*, če za vsaka $x, y \in A$ velja $xRy \wedge yRx \Rightarrow x = y$.
- *tranzitivna*, če za vsake $x, y, z \in A$ velja $xRy \wedge yRz \Rightarrow xRz$.
- *sovisna*, če za poljubna različna elementa $x, y \in A$ velja $xRy \vee yRx$.
- *strogo sovisna*, če za poljubna elementa $x, y \in A$ velja $xRy \vee yRx$.

Če je relacija R refleksivna, simetrična in tranzitivna, pravimo, da je R *ekvivalenčna* relacija. Če je R refleksivna, antisimetrična in tranzitivna, pravimo, da je R relacija *delne urejenosti*. Če je R delna urejenost, ki je hkrati še sovisna, je R *linearna urejenost*.

Opazimo, da je torej relacija strogo sovisna natanko tedaj, ko je sovisna in refleksivna. Prav tako je vsaka asimetrična relacija irefleksivna.

Zgled: Na množici naravnih števil imejmo relacijo R, podano z naslednjim predpisom. Velja naj aRb natanko tedaj, ko ima a v razcepu na praštevilske faktorje največ toliko faktorjev (šteto s kratnostjo) kot b. Tako na primer velja $6R8$, saj ima 6 dva praštevilska faktorja, 8 pa 3 (praštevilo 2 ima kratnost 3). Brž opazimo, da je relacija R refleksivna (potemtakem pa seveda ni irefleksivna). Relacija R seveda ni simetrična, ker na primer velja $6R8$ vendar pa $8 \not R 6$. Relacija R ni asimetrična, ker ni irefleksivna. Ni niti antisimetrična, saj na primer velja $6R10$ in $10R6$. Zlahka se prepričamo, da je relacija R tranzitivna in strogo sovisna. ▲

Če je množica A, na kateri definiramo relacijo, dovolj majhna, lahko relacijo predstavimo grafično. Narišemo tako imenovani *graf relacije*. To storimo tako, da vsak element množice A predstavimo kot neko točko v ravnini (in to tako, da različnima elementoma ustrezata različni točki), nato pa za vsak urejeni par $(a, b) \in R$ narišemo usmerjeno daljico od točke, ki ustreza a, do točke, ki ustreza b. Če je $a = b$, narišemo zanko v točki a. Morda velja omeniti, da včasih namesto usmerjenih daljic zaradi boljše preglednosti

rišemo kar usmerjene krivulje (rečemo pa jim kar povezave). Če je aRb in bRa, namesto dveh usmerjenih krivulj, od katerih je vsaka usmerjena v svojo stran, narišemo kar "dvosmerno" krivuljo. Lastnosti iz zgornje definicije se potem takole odražajo na grafu relacije:

- refleksivnost - zanka v vsaki točki
- irefleksivnost - nobene zanke
- simetričnost - vse povezave so dvosmerne
- antisimetričnost - razen morebitnih zank ni dvosmernih povezav
- asimetričnost - ni dvosmernih povezav (torej med drugim ni nobene zanke)
- tranzitivnost - za vsako "pot" v dveh korakih obstaja bližnjica
- sovisnost - poljubni dve različni točki sta povezani
- stroga sovisnost - poljubni dve točki sta povezani (torej imamo med drugim zanko v vsaki točki)

Zgled: V zgornjem zgledu smo se spraševali po vseh možnih relacijah na množici $A = \{1, 2\}$. Poiščimo tokrat vse ekvivalenčne relacije, vse relacije delne urejenosti, ter vse relacije linearne urejenosti R na množici $B = \{1, 2, 3\}$. Ker mora biti taka relacija v vsakem primeru refleksivna, mora R vsebovati vse tri pare $(1, 1), (2, 2)$ in $(3, 3)$. Poiščimo najprej vse ekvivalenčne relacije. Bralec se bo hitro prepričal, da so edine možnosti:

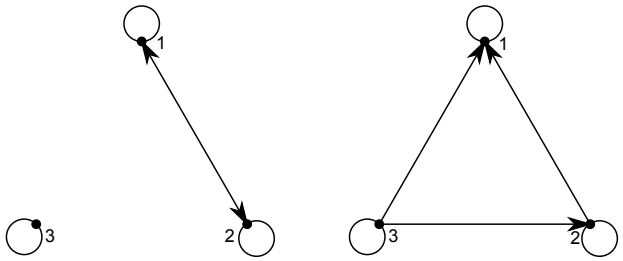
$$\begin{aligned} R &= \{(1,1),(2,2),(3,3)\} \\ R &= \{(1,1),(1,2),(2,1),(2,2),(3,3)\} \\ R &= \{(1,1),(1,3),(2,2),(3,1),(3,3)\} \\ R &= \{(1,1),(2,2),(2,3),(3,2),(3,3)\} \\ R &= B \times B \end{aligned}$$

Tudi delna urejenost je refleksivna, torej vsebuje vse tri urejene pare $(1, 1)$, $(2, 2)$ in $(3, 3)$. Zaradi antisimetričnosti lahko delna urejenost za vsak par različnih elementov $a, b \in B$ vsebuje največ enega izmed urejenih parov (a, b) in (b, a). Ker je delna urejenost tudi tranzitivna, tako hitro ugotovimo, da

so edine možne delne urejenosti:

$$
\begin{aligned}
R &= \{(1,1),(2,2),(3,3)\}\\
R &= \{(1,1),(1,2),(2,2),(3,3)\}\\
R &= \{(1,1),(1,3),(2,2),(3,3)\}\\
R &= \{(1,1),(2,2),(2,3),(3,3)\}\\
R &= \{(1,1),(2,1),(2,2),(3,3)\}\\
R &= \{(1,1),(2,2),(3,1),(3,3)\}\\
R &= \{(1,1),(2,2),(3,2),(3,3)\}\\
R &= \{(1,1),(1,2),(1,3),(2,2),(3,3)\}\\
R &= \{(1,1),(1,2),(2,2),(3,2),(3,3)\}\\
R &= \{(1,1),(1,3),(2,2),(2,3),(3,3)\}\\
R &= \{(1,1),(2,1),(2,2),(3,1),(3,3)\}\\
R &= \{(1,1),(2,1),(2,2),(2,3),(3,3)\}\\
R &= \{(1,1),(2,2),(3,1),(3,2),(3,3)\}\\
R &= \{(1,1),(1,2),(1,3),(2,2),(2,3),(3,3)\}\\
R &= \{(1,1),(1,2),(1,3),(2,2),(3,2),(3,3)\}\\
R &= \{(1,1),(1,3),(2,1),(2,2),(2,3),(3,3)\}\\
R &= \{(1,1),(2,1),(2,2),(2,3),(3,1),(3,3)\}\\
R &= \{(1,1),(1,2),(2,2),(3,1),(3,2),(3,3)\}\\
R &= \{(1,1),(2,1),(2,2),(3,1),(3,2),(3,3)\}
\end{aligned}
$$

Izmed vseh naštetih delnih urejenosti je samo zadnjih šest tudi linearnih urejenosti. Vidimo torej, da so zahtevane lastnosti zelo redke. Na primer, izmed vseh možnih 512 relacij na množici B je samo pet ekvivalenčnih (pri čemer sta dve na nek način nezanimivi), linearnih pa je šest. Na spodnji sliki 2.3 sta prikazani druga izmed ekvivalenčnih relacij ter zadnja izmed linearnih urejenosti. ▲



Slika 2.3: Ponazoritev ene izmed ekvivalenčnih relacij ter ene izmed linearnih urejenosti na množici $A = \{1, 2, 3\}$.

ZGLED: Na realnih številih je dobro znana relacija $\leq$. Ta relacija je relacija

linearne urejenosti. Po drugi strani, če na potenčni množici $\mathcal{P}(A)$ poljubne dane množice A definiramo relacijo vsebovanosti $\subseteq$, dobimo relacijo delne urejenosti, ki pa ni linearna, saj vsaj v splošnem nekatere podmnožice niso primerljive po vsebovanosti. ▲

Zgled: Na množici realnih števil $\mathbb{R}$ definirajmo relacijo $xRy \iff x-y \in \mathbb{Z}$. Prepričajmo se, da je to ekvivalenčna relacija na $\mathbb{R}$. Res, ker za vsak $x \in \mathbb{R}$ velja $x - x = 0 \in \mathbb{Z}$, je R refleksivna. Dalje, če za $x, y \in \mathbb{R}$ velja xRy, je $x - y \in \mathbb{Z}$, potem pa je tudi $y - x = -(x - y) \in \mathbb{Z}$, torej je R tudi simetrična relacija. Nazadnje, če za $x, y, z \in \mathbb{R}$ velja $x - y = a \in \mathbb{Z}$ in $y - z = b \in \mathbb{Z}$, je tudi $x - z = x - y + y - z = a + b \in \mathbb{Z}$, saj je vsota celih števil celo število. Tako je R tudi tranzitivna in posledično ekvivalenčna relacija na $\mathbb{R}$. ▲

Ekvivalenčne relacije običajno namesto s črko R označujemo z znakom $\sim$. Primer je bila recimo ekvivalenca med izjavami (bralec se bo prepričal, da ima ekvivalenca med izjavami zares vse lastnosti ekvivalenčne relacije).

Definicija. Naj bo $\sim$ ekvivalenčna relacija na množici A in naj bo $a \in A$. Tedaj množico $[a]_\sim = \{b \in A : a \sim b\}$ imenujemo *ekvivalenčni razred* elementa a pri relaciji $\sim$. Kadar ni možnosti za nesporazum namesto $[a]_\sim$ pišemo kar $[a]$. Množico vseh ekvivalenčnih razredov relacije $\sim$ na A označimo z $A/_\sim$ in ji rečemo *kvocientna množica* množice A glede na relacijo $\sim$.

Ekvivalenčni razredi imajo naslednjo zelo pomembno lastnost.

Izrek 2.13. *Naj bo $\sim$ ekvivalenčna relacija na množici A in naj bosta $x, y \in A$ poljubna. Tedaj je $x \sim y \iff [x] = [y]$. Posledično za vsaka $x, y \in A$ velja: če $[x] \cap [y] \neq \emptyset$, velja $[x] = [y]$.*

Dokaz: Denimo najprej, da velja $x \sim y$ in pokažimo, da tedaj velja $[x] = [y]$. Naj bo torej $z \in [x]$ poljuben. Po definiciji tedaj velja $x \sim z$. Ker je po predpostavki $x \sim y$, je po simetričnosti in tranzitivnosti tudi $y \sim z$ in tako $z \in [y]$. Tako je $[x] \subseteq [y]$. Druga vsebovanost gre povsem analogno. Denimo sedaj, da velja $[x] = [y]$. Zaradi refleksivnosti je $y \in [y]$, torej je $y \in [x]$ in tako po definiciji $x \sim y$, s čimer je dokaz prvega dela izreka končan.

No, drugi del sedaj takoj sledi. Če je namreč $z \in [x] \cap [y]$, je $x \sim z$ in $y \sim z$, od koder po zgornjem velja $[x] = [z]$ in $[y] = [z]$, od tod pa seveda tokoj dobimo $[x] = [y]$. □

Zgornji izrek torej pove, da vsaka ekvivalenčna relacija na množici A le-to "razkosa" na paroma disjunktne podmnožice, namreč ekvivalenčne razrede glede na to relacijo.

ZGLED: V zgornjem zgledu, kjer smo iskali vse ekvivalenčne relacije na množici $B = \{1, 2, 3\}$, smo našli pet ekvivalenčnih relacij. Prva je imela tri ekvivalenčne razrede (vsak $b \in B$ je v tem primeru v svojem ekvivalenčnem razredu), zadnja ima le enega (vsak element iz B je v relaciji z vsakim elementom iz B), preostale tri pa imajo po dva ekvivalenčna razreda, en singleton in en ekvivalenčni razred, ki vsebuje preostala dva elementa. ▲

ZGLED: Naj bo n poljubno naravno število in naj bo $\sim_n$ relacija na množici $\mathbb{Z}$, podana s predpisom

$$a \sim_n b \iff n \mid (b - a).$$

Ob upoštevanju dejstva, da velja $n \mid (b - a)$ natanko tedaj, ko obstaja celo število z, da je $b - a = nz$, se zlahka prepričamo, da je $\sim_n$ ekvivalenčna relacija na $\mathbb{Z}$. Ker velja $0 = n \cdot 0$, je $\sim_n$ refleksivna relacija. Naj velja $a \sim_n b$. Tedaj za nek $z \in \mathbb{Z}$ velja $b - a = nz$, torej je $a - b = n(-z)$ in tako je $b \sim_n a$. Relacija $\sim_n$ je torej simetrična. Denimo nazadnje, da je $a \sim_n b$ in $b \sim_n c$. Tedaj obstajata celi števili z_1 in z_2, za kateri je $b - a = nz_1$ in $c - b = nz_2$. Tedaj pa je $c - a = c - b + b - a = nz_2 + nz_1 = n(z_1 + z_2)$. Ker je $z_1 + z_2$ seveda celo število, od tod sledi $a \sim_n c$, s čimer smo dokazali še tranzitivnost relacije $\sim_n$. Bralec se bo prepričal, da ima relacija $\sim_n$ natanko n različnih ekvivalenčnih razredov in sicer

$$\begin{aligned}
[0] &= \{z \in \mathbb{Z} : z \equiv 0 \pmod{n}\} \\
[1] &= \{z \in \mathbb{Z} : z \equiv 1 \pmod{n}\} \\
[2] &= \{z \in \mathbb{Z} : z \equiv 2 \pmod{n}\} \\
&\vdots \\
[n-1] &= \{z \in \mathbb{Z} : z \equiv n-1 \pmod{n}\}.
\end{aligned}$$

Pripadajočo kvocientno množico $\mathbb{Z}/_{\sim_n}$ običajno označimo z $\mathbb{Z}_n$ in jo imenujemo množica ostankov pri deljenju z n. ▲

ZGLED: Spomnimo se še zgleda z začetka tega razdelka. Tokrat relacijo R definirajmo le na $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ (spomnimo se definicije $(a, b)R(c, d) \iff ad = bc$). Bralec se bo prepričal, da gre za ekvivalenčno relacijo. Ekvivalenčni razred elementa (a, b) je ravno množica vseh parov (c, d), ki dajo isti kvocient kot (a, b), to je $\frac{a}{b} = \frac{c}{d}$. Tako lahko kvocientno množico $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/_R$ dojemamo kot množico vseh racionalnih števil. ▲

Kot smo omenili že zgoraj, nam torej ekvivalenčna relacija na množici A poda neko "razbitje" te množice na paroma disjunktne podmnožice. Vpeljimo pojem razbitja formalno.

Definicija. Naj bo A poljubna množica. Neprazna družina nepraznih podmnožic $\{A_i : i \in I\}$ množice A je *razbitje* (tudi *particija*) množice A, če velja:

(i) $\bigcup_{i\in I} A_i = A$

(ii) za vsaka $i, i' \in I$ velja: če je $A_i \cap A_{i'} \neq \emptyset$, je $A_i = A_{i'}$.

Razbitje množice A je torej taka množica njenih nepraznih podmnožic, da vsak element te množice nastopa v natanko eni izmed množic iz razbitja.

Zgled: Poiščimo vse možne particije množice $B = \{1, 2, 3\}$. Brž se prepričamo, da so edine možnosti

$$\{\{1\}, \{2\}, \{3\}\}$$
$$\{\{1\}, \{2, 3\}\}$$
$$\{\{1, 3\}, \{2\}\}$$
$$\{\{1, 2\}, \{3\}\}$$
$$\{\{1, 2, 3\}\}$$

Bralec je najbrž opazil, da je možnih razbitij množice B ravno toliko, kolikor je možnih ekvivalenčnih relacij na množici B. Še več, posamezni "kosi" v teh razbitjih sovpadajo z ekvivalenčnimi razredi teh ekvivalenčnih relacij. Kot bomo kmalu videli, to ni slučaj. ▲

Zgled: Označimo z $\mathbb{R}^+ = \{x \in \mathbb{R} : x \geq 0\}$ množico vseh nenegativnih realnih števil. Za vsak $x \in \mathbb{R}^+$ definirajmo $A_x = \{y \in \mathbb{R} : |x| = |y|\}$. Tedaj je $\{A_x : x \in \mathbb{R}^+\}$ razbitje množice $\mathbb{R}$. Velja namreč $A_0 = \{0\}$ in $A_x = \{-x, x\}$ za vse $x > 0$, torej so množice A_x neprazne, paroma disjunktne, za vsak $x \in \mathbb{R}$ pa velja $x \in A_x$ oziroma $x \in A_{-x}$ odvisno od predznaka x. ▲

Zgled: Naj bo za vsak $z \in \mathbb{Z}$ množica A_z podana kot $A_z = [-z, z]$. Tedaj $\{A_z : z \in \mathbb{Z}\}$ ni razbitje množice $\mathbb{R}$. Po drugi strani, če za vsak $z \in \mathbb{Z}$ postavimo $B_z = [z, z + 1)$, je $\{B_z : z \in \mathbb{Z}\}$ razbitje množice $\mathbb{R}$. ▲

V zgornjem zgledu smo opazili, da so razbitja množice $B = \{1, 2, 3\}$ v tesni povezavi z ekvivalenčnimi relacijami na tej množici. Pokažimo, da to velja v splošnem.

Izrek 2.14. *Naj bo $\sim$ ekvivalenčna relacija na množici A. Tedaj je $\{[x]_\sim : x \in A\}$ particija množice A. Obratno, če je $\{A_i : i \in I\}$ particija množice A, je relacija R na A, podana s predpisom $xRy \iff \exists i \in I : x, y \in A_i$, ekvivalenčna relacija, katere ekvivalenčni razredi sovpadajo z elementi družine $\{A_i : i \in I\}$.*

Dokaz: Pokažimo najprej prvi del izreka. Jasno je, da je vsak ekvivalenčni razred $[x]$ neprazna podmnožica množice A, saj $[x]$ zaradi refleksivnosti vsebuje vsaj element x. Ker je vsak element vsebovan v nekem ekvivalenčnem razredu, je očitno tudi, da je unija vseh ekvivalenčnih razredov enaka množici A. Ostane še premislek, da so ekvivalenčni razredi paroma disjunktni, kar smo dokazali v izreku 2.13.

Pa naj bo sedaj $\{A_i : i \in I\}$ neko razbitje množice A in naj bo R kot v formulaciji izreka. Naj bo $x \in A$ poljuben. Ker je $\cup_{i\in I} A_i = A$, obstaja $i \in I$, da je $x \in A_i$. Da velja xRx, sedaj sledi neposredno iz definicije relacije R. Tudi simetričnost je povsem očitna. Naj bodo sedaj še $x, y, z \in A$ taki, da je xRy in yRz. Tedaj obstajata $i, i' \in I$, da je $x, y \in A_i$ in $y, z \in A_{i'}$. Tedaj je $y \in A_i \cap A_{i'}$, torej po definiciji razbitja velja $A_i = A_{i'}$. Tedaj pa je $x, z \in A_i$ in tako je xRz, kot smo želeli. Pokažimo nazadnje, da ekvivalenčni razredi relacije R sovpadajo z množicami A_i. Naj bo $x \in A$ poljuben. Po definiciji razbitja obstaja $i \in I$, da je $x \in A_i$, po definiciji naše relacije pa je $[x] = \{y \in A : (\exists j \in I : x, y \in A_j)\}$. Ker so "kosi" razbitja paroma disjunktni, tedaj avtomatsko sledi $[x] = \{y \in A : y \in A_i\} = A_i$. □

Morda bralca skrbi, da smo v prvem delu dokaza naredili napako, češ da ekvivalenčni razredi v družini $\{[x] : x \in A\}$ niso paroma disjunktni, saj za $x \sim y$ ekvivalenčna razreda $[x]$ in $[y]$ nista disjunktna. Da nista disjunktna, je sicer res, a je skrb kljub temu odveč. V tem primeru namreč velja $[x] = [y]$ in gre torej v množici $\{[x] : x \in A\}$, ki ji je po aksiomu o ekstenzionalnosti "vseeno" kolikokrat povemo, da je nek element vsebovan v njej, za en sam element.

Zgornji izrek je izrednega pomena, saj pove, da so ekvivalenčne relacije in razbitja neke dane množice v povratno enolični korespondenci. Med drugim to pomeni, da lahko ekvivalenčno relacijo na množici A predpišemo tako, da le povemo kakšni bodo ekvivalenčni razredi. Ob tem omenimo še naslednje. Število vseh različnih particij (in s tem ekvivalenčnih relacij) množice z n elementi imenujemo *Bellovo število* in ga označimo z B_n. Gre za precej dobro znana števila, o katerih lahko bralec v ustrezni literaturi izve marsikaj zanimivega. Mi zgolj omenimo, da je $B_1 = 1$, $B_2 = 2$, $B_3 = 5$, $B_4 = 15$, $B_5 = 52$, $B_6 = 203$, $B_7 = 877$, itd.

Pomudimo se za konec tega razdelka še pri pojmu kompozituma in inverza relacij.

Definicija. Naj bodo A, B in C množice in naj bo R relacija iz A v B, S pa relacija iz B v C. Tedaj je *inverz* R^{-1} relacije R relacija iz B v A podana z

$R^{-1} = \{(b,a) \in B \times A : (a,b) \in R\}$. *Kompozitum* relacij R in S je relacija $S \circ R$ iz A v C, podana s predpisom

$$S \circ R = \{(a,c) \in A \times C : (\exists b \in B : (aRb \wedge bSc))\}.$$

Zgled: Naj bo $A = \{1,2,3,4,5\}$ in $R = \{(1,1),(1,2),(2,4),(3,2),(4,5)\}$. Tedaj je

$$\begin{array}{rcl} R^{-1} & = & \{(1,1),(2,1),(2,3),(4,2),(5,4)\} \quad \text{in} \\ A \circ A & = & \{(1,1),(1,2),(1,4),(2,5),(3,4)\}. \end{array}$$

▲

Zgled: Če je R relacija pravokotnosti na množici vseh premic v ravnini $\mathbb{R}^2$, je $R \circ R$ relacija vzporednosti teh premic. ▲

Naloga 2.27. Poiščite potreben in zadosten pogoj, da je relacija vsebovanosti $\subseteq$ na potenčni množici $\mathcal{P}(A)$ množice A relacija linearne urejenosti.

Naloga 2.28. Na množici $\mathbb{Z}$ definiramo relaciji R in S s predpisoma $xRy \iff x = -y$ ter $xSy \iff 2 \mid (3x - 5y)$. Ali je katera izmed njiju ekvivalenčna relacija? Če je, kaj so njeni ekvivalenčni reazredi?

Naloga 2.29. Na množici $\mathbb{R}^2$ definiramo relaciji R in S s predpisoma

$$(x,y)R(z,w) \iff x^2+y^2 = z^2+w^2 \text{ ter } (x,y)S(z,w) \iff x^2+y^2 \leq z^2+w^2.$$

Ali je katera ekvivalenčna relacija? Je katera relacija delne urejenosti? Morda linearne urejenosti?

Naloga 2.30. Naj bo $A = \{1,2,3,4,5\}$. Če obstaja, poiščite kako relacijo na A, ki je:

- ekvivalenčna relacija
- linearna urejenost
- refleksivna, a ni ne simetrična ne tranzitivna
- simetrična, a ni ne refleksivna, ne tranzitivna
- tranzitivna, a ni ne refleksivna, ne simetrična

Naloga 2.31. Če obstaja poiščite kako relacijo R na množici $\mathbb{R}$, ki je relacija delne urejenosti, a ni linearna urejenost.

Naloga 2.32. Naj bosta relaciji $\sim_2$ in $\sim_3$ na množici celih števil definirani kot v enem izmed zgornjih zgledov. Ali je tedaj relacija $\sim_2 \circ \sim_3$ ekvivalenčna relacija na $\mathbb{Z}$. Če je, koliko ekvivalenčnih razredov ima?

2.7 Funkcije

V prejšnjem razdelku smo obravnavali predvsem relacije na dani množici, torej relacije iz neke množice A nazaj v A. V tem razdelku se bomo posvetili posebni vrsti relacij iz A v B, ki jim pravimo *funkcije* ali tudi *preslikave*. Funkcije so eden temeljnih in nepogrešljivih konceptov v matematiki (pa tudi v drugih vejah znanosti), zato je prav, da si jih natančno ogledamo.

Neko predstavo o funkcijah najbrž že imamo. Poznamo na primer realne funkcije, pa linearne funkcije med vektorskimi prostori, itd. Tudi številska zaporedja so le posebne vrste funkcije, ki slikajo iz množice naravnih števil v množico realnih ali kompleksnih števil. Na prvi pogled torej ni videti, da bi imele funkcije kaj opraviti z relacijami. In vendar niso funkcije nič drugega kot posebne vrste relacije. Preden podamo formalno definicijo, razmislimo, kaj "pričakujemo" od funkcij. Če bo f funkcija, ki slika iz množice A v množico B, bomo zahtevali, da se vsak $a \in A$ "preslika" v nek $b \in B$ in to v enega samega (sicer bi dobili takoimenovane "večlične funkcije").

Definicija. Naj bosta A in B množici in naj bo f relacija iz A v B. Relacija f je *funkcija* (tudi *preslikava*) iz A v B, če veljata naslednja dva pogoja:

(i) Za vsak $a \in A$ obstaja $b \in B$, da je afb.

(ii) Za vsak $a \in A$ in vsaka $b, c \in B$ velja naslednji sklep: če je afb in afc, je $b = c$.

V tem primeru potem namesto afb običajno pišemo $f(a) = b$ in rečemo, da je b *f-slika* elementa a. Množico A imenujemo *domena* (tudi *definicijsko območje*), množico B pa *kodomena* funkcije f. Dejstvo, da je f funkcija z domeno A in kodomeno B, običajno označimo z $f\colon A \to B$.

Kaj povesta zgornja dva pogoja? Prvi zagotovi, da ima vsak $a \in A$ neko f-sliko v B, drugi pa, da ima lahko nek $a \in A$ največ eno f-sliko v B. Oba skupaj torej povesta, da ima vsak $a \in A$ natanko eno f-sliko v B. Tako včasih tudi rečemo, da ima vsak element množice A natanko določeno f-sliko v množici B.

Zgled: Kot splošne relacije lahko seveda tudi funkcije podamo eksplicitno ali implicitno. Na primer, realna funkcija $f\colon \mathbb{R} \to \mathbb{R}$, podana s predpisom $f(x) = x^2 + 1$, je torej funkcija $f = \{(x, x^2 + 1) : x \in \mathbb{R}\}$. Opozorimo, da torej funkcija ni natanko podana le s predpisom. Zelo pomembni sta tudi domena in kodomena funkcije. Tako na primer funkcija $g = \{(x, x^2 + 1) : x \in \mathbb{R} \wedge x > 0\}$ ni enaka funkciji f. ▲

ZGLED: Naj bo $A = \{1, 2, 3\}$. Premislimo koliko je vseh funkcij $f\colon A \to A$. Ker je vsaka funkcija relacija, bomo kandidate iskali med $2^9 = 512$ možnimi relacijami na A. (Bralec se bo spomnil, da je na A le 5 ekvivalenčnih relacij in le 6 relacij linearne urejenosti.) Ker mora imeti vsak element iz množice A natanko eno sliko (ki je seveda vsebovana v A), ima vsaka funkcija f iz A v A natanko tri elemente, namreč $f = \{(1, f(1)), (2, f(2)), (3, f(3))\}$, kjer so seveda $f(1), f(2), f(3)$ neki elementi množice A. Ker zaenkrat nismo postavili prav nobene zahteve glede f-slik posameznih elementov (razen tega, da morajo biti v A), je torej možnosti $3^3 = 27$. Ena izmed možnih funkcij je na primer $f = \{(1, 1), (2, 2), (3, 3)\}$, ki bi jo lahko podali tudi s predpisom $f\colon A \to A$, $f(a) = a$ za vsak $a \in A$, spet druga pa na primer $f = \{(1, 1), (2, 1), (3, 1)\}$, ki bi jo lahko podali s predpisom $f\colon A \to A$, $f(a) = 1$ za vsak $a \in A$. ▲

ZGLED: Na množici naravnih števil lahko definiramo funkcijo $\varphi\colon \mathbb{N} \to \mathbb{N}$, ki je podana z naslednjim predpisom. Vrednost $\varphi(n)$ je število naravnih števil med vključno 1 in n, ki so tuja številu n. Tako je na primer $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, itd. Funkcija φ se imenuje *Eulerjeva φ funkcija*. ▲

Na kaj moramo torej paziti, če funkcijo podamo tako, da navedemo njeno domeno in kodomeno ter podamo predpis? Da zadostimo pogojem iz definicije, je treba poskrbeti, da ima res vsak element domene sliko v kodomeni, pri tem pa mora biti ta vrednost enolično določena. Rečemo, da je funkcija *dobro definirana*. Na primer, če bi "definirali funkcijo" $f\colon \mathbb{R} \to \mathbb{R}$ s predpisom $f(x) = \frac{1}{x}$, bi imeli težave, ker element $0 \in \mathbb{R}$ ne bi imel f-slike. Podobno, če bi želeli "definirati funkcijo" ψ iz množice vseh realnih funkcij v realna števila s predpisom, da je $\psi(f)$ ničla funkcije f, bi imeli težave s tem, da funkcije, ki nimajo realne ničle, ne bi imele ψ-slike, funkcije, ki imajo več kot eno realno ničlo, pa bi imele več možnih vrednosti za $\psi(f)$.

Kot pri relacijah, nas tudi pri funkcijah še posebej zanimajo funkcije, ki imajo določene lepe lastnosti. Izmed teh so injektivnost, surjektivnost in bijektivnost ene izmed najpomembnejših.

Definicija. Naj bo $f\colon A \to B$ funkcija iz množice A v množico B. Tedaj je funkcija f *injektivna*, če za vsak par elementov $a_1, a_2 \in A$ velja sklep: $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$. Funkcija f je *surjektivna*, če za vsak $b \in B$ obstaja $a \in A$, da je $b = f(a)$. Funkcija f je bijektivna, če je injektivna in surjektivna hkrati.

Funkcija $f\colon A \to B$ je torej injektivna, če imata poljubna dva različna

elementa domene A različni f-sliki in je surjektivna, če je vsak element kodomene B f-slika nekega elementa iz A.

Spomnimo se, da smo v razdelku o relacijah govorili o tem, da je moč relacije na množici predstaviti z grafom relacije. Tudi funkcije lahko predstavimo na podoben način. Tokrat elemente množic A in B predstavimo ločeno v ravnini, dejstvo, da je $f(a) = b$, pa označimo tako, da od a k b narišemo usmerjeno daljico. Da je relacija f funkcija, se torej iz pripadajočega grafa vidi tako, da se v vsaki točki, ki predstavlja kak element domene A, začne natanko ena usmerjena daljica (ki se konča v točki, ki predstavlja nek element kodomene B). Injektivnost se odraža v tem, da se nobeni dve usmerjeni daljici ne končata v isti točki, surjektivnost pa v tem, da je vsaka točka, ki predstavlja kak element kodomene B, končna točka kake usmerjene daljice.

ZGLED: Vrnimo se k zgledu, kjer smo ugotovili, da obstaja natanko 27 funkcij iz A v A, kjer je $A = \{1, 2, 3\}$. Katere izmed teh funkcij so injektivne? Katere so surjektivne? In katere bijektivne? Premislimo kako je z injektivnimi funkcijami. Ker mora imeti v tem primeru vsak element "svojo" f-sliko, tokrat vrednosti za $f(1)$, $f(2)$ in $f(3)$ ne moremo izbirati povsem poljubno. Če na primer izberemo $f(1) = 1$, smo s tem za $f(2)$ in $f(3)$ izločili možnost 1. Brez večjih težav ugotovimo, da je možnosti 6 in sicer:

$$\begin{array}{c|c|c|c|c|c} f(1)=1 & f(1)=1 & f(1)=2 & f(1)=2 & f(1)=3 & f(1)=3 \\ f(2)=2 & f(2)=3 & f(2)=1 & f(2)=3 & f(2)=1 & f(2)=2 \\ f(3)=3 & f(3)=2 & f(3)=3 & f(3)=1 & f(3)=2 & f(3)=1 \end{array}$$

Bralec se bo prepričal, da so to tudi edine surjektivne (in s tem bijektivne) funkcije iz A v A. Bralec se naj spomni, koliko linearnih urejenosti premore množica A. Ali je to slučaj? ▲

ZGLED: Naj bo $f\colon \mathbb{R}^{2\times 2} \to \mathbb{R}$ funkcija iz množice vseh kvadratnih realnih matrik dimenzije 2×2 v množico realnih števil, podana s predpisom $f(A) = \det(A)$, kjer je $\det(A)$ determinanta matrike A. Ker je $f(\begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}) = 0 = f(\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix})$, ta funkcija ni injektivna. Pokažimo, da je surjektivna. Za poljuben $y \in \mathbb{R}$ moramo najti matriko $A \in \mathbb{R}^{2\times 2}$, ki se z f preslika v y. To zlahka dosežemo tako, da vzamemo $A = \begin{bmatrix} 1 & 0 \\ 0 & y \end{bmatrix}$. Tako je f funkcija, ki je surjektivna, a ni bijektivna. ▲

ZGLED: Naj bo $f\colon \mathbb{R} \setminus \{1\} \to \mathbb{R} \setminus \{1\}$ funkcija, podana s predpisom $f(x) =$

$\frac{x+1}{x-1}$. Ali je ta funkcija injektivna? Je surjektivna?

Ko se odločamo o injektivnosti oziroma surjektivnosti realnih funkcij, je vedno priporočljivo narisati njihov graf (tokrat v pomenu iz srednje šole). V našem primeru je na primer moč iz grafa razbrati, da je v tem primeru f celo bijektivna funkcija.

Pokažimo najprej, da je f injektivna funkcija. Denimo torej, da za $x_1, x_2 \in \mathbb{R} \setminus \{1\}$ velja $f(x_1) = f(x_2)$. Tedaj je $\frac{x_1+1}{x_1-1} = \frac{x_2+1}{x_2-1}$. Ker sta tako x_1 kot x_2 različna od 1, lahko enakost pomnožimo z $x_1 - 1$ ter $x_2 - 1$. Dobimo $(x_1+1)(x_2-1) = (x_1-1)(x_2+1)$, to je, $x_1x_2-x_1+x_2-1 = x_1x_2+x_1-x_2-1$. Sledi $2x_2 = 2x_1$ in tako $x_2 = x_1$. Funkcija f je torej res injektivna.

Pokažimo, da je f tudi surjektivna funkcija. Za dani $y \in \mathbb{R} \setminus \{1\}$ iščemo $x \in \mathbb{R} \setminus \{1\}$, da bo veljalo $y = f(x) = \frac{x+1}{x-1}$. Ker mora biti $x \neq 1$, je ta enakost ekvivalentna enakosti $xy - y = x + 1$, to je, $x(y-1) = y+1$. Ker je $y \neq 1$, smemo deliti z $y - 1$, pa dobimo $x = \frac{y+1}{y-1}$. Našli smo torej ustrezen x. Prepričajmo se le še, da je tako izbrani x različen od 1. To je res, saj zaradi $y \neq 1$ enakost $1 = \frac{y+1}{y-1}$ implicira $y - 1 = y + 1$, to je, $-1 = 1$, kar seveda ni res. Funkcija f je torej res surjektivna, s tem pa tudi bijektivna. ▲

V prejšnjem razdelku smo vpeljali pojem kompozituma relacij. Ker so funkcije relacije (posebne vrste), lahko torej komponiramo tudi funkcije. Pokažimo najprej, da je kompozitum funkcij (če sta le domena ene in kodomena druge usklajeni) funkcija.

Trditev 2.15. *Naj bodo A, B, C in D take množice, da je $B \subseteq C$, in naj bosta $f\colon A \to B$ in $g\colon C \to D$ funkciji. Tedaj je kompozitum $g \circ f$ funkcija iz A v D in za vsak $a \in A$ velja $(g \circ f)(a) = g(f(a))$.*

Dokaz: Da dokažemo, da je $g \circ f$ zares funkcija iz A v D, je treba pokazati, da za vsak $a \in A$ obstaja natanko en $d \in D$, za katerega je $a(g \circ f)d$. Po definiciji kompozituma velja $a(g \circ f)d$ natanko tedaj, ko obstaja $b \in B$, da je afb in bgd. Ker je f funkcija iz A v B, obstaja natanko en $b \in B$, da je $b = f(a)$. Ker je $B \subseteq C$, je $b \in C$, ker pa je g funkcija iz C v D, obstaja natanko en $d \in D$, za katerega je $d = g(b) = g(f(a))$. Tako ustrezen $d \in D$, za katerega je $d = (g \circ f)(a)$, res obstaja, hkrati pa je še enolično določen. □

Naslednja trditev se sicer zdi samoumevna, a je tako izjemnega pomena, da jo velja formalno zapisati in dokazati.

Trditev 2.16. *Naj bodo A, B, C in D poljubne množice, $f\colon A \to B$, $g\colon B \to C$ in $h\colon C \to D$ pa poljubne funkcije. Tedaj velja $h \circ (g \circ f) = (h \circ g) \circ f$.*

Dokaz: Po trditvi 2.15 sta tako $h \circ (g \circ f)$ kot $(h \circ g) \circ f$ funkciji iz A v D. Pokazati je torej treba le, da za vsak $a \in A$ velja $(h \circ (g \circ f))(a) =$

$((h \circ g) \circ f)(a)$, kar sledi neposredno iz trditve 2.15:

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

□

Premislimo sedaj kako je z injektivnostjo in surjektivnostjo kompozituma funkcij.

Izrek 2.17. *Naj bodo A, B in C množice in naj bosta $f\colon A \to B$ in $g\colon B \to C$ funkciji. Tedaj velja naslednje:*

(i) Če je kompozitum $g \circ f$ injektivna funkcija, je tudi funkcija f injektivna.

(ii) Če je kompozitum $g \circ f$ surjektivna funkcija, je tudi funkcija g surjektivna.

(iii) Če sta f in g obe injektivni funkciji, je tudi kompozitum $g \circ f$ injektivna funkcija.

(iv) Če sta f in g obe surjektivni funkciji, je tudi kompozitum $g \circ f$ surjektivna funkcija.

Dokaz: Da dokažemo veljavnost trditve (i) privzemimo, da f ni injektivna funkcija, in pokažimo, da v tem primeru niti $g \circ f$ ni injektivna funkcija. Ker f ni injektivna funkcija, obstajata različna $a_1, a_2 \in A$, da je $f(a_1) = f(a_2)$. Tedaj pa je seveda $(g \circ f)(a_1) = g(f(a_1)) = g(f(a_2)) = (g \circ f)(a_2)$ in tako tudi $g \circ f$ ni injektivna funkcija.

Dokaz trditve (ii) je še lažji. Če je namreč $g \circ f$ surjektivna funkcija, za vsak $c \in C$ obstaja $a \in A$, da je $c = (g \circ f)(a) = g(f(a))$. Ker je seveda $b = f(a) \in B$, smo s tem našli $b \in B$, za katerega je $c = g(b)$. Ker je bil $c \in C$ poljuben, smo s tem dokazali surjektivnost funkcije g.

Da dokažemo točko (iii) privzemimo injektivnost funkcij f in g in vzemimo poljubna $a_1, a_2 \in A$, za katera je $(g \circ f)(a_1) = (g \circ f)(a_2)$. Sledi $g(f(a_1)) = g(f(a_2))$, od koder zaradi injektivnosti funkcije g dobimo $f(a_1) = f(a_2)$. A ker je tudi f injektivna funkcija, sledi $a_1 = a_2$, kar dokaže, da je $g \circ f$ res injektivna funkcija.

Pokažimo nazadnje še točko (iv). Denimo torej, da sta f in g surjektivni funkciji in naj bo $c \in C$ poljuben element. Zaradi surjektivnosti funkcije g obstaja $b \in B$, da je $c = g(b)$. Ker je tudi f surjektivna funkcija, obstaja $a \in A$, da je $b = f(a)$. Tedaj pa je $(g \circ f)(a) = g(f(a)) = g(b) = c$. Ker smo torej za vsak $c \in C$ našli $a \in A$, da je $c = (g \circ f)(a)$, je $g \circ f$ res surjektivna funkcija. □

Posvetimo se sedaj še inverzom funkcij. Spomnimo se, da smo za relacijo $R \subseteq A \times B$ inverzno relacijo R^{-1} definirali kot $R^{-1} = \{(b, a) : (a, b) \in R\}$. Naj bo sedaj $f\colon A \to B$ funkcija. Kdaj je relacija f^{-1} funkcija iz B v A? Po definiciji funkcij mora za vsak $b \in B$ obstajati natanko en $a \in A$, za katerega je $bf^{-1}a$, kar je ekvivalentno zahtevi, da za vsak $b \in B$ obstaja natanko en $a \in A$, za katerega je $f(a) = b$. Ker mora torej za vsak $b \in B$ obstajati $a \in A$, da je $b = f(a)$, mora biti f surjektivna funkcija. Ker mora za vsak $b \in B$ obstajati le en $a \in A$, da je $b = f(a)$, mora biti f tudi injektivna funkcija. S tem smo dokazali naslednjo trditev.

Trditev 2.18. *Naj bo $f\colon A \to B$ funkcija. Tedaj je relacija f^{-1} funkcija natanko tedaj, ko je funkcija f bijektivna.*

Definicija. Naj bo $f\colon A \to B$ bijektivna funkcija. Funkciji $f^{-1}\colon B \to A$ tedaj pravimo *inverzna funkcija* funkcije f.

Zgornji izrek 2.17 nam nemudoma da naslednji rezultat.

Trditev 2.19. *Naj bosta $f\colon A \to B$ in $g\colon B \to C$ bijektivni funkciji. Tedaj je tudi kompozitum $g \circ f\colon A \to C$ bijektivna funkcija in velja $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Dokaz: Da je kompozitum $g \circ f$ bijekcija, sledi neposredno iz izreka 2.17. Pokažimo še enakost $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Po definiciji inverzne funkcije za $a \in A$ in $c \in C$ velja $a = (g \circ f)^{-1}(c)$ natanko tedaj, ko je $c = (g \circ f)(a) = g(f(a))$. Zaradi bijektivnosti funkcije g slednje velja natanko tedaj, ko je $f(a) = g^{-1}(c)$, kar zaradi bijektivnosti funkcije f velja natanko tedaj, ko je $a = f^{-1}(g^{-1}(c)) = (f^{-1} \circ g^{-1})(c)$. Tako res velja $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$, kot smo trdili. □

Naslednji izrek podaja še eno karakterizacijo bijektivnih funkcij. Da bi ga lahko zapisali, se dogovorimo, da za dano množico A preslikavo iz A v A, ki vsak $a \in A$ preslika vase (torej nazaj v a), označimo z id_A in jo imenujemo *identiteta* na A.

Izrek 2.20. *Naj bo $f\colon A \to B$ bijektivna funkcija. Tedaj velja naslednje.*

(i) $f \circ f^{-1} = id_B$.

(ii) $f^{-1} \circ f = id_A$.

(iii) f^{-1} *je bijektivna funkcija.*

(iv) *Če je $g\colon B \to A$ poljubna taka funkcija, da velja $f \circ g = id_B$ ali $g \circ f = id_A$, potem je $g = f^{-1}$.*

Dokaz: Pokažimo točko (i), točko (ii) pa prepustimo bralcu. Naj bo torej $b \in B$ poljuben element množice B in pokažimo, da velja $(f \circ f^{-1})(b) = b$. Po trditivi 2.18 je f^{-1} funkcija, torej obstaja natanko določen element $a \in A$, da je $f^{-1}(b) = a$. Po definiciji inverza sledi $f(a) = b$. Tedaj pa je $(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b$, kot smo trdili. Tako res velja $f \circ f^{-1} = id_B$.

Dokaz točke (iii) sledi neposredno iz trditve 2.18. Po tej trditvi je namreč funkcija f^{-1} bijekcija natanko tedaj, ko je relacija $(f^{-1})^{-1}$ funkcija. A po defincji za $a \in A$ in $b \in B$ velja $a(f^{-1})^{-1}b$ natanko tedaj, ko je $bf^{-1}a$, kar se zgodi natanko tedaj, ko je afb, torej je $(f^{-1})^{-1} = f$. Ker je f seveda funkcija, je tako f^{-1} res bijekcija.

Za dokaz točke (iv) privzemimo, da za $g\colon B \to A$ velja $f \circ g = id_B$ in dokažimo, da tedaj velja $g = f^{-1}$ (drugi del točke (iv) prepuščamo bralcu). Vzemimo tedaj poljuben $b \in B$ in dokažimo, da je $g(b) = f^{-1}(b)$. Po točki (i) velja $f(f^{-1}(b)) = b$. Ker pa je $f \circ g = id_B$, velja tudi $b = (f \circ g)(b) = f(g(b))$. Ker je f injektivna funkcija, tako sledi $f^{-1}(b) = g(b)$. Ker je bil $b \in B$ poljuben, smo s tem dokazali enakost $g = f^{-1}$. □

Točka (iv) zgornjega izreka nam pomaga pri iskanju inverza dane bijektivne funkcije. Vse kar je treba storiti je to, da se prepričamo, da za funkcijo g, za katero trdimo, da je inverz funkcije f, velja bodisi $f \circ g = id_B$ bodisi $g \circ f = id_A$.

Zgled: Naj bo $f\colon (0,1) \to (1,10)$ funkcija, podana s predpisom $f(x) = 9x + 1$. Bralec se bo zlahka prepričal, da je f bijektivna funkcija. Po trditvi 2.18 tedaj obstaja inverzna funkcija f^{-1}. Ker za funkcijo $g\colon (1,10) \to (0,1)$, podano s predpisom $g(x) = \frac{x-1}{9}$, velja, da za vsak $x \in (0,1)$ velja $(g \circ f)(x) = g(f(x)) = g(9x+1) = \frac{9x}{9} = x = id_{(0,1)}(x)$, po izreku 2.20 velja $g = f^{-1}$. ▲

Zgled: Naj bo funkcija $f\colon \mathbb{N} \to \mathbb{Z}$ podana s predpisom

$$f(n) = \begin{cases} \frac{n}{2} & ; \quad n \equiv 0 \pmod 2 \\ -\frac{n-1}{2} & ; \quad n \equiv 1 \pmod 2 \end{cases}.$$

Najprej se je treba prepričati, da je f sploh zares funkcija iz $\mathbb{N}$ v $\mathbb{Z}$. Ker je število v številcu (n v primeru, ko je n sodo število, in $n-1$ v primeru, ko je n liho število) vedno sodo število, je $f(n)$ res celo število, torej s tem ni težav. Da dokažemo injektivnost najprej opazimo, da je $f(n) > 0$ natanko tedaj, ko je n sodo število. Tedaj pa iz enakosti $f(n) = f(m)$ za neki naravni števili n in m sledi, da sta bodisi tako n kot m lihi števili, bodisi sta tako n kot m sodi števili. Sledi, da je bodisi $-\frac{n-1}{2} = -\frac{m-1}{2}$, bodisi $\frac{n}{2} = \frac{m}{2}$. V vsakem primeru dobimo $n = m$, torej je f injektivna funkcija. Da dokažemo še surjektivnost,

naj bo $z \in \mathbb{Z}$ poljubno število. Če je $z > 0$, je $2z$ sodo naravno število, torej je $f(2z) = \frac{2z}{2} = z$. Če je $z \leq 0$, je $1 - 2z \geq 1 - 0 = 1$ liho naravno število, torej je $f(1-2z) = -\frac{1-2z-1}{2} = z$. V vsakem primeru smo tako našli naravno število n, ki se z f preslika v z, in tako je f res surjektivna in s tem tudi bijektivna funkcija.

Kako poiskati inverz funkcije f, smo spoznali že ob dokazu surjektivnosti funkcije f. Dobimo ga kot funkcijo $g\colon \mathbb{Z} \to \mathbb{N}$ s predpisom

$$g(z) = \begin{cases} 2z & ; \quad z > 0 \\ 1 - 2z & ; \quad z \leq 0 \end{cases}.$$

Bralec bo z analizo primerov dokazal, da velja $f \circ g = id_{\mathbb{Z}}$, kar po izreku 2.20 dokaže, da je res $g = f^{-1}$. ▲

Zgornji izrek 2.20 je sicer uporaben, a moramo za dano funkcijo f, katere inverz iščemo, vedeti, da je bijektivna. Če tega ne vemo, je precej bolj uporaben naslednji izrek, ki je neposredna posledica izrekov 2.17 in 2.20.

Izrek 2.21. *Naj bo $f\colon A \to B$ funkcija. Če obstaja funkcija $g\colon B \to A$, za katero velja $f \circ g = id_B$ in $g \circ f = id_A$, je f bijektivna funkcija in velja $g = f^{-1}$.*

Dokaz: Ker je $f \circ g = id_B$ surjektivna funkcija, je funkcija f po izreku 2.17 surjektivna. Podobno je zaradi $g \circ f = id_A$ funkcija f tudi injektivna. Tako je f bijektivna funkcija. Tedaj pa po izreku 2.20 zaradi $f \circ g = id_B$ velja tudi $g = f^{-1}$. □

Zgled: Oglejmo si funkcijo $f\colon \mathbb{R} \setminus \{2\} \to \mathbb{R} \setminus \{1\}$, podano s predpisom $f(x) = \frac{x+5}{x-2}$ (bralec se bo prepričal, da za vsako realno število x, različno od 2, zares velja $f(x) \neq 1$.) Da dokažemo, da je f bijektivna funkcija, je po izreku 2.21 dovolj preveriti, da za funkcijo $g\colon \mathbb{R} \setminus \{1\} \to \mathbb{R} \setminus \{2\}$, podano s predpisom $g(x) = \frac{2x+5}{x-1}$, velja $f \circ g = id_{\mathbb{R}\setminus\{1\}}$ ter $g \circ f = id_{\mathbb{R}\setminus\{2\}}$, v kar se zlahka prepričamo. Res, za $x \in \mathbb{R} \setminus \{1\}$ je

$$f(g(x)) = f\left(\frac{2x+5}{x-1}\right) = \frac{\frac{2x+5}{x-1} + 5}{\frac{2x+5}{x-1} - 2} = \frac{\frac{2x+5+5x-5}{x-1}}{\frac{2x+5-2x+2}{x-1}} = \frac{7x}{7} = x.$$

Da za $x \in \mathbb{R} \setminus \{2\}$ velja tudi $g(f(x)) = x$, bo preveril bralec. ▲

Za konec tega razdelka se posvetimo še slikam in praslikam funkcije. Vpeljimo oba pojma.

Definicija. Naj bo $f\colon A \to B$ funkcija. Za poljubno podmnožico $X \subseteq A$ množico $f(X) = \{f(x) : x \in X\}$ imenujemo *f-slika* množice X. Za poljubno podmnožico $Y \subseteq B$ množico $f^{-1}(Y) = \{a \in A : f(a) \in Y\}$ imenujemo *f-praslika* množice Y. Množico $f(A)$, torej f-sliko domene A, imenujemo *zaloga vrednosti* funkcije f.

Bralec naj bo pozoren, da oznaka f^{-1} ne pomeni, da gre za inverzno funkcijo funkcije f, saj funkcija f v splošnem ni bijektivna in zato inverzne funkcije morda sploh ne premore. Oznaka $f^{-1}(Y)$ torej označuje množico tistih elementov množice a, ki se z f preslikajo v množico Y.

Zgled: Za funkcijo $f\colon \mathbb{C} \to \mathbb{C}$, podano s predpisom $f(z) = z^4$, je na primer $f(\{2, -2\}) = \{16\}$ in $f^{-1}(\{1\}) = \{1, -1, i, -i\}$. ▲

Zgled: Naj bo $f\colon \mathbb{N} \setminus \{1\} \to \mathbb{N}$ funkcija, ki naravnemu številu n priredi število različnih praštevilskih deliteljev števila n. Tedaj na primer velja

$$\begin{aligned} &f(\{2,3,4,5,6,7,8,9,10\}) = \{1,2\},\\ &f(\{10,30,70,210\}) = \{2,3,4\} \quad \text{in}\\ &f^{-1}(\{1\}) = \{n \in \mathbb{N} : (\exists p \in P \exists m \in \mathbb{N} : n = p^m)\}, \end{aligned}$$

kjer je P množica vseh praštevil. ▲

V zvezi s slikami in praslikami funkcij podajmo za konec razdelka še naslednjo uporabno trditev.

Trditev 2.22. *Naj bo $f\colon A \to B$ funkcija in naj bo $X_1, X_2 \subseteq A$ ter $Y_1, Y_2 \subseteq B$. Tedaj velja naslednje:*

(i) *Če je $X_1 \subseteq X_2$, je $f(X_1) \subseteq f(X_2)$.*

(ii) *Če je $Y_1 \subseteq Y_2$, je $f^{-1}(Y_1) \subseteq f^{-1}(Y_2)$.*

(iii) $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$.

(iv) $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$.

(v) $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$.

(vi) $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$.

(vii) $f(f^{-1}(Y_1)) \subseteq Y_1$.

(viii) $X_1 \subseteq f^{-1}(f(X_1))$.

Dokaz: Dokazi posameznih točk sledijo neposredno iz definicij. Zato si oglejmo le dokaza točk (iii) in (vii), ostale točke pa prepustimo bralcu.

Za dokaz točke (iii) naj bo najprej $b \in f(X_1 \cup X_2)$. Tedaj je $b = f(a)$ za nek $a \in X_1 \cup X_2$. Če je $a \in X_1$, je $b \in f(X_1)$, če pa je $a \in X_2$, je $b \in f(X_2)$. V vsakem primeru je torej $b \in f(X_1) \cup f(X_2)$. S tem smo pokazali vsebovanost $f(X_1 \cup X_2) \subseteq f(X_1) \cup f(X_2)$. Naj bo sedaj $b \in f(X_1) \cup f(X_2)$. Če je $b \in f(X_1)$, obstaja $a \in X_1$, da je $b = f(a)$, če pa je $b \in f(X_2)$, obstaja $a \in X_2$, da je $b = f(a)$. V vsakem primeru torej obstaja $a \in X_1 \cup X_2$, da je $b = f(a)$, torej je $b \in f(X_1 \cup X_2)$. Tako res velja $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$, kot smo trdili.

Dokažimo še točko (vii). Naj bo torej $b \in f(f^{-1}(Y_1))$. Tedaj je $b = f(a)$ za nek $a \in f^{-1}(Y_1)$. Po definiciji množice $f^{-1}(Y_1)$ velja $f(a) \in Y_1$, torej je res $b \in Y_1$. □

Bralec bo s konkrentnimi primeri pokazal, da v točkah (iv), (vii) in (viii) zgornje trditve enakosti v splošnem ne veljajo.

Naloga 2.33. Katere izmed naslednjih relacij iz $A = \{1, 2, 3\}$ v $B = \{a, b, c\}$ so funkcije?

$$f = \{(1, a), (1, b), (2, c)\} \quad g = \{(1, a), (2, a), (3, a)\} \quad h = \{(1, a), (2, c), (3, b)\}.$$

Naloga 2.34. Naj bo $f\colon \mathbb{N} \to \mathbb{N}$ funkcija, ki število n preslika v maksimalno kratnost kakega praštevilskega faktorja števila n. Tako je na primer $f(10) = 1$, $f(24) = 3$ in $f(100) = 2$. Ali je funkcija f injektivna? Je surjektivna?

Naloga 2.35. Naj bo $f\colon \mathbb{R} \setminus \{3\} \to \mathbb{R} \setminus \{2/3\}$ funkcija, podana s predpisom $f(x) = \frac{2x+7}{3x-9}$. Ali je funkcija f injektivna? Je surjektivna? Če je odgovor na obe vprašanji pozitiven, poiščite predpis inverzne funkcije f^{-1}.

Naloga 2.36. Natančno zapišite kdaj neka funkcija $f\colon A \to B$ ni injektivna in kdaj ni surjektivna.

Naloga 2.37. Naj bo A poljubna neprazna množica in naj bo $B \subseteq A$ neka njena podmnožica. Ali je tedaj $\chi_B\colon A \to \{0, 1\}$, kjer je

$$\chi_B(a) = \begin{cases} 1 & ; \quad a \in B \\ 0 & ; \quad \text{sicer} \end{cases},$$

funkcija? Je injektivna? Je surjektivna?

Naloga 2.38. Naj bodo a, b, c in d taka realna števila, da je $a < b$ in $c < d$. Ali tedaj obstaja kaka bijektivna funkcija iz intervala $[a, b]$ na interval $[c, d]$?

Naloga 2.39. Naj bo $A = \{1, 2, 3, 4, 5\}$ in $B = \{a, b, c, d\}$ in naj bo $f\colon A \to B$ neka funkcija. Ali tedaj obstaja funkcija $g\colon B \to A$, da je $f \circ g = id_B$? Kaj pa $g\colon B \to A$, da je $g \circ f = id_A$?

Naloga 2.40. Naj bo A neka neprazna množica. Ali tedaj obstaja funkcija $f\colon A \to A$, za katero je $f \neq id_A$, a kljub temu velja $f \circ f = id_A$? Ali je takšna funkcija f injektivna? Je surjektivna?

Naloga 2.41. Ali obstaja neničelna realna funkcija $f\colon \mathbb{R} \to \mathbb{R}$, da je $(f \circ f)(x) = 0$ za vse $x \in \mathbb{R}$?