Logika in množice

c226358

Andrej Bauer Davorin Lešnik

2018-02-01

Predgovor

Kazalo

Poglavje 1

Matematično izražanje

Tako kot vsaka stroka ima tudi matematika svoj strokovni jezik, ki obsega matematične simbole in izraze ter svojevrsten način izražanja. Matematiki stremimo k popolni natančnosti in nedvoumnosti matematične misli. To je seveda le ideal, ki se mu bolj ali manj približamo, dejanska matematična besedila pa pišemo ljudje za ljudi, zato ni nič nenavadnega, da so prežeta s tradicijo in nepisanimi družbenimi dogovori, ki matematiko oddaljijo od formalnega ideala, a jo tudi naredijo humano. Pred študentom matematike je torej težka naloga, saj se mora hkrati z novo matematiko učiti še nekoliko nenavadnega jezika. V pomoč se zato najprej posvetimo samo formi matematičnega izražanja. In ne zamerite nam, če vam dobrohotno ponudimo še kak nasvet o študiju matematike.

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

Ker je namen tega učbenika postaviti dobre osnove matematičnega izražanja in mišljenja, bomo bolj natančni kot večina matematikov v praksi. Začetnik namreč potrebuje oporo v natančnosti, kasneje, ko razume stvari bolje, pa lahko ubere bližnjice, ki jih bolj izkušeni kolegi uporabljajo, ne da bi to sploh opazili. Sproti bomo opozarjali nanje, kakor tudi na manjše nedoslednosti v matematični praksi, ki izhajajo iz zgodovinskega razvoja matematike.

1.1 Pisave in simboli

Matematična abeceda vsebuje precej več simbolov, kot zgolj običajne črke in številke. Nekatere že poznamo, na primer $=$, $<$, $+$, $\emptyset$, $\cup$, $\cap$, $\int$ in tako naprej, precej jih še bomo spoznali. Poleg tega matematiki uporabljamo različne pisave, kot je prikazano v tabeli 1.1. Na tabli in v zvezku sicer težko ločimo med pokončno, odebeljeno in ležečo pisavo, ali med kaligrafsko in rokopisno, zato nabor pisav omejimo. V tiskanem besedilu se vedno držimo nekaterih pravil glede izbire pisav. Tako posamezne črke a, b, c, $\ldots$, x, y, z pišemo v ležeči pisavi, imena elementarnih funkcij pa pokončno: sin, cos, log, $\ldots$ Šumnikov običajno ne uporabljamo. Včasih z uporabo znakov nakažemo povezavo med dvema objektoma: f je funkcija in F njen integral,

$\mathcal{A}$ je linearna preslikava in A njej pripadajoča matrika itd.

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

Tabela 1.1: Pisave

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

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

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

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

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

Kljub temu obilju črk in oznak posežemo še po drugih abecedah, še posebej grški, zato se jo čimprej naučite! Grške črke skupaj z njihovo izgovorjavo najdete v tabeli 1.2. Prostoročni zapis grških črk se boste naučili v razredu. Pa tudi to matematikom še ni dovolj! V teoriji množic uporabljamo še hebrejske črke alef $\aleph$, bet $\beth$ in gimel $\gimel$.

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

1.2 Izrazi

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

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

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

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

Grška črka		**Izgovorjava**	
velika	*mala*	*v slovenščini*	*v grščini*
A	α	alfa	alfa
B	β	beta	vita
Γ	γ	gama	γama
Δ	δ	delta	delta
E	ϵ, ε	epsilon	epsilon
Z	ζ	zeta	zita
H	η	eta	ita
Θ	θ, ϑ	Θeta	Θita
I	ι	jota	jota
K	κ	kapa	kapa
Λ	λ	lambda	lamda
M	μ	mi	mi
N	ν	ni	ni
Ξ	ξ	ksi	ksi
O	o	omikron	omikron
Π	π, ϖ	pi	pi
P	ρ, ϱ	ro	ro
Σ	σ, ς	sigma	siγma
T	τ	tau̯	taf
Υ	υ	ipsilon	ipsilon
Φ	ϕ, φ	fi	fi
X	χ	hi	χi
Ψ	ψ	psi	psi
Ω	ω	omega	omeγa

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

Tabela 1.2: Grška abeceda.

Poglejmo na primer “množenje ima prednost pred seštevanjem”. Če tega dogovora ne bi imeli, bi bil zapis $3 + 4 \cdot 6$ dvoumen: ali naj najprej seštejemo 3 in 4 ter vsoto pomnožimo s 6, ali pa naj najprej zmnožimo 4 in 6 ter zmnožku prištejemo 3? Da se izognemo nesporazumom, moramo zapisati bodisi $(3 + 4) \cdot 6$ bodisi $3 + (4 \cdot 6)$, a ker so se pred mnogimi leti matematiki dogovorili, da ima množenje prednost pred seštevanjem, smemo v enem od obeh primerov oklepaje izpustiti in prihraniti nekaj črnila. Prav lahko si predstavljamo svet, v katerem bi obveljal drugačen dogovor in bi $3 + 4 \cdot 6$ pomenilo $(3 + 4) \cdot 6$.

Kar smo ravnokar povedali, je bolj pomembno, kot se zdi na prvi pogled. V šoli so vam namreč v glavo hkrati vlivali matematična dejstva in dogovore o matematičnem zapisu, kot da med enimi in drugimi ni nobene razlike. Morda res ni bilo časa za poglobljene pogovore o pisanju oklepajev. Tako marsikdo dobi vtis, da je matematika skupek predpisov, ki jih učencem vsiljujejo učitelji, učbeniki in šolski sistem. Na naučimo ločiti seme od plev. A da ne bomo preveč filozofirali, si poglejmo nekaj dogovorov in navad v zvezi s pisanjem matematičnih izrazov.

Aritmetične operacije $+$, $-$, $\cdot$ in / pišemo kot *medpone*, tako da operacija stoji med obema

operandoma, na primer $x + y$. Kadar zapišemo operator za operand, pravimo, da je *pripona*, na primer faktoriela $x!$. Zapis operatorja je *predpona* če stoji pred operandom, na primer nasprotna vrednost $-x$. Poleg teh poznamo tudi druge zapise: potenciranje pišemo z eksponentom x^y, deljenje z ulomkom $\frac{x}{y}$, kvadratni koren s posebnim simbolom $\sqrt{x}$ itn. Skrajni primer je zapis množenja brez simbola, ko namesto $x \cdot y$ zapišemo kar xy.

Nekatere operacije imajo *prednost* pred drugimi in nekatere *združujejo* levo ali desno. Prednost pove, katera operacija pride prej na vrsto, kadar ni oklepajev: potenciranje ima prednost pred množenjem in množenje pred seštevanjem. Operacija lahko tudi združuje levo ali desno. Na primer, seštevanje $+$ združuje levo, zato je $5 + 2 + 1$ enako $(5 + 2) + 1$. Pri seštevanju to sicer ni pomembno, pri odštevanju pa moramo upoštevati združevanje na levo: $5 - 2 - 1$ je enako $(5 - 2) - 1$ in ne $5 - (2 - 1)$. Potenciranje združuje na desno, saj 2^{3^4} pomeni $2^{(3^4)}$. Nekatere operacije ne združujejo in v takih primerih moramo uporabiti oklepaje.

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

1.3 Slike in diagrami

Matematiki uporabljamo tudi diagrame in slike, slednje predvsem v geometriji in analizi. Z njimi lahko razjasnimo pojme in si pomagamo pri predstavi zapletenih pojmov in konstrukcij, zato so nepogrešljivo orodje. To še posebej velja za poučevanje matematike.

Vendar pa moramo biti pri uporabi slik pazljivi, ker nas lahko zavedejo. Načeloma je možno vsako konstrukcijo in dokaz, tudi v geometriji, izpeljati brez uporabe slik, a takega početja ne priporočamo.

1.4 Vaje

Poglavje 2

Preproste množice

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

Ideja množice kot poljubne zbirke elementov je zavajajoče preprosta, kar so na lastni koži izkusili matematiki na prelomu iz 19. v 20. stoletje. Takrat so že vedeli, da so množice zelo uporabne in da lahko iz njih tvorimo razne vrste matematičnih objektov. A znameniti matematik in filozof Bertrand Russell je odkril paradoks, ki se imenuje po njem, in gre takole. Naj bo R množica vseh množic, ki niso element same sebe. Ali R je element R? Če je R element R, potem iz definicije R sledi, da R ni element R. In če R ni element R, spet iz definicije R sledi, da R je element R. Torej R hkrati je in ni svoj element, kar je protislovje! Russellov paradoks ste morda že spoznali v priljubljeni različici, ki govori o vaškem brivcu, ki brije vse vaščane, ki ne brijejo samih sebe.

Russellov paradoks je povzročil pravo krizo v temeljih matematike. Ker so bile množice nepogrešljivo orodje, jih niso hoteli kar zavreči, po drugi strani pa je bilo treba preprečiti Russellov in druge paradokse, ki so jih še odkrili. Bertrand Russell je predlagal rešitev, ki jo je poimenoval ***teorija tipov***. Russellova teorija tipov je pomembno vplivala na nadaljni razvoj temeljev matematike, sodobna teorija tipov pa je pomembno orodje v računalništvu. Tako kot množice so bili tipi skupki elementov, a so tvorili neskončno hierarhijo, v kateri so bili elementi tipa vedno iz nižjega nivoja hierarhije kot tip, ki so mu pripadali. Za potrebe večine matematike zadostuje že preprostejša dvoslojna hierarhija množic in ***razredov***. Množice smejo biti elementi množic in razredov, razredi pa ne. Russellov paradoks izgine, ker je R razred vseh tistih množic, ki niso same svoj element. Vprašanje, ali je R element samega sebe, tako postane nesmiselno, saj R ni množica. A zaenkrat odložimo podrobnejšo obravnavo razredov in se raje posvetimo osnovnima pojmoma, množica in preslikava.

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

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

množice izračunljivi? To so vprašanja, ki nimajo enoznačnega odgovora. In res je znanih več med seboj nezdružljivih zvrsti teorije množic, ki matematično opredeljujejo različne vidike običajnega razumevanja besede 'množica'. Mi bomo spoznali "standardno" teorijo množic, ki jo uporablja velika večina matematikov.

2.1 Načelo ekstenzionalnosti

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

Pravilo 2.1 (Ekstenzionalnost množic)**.** *Množici sta enaki, če vsebujeta iste elemente.*

Kaj pravzaprav pomeni, da je to "pravilo", "matematični zakon" ali "načelo"? So ga razglasili v parlementu, je to zakon narave, ali morda dogma, ki jo je razglasil profesor na predavanjih? Bodo tisti, ki načela ekstenzionalnosti ne spoštujejo, deležni Lešnikove masti? Ne. Matematični zakoni so *dogovori*, nekakšna pravila matematične igre. V zgodovinskem razvoju matematike so se uveljavili tisti dogovori, ki so bili uporabni v naravoslovju in tehniki, ali pa so v njih matematiki videli notranjo lepoto in lastno uporabno vrednost.

Pravkar smo se dogovorili, da bomo obravnavali matematične objekte množice, ki vsebujejo elemente in da zanje velja načelo ekstenzionalnosti. Namesto besed 'množica' in 'element' bi lahko izbrali tudi kaki drugi besedi, denimo 'zbor' in 'član', ali celo 'morje' in 'riba', s čimer se matematična vsebina pojmov ne bi čisto nič spremenila, čeprav ne gre preveč izzivati svojih stanovskih kolegic in kolegov. Strukturo, lastnosti in povezave med matematičnimi objekti namreč določajo dogovorjeni matematični zakoni in ne besede, s katerimi jih poimenujemo.

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

Vrnimo se k našim množicam. Načelo ekstenzionalnosti nam pove, da lahko množico podamo tako, da natančno opredelimo njene elemente. A to ne pomeni, da množica obstaja, brž ko jo lahko natančno opredelimo! To je pot, ki vodi naravnost do Russelovega paradoksa, saj so elementi paradoksalne množice R natančno opredeljeni. Potrebujemo dodatna pravila, ki določajo dopustne ***konstrukcije množic***. Izbrati jih moramo previdno, da se izognemo težavam.

2.2 Končne množice

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

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

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

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

Fraza "če in samo če" tu pomeni, da velja dvoje:

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

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

Splošna konstrukcija končnih množic poteka takole.

Pravilo 2.2. *Za vse objekte a, b, ..., z je $\{a, b, \ldots, z\}$ množica, katere elementi so natanko objekti a, b, ..., z.*

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

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

liha števila med 3 in 31, ali samo praštevila? Zapis res ni dovolj natančen. Kljub temu tak zapis v praksi uporabljamo, ker v praksi bralec večinoma pravilno ugane, kaj je bilo mišljeno, saj imamo ljudje zelo podobne sposobnosti prepoznavanja vzorcev. Z matematičnega vidika pa to ni dopustno, saj lahko tropičje *vedno* razumemo na več načinov. (Ne verjamete? Naslednji člen v zaporedju $1, 2, 3, \ldots$ je seveda 5, ker je naslednji člen vsota prejšnjih dveh, kot v Fibonaccijevem zaporedju.)

Kot smo že omenili, želimo pojem množice, pri kateri vrstni red elementov ni pomemben. Torej bi morali biti množici $\{1, 2\}$ in $\{2, 1\}$ enaki. Pa je to res? Velja ena od treh možnosti:

1. Iz načela ekstenzionalnosti in konstrukcije množic $\{1, 2\}$ in $\{2, 1\}$ sledi, da sta enaki.
2. Iz načela ekstenzionalnosti in konstrukcije množic $\{1, 2\}$ in $\{2, 1\}$ sledi, da nista enaki.
3. Načelo ekstenzionalnosti in konstrukcije množic $\{1, 2\}$ in $\{2, 1\}$ ne določajo, ali sta enaki.

V prvem primeru bi želeli dokazati enakost. V drugem primeru smo v zagati, saj smo se dogovorili za matematična pravila, ki imajo neželene posledice. V tretjem primeru moramo dodati še kakšne nove zakone o množicah. Na srečo obvelja prva možnost.

Trditev 2.3. *Množici $\{1, 2\}$ in $\{2, 1\}$ sta enaki.*

Dokaz. Dokaz, ki ga bomo zapisali je izjemno podroben in ga v praksi matematik ne bi zapisal, saj je z njegovim branjem več dela, kot če bi naredili sami. Ker pa želimo pokazati, da tudi najbolj trivialna dejstva lahko dokažemo, ga zapišimo.

Izhajati smemo izključno iz naslednji dejstev:

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

Najprej uporabimo načelo ekstenzionalnosti, ki zagotavlja, da sta $\{1, 2\}$ in $\{2, 1\}$ enaki, če imata iste elemente. Dokažimo torej, da imata iste elemente. To naredimo v dveh korakih:

1. Dokažimo, da za vsak element $\{1, 2\}$ dokažemo, da je element $\{2, 1\}$. Naj bo $x \in \{1, 2\}$. Iz definicije množice $\{1, 2\}$ sledi, da je $x = 1$ ali $x = 2$. Obravnavamo dva podprimera:

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

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

2. Dokažimo, da za vsak element $\{2, 1\}$ dokažemo, da je element $\{1, 2\}$.

   Ta korak je povsem podoben prvemu, le da je treba povsod zamenjati 1 in 2. Matematik bi zato na tem mestu zapisal, da je drugi korak podoben prevemu in dokaz zaključil. A tega tokrat ne bomo storili in bomo zapisali popoln dokaz.

   Naj bo $x \in \{2, 1\}$. Iz definicije množice $\{2, 1\}$ sledi, da je $x = 2$ ali $x = 1$. Obravnavamo dva primera:

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

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

Mimogrede, črn kvadratek označuje konec dokaza. Imenuje se tudi "Halmos" po matematiku Paulu Halmosu, ki ga je prvi uporabljal. S podobnim razmislekom, ki ga prepuščamo za vajo, lahko dokažemo, da ni pomembno, ali se element pojavi enkrat ali večkrat.

Naloga 2.4. Podrobno dokažite, da sta množici $\{1, 1, 2\}$ in $\{1, 2\}$ enaki.

V prejšnji nalogi smo zapisali $\{1, 1, 2\}$. Pa je to sploh dovoljeno? Pravilo 2.2 pravi, da lahko iz objektov $a, b, c, \ldots, z$ tvorimo končno množico $\{a, b, \ldots, z\}$. Nikjer ne piše, da smeta biti a in b enaka, zato je upravičeno vprašanje, ali je dovoljeno za a in b vzeti 1. V matematiki vse razumemo dobesedno. V pravilu 2.2 piše "Za vse objekte", torej imamo povsem proste roke. Povedano z drugimi besedami, množico $\{1, 1, 2\}$ smemo tvoriti, ker nikjer ne piše, da morajo biti elementi različni.

V zvezi s pravilom 2.2 se pojavljajo še drugi dvomi. Ali smemo tvoriti množico, ki ima več elementov, kot je črk abecede? Ali bi bilo pravilo še vedno isto, če bi namesto "$a, b, \ldots, z$" zapisali "$a, b, \ldots, j$"? Ali smemo tvoriti množico z nič elementi? Če namreč vstavimo nič elementov, se pravilo glasi "Za vse objekte je $\{\ \}$ množica, katere elementi so natanko objekti," kar je vsaj nenavadno. Iz nesrečnega tropičja se res ne vidi, kaj je in kaj ni dovoljeno. Če poškilite v razdelek 11.1, kjer so našteti "uradni" aksiomih teorije množic, tam pravila o končnih množicah ne boste našli, saj sledi iz treh bolj osnovnih pravil.

Pravilo 2.5. Prazna množica $\emptyset$ *je množica, ki nima elementov.*

Pravilo 2.6. *Za vsak x in y je* **(neurejeni) par** *ali* **dvojec** $\{x, y\}$ *množica, katere elementa sta natanko x in y.*

Pravilo 2.7. *Za vsaki množici A in B je* **unija** $A \cup B$ *množica, ki ima za elemente natanko vse objekte, ki so element A ali element B.*

V pravilu 2.6 smo besedo "neurejeni" zapisali v oklepaju, kar pomeni, da beseda pravzaprav ni pombembna in bi jo lahko tudi izpustili. Se pravi, da "neurejeni dvojec" in "dvojec" pomenita isto. V primeru nejasnosti raje uporabimo daljšo obliko.

Tri nova pravila skupaj nadomestijo pravilo 2.2 in odstranijo marsikateri dvom o uporabi. Prvo pravilo pojasni, da lahko tvorimo množico brez elementov. Poleg oznake $\emptyset$ je za prazno množico smiselno uporabiti tudi zapis $\{\ \}$.

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

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

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

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

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

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

Seveda bi morali dokazati, da so vse te množice enake, a tega ne bomo storili.

Pogosto nam bo prišlo prav, da bomo imeli pri roki množico z enim elementom, pri čemer nam bo vseeno, kaj ta element je. V ta namen postavimo pravilo, ki zagotavlja obstoj množice z enim elementom.

Pravilo 2.8. Standardni enojec *je množica* **1**, *katere edini element je* $()$.

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

Edini element množice **1** smo označili z nenavadnim zapisom $()$. Na tem mestu ne bomo pojasnili, zakaj pišemo tako, radovedneži pa lahko pogledajo v razdelek 2.8. Mimogrede, seveda velja $\mathbf{1} = \{()\}$.

Pravilo 2.8 ni nujno potrebno, saj lahko tvorimo veliko različnih enojcev kar sami $\{\emptyset\}$, $\{42\}$, $\{\{\emptyset\}\}$ itn. Ali je kateri od njih "prvi med enakimi" in bi ga lahko uporabljali kot "standardni" enojec? Ker je odgovor v veliki meri stvar osebnega mnenja, je bolje, da razglasimo pravilo, ki ustoliči standardni enojec. S prazno množico nimamo podobnih težav, saj je ena sama.

2.3 Preslikave

Temelj matematike ne tvorijo le množice, ampak tudi drugi matematični pojmi. Prvi izmed njih je ***preslikava***, oziroma s tujko ***funkcija***.[1] V srednji šoli ste že spoznali nekatere preslikave, kot so na primer linearne preslikave, trigonometrijske funkcije, logaritem itd. Nas pa ne bodo zanimale posamezne preslikave, ali posebne lastnosti preslikav, ampak preslikave na splošno.

Vsaka preslikava ima tri sestavne dele: ***domeno*** ali ***začetno množico***, ***kodomeno*** ali ***ciljno množico*** in ***predpis***. Domeni se pogosto reče tudi ***definicijsko območje***. Če govorimo o preslikavi, ki ima domeno X in kodomeno Y, to ponazorimo s puščico med X in Y, takole

$$X \longrightarrow Y$$

Če želimo preslikavo poimenovati, na primer f, zapišemo

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

[1] Nekateri uporabljajo izraz "funkcija" samo za tiste preslikave, ki slikajo v realna ali kompleksna števila, vendar to navado izpodriva računalništvo, saj funkcije v programskih jezikih nimajo omejitev. Dandanes večina matematikov besedo "funkcija" obravnava kot sopomenko besede "preslikava" in tako jo bomo uporabljali tudi mi.

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

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

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

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

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

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

V teoriji množic razumemo besedo 'predpis' kot kakršnokoli prirejanje med elementi množic domene X in kodomene Y, mora pa veljati:

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

Za vsako množico A je ***identiteta*** na A preslikava

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

ki poljubnemu elementu $x \in A$ priredi x. To je celovito prirejanje, saj vsak $x \in A$ ima prirejeni element, namreč kar x, je pa tudi enolično: če sta y_1 in y_2 prirejena $x \in A$, potem sta oba enaka x in zato enaka drug drugemu.

Za vsaki množici A in B ter $b \in B$ ***konstantna preslikava***

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

priredu vsakemu elementu iz A element b. Sami premislite, da je tako prirejanje celovito in enolično.

2.3.1 Funkcijski predpisi

Predpise lahko podamo na različne načine, najbolj pogost pa je ***funkcijski predpis***, ki se mu še posebej posvetimo in se ob njem naučimo nekaj natančnosti. Funkcijski predpis ima obliko

$$x \mapsto \cdots,$$

ki smo jo že videli maloprej. Na desni, lahko namesto $\cdots$ zapišemo izraz, v katerem se sme pojaviti simbol x, denimo

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

S funkcijskip predpisom zapišemo identiteto in konstantno preslikavo takole:

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

Ni nujno, da se x pojavi, denimo $x \mapsto 42$ vsakemu elementu iz domene priredi število 42. V funkcijskem predpisu se smejo pojaviti tudi drugi simboli, ki jim pravimo ***parametri***. Tako je

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

funkcijski predpis s parametroma a in b, ki elementu x priredi element $a \cdot x + b$.

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

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

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

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

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

niso veljavni funkcijski predpisi.

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

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

sta torej veljavna.

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

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

To preberemo "f slika x v ena plus x na kvadrat." Običajna sta tudi zapisa

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

Funkcijske predpise je podrobno prvi preučeval Alonzo Church,[2] ki je uporabljal zapis

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

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

- v Pythonu pišemo `lambda x : 1+x**2`,
- v Haskellu pišemo `\x -> 1+x**2` in
- v OCamlu pišemo `fun x => 1+x*x`.

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

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

Nekateri starejši zapisi funkcijskih predpisov so slabi, a jih ljudje vztrajno uporabljajo. Opozorimo le na en slab zapis, ki povzroča precej preglavic, ne da bi se matematiki tega zares zavedali. Funkcijski predpis mora določati vezano spremenljivko, sicer ne vemo, kako vstaviti vrednosti, a na žalost jo matematiki pogosto izpustijo skupaj z $\mapsto$, da ostane samo izraz na desni. Težava je v tem, da se lahko v funkcijskem predpisu pojavi več kot en simbol. Če vam na primer povem, da imam v mislih funkcijski predpis

$$a \cdot x + b$$

boste vsi mislili, da je mišljeno $x \mapsto a \cdot x + b$. A pravzprav bi lahko bilo tudi $a \mapsto a \cdot x + b$ ali $b \mapsto a \cdot x + b$ ali celo $t \mapsto a \cdot x + b$! Namreč, nič ni narobe s funkcijskim predpisom, v katerem se pojavijo dodatni simboli.

Morda pa lahko vezano spremenljivko in $\mapsto$ brez škode izpustimo, če v izrazu nastopa samo en simbol, denimo $1 + x^2$? A spet bi zabredli v težave. Je 42 število ali funkcijski predpis $x \mapsto 42$? Je $1 + x^2$ funkcijski predpis $x \mapsto 1 + x^2$ ali $a \mapsto 1 + x^2$?

Velikokrat površno rečemo, da funkcijski predpis podaja preslikavo. To ni res, saj smo že prej povedali, da ima vsaka preslikava tri sestavne dele: domeno, kodomeno in prirejanje. Res, če ne poznamo domene, ne moremo preveriti, ali je funkcijski predpis celovit. Denimo, funkcijski predpis

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

ni celovit, če je domena množica realnih števil, in je celovit, če je domena množica racionalnih števil. Tudi kodomeno moramo poznati, sicer ne moremo določiti nekaterih lastnosti preslikave, kot je na primer surjektivnost, glej razdelek 6.2.

2.3.2 Ostali načini podajanja preslikav

Funkcijski predpisi niso edini način za podajanje prirejanja, zato omenimo še nekatere druge.

Preslikavo s končno domeno lahko podamo s tabelo, na primer:

$$f : \{1, 2, 3, 5\} \to \{10, 20, 30\}$$

1	10
2	10
3	20
5	10

To seveda pomeni, da f elementu 1 priredi 10, 2 priredi 10, 3 priredi 20 in 5 priredi 10. Tabelo lahko predstavimo na različne načine, lahko kar naštejemo vsa prirejanja:

$$f(1) = 10$$
$$f(2) = 10$$
$$f(3) = 20$$
$$f(5) = 10.$$

Tudi

$$1 \mapsto 10$$
$$2 \mapsto 10$$
$$3 \mapsto 20$$
$$5 \mapsto 10.$$

je še vedno le tabela, ki prikazuje prirejanje. Ne sme nas motiti dejstvo, da smo $\mapsto$ uporabili za naštevanje prirejanj, namesto za funkcijski prdpis.

Preslikava je lahko določena tudi z opisom računskega postopka, pravimo mu ***algoritem***, s pomočjo katerega izračunamo vrednost preslikave pri danem argumentu. Paziti moramo, da je opis postopka res natančen in nedvoumen, lahko ga kar zapišemo kot program. Teoretični računalničar bi pripomnil, da je treba pri tem izbrati programski jezik, ki ima ustrezno matematično definicijo.

Preslikave lahko podamo tudi tako, da opišemo pogoje, pri katerih je element kodomene prirejen elementu domene. Na primer, preslikavo $f : \mathbb{N} \to \mathbb{Z}$ bi lahko definirali z zahtevo, da naravnemu številu $n \in \mathbb{N}$ priredimo celo število $k \in \mathbb{Z}$, kadar velja

$$k^2 \leq n < (k+1)^2.$$

To prirejanje je veljavno, če je celovito in enolično, česar ne bomo preverjali, lahko pa poskusite sami. Nekaj prirejanj f prikazuje naslednja razpredelnica:

$0 \mapsto 0$	$4 \mapsto 2$	$8 \mapsto 2$	$12 \mapsto 3$
$1 \mapsto 1$	$5 \mapsto 2$	$9 \mapsto 3$	$13 \mapsto 3$
$2 \mapsto 1$	$6 \mapsto 2$	$10 \mapsto 3$	$14 \mapsto 3$
$3 \mapsto 1$	$7 \mapsto 2$	$11 \mapsto 3$	$15 \mapsto 3$

Ali znate z besedami opisati preslikavo f?

V splošnem je lahko preslikava podana s precej zapleteno konstrukcijo, ki zahteva veliko preverjanja in dokazovanja. Osnovne načine podajanja preslikav bomo spoznali skupaj s konstrukcijami množic.

2.3.3 Aplikacija in substitucija

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

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

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

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

Preslikavo lahko uporabimo na argumentu tudi, če je nismo poimenovali. Na primer, preslikavo $\mathbb{R} \to \mathbb{R}$, podano s funkcijskim predpisom

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

uporabimo na argumentu 3:

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

Se vam zdi tak zapis nenavaden? Verjetno, a pomislite, zakaj je tako: ker običajno preslikave poimenujemo in se nanje vedno sklicujemo z njihovim imenom. Prav nobenega razloga ni, da ne bi s funkcijskimi predpisi delali tako, kot s števili, vektorji in ostalimi matematičnimi objekti, na katere smo že navajeni. Računalničarji radi rečejo, da je treba tudi preslikave obravnavati kot "enakopravne državljane". Prav imajo, zato bomo vadili uporabo funkcijskih predpisov ter z njimi delali, kot da niso nič posebnega, saj niso!

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

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

potem je vrednost $f(3)$ enaka $1 + 3^2$, kar je seveda enako 10, a to zahteva dodaten račun, ki nas v tem trenutku ne zanima. Pravimo, da smo simbol x ***zamenjali*** ali ***substituirali*** s 3, oziroma da smo 3 ***vstavili*** v f namesto x. Seveda lahko vstavimo argument neposredno v funkcijski predpis, zato je aplikacija

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

seveda spet enaka $1 + 3^2$.

Preslikavo smemo uporabiti na poljubnem elementu domene, ki je lahko zapisan na bolj ali manj zapleten način, pri čemer gre še vedno samo za zamenjavo. Na primer, v zgornjo preslikavo f lahko vstavimo $3 + 4$ in dobimo $1 + (3 + 4)^2$ ali pa za neki $u \in \mathbb{R}$ vstavimo $u + 2$ in dobimo $1 + (u + 2)^2$. V razdelku 2.6 bomo spoznali še dodatna pravila za vstavljanje izrazov, ki se vrtijo okoli vezanih spremenljivk.

2.3.4 Načelo ekstenzionalnosti preslikav

Kot smo že omenili, je možih več pogledov na preslikave. Ali je pomembno, kako učinkovito računamo vrednosti preslikave? Vsekakor, ampak ali naj to pomeni, da sta preslikavi različni, če imata enake vrednosti, a je ena podana z učinkovitim pravilom in druga z neučinkovitim? V matematiki je odgovor nikalen.

Pravilo 2.9 (Ekstenzionalnost preslikav)**.** *Preslikavi sta enaki, če imata enaki domeni in kodomeni ter imata za vse argumente enaki vrednosti.*

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

Takoj opozorimo na razliko med

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

saj bi marsikdo trdil, da med njima ni razlike. Levi izraz pravi, da sta $f(x)$ in $g(x)$ enaka elementa množice C, desni pa da sta f in g enaki preslikavi iz A v B. Na sploh je treba razlikovati

med f in $f(x)$, saj to nikakor nista enaka objekta: prvi je preslikava, drugi pa vrednost te preslikave pri x. Verjetno nihče ne bi trdil, da je preslikava cos isto kot cos $\frac{\pi}{4}$, ali ne? Isti razmislek veleva, da cos x ni isto kot cos, če tudi si mislimo, da je x poljuben. Zmeda izhaja iz neprimernega zapisa preslikav. Če bi že od malih nog pravilno uporabljali funkcijske predpise, bi seveda vedeli, da načelo ekstenzionalnosti za preslikave zagotavlja enakost cos in $x \mapsto \cos x$, oba pa sta različna od cos x, ki sploh ni preslikava, ampak neko realno število. Čeprav je število cos x odvisno od parametra x, je še vedno le število.

V bran tradicionalnemu zapisu pa moramo vseeno povedati, da se lahko *dogovorimo* za nekoliko napačen zapis, če to ne povzroča zmede. S tem se izognemu preveč birokratskemu pisanju nebistvenih podrobnosti in lahko bistveno izboljšamo komunikacijo in razumevanje med izkušenimi matematiki. A začetnikom priporočamo, da v dobrobit boljšega razumevanja snovi vsaj na začetku študija raje vztrajajo pri doslednem zapisu.

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

2.4 Zmnožek

Množice lahko ***tvorimo*** ali ***konstruiramo*** iz drugih množic na različne načine. V tem poglavju bomo spoznali tri osnovne konstrukcije, ostale pa kasneje, ko bomo že nekaj vedeli o logiki. Najprej obravnavajmo zmnožek ali kartezični produkt.

Takoj se zastavi vprašanje, kako sploh opisati novo konstrukcijo množic. Načelo ekstenzionalnosti pove, da je množica opredeljena s svojimi elementi. Torej moramo pojasniti, kaj so elementi nove množice, se pravi, kako jih vpeljemo, kaj lahko z njimi počnemo in kakšne so njihove zakonitosti. Natančneje, novo konstrukcijo množic določajo naslednja pravila:

1. pravilo ***tvorbe***, ki vpelje novo množico,
2. pravila ***vpeljave*** elementov, ki podajo operacije, s katerimi gradimo elemente,
3. pravila ***uporabe***, ki podajo opreacije, s katerimi razgradimo ali uporabimo elemente,
4. ***enačbe***, ki opredeljujejo zakonitosti, ki veljajo za operacije vpeljave in uporabe.

Najbolje je, da si postopek ogledamo na primeru.

Pravilo 2.10 (Tvorba zmnožka)**.** *Za vsaki množici A in B je $A \times B$ množica, ki se imenuje* **zmnožek** *ali* **kartezični produkt** *A in B.*

Pravilo tvorbe pove, da lahko tvorimo novo množico $A \times B$, ne pove pa, kakšne elemente ima. To je vsebina naslednjih dveh pravil, ki povesta, kako sestavimo in razstavimo elemente zmnožka.

Pravilo 2.11 (Vpeljava urejenih parov)**.** *Za vse $a \in A$ in $b \in B$ je $(a, b) \in A \times B$. Element (a, b) imenujemo* **urejeni par***.*

Pravilo 2.12 (Uporaba urejenih parov)**.** *Za vsak $p \in A \times B$ je $\pi_1(p) \in A$* **prva projekcija** *in $\pi_2(p) \in B$* **druga projekcija** *elementa p.*

Nazadnje podamo še enačbe.

Pravilo 2.13 (Računsko pravilo za urejene pare)**.** *Za vse $a \in A$, $b \in B$ velja $\pi_1(a,b) = a$ in $\pi_2(a,b) = b$.*

Pravilo 2.14 (Ekstenzionalnost urejenih parov)**.** *Za vse $p, q \in A \times B$ velja: če $\pi_1(p) = \pi_1(q)$ in $\pi_2(p) = \pi_2(q)$, potem $p = q$.*

Računsko pravilo se tako imenuje, ker lahko z njim poenostavljamo izraze, drugo pa je načelo ekstenzionalnosti, ker pravi, da je urejeni par določen s prvo in drugo projekcijo.

Kadar imamo opravka z večimi zmnožki, na primer $A \times B$ in $C \times D$, bi lahko prišlo do zmede glede projekcij. Takrat jih opremimo še z dodatnimi oznakami množic, da razločimo projekciji $\pi_1^{A,B} : A \times B \to A$ in $\pi_1^{C,D} : C \times D \to C$, in podobno za π_2.

Malo bolj naivna konstrukcija zmnožka bi se glasila takole: kartezični produkt $A \times B$ je množica vseh urejenih parov (a,b), kjer je $a \in A$ in $b \in B$. A taka konstrukcija ni popolna, saj ne pove, kaj lahko z urejenim parom počnemo. Kako naj vemo, da iz (a,b) lahko izluščimo a in b, in kako preverimo, ali sta dva urejena para enaka? Če takih zadev ne določimo, bi lahko kdo mislil, da je urejeni par kaka druga operacija, denimo seštevanje, unija, ali kdovekaj.

Dejstvo, da je vsak element zmnožka množic urejen par, in to celo na en sam način, lahko dokažemo.

Trditev 2.15. *Naj bosta A in B množici. Za vsak element $p \in A \times B$ obstaja natanko en $a \in A$ in natanko en $b \in B$, da velja $p = (a,b)$.*

Dokaz. Naj bosta A in B množici in $p \in A \times B$. Najprej pokažimo, da p res je enak nekemu urejenemu paru, namreč

$$p = (\pi_1(p), \pi_2(p)).$$

Uporabimo načelo ekstenzionalnosti za pare, ki nam zagotavlja to enačbo, če dokažemo

$$\pi_1(p) = \pi_1(\pi_1(p), \pi_2(p)) \qquad \text{in} \qquad \pi_2(p) = \pi_2(\pi_1(p), \pi_2(p)).$$

Ti dve enačbi pa veljata, ker sta primerka računskih pravil za pare.

Preveriti moramo še, da je $(\pi_1(p), \pi_2(p))$ edini urejeni par, ki je enak p. Povedano z drugimi besedami, dokazati moramo: če je $p = (a,b)$ za neki $a \in A$ in $b \in B$, potem velja $a = \pi_1(p)$ in $b = \pi_2(p)$. Pa denimo, da bi za neki $a \in A$ in $B \in B$ veljalo $p = (a,b)$. Tedaj bi lahko uporabili računska pravila za pare in dobili

$$\pi_1(p) = \pi_1(a,b) = a \qquad \text{in} \qquad \pi_2(p) = \pi_2(a,b) = b,$$

kar smo želeli dokazati. □

Trditev je prikladna, ko želimo podati funkcijsko pravilo za preslikavo, katere domena je zmnožek množic. Primer take preslikave je

$$\begin{aligned} \mathbb{R} \times \mathbb{R} &\to \mathbb{R} \\ p &\mapsto \pi_1(p) + \pi_2(p)^2 \cdot \pi_1(p). \end{aligned}$$

Ta zapis je precej nepregleden, a sledili smo navodilu, da mora stati na levi strani funkcijskega predpisa simbol. Prejšnja trditev nam zagotavlja, da lahko vsak element $\mathbb{R} \times \mathbb{R}$ na en sam

način izrazimo kot urejeni par (x, y), in zato ne bo nič narobe, če zapišemo ta isti funkcijski predpis bolj pregledno tako, da upoštevamo, da je p enak (x, y) za enolično določena x in y:

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

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

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

Za tako preslikavo pravimo, da je "funkcija dveh spremenljivk", ker si mislimo, da smo podali argumenta x in y ločeno drug od drugega. Tu pravzaprav vidimo, da bi lahko rekli tudi, da je funkcija dveh spremenljivk pravzaprav običajna funkcija, katere arugmenti so urejeni pari.

Poleg zmnožka dveh množic bi lahko tvorili tudi zmnožek treh ali več množic. Pravila bodo podobna kot za zmnožek dveh množic, le da bi namesto urejenih parov tvorili ***urejene večterice*** in da bi imeli več projekcij. Za vsako projekcijo bi zapisali eno računsko pravilo, princip ekstenzionalnosti pa bi bil tudi podoben tistemu za urejene pare. Podorobnosti prepustimo za vajo.

2.5 Vsota

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

Pravilo 2.16 (Vsota)**.** *Za vsaki množici A in B je $A + B$ množica, ki se imenuje* **vsota** *ali* **koprodukt** *množic A in B.*

Pravilo 2.17 (Vpeljava elementov vsote)**.** *Za vsaki množici A in B velja:*

1. *za vsak $a \in A$ je $\iota_1(a) \in A + B$,*
2. *za vsak $b \in B$ je $\iota_2(b) \in A + B$.*

S pravilom vpeljave smo pojasnili, da uporabljamo oznaki ι_1 in ι_2, prvo za elemente iz A in drugo za elemente iz B. Oznakama pravimo tudi ***injekciji***[3] in sta preslikavi

$$\iota_1 : A \to A + B \qquad \text{and} \qquad \iota_2 : B \to A + B.$$

Kadar imamo opravka z večimi vsotami, na primer $A + B$ in $C + D$, bi lahko prišlo do zmede glede oznak. Takrat injekcije opremimo še z dodatnimi oznakami množic, da razločimo injekciji $\iota_1^{A,B} : A \to A + B$ in $\iota_1^{C,D} : C \to C + D$, in podobno za ι_2.

Potrebujemo še pravili za uporabo in enakost elementov vsote, ki ju združimo v eno samo pravilo.

[3]Pravzaprav niti ni pomembno, kako poimenujemo oznaki, da sta le različni. V funkcijskem programiranju, kjer poznamo vsote podatkovnih tipov, programer sam določi, kakšne oznake bo uporabljal za injekcije.

Pravilo 2.18. *Za vsaki množici A in B in za vsak $u \in A + B$, bodisi obstaja natanko en $a \in A$, da je $u = \iota_1(a)$, bodisi obstaja natanko en $b \in B$, da je $u = \iota_2(b)$.*

Fraza "bodisi ... bodisi" pomeni, da je vsak element $u \in A + B$ enak $\iota_1(a)$ za natanko en $a \in A$ ali $\iota_2(b)$ za natanko en $b \in B$, ne more pa se zgoditi oboje hkrati ali nič od tega. Torej $\iota_1(a) = \iota_2(b)$ ne drži in celo v primeru, ko je $A = B$ in $a = b$, je $\iota_1(a) \neq \iota_2(b)$. S tem smo v $A + B$ res ločili elemente A od elementov B. Fraza "natanko en" pove, da iz $u = \iota_1(a_1)$ in $u = \iota_1(a_2)$ sledi $a_1 = a_2$. Povedano drugače, če velja $\iota_1(a_1) = \iota_1(a_2)$, potem je $a_1 = a_2$. Podobno iz $\iota_2(b_1) = \iota_2(b_2)$ sledi $b_1 = b_2$. Podajmo prepost primer, ki verjetno marsikaj pojasni:

$$\{a, b, c\} + \{a, d, e\} = \{\iota_1(a), \iota_1(b), \iota_1(c), \iota_2(a), \iota_2(d), \iota_2(e)\}.$$

Kako definiramo preslikavo $A + B \to C$? Ker je vsak element domene $A + B$ bodisi $\iota_1(a)$ za neki $a \in A$ bodisi $\iota_2(b)$ za neki $b \in B$, *obravnavamo oba primera*. Tako funkcijski zapis za preslikavo $A + B \to C$ zapišemo kot

$$u \mapsto \begin{cases} \cdots a \cdots & \text{če } u = \iota_1(a), \\ \cdots b \cdots & \text{če } u = \iota_2(b), \end{cases}$$

kjer smemo v $\cdots a \cdots$ zapisati izraz, ki vsebuje simbol a, in v $\cdots b \cdots$ izraz, ki vsebuje simbol b. Ker je tak zapis nekoliko neroden, se dogovorimo, da ga lahko zapišemo tudi s *večdelnim* funkcijskim predpisom:

$$\begin{aligned} \iota_1(a) &\mapsto \cdots a \cdots, \\ \iota_2(b) &\mapsto \cdots b \cdots. \end{aligned}$$

Če želimo preslikavo poimenovati, zapišemo

$$\begin{aligned} f : A + B &\to C, \\ f(\iota_1(a)) &= \cdots a \cdots \\ f(\iota_2(b)) &= \cdots b \cdots. \end{aligned}$$

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

$$\begin{aligned} (A + B) \times C &\to B + A \\ (\iota_1^{A,B}(a), c) &\mapsto \iota_2^{B,A}(a) \\ (\iota_2^{A,B}(b), c) &\mapsto \iota_1^{B,A}(b) \end{aligned}$$

je celovit in enoličen, medtem ko predpis

$$\begin{aligned} (A \times A) + B &\to A \\ \iota_1(a_1, a_2) &\mapsto a_2 \end{aligned}$$

ni veljaven, ker ni celovit, saj manjka primer $\iota_2(b) \mapsto \cdots$.

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

2.6 Eksponent

Denimo, da sta A in B množici. Tedaj lahko obravnavamo preslikave

$$A \to B$$

z domeno A in kodomeno B. Ali vse take preslikave tvorijo množico? Russellov paradoks nas je izučil, da moramo pazljivo postaviti pravila za konstrukcije množic, nato pa jih strogo držati. Pravila, ki smo jih podali do sedaj, ne zagotavljajo knostrukcije množic vseh preslikav iz A v B. Potrebujemo novo pravilo.

Pravilo 2.19 (Eksponent)**.** *Za vsaki množici A in B ima* **eksponent** *ali* **eksponentna množica** B^A *za elemente natanko vse preslikave iz A v B.*

Potemtakem je zapis $f : A \to B$ enakovreden zapisu $f \in B^A$.

Pravila, ki opredeljujejo elemente množice B^A smo že spoznali. Pravilo vpeljave pravi, da je preslikava podana z domeno, kodomeno ter celovitim in enoličnim prirejanjem med njima. Pravilo uporabe je kar aplikacija: če je $f \in B^A$ in $a \in A$, lahko tvorimo $f(a) \in B$. Tudi računsko pravilo za preslikave smo že spoznali, saj je to kar pravilo zamenjave: funkcijski predpis uporabimo na argumentu tako, da vezano spremenljivko v predpisu zamenjamo z argumentom. In ekstenzionalnost preslikav pove, kdaj sta dve preslikavi enaki.

Preslikavi, ki sprejme kot argument preslikavo, pravimo ***funkcional*** ali ***preslikava višjega reda***. Primer take preslikave je ***kompozicija***:

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

Pišemo jo kot operacijo, torej $g \circ f$ namesto $\circ(g, f)$. V zgornjem zapisu smo uporabili eksponente, a v tem primeru je bolj pregleden diagram:

$$A \xrightarrow{f} B \xrightarrow{g} C, \quad A \xrightarrow{g \circ f} C$$

Zakaj smo $\circ$ definirali tako, da kompozicijo f in g pišemo $g \circ f$ namesto $f \circ g$? Ker si je mnogo lažje zapomniti računsko pravilo

$$(g \circ f)(x) = g(f(x)),$$

ki velja z našo definicijo, kot pa $(f \circ g)(x) = g(f(x))$, kar bi veljalo, če bi zamenjali vlogi f in g.

Trditev 2.20.

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

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

Takoj vidimo, da je A množica, sicer zapis id_A ne bi bil smiselen, in podobno je tudi B množica. Simboli f, g in h zagotovo označujejo preslikave, saj nastopajo v kompoziciji. Kaj pa

njihove domene in kodomene? Preslikava f mora imeti domeno A, sicer ne bi bilo dovoljeno komponirati $f \circ \mathrm{id}_A$, in mora imeti kodomeno B, sicer ne bi bilo dovoljeno komponirati $\mathrm{id}_B \circ f$. Ostaneta še domeni in kodomeni preslikav g in h. Kompozicija $g \circ f$ kaže, da mora biti domena g enaka kodomeni f, torej B. Kompozicija $h \circ g$ pa pove, da je kodomena C enaka domeni h. Če vse to zložimo v diagram, dobimo

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

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

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

Preverimo, ali smo trditev pravilno razumeli. Ko vstavimo podrobnosti, se prvi del glasi: "Za vse množice A in B ter preslikavo $f : A \to B$ velja $\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A$." Ker je to smiselna izjava, jo dokažimo. Enakost preslikav se dokaže z ekstenzionalnostjo preslikav, torej preverimo, ali imajo $\mathrm{id}_B \circ f$, f in $f \circ \mathrm{id}_A$ enako vrednost za poljuben $x \in A$:

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

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

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

Kompozicijo smo zapisali z *vgnezdenim* funkcijskim predpisom, ki argumentu priredi preslikavo, ki je spet podana s funkcijskim predpisom. V splošnem je vgnezdeni funkcijski predpis oblike

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

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

Pri računanju s preslikavami višjega reda včasih hkrati obravnavamo več funkicjskih predpisov in lahko pride do zmede, če za vse uporabimo isto vezano spremenljivko. Na primer, kompozitum preslikav

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

bi lahko izračunali takole:

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

Tu imamo tri pojavitve x, ki bi jih morali ločiti, ker vsaka nastopa kot vezana spremenljivka v svojem funkcijskem predpisu. Še posebej nejasen je računski korak $(x \mapsto (x \mapsto x^2 - 4)(2 - x)) = (x \mapsto (2 - x)^2 - 4)$, ko vezano spremenljivko x v funkcijskem predpisu zamenjamo z izrazom $2 - x$, ki tudi vsebuje x. To sta dva različna x-a! Spomnimo se, da lahko vezane spremenljivke vedno preminujemo. Ponovimo račun, a tokrat tako, da imajo različni funkcijski predpisi različne vezane spremenljivke. Kompozitum

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

izračunamo takole:

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

To je dosti bolj pregledno. Da ne bo prihajalo do zapletov z vezanimi spremenljivkami, se dogovorimo: *kadar imamo opravka z večimi vezanimi spremenljivkami, jih vedno preimenujemo tako, da so med seboj različne.*

Funkcionale srečamo v analizi in funkcijskem programiranju. Limita zaporedja je funkcional, ker sprejme kot argument zaporedje realnih števil, se pravi element $\mathbb{R}^{\mathbb{N}}$, in mu priredi realno število. Odvod je funkcional, ki sprejme element $\mathbb{R}^{\mathbb{R}}$ in mu priredi element $\mathbb{R}^{\mathbb{R}}$. Če smo povsem natančni, limita kot preslikava $\mathbb{R}^{\mathbb{N}} \to \mathbb{R}$ ni celovit funkcional, ker nekatera zaporedja ne konvergirajo. Prav tako odvod kot preslikave $\mathbb{R}^{\mathbb{R}} \to \mathbb{R}^{\mathbb{R}}$ ni celovit, ker nekatere preslikave niso odvedljive. Preslikavam, ki niso celovite, pravimo *delne* in o njih bomo več povedali v razdelku **??**.

2.7 Izomorfizem množic

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

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

Definicija 2.21. Množici A in B sta ***izomorfni*** in pišemo $A \cong B$, kadar obstajata preslikavi

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

za kateri velja

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

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

Preverimo, da velja $A \times B \cong B \times A$ za poljubni množici A in B. To storimo tako, da zapišemo preslikavi med zmnožkoma in preverimo, da tvorita izomorfizem:[4]

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

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

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

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

Zgled 2.22. Primere izmorfizmov poznamo že iz srednje šole. Naj bo $\mathbb{R}$ množica vseh realnih števil (glej razdelek 9.4) in $\mathbb{R}_{>0}$ množica vseh pozitivnih realnih števil. Tedaj logaritem in eksponentna funkcija,

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

tvorita izomorfizem, saj za $x \in \mathbb{R}$ velja $\log(\exp x) = x$ in za $y \in \mathbb{R}_{>0}$ velja $\exp(\log y) = y$. Eksponentna funkcija seštevanje slika v množenje: $\exp 0 = 1$ in $\exp(x + y) = \exp x \cdot \exp y$, zato ni samo izomorfizem med množicama, ampak celo izomorfizem med grupama $(\mathbb{R}, +, 0)$ in $(\mathbb{R}_{>0}, \cdot, 1)$.

Če ne veste, kaj je grupa in izomorfizem grup, nikar ne obupavajte. Vsak matematik se v vsakdanjem delu nenehno srečuje z neznanimi pojmi. Veste, da je znameniti profesor France Križanič[5] v enega od svojih učbenikov zapisal, da naj tisti, ki mu je branje dokazov odveč, ravna tako kot Du Fu:[6]

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

Naloga 2.23. Odkorakajte v knjižnico, izposodite si knjigo profesorja Križaniča in jo preberite.

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

Trditev 2.24. *Če je $f : A \to B$ izomorfizem med množicama A in B ter sta preslikavi $g : B \to A$ in $h : B \to A$ obe obrata f, potem je $g = h$.*

[4] Držimo se pravila, da nikoli ne uporabimo iste vezane spremenljivke dvakrat, zato pravilo za f zapišemo z x in y in pravilo za g z v in u. Marsikdo bi oba funkcisjka predpisa zapisal z x in y, torej $f : (x, y) \mapsto (y, x)$ in $g : (y, x) \mapsto (x, y)$. To zmede nekatere študente, ker mislijo, da "sta je x v definiciji f isti kot v definiciji g", karkoli že naj bi to pomenilo. Poudarimo še enkat: vezana spremenljivka v funkcijskem predpisu nima nikakršne zveze z nobeno drugo pojavitvijo iste spremenljivke kje druge.

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

[6] Du Fu (712–770 pr. n. š), kitajski pesnik

Dokaz. Ker je g obrat f, velja

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

in ker je h obrat f, velja

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

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

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

□

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

Oznaka za obrat je nekoliko nerodna, ker se prekriva z zapisom za obratno vrednost števila: če je $x \in \mathbb{R}$ neničelno realno število, potem je x^{-1} tisto realno število, za katerega velja $x \cdot x^{-1} = 1$. Torej moramo paziti: če je $f : \mathbb{R} \to \mathbb{R}$ izomorfizem in $x \in \mathbb{R}$, je $(f(x))^{-1}$ obrat števila $f(x)$, medtem ko je $f^{-1}(x)$ število, ki ga dobimo, ko obrat preslikave f uporabimo na x. Sami premislite, kaj je $(f^{-1}(x))^{-1}$.

Naloga 2.25. Podajte primer izomorfizma $f : \mathbb{R} \to \mathbb{R}$ in števila $x \in \mathbb{R}$, da velja $f^{-1}(x) = (f(x))^{-1}$. Nato podajte še primer, ko velja $f^{-1}(x) \neq (f(x))^{-1}$.

Naloga 2.26. Ozrimo se še enkrat na dokaz prejšnje trditve. Ali smo uporabili vse štiri predpostavke? Zapišite *bolj splošno trditev*, se pravi tako, ki navede samo tiste predpostavke, ki jih res potrebujemo v dokazu.

Trditev 2.27. *Za vse izmorfizme $f : A \to B$ in $g : B \to C$ velja*

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

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

Trditev 2.28. *Za vse množice A, B in C velja:*

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

Dokaz.

1. id_A je izomorfizem iz A v A, ki je sam svoj obrat,

2. če je $f : A \to B$ izomorfizem iz A v B, potem je f^{-1} izomorfizem iz B v A in f,

3. če je $f : A \to B$ izomorfizem iz A v B in $g : B \to C$ izomorfizem iz B v C, potem je $g \circ f$ izomorfizem iz $A \to C$. □

Trditev 2.29. *Preslikava ima največ en inverz.*

Naloga 2.30. Pogosto rečemo, da sta seštevanje in odštevanje obratni operaciji. Strogo vzeto, ti dve operaciji nista obratni kot preslikavi, saj obe slikata (recimo, da ju gledamo na realnih številih) $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$, tj. ne slikata v nasprotnih smereh. Ugotovi, v kakšnem smislu točno sta seštevanje in odštevanje obratni, tj. kateri dve preslikavi sta pravzaprav druga drugi obratni.

2.8 Algebra množic

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

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

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

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

Izrek 2.31. *Za vse množice A, B in C velja:*

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

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

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

Asociativnost

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

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

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

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

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

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

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

$$\begin{aligned} &f : A + (B + C) \to (A + B) + C && \qquad g : (A + B) + C \to A + (B + C) \\ &f : \iota_1^{A,B+C}(x) \mapsto \iota_1^{A+B,C}(\iota_1^{A,B}(x)) && \qquad g : \iota_1^{A+B,C}(\iota_1^{A,B}(u)) \mapsto \iota_1^{A,B+C}(u) \\ &f : \iota_2^{A,B+C}(\iota_1^{B,C}(y)) \mapsto \iota_1^{A+B,C}(\iota_2^{A,B}(y)) && \qquad g : \iota_1^{A+B,C}(\iota_2^{A,B}(v)) \mapsto \iota_2^{A,B+C}(\iota_1^{B,C}(v)) \\ &f : \iota_2^{A,B+C}(\iota_2^{B,C}(z)) \mapsto \iota_2^{A+B,C}(z) && \qquad g : \iota_2^{A+B,C}(w) \mapsto \iota_2^{A,B+C}(\iota_2^{B,C}(w)) \end{aligned}$$

Isti zapis brez oznak množic je precej bolj čitljiv:

$$\begin{aligned} &f : A + (B + C) \to (A + B) + C && \qquad g : (A + B) + C \to A + (B + C) \\ &f : \iota_1(x) \mapsto \iota_1(\iota_1(x)) && \qquad g : \iota_1(\iota_1(u)) \mapsto \iota_1(u) \\ &f : \iota_2(\iota_1(y)) \mapsto \iota_1(\iota_2(y)) && \qquad g : \iota_1(\iota_2(v)) \mapsto \iota_2(\iota_1(v)) \\ &f : \iota_2(\iota_2(z)) \mapsto \iota_2(z) && \qquad g : \iota_2(w) \mapsto \iota_2(\iota_2(w)) \end{aligned}$$

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

Preslikave in enojec

Preslikavi

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

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

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

Lahko bi rekli, da je $\mathbf{1}$ nevtralni element za zmnožek *do izomorfizma natančno*, s čimer povemo, da ne velja *enakost* $A \times \mathbf{1} = A$, ampak le *izomorfizem* $A \times \mathbf{1} \cong A$. Na tem mestu lahko tudi

pojasnimo nenavadni zapis edinega elementa $\mathbf{1}$. Elementi zmnožka dveh množic so urejene dvojice, zmnožka treh množic urejene trojice itd. Zmnožek nič množic je nevtralni element za množenje, torej so njegovi elementi urejen ničterice, oziroma urejena ničterica $()$, ker je ena sama.

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

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

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

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

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

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

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

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

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

Preslikave in prazna množica

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

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

Trditev 2.32. *Za vsako množico A obstaja natanko ena preslikava $\emptyset \to A$.*

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

Izomorfizmi in eksponenti

Nazadnje se posvetimo še zakonu $A^{B\times C} \cong (A^B)^C$. Preverimo, da preslikavi[7]

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

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

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

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

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

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

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

2.9 Vaje

Vaja 2.1. Kaj veste povedati o množici A, če zanjo velja, da so vsi njeni elementi enaki?

Vaja 2.2. Načelo ekstenzionalnosti preslikav bi lahko zapisali tudi takole:

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

Dokažite, da je ta različica enakovredna običajnem načelu ekstenzionalnosti.

Vaja 2.3. Zapišite pravila za zmnožek treh množic. Nato premislite še, kako bi podali pravila za zmnožek n množic, kjer je n naravno število.

Vaja 2.4. Naštejte vse elemente množice $\mathbf{1} + \mathbf{1} + \mathbf{1}$.

Vaja 2.5. Preveri tiste izomorfnosti iz izreka 2.31, ki jih v razdelku 2.8 nismo utemeljili.

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

Poglavje 3

Logika

3.1 Logični simboli

Preproste izjave, kot na primer "*n je sodo število.*", že znamo zapisati s simboli: $2 \mid n$. Povečini pa delamo z bolj kompleksnimi, sestavljenimi izjavami. Tudi za te obstaja simbolni zapis; na primer, izjavo "*Če je n sodo število, je tudi kvadrat števila n sod.*", zapišemo kot $2 \mid n \implies 2 \mid n^2$. Seveda ta izjava velja za vsa naravna števila (znaš to dokazati?). To zapišemo takole: $\forall n \in \mathbb{N}. (2 \mid n \implies 2 \mid n^2)$. V tem razdelku si bomo ogledali, kako povezati preprostejše izjave v bolj sestavljene in kako to v splošnem simbolno zapisati.

Kot smo navajeni iz naravnih jezikov, posamične stavke povežemo v sestavljeno poved z *vezniki*. Najpogosteje uporabljeni matematični vezniki so v tabeli 3.1.

Izjavni veznik	Oznaka	Kako preberemo
negacija	$\neg p$	ne p
konjunkcija	$p \wedge q$	p in q
disjunkcija	$p \vee q$	p ali q
implikacija	$p \Rightarrow q$	če p, potem q
ekvivalenca	$p \Leftrightarrow q$	p natanko tedaj, ko q

Tabela 3.1: Standardni izjavni vezniki

Opomba 3.1. V matematiki se za izjavne veznike običajno uporabljajo zgoraj navedene tujke, ampak vsaka od njih seveda ima svoj pomen. Dobesedni prevodi teh tujk so:

- negacija $\rightarrow$ zanikanje,
- konjunkcija $\rightarrow$ vezava,
- disjunkcija $\rightarrow$ ločitev,
- implikacija $\rightarrow$ vpletenost,
- ekvivalenca $\rightarrow$ enakovrednost.

Za primerjavo: spomnite se vezalnega in ločnega priredja iz slovenščine!

Zgled 3.2. Naj p označuje stavek "*Zunaj dežuje.*" in q stavek "*Vzamem dežnik.*". Tedaj $\neg p$ pomeni "*Zunaj ne dežuje.*" in $p \Rightarrow q$ pomeni "*Če zunaj dežuje, potem vzamem dežnik.*".

Kose sestavljene izjave lahko veže več kot en veznik. V tem primeru se (tako kot pri računanju s števili) dogovorimo o prednosti veznikov. Po dogovoru je vrstni red veznikov tak, kot v tabeli 3.1, tj. najmočneje veže negacija, nato konjunkcija, nato disjunkcija, nato implikacija, nato ekvivalenca. Kadar želimo, da se najprej izvede veznik z nižjo prednostjo, uporabimo oklepaje.

Zgled 3.3. Označimo sledeče stavke:

p ..... "*Imam čas.*"
q ..... "*Ostanem doma.*"

Tedaj $\neg p \wedge q$ pomeni isto kot $(\neg p) \wedge q$, to je "*Nimam časa in ostanem doma.*", medtem ko $\neg(p \wedge q)$ pomeni "*Ni res, da imam čas in ostanem doma.*".

(Če komu pade na pamet primer boljših stavkov, je zaželjeno, da popravi... –Davorin)

Poleg zgoraj navedenih izjavnih veznikov se včasih uporabljajo še sledeči (tabela 3.2).

Izjavni veznik	Oznaka	Kako preberemo
stroga disjunkcija	$p \veebar q$	bodisi p bodisi q
Shefferjev[1] veznik	$p \uparrow q$	ne hkrati p in q
Łukasiewiczev[2] veznik	$p \downarrow q$	niti p niti q

Tabela 3.2: Nekateri nadaljnji izjavni vezniki

Za strogo disjunkcijo (tudi: ekskluzivna disjunkcija, izključitvena disjunkcija) se uporabljajo še druge oznake: $p \oplus q$, $p + q$. Razlika med navadno in strogo disjunkcijo je sledeča: $p \vee q$ pomeni, da *vsaj eden* od p in q velja, medtem ko $p \veebar q$ pomeni, da velja *natanko eden*.

Zgled 3.4. Stavek "*Pisni del predmeta je potrebno opraviti s kolokviji ali pisnim izpitom.*" je primer navadne disjunkcije (seveda se vam prizna pisni del predmeta tudi, če uspešno odpišete tako kolokvije kot pisni izpit), stavek "*Grem bodisi na morje bodisi v hribe.*" pa je primer stroge disjunkcije (ne da se biti na dveh mestih hkrati).

Pogosto veznike iz tabele 3.2 (in vse preostale, ki jih nismo navedli) kar izrazimo s standardnimi na sledeči način.

Izjavni veznik	Nekatere izražave s standardnimi vezniki	
$p \veebar q$	$(p \vee q) \wedge \neg(p \wedge q)$	$(p \wedge \neg q) \vee (\neg p \wedge q)$
$p \uparrow q$	$\neg(p \wedge q)$	$\neg p \vee \neg q$
$p \downarrow q$	$\neg(p \vee q)$	$\neg p \wedge \neg q$

Včasih pa vendarle raje delamo neposredno z dodatnimi vezniki. Služijo lahko kot koristna okrajšava, so pa še drugi razlogi. Na primer, stroga disjunkcija igra vlogo seštevanja v Boolovem kolobarju (glej (razdelek o Boolovih kolobarjih)), Shefferjev in Łukasiewiczev veznik pa se uporabljata pri preklopnih vezjih, saj je z vsakim od njiju možno izraziti vse izjavne veznike (glej vajo 3.11). V računalništvu imajo ti trije vezniki standardne oznake XOR, NAND, NOR.

(Nekje tukaj povejmo, kakšno prednost damo tem trem veznikom v primerjavi s standardnimi. Kateremu dogovoru sledimo? –Davorin)

[1] Henry Maurice Sheffer (1882 – 1964) je bil ameriški logik.
[2] Jan Łukasiewicz (beri: ụukaśjêvič) (1878 – 1956) je bil poljski logik in filozof.

Včasih so izjave odvisne od kakšnih parametrov. Na primer, naj $\phi(x)$ pomeni "*x je zelen.*"; tedaj $\phi(\text{trava})$ pomeni "*Trava je zelena.*". Simbol ϕ torej predstavlja lastnost določenih objektov. Takšne primere smo imeli že v razdelku **??**, kjer smo navedli oznako za podmnožico tistih elementov, ki zadoščajo dani lastnosti.

Lastnosti, odvisne od spremenljivk, lahko *kvantificiramo* po njihovih spremenljivkah, tj. povemo, "kako pogosto" velja lastnost. Tabela 3.3 podaja najpogosteje uporabljane kvantifikatorje in njihove oznake.

Kvantifikator	Oznaka	Kako preberemo
univerzalni kvantifikator	$\forall x \in X. \phi(x)$	za vsak x iz X velja lastnost ϕ
eksistenčni kvantifikator	$\exists x \in X. \phi(x)$	obstaja x iz X z lastnostjo ϕ
(enolični eksistenčni kvantifikator?)	$\exists! x \in X. \phi(x)$	obstaja natanko en x iz X z lastnostjo ϕ

Tabela 3.3: Kvantifikatorji

Oznaki $\forall$ in $\exists$ sta narobe obrnjena A in E in izhajata iz nemščine (**a**ll, **e**xistiert).

Seveda je tudi kvantificirana spremenljivka nema in jo lahko poljubno preimenujemo. Izjavi $\forall x \in X. \phi(x)$ in $\forall y \in X. \phi(y)$ povesta natanko isto: vsi elementi množice X imajo lastnost ϕ.

Zgled 3.5. Vemo, da za vsako nenegativno realno število obstaja enolično določen nenegativen kvadratni koren; to izjavo lahko zapišemo na sledeči način.

$$\forall a \in \mathbb{R}_{\geq 0}. \exists! b \in \mathbb{R}_{\geq 0}. b^2 = a$$

Zaradi tega lahko definiramo kvadratni koren kot funkcijo $\sqrt{\ } : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ (več o tem kasneje).

Po dogovoru kvantifikatorji vežejo močneje kot izjavni vezniki. Izjavo, da je vsako celo število bodisi sodo bodisi liho, torej zapišemo takole.

$$\forall a \in \mathbb{Z}. (2 \mid a \veebar 2 \mid (a-1))$$

Zgled 3.6. Za poljubno naravno število $n \in \mathbb{N}$ naj $P(n)$ označuje izjavo, da je n praštevilo. Torej, P definiramo takole.

$$P(n) := \forall x \in \mathbb{N}_{\geq 1}. (x \mid n \implies x = 1 \veebar x = n)$$

(Premisli, kaj bi se zgodilo, če bi namesto stroge disjunkcije vzeli navadno. Bi še vedno dobili pravilni pojem praštevila?)

Naj $S(n)$ označuje, da je n sestavljeno število.

$$S(n) := \exists x, y \in \mathbb{N}_{(1,n)}. x \cdot y = n$$

(Kadar imamo več zaporednih kvantifikatorjev iste vrste, jih po dogovoru lahko strnemo kot zgoraj. Dana formula za $S(n)$ je krajši zapis za $\exists x \in \mathbb{N}_{(1,n)}. \exists y \in \mathbb{N}_{(1,n)}. x \cdot y = n$.)

Zdaj lahko na pregleden način zapišemo, da je vsako naravno število od 2 naprej bodisi praštevilo bodisi sestavljeno.

$$\forall n \in \mathbb{N}_{\geq 2}. (P(n) \veebar S(n))$$

3.2 Definicije

(Predlagam, da v definicijah konsistentno uporabljamo 'kadar' namesto 'če' ("Funkcija je zvezna, kadar velja to in to."). V definicijah gre za ekvivalenco, ne implikacijo. –Davorin)

(Verjetno je smiselno v tem razdelku razložiti definicijsko enakost := (oz. =:). Če se tako odločimo, odstranimo zgornje uporabe teh simbolov. –Davorin)

(uvod)

3.3 Izjavni vezniki

V razdelku 3.1 smo omenili nekaj izjavnih veznikov, podali oznake zanje in opisali njihov intuitivni pomen. Ampak če se hočemo zanašati na pravilnost naših sklepov, moramo tem oznakam dati *formalni matematični pomen*.

Če imamo neko izjavo, lahko določimo njeno resničnost, tj. povemo, do kolikšne mere je resnična. Temu rečemo ***resničnostna vrednost*** izjave. Množico vseh možnih resničnostnih vrednosti označimo z Ω. Seveda ni kaj dosti možnih resničnostnih vrednosti: to sta ***resnica*** (dogovorimo se, da bomo zanjo uporabljali oznako $\top$) in ***neresnica*** (oznaka $\bot$). Se pravi, $\Omega = \{\top, \bot\}$.

Opomba 3.7. Logiki, kjer sta edini resničnostni vrednosti resnica in neresnica, rečemo ***dvovrednostna*** oziroma ***klasična logika***. Obstajajo splošnejše vrste logike, kjer je $\{\top, \bot\}$ prava podmnožica Ω, ampak v tej knjigi se bomo omejili na klasično logiko, na katero ste navajeni in ki se uporablja v večjem delu matematike.

(Kako izrecno bomo ločevali med izjavami in njihovimi logičnimi vrednostmi? –Davorin)

Izjavne veznike lahko potem formalno podamo kot preslikave. Na primer, negacija je preslikava $\neg\colon \Omega \to \Omega$ (vsaki resničnostni vrednosti pripišemo njeno nasprotno vrednost). Preslikavo, definirano na majhni končni množici, lahko preprosto podamo s tabelo vseh njenih vrednosti. V primeru izjavnih veznikov takim tabelam rečemo ***resničnostne tabele***. Resničnostna tabela za negacijo je videti takole.

p	$\neg p$
$\top$	$\bot$
$\bot$	$\top$

Ta tabela povsem natančno definira negacijo kot preslikavo $\neg\colon \Omega \to \Omega$. Seveda smo negacijo definirali tako, kot bi pričakovali: negacija resnice je neresnica, negacija neresnice je resnica.

Podobno lahko naredimo z ostalimi izjavnimi vezniki, le da preostali vežejo dve izjavi. Se pravi, npr. konjunkcija vzame dve resničnostni vrednosti in vrne resničnostno vrednost, ki pove, ali sta obe dani vrednosti resnični. Konjunkcijo lahko torej interpretiramo kot preslikavo $\wedge\colon \Omega \times \Omega \to \Omega$ (ali na kratko $\wedge\colon \Omega^2 \to \Omega$).

V splošnem definiramo, da je ***n-mestni izjavni veznik*** preslikava oblike $\Omega^n \to \Omega$. Negacija je torej enomestni izjavni veznik, ostali vezniki, ki smo jih do zdaj omenili, pa so dvomestni.

Definirajmo zdaj konjunkcijo natančno s pomočjo resničnostne tabele. Množica $\Omega \times \Omega$ ima štiri elemente — vse možne pare, sestavljene iz $\top$ oz. $\bot$. Intuitivni pomen konjunkcije razumemo: konjunkcija dveh izjav je resnična natanko tedaj, ko sta obe izjavi resnični. To nas vodi do naslednje tabele.

p	q	$p \wedge q$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$

Za disjunkcijo smo že rekli, da pride v dveh različicah: navadna pomeni, da vsaj ena od izjav velja, izključitvena pa pomeni, da velja natanko ena od izjav. Posledično je torej smiselno definirati funkciji $\vee, \veebar \colon \Omega \times \Omega \to \Omega$ na sledeči način.

p	q	$p \vee q$	$p \veebar q$
$\top$	$\top$	$\top$	$\bot$
$\top$	$\bot$	$\top$	$\top$
$\bot$	$\top$	$\top$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$

Bodi pozoren na razliko med zadnjima dvema stolpcema!

Obenem lahko še na hitro opravimo z veznikoma $\uparrow$ in $\downarrow$. Spomnimo se, da $p \uparrow q$ pomeni "ne hkrati p in q", medtem ko $p \downarrow q$ pomeni "niti p niti q".

p	q	$p \uparrow q$	$p \downarrow q$
$\top$	$\top$	$\bot$	$\bot$
$\top$	$\bot$	$\top$	$\bot$
$\bot$	$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\top$	$\top$

Implikacija je nekoliko bolj subtilna. Kaj točno trdimo z izjavo $p \Rightarrow q$, se pravi, kakor hitro velja p, mora veljati tudi q? No, če p ne velja, potem sploh nismo postavili nobenega pogoja — izjava je avtomatično izpolnjena. Če p velja, pa zraven zahtevamo še q. Resničnostna tabela za implikacijo je potemtakem sledeča.

p	q	$p \Rightarrow q$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\top$

Ekvivalenca je spet preprosta — izjavi sta ekvivalentni, kadar imata isto resničnostno vrednost. Od tod dobimo sledečo resničnostno tabelo.

p	q	$p \Leftrightarrow q$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\top$

Za lažjo referenco zberimo resničnostne tabele vseh do zdaj omenjenih veznikov na eno mesto (tabela 3.4).

Zdaj ko imamo natančno definicijo izjavnih veznikov, lahko trditve v zvezi z njimi tudi formalno utemeljimo. Na primer, spomnimo se, da smo že malo po omembi veznikov $\veebar, \uparrow, \downarrow$

p	$\neg p$
$\top$	$\bot$
$\bot$	$\top$

p	q	$p \wedge q$	$p \vee q$	$p \veebar q$	$p \uparrow q$	$p \downarrow q$	$p \Rightarrow q$	$p \Leftrightarrow q$
$\top$	$\top$	$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top$	$\top$	$\top$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$	$\top$	$\top$	$\top$	$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\top$	$\top$	$\top$	$\top$

Tabela 3.4: Resničnostna tabela osnovnih izjavnih veznikov

podali njihovo izražavo z vezniki $\neg$, $\wedge$, $\vee$. Če na glas preberemo vse izjave, nam je intuitivno jasno, katere se ujemajo in zakaj, ampak zdaj lahko dejansko preverimo, da te izražave veljajo.

Na primer, kaj pomeni, da se $p \downarrow q$ lahko izrazi kot $\neg(p \vee q)$? To pomeni, da sta funkciji $\Omega \times \Omega \to \Omega$, dani s predpisoma $(p, q) \mapsto p \downarrow q$ in $(p, q) \mapsto \neg(p \vee q)$, enaki. (Slednja funkcija je sestavljena, tj. sklop dveh funkcij. Lahko bi tudi zapisali, da velja $\downarrow = \neg \circ \vee$.) Funkciji z isto domeno in kodomeno sta enaki, kadar pri vsakem argumentu vrneta isti vrednosti, kar v našem primeru pomeni, da imata enaka stolpca v resničnostni tabeli. Poračunajmo torej vse izraze v danih izražavah. Ko dobimo enake rezultate, bomo vedeli, da izražave dejansko veljajo.

p	q	$p \uparrow q$	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
$\top$	$\top$	$\bot$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$
$\top$	$\bot$	$\top$	$\bot$	$\top$	$\bot$	$\top$	$\top$
$\bot$	$\top$	$\top$	$\bot$	$\top$	$\top$	$\bot$	$\top$
$\bot$	$\bot$	$\top$	$\bot$	$\top$	$\top$	$\top$	$\top$

p	q	$p \downarrow q$	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
$\top$	$\top$	$\bot$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$
$\top$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$	$\top$	$\bot$
$\bot$	$\top$	$\bot$	$\top$	$\bot$	$\top$	$\bot$	$\bot$
$\bot$	$\bot$	$\top$	$\bot$	$\top$	$\top$	$\top$	$\top$

p	q	$p \veebar q$	$p \vee q$	$p \wedge q$	$\neg(p \wedge q)$	$(p \vee q) \wedge \neg(p \wedge q)$
$\top$	$\top$	$\bot$	$\top$	$\top$	$\bot$	$\bot$
$\top$	$\bot$	$\top$	$\top$	$\bot$	$\top$	$\top$
$\bot$	$\top$	$\top$	$\top$	$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\top$	$\bot$

p	q	$p \veebar q$	$\neg q$	$p \wedge \neg q$	$\neg p$	$\neg p \wedge q$	$(p \wedge \neg q) \vee (\neg p \wedge q)$
$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
$\top$	$\bot$	$\top$	$\top$	$\top$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\bot$	$\bot$	$\top$	$\top$	$\top$
$\bot$	$\bot$	$\bot$	$\top$	$\bot$	$\top$	$\bot$	$\bot$

Kako simbolno zapisati, da sta dve izražavi enaki? Lahko bi pisali

$$\big((p, q) \mapsto p \uparrow q\big) = \big((p, q) \mapsto \neg(p \wedge q)\big),$$

ampak to je nekoliko nerodno in nepregledno. Kasneje (v razdelku (o anonimnih funkcijah)) se bomo naučili λ-notacijo, s katero dobimo

$$(\lambda(p, q) \in \Omega^2.\, p \uparrow q) = (\lambda(p, q) \in \Omega^2.\, \neg(p \wedge q)),$$

ampak to je še vedno nepregledno. Uveljavil se je običaj, da se izraze, ki so enakovredni v smislu, da dajo isti rezultat pri vsaki izbiri argumentov, poveže s simbolom $\equiv$, torej zapišemo

$$p \uparrow q \equiv \neg(p \wedge q).$$

Konkretno za izraze v logiki se uporablja tudi $\sim$, se pravi, zapišemo lahko tudi

$$p \uparrow q \sim \neg(p \wedge q).$$

V tej knjigi se bomo držali uporabe simbola $\equiv$. (Recimo. Po mojem je to boljše, ker lahko $\equiv$ uporabljamo še za druge funkcije (npr. $f(x) \equiv 0$ pomeni, da je f konstantno enaka 0, medtem ko $f(x) = 0$ predstavlja enačbo, s katero iščemo ničle funkcije) in ker bomo kasneje $\sim$ uporabljali za ekvivalenčne relacije. –Davorin)

Med drugim smo s temi tabelami izpeljali tako imenovana ***de Morganova zakona*** za izjavno logiko (Verjetno je smiselno specificirati "za izjavno logiko". Imeli bomo namreč še zakona za predikatno logiko (za $\forall$ in $\exists$) ter za množice (za preseke in unije). –Davorin), ki povesta, kako negacija vpliva na konjunkcijo in disjunkcijo:

$$\neg(p \wedge q) \equiv \neg p \vee \neg q,$$

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

To je smiselno: kadar ni res, da veljata oba p in q, vsaj eden od njiju ne velja. Kadar ni res, da velja vsaj eden od njiju, nobeden od njiju ne velja.

Z resničnostnimi tabelami lahko preverimo še mnoge druge formule. ***Zakon dvojne negacije*** pravi $\neg\neg p \equiv p$, tj. če dvakrat zanikamo izjavo, dobimo izjavo, enakovredno začetni. Poračunajmo tabelo.

p	$\neg p$	$\neg\neg p$	p
$\top$	$\bot$	$\top$	$\top$
$\bot$	$\top$	$\bot$	$\bot$

Spomnimo se: za poljubno dvomestno operacijo $\circledast$ na neki množici X rečemo, da je

- ***izmenljiva*** ali ***komutativna***, kadar velja $a \circledast b = b \circledast a$ za vse $a, b \in X$ (na kratko: $a \circledast b \equiv b \circledast a$),
- ***družilna*** ali ***asociativna***, kadar velja $(a \circledast b) \circledast c = a \circledast (b \circledast c)$ za vse $a, b, c \in X$ (na kratko: $(a \circledast b) \circledast c \equiv a \circledast (b \circledast c)$),
- ***idempotentna*** (a imamo slovenski izraz za to? –Davorin), kadar velja $a \circledast a = a$ za vse $a \in X$ (torej $a \circledast a \equiv a$).

Preverimo z resničnostno tabelo, da je konjunkcija komutativna, torej $p \wedge q \equiv q \wedge p$.

p	q	$p \wedge q$	$q \wedge p$
$\top$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$	$\bot$
$\bot$	$\bot$	$\bot$	$\bot$

Še hitreje lahko preverimo, da je konjunkcija idempotentna.

p	$p \wedge p$	p
$\top$	$\top$	$\top$
$\bot$	$\bot$	$\bot$

Kako pa preveriti, da je konjunkcija asociativna, torej $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$? Vidimo, da v teh izrazih nastopajo tri spremenljivke in torej potrebujemo resničnostno tabelo, kjer upoštevamo vseh osem možnosti za izbiro p, q, r.

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

To pomeni, da lahko v izrazih, kjer nastopa več zaporednih konjunkcij, spuščamo oklepaje: namesto $p \wedge (\neg q \wedge r)$ pišemo kar $p \wedge \neg q \wedge r$.

Enako velja tudi za disjunkcijo.

Naloga 3.8. Dokaži, da je disjunkcija komutativna, asociativna in idempotentna!

Preostali dvomestni vezniki, ki smo jih omenili, ne zadoščajo vsem trem lastnostim naenkrat.

Naloga 3.9. Preveri, kateri znani dvomestni izjavni vezniki so komutativni, asociativni oziroma idempotentni!

Ko rešite zgornjo vajo, boste med drugim opazili: implikacija ni komutativna. To pomeni, da lahko definiramo nov izjavni veznik $\Leftarrow$ na naslednji način: $p \Leftarrow q := q \Rightarrow p$ za vse $p, q \in \Omega$. Z drugimi besedami, $\Leftarrow$ je dan s sledečo resničnostno tabelo.

p	q	$p \Leftarrow q$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\top$

(dokazi s pomočjo resničnostnih tabel še vseh ostalih formul, ki jih hočemo imeti, med drugim distributivnosti)

Do zdaj smo omenili zgolj nekaj posamičnih izjavnih veznikov. Koliko pa je vseh skupaj? Spomnimo se, da je n-mestni izjavni veznik definiran kot preslikava $\Omega^n \to \Omega$. Množica Ω^n vsebuje vse urejene n-terice elementov $\top$ in $\bot$; teh je 2^n (za vsako od n mest v n-terici imamo dve možnosti in vse te izbire so neodvisne med sabo). Za vsako od teh 2^n večteric imamo dve možnosti, kam jo preslikamo: v $\top$ ali v $\bot$. Vseh možnosti — torej vseh n-mestnih veznikov — je potemtakem 2^{2^n}. (Vseh izjavnih veznikov, ko dopuščamo vse možne n, je seveda neskončno.)

Za boljšo predstavo si oglejmo vse n-mestne veznike za majhne $n \in \mathbb{N}$. Prva možnost je $n = 0$. Formula nam pravi, da je število ničmestnih izjavnih veznikov enako $2^{2^0} = 2^1 = 2$. Kaj

pomeni, da pri nič vhodnih podatkih vrnemo $\top$ ali $\bot$? To pomeni, da preprosto izberemo resničnostno vrednost — z drugimi besedami, ničmestni izjavni vezniki so isto kot resničnostne vrednosti.

Koliko je vseh enomestnih izjavnih veznikov? Formula pravi $2^{2^1} = 2^2 = 4$. Zapišimo vse možnosti.

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

Vidimo: enomestni izjavni vezniki so obe konstantni funkciji na Ω, identiteta na Ω in negacija.

Kar se dvomestnih veznikov tiče, vidimo, da jih je $2^{2^2} = 2^4 = 16$.

Naloga 3.10. Preveri, da so vsi dvomestni vezniki natanko: konstanta z vrednostjo $\top$, projekcija na prvo komponento (tj. $(p, q) \mapsto p$), projekcija na drugo komponento (tj. $(p, q) \mapsto q$), konjunkcija $\wedge$, disjunkcija $\vee$, implikacija $\Rightarrow$, povratna implikacija $\Leftarrow$, ekvivalenca $\Leftrightarrow$ in negacije vseh teh.

Tromestnih veznikov je že $2^{2^3} = 2^8 = 256$ in ne bomo vseh naštevali. Kako pa bi kakega dobili? Preprost način je, da vzamemo tri spremenljivke in jih združimo z večimi znanimi vezniki, na primer $(p, q, r) \mapsto p \wedge \neg q \Rightarrow r$.[3]

Seveda se pojavi vprašanje, ali obstajajo izjavni vezniki, ki jih ne bi mogli sestaviti iz osnovnih. Izkaže se, da je odgovor nikalen: *vsak veznik (ne glede na mestnost) je možno izraziti z osnovnimi*; pravzaprav zadostujejo že $\neg$, $\wedge$ in $\vee$.

Ideja je sledeča. Katerikoli izjavni veznik je oblike $V\colon \Omega^n \to \Omega$ in v celoti podan z resničnostno tabelo. Vzemimo konkreten primer; naj bo V tromestni veznik, podan z naslednjo tabelo.

p	q	r	$V(p,q,r)$
$\top$	$\top$	$\top$	$\bot$
$\top$	$\top$	$\bot$	$\top$
$\top$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$	$\top$
$\bot$	$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$	$\bot$

Tedaj lahko rečemo: V je resničen tedaj, ko smo v 2., 3., 5. ali 6. vrstici. Kdaj smo v drugi vrstici? Točno tedaj, ko p in q veljata, r pa ne, se pravi, ko velja $p \wedge q \wedge \neg r$. Podobno naredimo še za preostale vrstice: tretja je določena s $p \wedge \neg q \wedge r$, peta z $\neg p \wedge q \wedge r$ in šesta z $\neg p \wedge q \wedge \neg r$. Potemtakem lahko zapišemo:

$$V(p, q, r) \equiv (p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge q \wedge \neg r).$$

Temu rečemo ***disjunktivna normalna oblika*** (s kratico DNO) veznika V.

[3] Načeloma sploh ni nujno, da vse tri spremenljivke dejansko uporabimo. Na primer, $(p, q, r) \mapsto p \wedge q$ še vedno podaja tromestni veznik, saj gre za preslikavo $\Omega^3 \to \Omega$.

Obstaja še dualna oblika take izražave. Lahko si rečemo tudi, da je V resničen, kadar nismo v 1., 4., 7. oz. 8. vrstici. Kdaj nismo v prvi vrstici? Kadar niso vsi p, q, r resnični, torej ko je vsaj eden od njih neresničen — s formulo $\neg p \vee \neg q \vee \neg r$. Kdaj nismo v četrti vrstici? Ko ni res, da je p resničen, q in r pa ne, torej ko prekršimo vsaj enega teh pogojev, kar nam da formulo $\neg p \vee q \vee r$. Podobno sklepamo, da nismo v sedmi vrstici, kadar velja $p \vee q \vee \neg r$, in da nismo v osmi vrstici, kadar velja $p \vee q \vee r$. To nam da sledečo izražavo za V:

$$V(p,q,r) \equiv (\neg p \vee \neg q \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (p \vee q \vee \neg r) \wedge (p \vee q \vee r).$$

Temu rečemo ***konjunktivna normalna oblika*** (s kratico KNO) veznika V.

Spremenljivkam in njihovim negacijam z eno besedo rečemo ***literali***. Disjunktivna normalna oblika je torej disjunkcija konjunkcij literalov, konjunktivna normalna oblika pa konjunkcija disjunkcij literalov.

Iz tega primera je jasno, kako postopamo za poljuben izjavni veznik in zanj zapišemo DNO ali KNO. Opazimo: dolžina posamičnega člena, ki ga omejujejo oklepaji, je vedno enaka (vsebuje toliko literalov, kolikor je mestnost veznika), število teh členov pa razberemo iz stolpca, ki podaja vrednosti veznika v resničnostni tabeli. V primeru DNO je to število enako številu resnic $\top$, v primeru KNO pa številu neresnic $\bot$. V zgornjem primeru sta bili DNO in KNO enako dolgi, ker smo imeli štiri $\top$ in $\bot$, v splošnem pa se nam morda bolj splača uporabiti eno obliko kot drugo. Na primer, DNO implikacije se glasi $p \Rightarrow q \equiv (p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)$, KNO pa je precej krajša: $p \Rightarrow q \equiv \neg p \vee q$.

Vidimo pa, da tu naletimo na problem: kaj se zgodi, če se katera resničnostna vrednost v stolpcu veznika sploh ne pojavi — z drugimi besedami, kaj če je funkcija, ki podaja veznik, konstantna? Najprej dajmo takim veznikom ime: izjavni veznik, ki je pri vseh argumentih resničen, se imenuje ***istorečje*** ali ***tavtologija***, izjavni veznik, ki je vedno neresničen, pa se imenuje ***protislovje*** ali ***kontradikcija***.

Za istorečje lahko vedno (ne glede na mestnost) zapišemo DNO (ki je sicer najdaljša možna), medtem ko bi KNO načeloma bila konjunkcija nič členov. Je to smiselno? V bistvu ja: če zahtevamo, da hkrati velja nič pogojev, je naša zahteva vedno izpolnjena. V tem smislu je konjunkcija nič členov enaka $\top$.

Poglejmo podobne primere iz računstva. Kaj je vsota nič členov? Odgovor je seveda 0. To je enota za seštevanje, kar je smiselno: če nič členom prištejemo en člen, moramo imeti zgolj ta člen. Podobno sklepamo: zmnožek nič členov je enota za množenje 1 — če nič faktorjem dodamo še en faktor, imamo skupaj zgolj ta faktor. Spomni se tudi: $a^0 = 1$ in $0! = 1$. To, da je ničkratna uporabe neke operacije enaka enoti za to operacijo, se izide tudi za konjunkcijo: dejansko velja $p \wedge \top \equiv p \equiv \top \wedge p$ (preveri z resničnostno tabelo!).

Enak razmislek velja za protislovje. Zanj lahko zapišemo KNO na običajen način, medtem ko bi DNO bila disjunkcija nič členov. Smiselno je, da je disjunkcija nič členov enaka $\bot$, tako zaradi tega, ker je $\bot$ enota za disjunkcijo (preveri!), kot zaradi čisto intuitivnega razmisleka: kdaj je vsaj en člen od nič členov resničen? Nikoli.

Vseeno je nekoliko nerodno delati s konjunkcijo ali disjunkcijo nič členov — kako točno bi to zapisali? Da velja $V(p_1, p_2, \ldots, p_n) \equiv$? Če nič ne zapišemo, kako sploh vemo, ali smo mislili na ničkratno konjunkcijo, disjunkcijo ali katerokoli drugo operacijo? Nekateri se zato preprosto dogovorijo, da ne dopuščajo ničkratnih operacij v DNO oz. KNO in potem štejejo, da istorečja nimajo KNO, protislovja pa ne DNO.

Tudi če ne dopuščamo ničkratnih operacij, pa še vedno velja: vsak izjavni veznik z mestnostjo vsaj 1 ima vsaj eno od DNO oz. KNO in ga torej lahko izrazimo samo z negacijo,

konjunkcijo in disjunkcijo. Družini izjavnih veznikov, s katerimi lahko izrazimo vse veznike z mestnostjo vsaj 1, rečemo ***poln nabor***. Na kratko lahko torej rečemo, da je $\{\neg, \wedge, \vee\}$ poln nabor.

Jasno, če je neka množica veznikov poln nabor, je tudi vsaka njena nadmnožica poln nabor. Sledi, da je tudi na primer $\{\neg, \wedge, \vee, \Rightarrow\}$ poln nabor.

Spomnimo se zdaj de Morganovih zakonov in zakona o dvojni negaciji — iz njih lahko izpeljemo $p \wedge q \equiv \neg(\neg p \vee \neg q)$ in $p \vee q \equiv \neg(\neg p \wedge \neg q)$. Se pravi, konjunkcijo lahko izrazimo z disjunkcijo in negacijo in prav tako lahko disjunkcijo izrazimo s konjunkcijo in negacijo. To pomeni, da sta že $\{\neg, \vee\}$ in $\{\neg, \wedge\}$ polna nabora! Se pravi, vse veznike s pozitivno mestnostjo je možno izraziti že samo z dvema.

Je možno iti še dlje in najti en sam veznik, s katerim lahko izrazimo ostale? Odgovor je da: $\{\uparrow\}$ in $\{\downarrow\}$ sta polna nabora. (Izkaže se, da sta to edina taka veznika med dvomestnimi vezniki.)

Naloga 3.11.

1. Izrazi negacijo samo z veznikom $\uparrow$. Izrazi še konjunkcijo ali disjunkcijo samo z veznikom $\uparrow$. Sklepaj, da je $\{\uparrow\}$ poln nabor.

2. Izrazi negacijo samo z veznikom $\downarrow$. Izrazi še konjunkcijo ali disjunkcijo samo z veznikom $\downarrow$. Sklepaj, da je $\{\downarrow\}$ poln nabor.

(Bi na tem mestu predebatirali preklopna vezja? –Davorin)

(Mogoče lahko zavoljo celovitosti podamo karakterizacijo polnih naborov kot izrek (in se za dokaz skličemo na literaturo). Nabor je poln, kadar za vsako sledečih lastnosti obstaja veznik v njem, ki jo prekrši: ohranjanje resnice, ohranjanje neresnice, monotonost, sebi-dualnost, afinost (kot polinom Žegalkina). –Davorin)

3.4 Predikati in kvantifikatorji

("Lastnostim" elementov množic, ki smo jih prej uporabljali za podajanje podmnožic in pri kvantifikatorjih, zdaj "uradno" rečemo ***predikati*** in jih formalno definiramo: predikat na množici X je preslikava $X \to \Omega$. Karakteristične preslikave podmnožic. Spomnimo se kvantifikatorjev in jih definiramo kot preslikave $\Omega^X \to \Omega$. Povemo, da lahko imajo predikati več spremenljivk in da lahko kvantificiramo po samo nekaterih (dobimo torej preslikave oblike $\Omega^{X \times Y} \to \Omega^Y$). Vezane, proste spremenljivke. Pravila, ki veljajo za kvantifikatorje (de Morgan itd.).)

3.5 Vaje

Vaja 3.1. Preverite, da je $(p \Rightarrow q) \vee (q \Rightarrow p)$ tavtologija z resničnostno tabelo in s poenostavljanjem.

(Ali želimo imeti toliko nalog iz polnih naborov? Jaz sem samo skopirala te naloge od prejšnjih vaj. –Anja)

Vaja 3.2. Pokaži, da so naslednji nabori izjavnih povezav polni.

1. $\{\wedge, \not\leq, \top\}$

2. $\{\Rightarrow, \neg\}$

3. $\{\Rightarrow, \bot\}$
4. $\{\wedge, \bot, \top, \Delta\}$, kjer je $\Delta(p,q,r) \equiv p \veebar q \veebar r$.

Vaja 3.3. Naslednje izjave izrazi le z veznikoma $\neg$ in $\Rightarrow$.

- $p \wedge q$
- $(p \veebar q) \Leftrightarrow (p \vee q)$
- $p \downarrow q$

Vaja 3.4. Pokaži, da spodnja nabora izjavnih veznikov *nista* polna:

- $\{\wedge, \Leftrightarrow\}$,
- $\{\wedge, \veebar\}$.

Vaja 3.5. Kateri izmed naslednjih izjavnih veznikov sestavlja poln nabor?

- $\Lambda(p,q,r) \equiv p \Rightarrow (q \vee r)$
- $\Lambda(p,q,r) \equiv (p \uparrow q) \downarrow r$
- $\Lambda(p,q,r) \equiv (\neg p \wedge \neg r) \Rightarrow q$
- $\Lambda(p,q,r) \equiv p \Rightarrow (q \Rightarrow \neg r)$

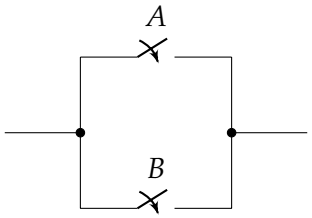
Vaja 3.6. Ali sestavljata izjavni povezavi $\{\Rightarrow, \not\Rightarrow\}$, kjer je $p \not\Rightarrow q \equiv \neg(p \Rightarrow q)$, poln nabor?

Vaja 3.7. Izjavna povezava $\Box$ je določena z $p \Box q \equiv p \wedge \neg q$. Ugotovi, kateri nabori od spodnjih naborov izjavnih povezav so polni.

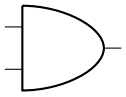
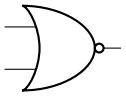
- $\{\Box\}$
- $\{\Box, \neg\}$
- $\{\Box, \Rightarrow\}$

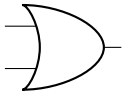
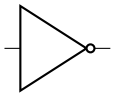
Vaja 3.8. Preklopna vezja so sestavljena iz stikal in žic. Stikala so lahko vklopljena ali izklopljena, glede na njihovo stanje pa je odvisno, ali bo tok tekel po žici ali ne. Denimo, da imamo dve stikali A in B. Če sta stikali vezani zaporedno, tj.

potem tok teče, kadar sta obe stikali vklopljeni. Če pa sta stikali vezani vzporedno, tj.

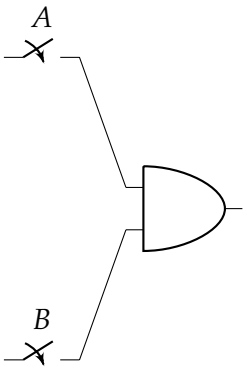


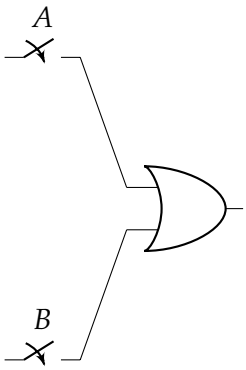
potem tok teče, če je vklopljeno stikalo A ali stikalo B. Tako lahko simuliramo logične veznike. Stikala so izjavne spremenljivke, takšni bloki pa predstavljajo vrata "in" ter "ali". Vrata za logične veznike predstavljamo z naslednjimi simboli:


in

niti


ali

ne

Prvi dve vezji lahko torej z vrati zapišemo takole



ter


Andrej prenavlja stanovanje in načrtuje električno napeljavo. Ker se mu pred spanjem ne ljubi vstajati, da bi ugasnil luč, si želi v spalnici imeti dve stikali, eno ob postelji in eno pri vhodu. Seveda pa morata obe stikali delovati, torej ko pritisnemo na katero koli stikalo, se mora luč prižgati ali pa ugasniti, če je že prižgana. Pri izdelavi električnega omrežja sme Andrej uporabiti le vrata "in", "ali" ter "ne". Ker pa so vrata draga, si želi uporabiti čim manj vrat. Pomagajte Andreju načrtovati vezje za njegovo spalnico. Kaj pa če lahko uporabi samo vrata "in" ter "ali"? Ali lahko uporabi le vrata "niti" ($\downarrow$)?

Poglavje 4

Dokazovanje

Matematične izsledke običajno podajamo preko jasno izraženih izjav. Med študijem matematike hitro opazite, da se takšne izjave podajajo pod imeni 'izrek', 'trditev', 'lema', posledica in podobno. Kdaj uporabiti katerega teh imen ni natanko določeno, pač pa je prepuščeno presoji matematika. Približno vodilo je naslednje:

- ***izrek***: osrednji, bistven rezultat,
- ***trditev***: stranski rezultat,
- ***lema***: rezultat, ki sam po sebi nima toliko vsebine, se pa uporabi pri dokazovanju pomembnejšega rezultata,[1]
- ***posledica***: rezultat, ki je zanimiv sam po sebi, ki pa hitro sledi iz predhodne izjave.

Če skrbno analizirate izreke, trditve itd. s predavanj (ali iz matematičnih člankov), opazite, da sestojijo iz treh delov: kontekst, predpostavke, sklepi.

- ***Kontekst*** pove, katere objekte obravnavamo in kakšne vrste so.
- ***Predpostavke*** so izjave, ki jih privzamemo.
- ***Sklepi*** so izjave, ki jih (pri danih predpostavkah) dokazujemo.

Oglejmo si konkreten primer. Rolleov izrek je znan in uporaben izrek v analizi (če ga še niste spoznali, ga boste v kratkem).

Izrek 4.1 (Rolle)**.** *Naj bo f realna funkcija, definirana na intervalu $\mathbb{R}_{[a,b]}$, kjer sta a in b realni števili in $a < b$. Če je f zvezna na celem $\mathbb{R}_{[a,b]}$ in odvedljiva na odprtem intervalu $\mathbb{R}_{(a,b)}$ ter zavzame enaki vrednosti v krajiščih, tj. $f(a) = f(b)$, tedaj ima f stacionarno točko na $\mathbb{R}_{(a,b)}$.*

Analizirajmo, kaj so kontekst, predpostavke in sklepi pri tem izreku.

- Kontekst je sledeč:

$$a \in \mathbb{R}, \qquad b \in \mathbb{R}_{>a}, \qquad f \in \mathbb{R}^{\mathbb{R}_{[a,b]}}.$$

[1] Sicer ni nujno, da se resnična pomembnost izjav takoj pokaže. Mnogo je primerov, ko se kak matematični članek po določenem času začne ceniti ne toliko zaradi glavnega izreka, pač pa zaradi neke leme, ki se je za dokaz glavnega izreka uporabila.

To so objekti (in njihove vrste), o katerih govori izrek. Smiselno je, da jih zapišemo v tem vrstnem redu; na primer, f zapišemo nazadnje, saj je njena domena odvisna od a in b. Kadar imamo objekte, ki so neodvisni med sabo, jih lahko zapišemo v poljubnem vrstnem redu.

- Predpostavke so tri. Vsako navedimo v običajnem jeziku in nato še s simbolnim matematičnim zapisom.
  - f je zvezna na $\mathbb{R}_{[a,b]}$.

    $$\forall x \in \mathbb{R}_{[a,b]}. \forall \epsilon \in \mathbb{R}_{>0}. \exists \delta \in \mathbb{R}_{>0}. \forall y \in \mathbb{R}_{[a,b]}. (|x-y| < \delta \Rightarrow |f(x) - f(y)| < \epsilon)$$

  - f je odvedljiva na $\mathbb{R}_{(a,b)}$.

    $$\forall x \in \mathbb{R}_{(a,b)}. \exists v \in \mathbb{R}. \forall \epsilon \in \mathbb{R}_{>0}. \exists \delta \in \mathbb{R}_{>0}. \forall h \in \mathbb{R}_{\neq 0}. \\ (|h| < \delta \implies \left|\frac{f(x+h) - f(x)}{h} - v\right| < \epsilon)$$

  - f na krajiščih intervala zavzame enaki vrednosti.

    $$f(a) = f(b)$$

  Če se vam morda zdita formuli za zveznost in odvedljivost begajoči, imate dve tolažbi. Prva je ta, da se boste čez čas takšnih formul navadili. ;) Druga je, da so tudi drugi matematiki leni po naravi in zato uvedejo oznake za daljše izraze, ki se pogosto uporabljajo. Zgornja zveznost se na krajše zapiše $f \in \mathcal{C}(\mathbb{R}_{[a,b]})$ ($\mathcal{C}$ kot "continuous", tj. zvezen), odvedljivost pa $f \in \mathcal{D}^1(\mathbb{R}_{(a,b)})$ ($\mathcal{D}$ kot "differentiable", tj. odvedljiv, enka pa pomeni "(vsaj) enkrat odvedljiv").

- Sklep je eden: f ima stacionarno točko na $\mathbb{R}_{(a,b)}$, kar simbolno zapišemo takole.

  $$\exists x \in \mathbb{R}_{(a,b)}. f'(x) = 0$$

V splošnem imamo določeno mero svobode, kako natančno razčleniti izrek. Na primer, za Rolleov izrek bi lahko kontekst zapisali tudi kot $a \in \mathbb{R}, b \in \mathbb{R}, f \in \mathbb{R}^{\mathbb{R}_{[a,b]}}$ in pogoj $a < b$ dodali med predpostavke.

Da ne bomo pisali dolgih seznamov, se dogovorimo za sledeče oznake. Izrek podamo tako, da najprej zapišemo kontekst, nato dvopičje, nato narišemo vodoravno črto, nad črto zapišemo predpostavke (ločene z vejicami), pod črto pa sklepe (ločene z vejicami). Rolleov izrek bi potemtakem povzeli takole.

$$a \in \mathbb{R}, b \in \mathbb{R}_{>a}, f \in \mathbb{R}^{\mathbb{R}_{[a,b]}} : \quad \frac{f \in \mathcal{C}(\mathbb{R}_{[a,b]}), f \in \mathcal{D}^1(\mathbb{R}_{(a,b)}), f(a) = f(b)}{\exists x \in \mathbb{R}_{(a,b)}. f'(x) = 0}$$

V splošnem velja: vse proste spremenljivke, ki se pojavijo v predpostavkah ali sklepih, morajo biti navedene v kontekstu. Po domače povedano: če trdite, da za neko stvar nekaj velja, morate najprej povedati, o kateri stvari sploh govorite.

Medtem ko je za težje matematične izreke potrebno obilo ustvarjalnosti, da se jih dokaže, pa lažje trditve pogosto lahko avtomatično dokažemo (dobesedno — obstajajo avtomatični dokazovalniki (koliko povemo na to temo? –Davorin)), pa tudi za težje je pomembno, da vemo, kako pristopiti k dokazu. Gre za to, da za vse logične veznike in kvantifikatorje obstajajo splošna pravila, kako ravnamo, če nastopajo kot predpostavke oziroma kot sklepi. To si bomo zdaj ogledali.

- **Konjunkcija**
  - Če $p \wedge q$ nastopa kot *predpostavka*:

    predpostavko $p \wedge q$ nadomestimo s predpostavkama p, q (to se pravi, pri dokazovanju lahko uporabimo tako predpostavko p kot predpostavko q). S simboli, od trditve
    $$\Gamma : \frac{\Pi', p \wedge q, \Pi''}{\Sigma}$$
    preidemo do trditve
    $$\Gamma : \frac{\Pi', p, q, \Pi''}{\Sigma}$$
    (pri zapisih splošnih izrekov bomo kontekst označevali z Γ, predpostavke s Π in sklepe s Σ).
  - Če $p \wedge q$ nastopa kot *sklep*:

    sklep $p \wedge q$ dokažemo tako, da dokažemo posebej p in posebej q. S simboli:
    $$\Gamma : \frac{\Pi}{\Sigma', p \wedge q, \Sigma''}$$
    preoblikujemo v
    $$\Gamma : \frac{\Pi}{\Sigma', p, q, \Sigma''}$$
    (in se zavedamo, da je za dokaz izreka potrebno dokazati *vse* sklepe).
- **Disjunkcija**
  - Če $p \vee q$ nastopa kot *predpostavka*:

    ločimo primere: sklepe dokažemo posebej pri predpostavki p (skupaj z ostalimi predpostavkami) in posebej pri predpostavki q (skupaj z ostalimi). Torej, dokazati
    $$\Gamma : \frac{\Pi', p \vee q, \Pi''}{\Sigma}$$
    pomeni isto, kot dokazati tako
    $$\Gamma : \frac{\Pi', p, \Pi''}{\Sigma} \qquad \text{kot} \qquad \Gamma : \frac{\Pi', q, \Pi''}{\Sigma}.$$
  - Če $p \vee q$ nastopa kot *sklep*:

    izberemo si enega od p, q in ga dokažemo. Se pravi, če imamo
    $$\Gamma : \frac{\Pi}{\Sigma', p \vee q, \Sigma''},$$
    si izberemo eno od trditev
    $$\Gamma : \frac{\Pi}{\Sigma', p, \Sigma''} \qquad \text{oziroma} \qquad \Gamma : \frac{\Pi}{\Sigma', q, \Sigma''}$$
    in jo izpeljemo.
- **Implikacija**

– Če $p \Rightarrow q$ nastopa kot *predpostavka*:

  če nam kadarkoli uspe izpeljati p, lahko dodamo q med predpostavke. Torej, če znamo dokazati

$$\Gamma : \ \frac{\Pi', p \Rightarrow q, \Pi''}{q},$$

  potem za dokaz

$$\Gamma : \ \frac{\Pi', p \Rightarrow q, \Pi''}{\Sigma}$$

  zadostuje dokazati

$$\Gamma : \ \frac{\Pi', p \Rightarrow q, q, \Pi''}{\Sigma}$$

  (kar je lažje, ker imamo eno predpostavko več). To je smiselno: če vemo, da velja $p \Rightarrow q$ in dodatno ugotovimo, da velja p, potem vemo, da velja tudi q.

– Če $p \Rightarrow q$ nastopa kot *sklep*:

  sklep $p \Rightarrow q$ nadomestimo s q, medtem ko p dodamo med predpostavke. Pojasnimo. Trditev $p \Rightarrow q$ trdi nekaj samo v primeru, kadar p velja — v nasprotnem primeru je avtomatično resnična in ni ničesar za dokazati. Torej se lahko omejimo na primer, ko p velja, se pravi, lahko predpostavimo p. Kadar p velja, pa trditev $p \Rightarrow q$ pravi, da mora veljati tudi q. To pomeni, da pri predpostavki p dokazujemo q. Simbolno, da dokažemo

$$\Gamma : \ \frac{\Pi}{\Sigma', p \Rightarrow q, \Sigma''},$$

  zadostuje dokazati

$$\Gamma : \ \frac{\Pi}{\Sigma', \Sigma''} \qquad \text{in} \qquad \Gamma : \ \frac{\Pi, p}{q}.$$

- **Univerzalni kvantifikator**

– Če $\forall x \in X. \phi(x, y)$ nastopa kot *predpostavka*:

  če vemo za (ali med dokazom najdemo) katerikoli konkreten element $a \in X$, tedaj lahko med predpostavke dodamo $\phi(a, y)$. Namreč, če vemo, da lastnost ϕ (z morebitnimi nadaljnjimi parametri) velja za vse elemente množice X, potem ta lastnost velja za poljuben konkreten element. Simbolno, od

$$\Gamma', a \in X, \Gamma'' : \ \frac{\Pi', \forall x \in X. \phi(x, y), \Pi''}{\Sigma}$$

  preidemo do

$$\Gamma', a \in X, \Gamma'' : \ \frac{\Pi', \forall x \in X. \phi(x, y), \phi(a, y), \Pi''}{\Sigma}.$$

– Če $\forall x \in X. \phi(x, y)$ nastopa kot *sklep*:

  v kontekst dodamo $x \in X$, sklep $\forall x \in X. \phi(x, y)$ pa nadomestimo s sklepom $\phi(x, y)$. S simboli, od

$$\Gamma : \ \frac{\Pi}{\Sigma', \forall x \in X. \phi(x, y), \Sigma''}$$

preidemo do

$$\Gamma, x \in X : \ \frac{\Pi}{\Sigma', \phi(x,y), \Sigma''}$$

Zakaj tako postopamo in kaj smo s tem pravzaprav naredili? Premislimo: želimo dokazati, da neka lastnost velja za vse elemente dane množice X. Če ima X slučajno samo končno mnogo elementov, bi lahko lastnost preverili za vsakega posebej, ampak povečini delamo z neskončnimi množicami, kjer to ne deluje. Morda ima množica X kakšno posebno lastnost, zaradi katere lahko univerzalni kvantifikator dokažemo na svojevrsten način (na primer, univerzalno kvantificirane izjave nad $\mathbb{N}$ lahko dokazujemo z matematično indukcijo — glej (razdelek o naravnih številih)), ampak to se zgodi v izjemnih primerih.

V splošnem nimamo druge možnosti, kot da si izberemo simbol (tipično kar spremenljivko v kvantifikatorju), ki nam predstavlja poljuben, katerikoli element množice in zanj dokažemo želeno lastnost. Ideja je, da spremenljivka spet nastopa v vlogi "škatlice", kamor lahko vstavimo poljuben element množice X. Če nam je dokaz lastnosti uspel, ne da bi za spremenljivko predpostavili karkoli več, kot da predstavlja element množice X, tedaj dobimo dokaz lastnosti za katerikoli dejanski element množice X tako, da v dobljeni dokaz namesto spremenljivke vstavimo ta element. Na ta način smo potem dejansko dobili dokaz lastnosti za vse elemente množice X.

Besedni dokazi univerzalno kvantificirane izjave se zato tipično začnejo takole: "Vzemimo poljuben $x \in X$. Dokažimo, da zanj velja dana lastnost."

- **Eksistenčni kvantifikator**
  - Če $\exists x \in X. \phi(x,y)$ nastopa kot *predpostavka*:

    v kontekst dodamo $x \in X$, eksistenčno predpostavko pa nadomestimo s $\phi(x,y)$. S simboli,

    $$\Gamma : \ \frac{\Pi', \exists x \in X. \phi(x,y), \Pi''}{\Sigma}$$

    popravimo v

    $$\Gamma, x \in X : \ \frac{\Pi', \phi(x,y), \Pi''}{\Sigma}.$$

    Zakaj to deluje? Naša predpostavka je, da v množici X obstaja element z lastnostjo ϕ (z morebitnimi nadaljnjimi parametri). Torej si lahko vzamemo neki konkreten element množice X s to lastnostjo, ki ga lahko uporabljamo kasneje v dokazu (za to ga moramo nekako označiti; v praksi ga tipično označimo kar z isto spremenljivko, kot v kvantifikatorju).
  - Če $\exists x \in X. \phi(x,y)$ nastopa kot *sklep*:

    da dokažemo eksistenčno izjavo, moramo podati neki konkreten element $x \in X$ in zanj dokazati dano lastnost $\phi(x,y)$. (Hm, kako točno to zapišemo simbolno v zgornji obliki? –Davorin)

V zgornjem seznamu nismo omenili vseh veznikov in kvantifikatorjev. To je zato, ker jih pri dokazovanju nadomestimo z zgornjimi. Konkretno:

- Za negacijo velja $\neg p \equiv p \Rightarrow \bot$. Med drugim to pomeni, da $\neg p$ dokažemo na sledeči način: predpostavimo p in iz tega izpeljemo neresnico.
- Za ekvivalenco velja $p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (p \Leftarrow q)$. To pomeni, da ekvivalenco dokažemo tako, da dokažemo implikacijo med p in q v obe smeri — se pravi, enkrat predpostavimo p in izpeljemo q, drugič pa predpostavimo q in izpeljemo p.
- Za veznike $\veebar$, $\uparrow$, $\downarrow$ si preprosto izberemo eno od izražav z negacijo, konjunkcijo in disjunkcijo in nato delamo z njo.
- Kvantifikator $\exists! x \in X. \phi(x, y)$ ločimo na dva dela: na obstoj in enoličnost, in vsakega posebej dokažemo. Se pravi, skličemo se na izražavo

  $$\exists! x \in X. \phi(x, y) \equiv \exists x \in X. \phi(x, y) \wedge \forall a, b \in X. (\phi(a, y) \wedge \phi(b, y) \implies a = b).$$

  Včasih je lažje, če najprej dokažemo obstoj elementa in ta element pri dokazu enoličnosti že uporabimo, torej dokazujemo izražavo

  $$\exists! x \in X. \phi(x, y) \equiv \exists x \in X. (\phi(x, y) \wedge \forall a \in X. (\phi(a, y) \implies a = x)).$$

Seveda ne bo možno dokazati vsakega izreka s slepim sledenjem zgornjim pravilom; včasih moramo uporabiti še kakšno dodatno strategijo. Spodnji dve sta zelo pogosti.

- Med predpostavke dodamo trditev, za katero že vemo, da je resnična. Morda gre za trditev, ki smo jo že dokazali, morda pa gre kar za istorečje. Pogost primer tega je, da uporabimo zakon o izključenem tretjem in za dodatno predpostavko vzamemo $p \vee \neg p$ (kjer je p katerakoli konkretna izjava). Po zgornjih pravilih to potem pomeni, da ločimo primere in trditev dokažemo posebej pri predpostavki p ter posebej pri predpostavki $\neg p$.
- Nekatere predpostavke ali sklepe nadomestimo z enakovrednimi izjavami. Na primer, velja

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

  To pomeni, da lahko disjunkcijo (poleg zgoraj omenjenega načina) dokažemo tudi tako, da predpostavimo, da nobena od možnosti ne velja, in od tod izpeljemo neresnico, ali pa predpostavimo, da ena od možnosti ne velja, in od tod izpeljemo drugo.

  Zelo pogosta uporaba te ideje je ***dokaz s protislovjem***, ki temelji na zakonu o dvojni negaciji $p \equiv \neg\neg p$. Izjavo torej lahko dokažemo tako, da predpostavimo njeno negacijo, in od tod izpeljemo neresnico. Tipičen besedni dokaz s protislovjem izgleda takole: "Dokazujemo p. Pa recimo, da p ne velja. Potem /neki sklepi/. To je v nasprotju s tem, kar smo dokazali prej, torej smo izpeljali protislovje. Se pravi, ni možno, da p ne bi veljal, torej mora veljati."

(mnogo zgovornih primerov dokazov, ki ponazorijo zgornje postopke)

4.1 Vaje

(Kako bomo zapisovali rešitve nalog z navodilom "*dokaži*"? Ali jih bomo pisali tako kot na predavanjih in bomo posodobili to poglavje v učbeniku? –Anja)

Vaja 4.1. Dokažite naslednje izjave:

1. $p \wedge q \Rightarrow p \vee q$
2. $p \Rightarrow (q \Rightarrow p)$
3. $p \wedge q \Rightarrow \neg(\neg p \vee \neg q)$
4. $(p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$
5. $(p \Rightarrow (q \vee r) \wedge q \Rightarrow \neg p) \Rightarrow (p \Rightarrow r)$

Vaja 4.2. Preveri veljavnost naslednjih sklepov. (Ali to nalogo nekoliko preoblikujemo, ali pa povemo, da imamo lahko več predpostavk? –Anja)

1. Študent se je s trolejbusom peljal na izpit. Rekel si je: "*Če bo semafor pri Drami zelen, bom naredil izpit.*" No, ko je avtobus pripeljal na križišče, je semafor svetil rdečo, študent pa si je dejal: "*Presneto, spet bom padel.*"
2. Če preveč pijem ali kadim, slabo spim. Če slabo spim ali premalo jem, sem utrujen. Če sem utrujen, ne telovadim in ne študiram. Preveč kadim. Torej ne študiram.
3. Če ima Biblija prav, potem obstajata Bog in hudič. Če obstaja Bog, je na svetu veselje. Če obstaja hudič, je na svetu žalost. Na svetu sta veselje in žalost. Sklep: Biblija ima prav.
4. Razglednik Vid vsako soboto obišče Ljubljanski grad. Na grič se vzpne po Študentovski poti (s tržnice) ali Mačji stezi (skozi gozd), včasih pa kar po cesti. Če gre po prvi poti, s seboj nosi svežo zelenjavo s tržnice. Kadar se vzpne po Mačji stezi, spotoma nabere za pest odpadlega listja. To soboto Vid na grad ni šel po cesti in s sabo ni nosil zelenjave. Torej je na grad dospel z listjem v rokah.

Vaja 4.3. Dokažite naslednje izjave:

1. $(\forall x \in A.\, p(x)) \vee (\forall y \in A.\, q(y)) \Rightarrow \forall z \in A.\, p(z) \vee q(z)$
2. $(\exists x \in A.\, p(x)) \vee (\exists y \in A.\, q(y)) \Rightarrow \exists z \in A.\, p(z) \vee q(z)$
3. $(\exists x \in A. \forall y \in B.\, p(x,y)) \Rightarrow \forall b \in B. \exists a \in A.\, p(a,b)$

Vaja 4.4. Dokažite naslednje izjave:

1. $(\exists n \in \mathbb{N}.\, 24 \cdot n = a) \Rightarrow \exists k \in \mathbb{N}.\, 3 \cdot k = a.$
2. $\forall m \in \mathbb{N}. \exists \ell \in \mathbb{N}.\, (m^2 = 4\ell \vee m^2 = 4\ell + 1).$
   Namig: brez dokaza smemo uporabiti dejstvo $\forall n \in \mathbb{N}. \exists k \in \mathbb{N}.\, (n = 2k \vee n = 2k+1)$.

Vaja 4.5. Dana je funkcija $f : \mathbb{R} \to \mathbb{R}$. Dokažite naslednje izjave:

1. $\forall x \in \mathbb{R}. \exists y \in \mathbb{R}.\, f(x) \leq y.$
2. $(\exists M \in \mathbb{R}. \forall x \in \mathbb{R}.\, f(x) \leq M) \Rightarrow \forall x \in \mathbb{R}. \exists y \in \mathbb{R}.\, f(x) \leq y.$
3. $(\exists M \in \mathbb{R}. \forall x \in \mathbb{R}.\, f(x) \leq M) \Rightarrow \exists N \in \mathbb{R}. \forall x \in \mathbb{R}.\, 2 \cdot f(x) + 7 \leq N.$
4. $(\exists M \in \mathbb{R}. \forall x \in \mathbb{R}.\, x^2 + 7 \leq M) \Rightarrow \forall x \in \mathbb{R}. \exists y \in \mathbb{R}.\, x^2 + 7 \leq y.$

Vaja 4.6. Dokažite naslednji ekvivalenci:

1. $\neg(\exists x \in A.p(x)) \iff \forall x \in A.\neg p(x)$.
2. $\neg(\forall x \in A.p(x)) \iff \exists x \in A.\neg p(x)$.

Za dokaz druge ekvivalence lahko uporabite prvo.

Poglavje 5

Konstrukcije množic

(podmnožice, potenčne množice, kvocientne množice,...)

(Če "embedding" prevajamo kot "vložitev", kako potem prevedemo "inclusion"? Imamo sicer tujko "inkluzija", ampak fino bi bilo imeti še slovenski izraz. Vključitev? –Davorin)

5.1 Vaje

Poglavje 6

Preslikave

6.1 Slike in praslike

Preslikava kot taka nam pove za posamične elemente, kam se slikajo. Marsikdaj pa nas zanima več: kam se slikajo celotne množice elementov. Na primer, zanima nas lahko, v kaj se projicira neko prostorsko telo na ravnino.

(luštna slika projekcije nekega prostorskega objekta na neko ravnino)

Da dobimo sliko celotne množice, moramo zbrati skupaj slike vseh posamičnih elementov množice. Smiselna je torej naslednja definicija.

Definicija 6.1. Naj bo $f\colon X \to Y$ preslikava. ***Slika*** množice $A \subseteq X$ je označena in definirana kot

$$f_*(A) := \{f(x) \mid x \in A\} = \{y \in Y \mid \exists x \in A.\, y = f(x)\}.$$

Ta predpis definira preslikavo $f_*\colon \mathcal{P}(X) \to \mathcal{P}(Y)$.

Opomba 6.2. Kot običajno, obstajajo različne oznake v uporabi. Sliko $f_*(A)$ se označuje tudi kot $f[A]$ ali celo kar kot $f(A)$. V slednjem primeru se predpostavlja zadostna matematična zrelost bralca, da zna razbrati, kdaj f označuje preslikavo $f\colon X \to Y$, kdaj pa preslikavo $f\colon \mathcal{P}(X) \to \mathcal{P}(Y)$.

V tej knjigi se bomo načrtno izogibali takšnim dvoumnostim in za sliko dosledno uporabljali oznako iz definicije 6.1.

Naloga 6.3. Prepričaj se, da za poljubno preslikavo $f\colon X \to Y$ velja sledeče:

- $f_*(X) = Z_f$,
- $f_*(\emptyset) = \emptyset$,
- $f_*(\{x\}) = \{f(x)\}$ za vsak $x \in X$.

(primeri in lastnosti slik že tu ali kasneje skupaj s primeri/lastnostmi praslik?)

Včasih pa imamo obratno nalogo: iz dane slike ugotoviti, kaj vse se je z neko preslikavo vanjo preslikalo. Zato vpeljemo še sledečo definicijo.

Definicija 6.4. Naj bo $f\colon X \to Y$ preslikava. ***Praslika*** množice $B \subseteq Y$ je označena in definirana kot

$$f^*(B) := \{x \in X \mid f(x) \in B\}.$$

Ta predpis definira preslikavo $f^*\colon \mathcal{P}(Y) \to \mathcal{P}(X)$.

Opomba 6.5. Tudi za prasliko obstajajo različne oznake. Praslika $f^*(B)$ se označi tudi kot $f^{-1}[B]$ ali kar kot $f^{-1}(B)$. V slednjem primeru se spet zanašamo na izkušenost bralca, da praslike $f^{-1}\colon \mathcal{P}(Y) \to \mathcal{P}(X)$ ne zamenja z obratom $f^{-1}\colon Y \to X$. Slednji morda sploh ne obstaja! (Praslika seveda obstaja za vse funkcije.)

Če obrat funkcije obstaja, tedaj velja $f^*(\{y\}) = \{f^{-1}(y)\}$ za vsak $y \in Y$ (premisli!), kar nekoliko pojasni oznako f^{-1} tudi za prasliko. Kljub vsemu, z namenom izogibanja dvoumnostim se bomo v tej knjigi skrbno držali oznake iz definicije 6.4 za prasliko.

Ko smo že pri alternativnih, potencialno zavajajočih oznakah: pri prasliki enojca se tipično izpuščajo zaviti oklepaji, torej se namesto $f^*(\{y\})$ piše $f^*(y)$ (ali celo $f^{-1}(y)$).

(primeri, vaje)
(lastnosti: ohranjanje unij, presekov, komplementov)

6.2 Injektivnost in surjektivnost

(Vključno z ekvivalenco z mono- in epimorfizmi.)

6.3 Bijektivnost in obratne preslikave

Kot dobro veste že iz srednje šole, nam injektivnost in surjektivnost omogočata definicijo bijektivnosti.

Definicija 6.6. Preslikava je ***bijektivna***, kadar je injektivna in surjektivna.

To pomeni: če imamo bijektivno preslikavo (na kratko kar: ***bijekcijo***) $f\colon X \to Y$, smo povezali elemente množice X z elementi množice Y, in sicer tako, da vsakemu elementu v katerikoli od množic X oz. Y pripišemo natanko en element druge množice.

(slika dveh množic s poparjenimi pikami) (Nevarno se je igrati s kropom. –Andrej)

Rečemo, da so elementi množice X v ***bijektivni korespondenci*** (ali po slovensko ***povratno enolični zvezi***) z elementi množice Y. Bijektivnost se na grafih kaže takole: preslikava je bijektivna, kadar vsaka vodoravnica seka njen graf natanko enkrat.

Bijektivne preslikave igrajo pomembno vlogo v matematiki. Oglejmo si tri primere.

- Če imamo povratno enolično zvezo med elementi dveh množic, je jasno, da imata isto število elementov. To nam omogoča definicijo ***kardinalnosti*** množic — glej poglavje (o kardinalnosti).

- Predstavljajmo si, da so elementi neke množice X imena za določene objekte. Na bijektivno preslikavo $f\colon X \to Y$ lahko potem gledamo kot na preimenovanje teh objektov. Seveda preimenovanje ne spremeni narave (ali če hočete natančnejši izraz, matematične strukture) objektov — z drugimi besedami, X in Y se razlikujeta zgolj po imenih svojih elementov. To nas privede do pojma ***izomorfizma***. Za več podrobnosti glej poglavje (o strukturiranih množicah).

- Če imamo povratno enolično zvezo med elementi množic X in Y, potem ta zveza ne podaja zgolj preslikave v smeri $X \to Y$, pač pa tudi v smeri $Y \to X$, ker za vsak element iz Y obstaja enolično določen element iz X, ki se vanj preslika. Z drugimi besedami, bijektivne preslikave imajo ***obrate***.

(Od tu sem iztrgal robo o obratih in izomorfizmih, tako da bo treba ta razdelek še popraviti. –Andrej)

Zakaj se sploh ukvarjamo z obrati? Pogosto obravnavamo preslikavo, ki izhaja iz nekega konkretnega (na primer fizikalnega) problema, v smislu, da preslikava vzame začetne podatke in nam vrne, kaj se bo na koncu zgodilo. Marsikdaj pa hočemo rešiti obraten problem: želimo določene končne rezultate in se sprašujemo, kakšni morajo biti začetni pogoji, da jih bomo dosegli. V takem primeru pride prav obratna preslikava.

Kot omenjeno, je obrat preslikave enoličen. Ne velja pa, da za poljubne preslikave sploh obstaja. Na primer, naj bo f edina možna preslikava $\{0,1\} \to \{()\}$, torej tista, ki tako 0 kot 1 preslika v $()$. Nobena preslikava $g\colon \{()\} \to \{0,1\}$ ne more biti obrat preslikave f, saj je $g \circ f$ gotovo konstantna in potemtakem ne more biti identiteta na $\{0,1\}$.

Kdaj torej obstaja obrat preslikave?

Trditev 6.7. *Za poljubno preslikavo $f\colon X \to Y$ sta ekvivalentni sledeči trditvi.*

1. *Preslikava f je obrnljiva.*
2. *Preslikava f je bijektivna.*

Dokaz. $(1 \Rightarrow 2)$

Predpostavljamo, da obstaja obrat f^{-1}.

Dokažimo, da je f injektivna. Vzemimo poljubna $x, y \in X$, za katera velja $f(x) = f(y)$. Tedaj $x = f^{-1}\big(f(x)\big) = f^{-1}\big(f(y)\big) = y$.

Dokažimo, da je f surjektivna. Vzemimo poljuben $y \in Y$. Tedaj $y = f\big(f^{-1}(y)\big)$.

$(2 \Rightarrow 1)$

Če je f bijekcija, za vsak $y \in Y$ velja, da je $f^*\big(\{y\}\big)$ enojec (glej (ustrezne predhodne trditve v razdelku o injektivnosti in surjektivnosti)). Definirajmo $g\colon Y \to X$ na naslednji način: za vsak $y \in Y$ naj bo $g(y)$ tisti element $x \in X$, za katerega velja $f^*\big(\{y\}\big) = \{x\}$. (Iz lastnosti praslike sledi, da je g obrat f.)

□

Iz dokaza te trditve vidimo, da bi bilo koristno imeti oznako za "tisti element", če želimo podajati tovrstne preslikave s simboli. Naj bo ϕ lastnost elementov množice X (torej predikat $\phi\colon X \to \Omega$), ki je resnična za natanko en element. Dogovorimo se, da

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

pomeni "tisti (edini) element množice X, ki ima lastnost ϕ" (simbolček na začetku je mala grška črka jota). Zdaj lahko izrecno zapišemo: če je $f\colon X \to Y$ bijekcija, tedaj je njen obrat $f^{-1}\colon Y \to X$ dan s predpisom

$$f^{-1}(y) = \iota x \in X.\, (f(x) = y).$$

(Andrej, omenjal si, da želiš imeti to oznako. Če sem kaj zgrešil, prosim popravi. –Davorin)

Zaenkrat smo to joto uporabljali zgolj kot okrajšavo za stavek v običajnem jeziku, ampak če želimo ι-izraze uporabljati v matematičnih dokazih, jim moramo dati natančen matematični pomen. Definirajmo torej joto formalno matematično.

Naj bo X poljubna množica. Na njej imamo enakost; obravnavajmo jo na tem mestu kot lastnost dvojic elementov iz X, torej kot predikat $=_X\colon X \times X \to \Omega$ (za vsak par elementov

vrnemo resničnostno vrednost izjave, da sta komponenti para enaki). Transponirajmo to preslikavo; dobimo $\widehat{=_X}\colon X \to \Omega^X$. Ta transponiranka je injektivna: če se za $a, b \in X$ preslikavi $\lambda x \in X.\,(a = x)$ in $\lambda x \in X.\,(b = x)$ ujemata, se ujemata tudi njuni vrednosti pri b. Ker drži $b = b$, potem drži tudi $a = b$.

Če zožimo kodomeno preslikave $\widehat{=_X}$ na njeno sliko, potemtakem dobimo bijekcijo. Naj bo jota njen obrat, torej $\iota := \left(\widehat{=_X}|^{Z_{\widehat{=_X}}} \right)^{-1}$. V tem smislu je zgornja oznaka $\iota x \in X.\,\phi(x)$ okrajšava za $\iota(\lambda x \in X.\,\phi(x))$ (kar bi seveda lahko še skrajšali do $\iota(\phi)$, ampak v praksi je to običajno manj zgovorno).

6.4 Vaje

Poglavje 7

Relacije

7.1 Splošno o relacijah

V matematiki pogosto želimo izraziti, da so določeni objekti v nekem odnosu, npr. eno število je večje od drugega; temu s tujko rečemo ***relacija***. Kako to formalno izraziti? Ideja je, da relacijo podamo z množico vseh skupin elementov, ki so v relaciji. Na primer, relacijo $\leq$ na naravnih številih podamo kot podmnožico

$$\{(a, b) \in \mathbb{N} \times \mathbb{N} \mid \exists n \in \mathbb{N}.\, a + n = b\}.$$

Torej, število a je v relaciji $\leq$ s številom b takrat, ko par (a, b) pripada tej množici.

Splošne relacije so lahko med poljubno mnogo elementi iz poljubnih (ne nujno istih) množic. Na primer, relacija komplanarnosti štirih točk v prostoru je podmnožica produkta $\mathbb{R}^3 \times \mathbb{R}^3 \times \mathbb{R}^3 \times \mathbb{R}^3$, relacija pripadnosti $\in$ med elementi neke množice X in podmnožicami množice X pa je podmnožica produkta $X \times \mathcal{P}(X)$.

Splošna definicija relacije je potemtakem naslednja.

Definicija 7.1. ***Relacija*** na družini množic $\mathscr{D}$ je podmnožica produkta $\prod_{X \in \mathscr{D}} X$, skupaj s podatkom, za katero družino $\mathscr{D}$ gre.

Opomba 7.2. Kaj mislimo tu z izrazom "skupaj s podatkom"? Določena podmnožica ima mnogo nadmnožic in podatek, med elementi katerih množic opazujemo odnos, je za relacijo prav tako pomemben, saj so od tega odvisne lastnosti relacije. Lastnosti relacij obravnavamo kasneje v razdelku 7.3, ampak če že zdaj damo primer: $\{(a, a) \mid a \in \mathbb{N}\}$ je refleksivna kot relacija na naravnih številih (tj. kot podmnožica $\mathbb{N} \times \mathbb{N}$), ne pa tudi kot relacija na celih številih (tj. kot podmnožica $\mathbb{Z} \times \mathbb{Z}$).

Kako "priložiti" podatek o družini? Ena možnost je, da relacijo podamo kot urejeni par $\mathscr{R} = (R, \mathscr{D})$, kjer $R \subseteq \prod_{X \in \mathscr{D}} X$. Še ena možnost je, da relacijo podamo kot družino preslikav $(\mathscr{R} \to X)_{X \in \mathscr{D}}$, ki skupaj porodijo inkluzijo $\mathscr{R} \hookrightarrow \prod_{X \in \mathscr{D}} X$. Ampak načeloma je povsem vseeno, ali vzamemo katero od teh dveh možnosti ali še kaj tretjega. V tej knjigi se ne bomo omejevali na posamičen formalen zapis za relacijo, bo pa seveda v vseh primerih jasno, za katero družino gre.

(Verjetno bi bilo smiselno omeniti še možnost podajanja relacije kot predikat $\prod_{X \in \mathscr{D}} X \to \Omega$. –Davorin)

V praksi se povečini uporabljajo relacije med dvema elementoma.

Definicija 7.3. ***Dvomestna*** (ali ***dvojiška*** ali ***binarna***) ***relacija*** $\mathscr{R}$ med elementi množic X in Y je podmnožica produkta $X \times Y$, skupaj s podatkom o X in Y. Za takšno relacijo definiramo:

- množica X je ***začetna množica*** ali ***domena*** relacije $\mathscr{R}$, kar označimo $\mathrm{dom}(\mathscr{R})$,
- množica Y je ***ciljna množica*** ali ***kodomena*** relacije $\mathscr{R}$, kar označimo $\mathrm{cod}(\mathscr{R})$,
- ***območje definiranosti*** ali ***nosilec*** relacije $\mathscr{R}$ je množica $D_{\mathscr{R}} := \{x \in X \mid \exists y \in Y.\, x \mathscr{R} y\}$ (torej $D_{\mathscr{R}} \subseteq \mathrm{dom}(\mathscr{R})$),
- ***zaloga vrednosti*** ali ***slika*** (razpon?) relacije $\mathscr{R}$ je množica $Z_{\mathscr{R}} := \{y \in Y \mid \exists x \in X.\, x \mathscr{R} y\}$ (torej $D_{\mathscr{R}} \subseteq \mathrm{cod}(\mathscr{R})$).

Skoraj vse relacije, ki nas zanimajo v tej knjigi, so dvomestne. Zato se dogovorimo, da z izrazom "relacija" vselej mislimo dvomestno relacijo, razen če je izrecno rečeno drugače.

Če je $\mathscr{R} \subseteq X \times Y$ relacija, potemtakem lahko zapišemo, da sta $x \in X$ in $y \in Y$ v relaciji $\mathscr{R}$ takole: $(x, y) \in \mathscr{R}$. Ampak to vodi do čudnih zapisov v primeru običajnih relacij, npr. $(2, 3) \in <$. To je bolje zapisati $2 < 3$ in posledično se dogovorimo, da v primeru dvojiške relacije raje uporabljamo zapis $x \mathscr{R} y$.

Povečini se še dodatno omejimo na relacije z isto domeno in kodomeno.

Definicija 7.4. ***Dvomestna*** (***dvojiška***, ***binarna***) ***relacija*** na množici X je podmnožica produkta $X \times X$, skupaj s podatkom o X.

Takšne relacije lahko lepo ponazorimo z usmerjenimi grafi. Graf relacije $\mathscr{R} \subseteq X \times X$ je definiran takole: vozlišča grafa so elementi množice X in za vsaka dva elementa $a, b \in X$, za katera velja $a \mathscr{R} b$, narišemo puščico od a do b.

Zgled 7.5. Naj bo $X = \{A, B, C, D, E, F\}$ in naj bo

$$\mathscr{R} := \{...\}$$

relacija na X. Njen graf je videti takole.

(graf relacije $\mathscr{R}$)

7.2 Operacije z relacijami

Običajno je, da iz že danih matematičnih objektov lahko skonstruiramo nove s pomočjo določenih operacij. Z relacijami ni nič drugače; v tem razdelku si bomo ogledali običajne operacije na relacijah.

Ker so relacije podmnožice, imamo za začetek vse operacije na podmnožicah. Torej, za poljubno družino $(\mathscr{R}_i)_{i \in I}$ podmnožic produkta $X \times Y$ sta tudi unija $\bigcup_{i \in I} \mathscr{R}_i$ in presek $\bigcap_{i \in I} \mathscr{R}_i$ relaciji. Če je $\mathscr{R} \subseteq X \times Y$ relacija, je njena komplementarna relacija $\mathscr{R}^{\mathsf{C}} = X \times Y \setminus \mathscr{R} \subseteq X \times Y$.

Posebej imamo ***prazno relacijo*** $\emptyset \subseteq X \times Y$ (nobena dva elementa nista v relaciji) in ***polno relacijo*** $X \times Y \subseteq X \times Y$ (vsaka dva elementa sta v relaciji), ki sta si medsebojno komplementarni.

Poleg operacij, ki jih relacije podedujejo od podmnožic, imamo še operacije, ki upoštevajo produktno strukturo.

Če so X, Y, Z množice in $\mathscr{R} \subseteq X \times Y$, $\mathscr{S} \subseteq Y \times Z$ relaciji, tedaj je ***sklop*** (***kompozicija***, ***kompozitum***) ***relacij*** definiran kot

$$\mathscr{S} \circ \mathscr{R} := \left\{(x, z) \in X \times Z \;\middle|\; \exists y.\, [Y] x \mathscr{R} y \wedge y \mathscr{S} z\right\}$$

(po vzoru preslikav tudi sklop relacij pišemo v obratnem vrstnem redu; glej razdelek 7.4). Opazimo: domena $\mathscr{S} \circ \mathscr{R}$ je domena $\mathscr{R}$, kodomena $\mathscr{S} \circ \mathscr{R}$ je kodomena $\mathscr{S}$. Sklapljanje je asociativna operacija, torej pri sklopu več relacij oklepaji niso pomembni.

Naloga 7.6. Dokaži, da je sklapljanje relacij asociativno!

Večkraten sklop relacije $\mathscr{R} \subseteq X \times X$ same s sabo označimo

$$\mathscr{R}^n := \underbrace{\mathscr{R} \circ \mathscr{R} \circ \ldots \circ \mathscr{R}}_{n\ \mathscr{R}\text{-jev}}$$

za $n \in \mathbb{N}_{\geq 2}$. Seveda je smiselno definirati, da je $\mathscr{R}^1$ enak $\mathscr{R}$ in da je $\mathscr{R}^0$ relacija enakosti na množici X, saj je to enota za sklapljanje relacij na X, tj. $=_X \circ \mathscr{R} = \mathscr{R} = \mathscr{R} \circ =_X$ (premisli, da je to res!).

Zgled 7.7. Naj bo $\mathscr{R} \subseteq X \times X$ relacija. Tedaj iz grafa relacije zlahka razberemo, kaj je $\mathscr{R}^n$: elementa $a, b \in X$ sta v relaciji $\mathscr{R}^n$ natanko tedaj, ko imamo pot dolžine n od a do b (to deluje tudi za $n = 1$ in $n = 0$). Naj primer, če je $\mathscr{R}$ relacija iz zgleda 7.5, tedaj graf relacije $\mathscr{R}^3$ izgleda takole.

(graf $\mathscr{R}^3$)

Za poljubno relacijo $\mathscr{R} \subseteq X \times Y$ definiramo ***obratno*** (***inverzno***) ***relacijo*** kot

$$\mathscr{R}^{-1} := \{(y, x) \in Y \times X \mid x \mathscr{R} y\}$$

(torej ima obratna relacija glede na izvorno zamenjano domeno in kodomeno). Posledično lahko za poljubno relacijo $\mathscr{R} \subseteq X \times X$ definiramo njeno potenco s poljubno celo stopnjo: $\mathscr{R}^{-n} := (\mathscr{R}^{-1})^n = (\mathscr{R}^n)^{-1}$.

Naloga 7.8. Preveri, da velja $(\mathscr{S} \circ \mathscr{R})^{-1} = \mathscr{R}^{-1} \circ \mathscr{S}^{-1}$!

Zgled 7.9. Graf relacije, ki je obratna relaciji $\mathscr{R} \subseteq X \times X$, dobimo tako, da v grafu relacije $\mathscr{R}$ obrnemo puščice. Na primer, če je $\mathscr{R}$ relacija iz zgleda 7.5, tedaj je graf relacije $\mathscr{R}^{-1}$ videti takole.

(graf $\mathscr{R}^{-1}$)

Zgled 7.10. Naj bo L množica ljudi. Vpeljimo oznake za naslednje relacije na L:

- `St` je relacija "je starš od",
- `Oč` je relacija "je oče od",
- `Ma` je relacija "je mati od",
- `Si` je relacija "je sin od",
- `Hč` je relacija "je hči od",
- `Br` je relacija "je brat od",
- `Se` je relacija "je sestra od"

Na primer: Marko `Br` Metka pomeni "Marko je brat od Metke." (oz. v lepši slovenščini "Marko je Metkin brat.").

Velja med drugim:

$\texttt{Oč} \cup \texttt{Ma} = \texttt{St}$,
$\texttt{St} \circ \texttt{St} = \texttt{St}^2 =$ "je stari starš od",
$\texttt{St} \circ \texttt{Br} =$ "je stric od",
$\texttt{Br} \cup \texttt{Se} =$ "je sorojenec od",
$\texttt{St}^{-1} =$ "je otrok od",
$\bigcup_{n \in \mathbb{N}_{\geq 1}} \texttt{St}^n =$ "je prednik od",
$\bigcup_{n \in \mathbb{N}_{\geq 1}} \texttt{St}^{-n} =$ "je potomec od",
$\texttt{St} \circ (\texttt{Br} \cup \texttt{Se}) \circ \texttt{Hč} =$ "je sestrična od".

Sklapljanje relacij ni komutativno; na primer $\texttt{Ma} \circ \texttt{Oč}$ je stari oče po materini strani, $\texttt{Oč} \circ \texttt{Ma}$ pa stara mama po očetovi strani.

(V tem zgledu sicer predpostavljamo, da je vsaka oseba bodisi moškega bodisi ženskega spola, kar ni čisto res. Ima kdo kakšno idejo, kako se temu izogniti (in še vedno imeti lahko razumljiv zgled)? –Davorin)

(Na smiselnem mestu omenimo še zožitve relacij (tako domene kot kodomene).)

7.3 Lastnosti relacij

Vemo, da so na primer racionalna števila uporabnejša od celih, saj lahko v okviru njih dodatno delimo — z drugimi besedami, racionalna števila imajo več uporabne *strukture* oz. več uporabnih *lastnosti*. Podobno za relacije obstajajo lastnosti, ki so se skozi prakso izkazale za zelo uporabne. Nekatere izmed njih si bomo ogledali v tem razdelku.

Vse sledeče lastnosti se nanašajo na dvomestno relacijo z isto domeno in kodomeno.

Definicija 7.11. Naj bo $\mathscr{R} \subseteq X \times X$ relacija.

- Relacija $\mathscr{R}$ je ***povratna*** (ali ***refleksivna***), kadar velja

  $$\forall x \in X. \, x \mathscr{R} x,$$

  tj. vsak element je v relaciji s samim sabo.

- Relacija $\mathscr{R}$ je ***nepovratna*** (ali ***irefleksivna***), kadar velja

  $$\forall x \in X. \, \neg(x \mathscr{R} x),$$

  tj. noben element ni v relaciji s samim sabo.

- Relacija $\mathscr{R}$ je ***somerna*** (ali ***simetrična***), kadar velja

  $$\forall x, y \in X. \, (x \mathscr{R} y \implies y \mathscr{R} x),$$

  tj. če je en element v relaciji z drugim, je tudi drugi s prvim.

- Relacija $\mathscr{R}$ je ***protisomerna*** (ali ***antisimetrična***), kadar velja

  $$\forall x, y \in X. \, (x \mathscr{R} y \wedge y \mathscr{R} x \implies x = y),$$

  tj. dva elementa sta obojestransko v relaciji samo v primeru, če gre za en in isti element.

  (Mogoče pretiravam s slovenskimi imeni... –Davorin)

- Relacija $\mathscr{R}$ je ***nesomerna*** (ali ***asimetrična***), kadar velja

$$\forall x, y \in X. \, (\neg(x \mathscr{R} y \wedge y \mathscr{R} x)),$$

  tj. nobena dva elementa nista obojestransko v relaciji.

- Relacija $\mathscr{R}$ je ***prehodna*** (ali ***tranzitivna***), kadar velja

$$\forall x, y, z \in X. \, (x \mathscr{R} y \wedge y \mathscr{R} z \implies x \mathscr{R} z),$$

  tj. če je en element v relaciji z drugim in drugi s tretjim, je tudi prvi v relaciji s tretjim.

- Relacija $\mathscr{R}$ je ***neprehodna*** (ali ***intranzitivna***), kadar velja

$$\forall x, y, z \in X. \, \neg(x \mathscr{R} y \wedge y \mathscr{R} z \wedge x \mathscr{R} z),$$

  tj. če je en element v relaciji z drugim in drugi s tretjim, prvi ne more tudi biti v relaciji s tretjim.

- Relacija $\mathscr{R}$ je ***enolična***, kadar velja

$$\forall x, y, z \in X. \, (x \mathscr{R} y \wedge x \mathscr{R} z \implies y = z),$$

  tj. vsak element je v relaciji s kvečjemu enim elementom.

- Relacija $\mathscr{R}$ je ***celovita***, kadar velja

$$\forall x \in X. \, \exists y \in Y. \, x \mathscr{R} y,$$

  tj. vsak element je v relaciji z vsaj enim elementom, se pravi $D_f = \mathrm{dom}(f)$.

- Relacija $\mathscr{R}$ je ***sovisna***, kadar velja

$$\forall x, y \in X. \, (x \neq y \implies x \mathscr{R} y \vee y \mathscr{R} x),$$

  tj. za vsaka dva različna elementa velja, da je vsaj eden od njiju v relaciji z drugim.

- Relacija $\mathscr{R}$ je ***strogo sovisna***, kadar velja

$$\forall x, y \in X. \, (x \mathscr{R} y \vee y \mathscr{R} x),$$

  tj. za vsaka dva elementa velja, da je vsaj eden od njiju v relaciji z drugim.

Zgled 7.12. Za nekaj običajnih relacij si oglejmo njihove lastnosti.

- Relacija $\leq$ na $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ je refleksivna, antisimetrična, tranzitivna in strogo sovisna.
- Relacija $<$ na $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ je irefleksivna, asimetrična, tranzitivna in sovisna.
- Relacija deljivosti $\mid$ na $\mathbb{N}_{\geq 1}$ je refleksivna, antisimetrična in tranzitivna.
- Relacija $\subseteq$ na $\mathcal{P}(X)$ je refleksivna, antisimetrična in tranzitivna.
- Relacija enakosti $=_X$ na katerikoli množici X je refleksivna, simetrična, antisimetrična, tranzitivna in enolična.

Lastnost relacije	**Izražava z operacijami**	**Lastnost grafa**
refleksivnost	$=_X \subseteq \mathscr{R}$	Vsako vozlišče ima zanko.
irefleksivnost	$=_X \cap \mathscr{R} = \emptyset$	Nobeno vozlišče nima zanke.
simetričnost	$\mathscr{R} = \mathscr{R}^{-1}$	Vsaka puščica ima nasprotno puščico.
antisimetričnost	$\mathscr{R} \cap \mathscr{R}^{-1} \subseteq =_X$	Edine puščice z nasprotnimi puščicami so zanke.
asimetričnost	$\mathscr{R} \cap \mathscr{R}^{-1} = \emptyset$	Nobena puščica nima nasprotne puščice.
tranzitivnost	$\mathscr{R}^2 \subseteq \mathscr{R}$	Za vsako pot pozitivne dolžine obstaja puščica, ki gre od začetka do konca poti.
intranzitivnost	$\mathscr{R}^2 \cap \mathscr{R} = \emptyset$	Za nobeno pot pozitivne dolžine ne obstaja puščica, ki gre od začetka do konca poti.
enoličnost	$\mathscr{R} \circ \mathscr{R}^{-1} \subseteq =_X$	Iz vsakega vozlišča gre kvečjemu ena puščica.
celovitost	$=_X \subseteq \mathscr{R}^{-1} \circ \mathscr{R}$	Iz vsakega vozlišča gre vsaj ena puščica.
sovisnost	$=_X \cup \mathscr{R} \cup \mathscr{R}^{-1} = X$	Vsaki dve različni vozlišči sta povezani s puščico.
stroga sovisnost	$\mathscr{R} \cup \mathscr{R}^{-1} = X$	Vsaki dve vozlišči sta povezani s puščico.

Tabela 7.1: Lastnosti relacije $\mathscr{R} \subseteq X \times X$ in njihove karakterizacije

Lastnosti operacij smo podali z izjavami, ampak lahko jih na ekvivalenten način podamo z operacijami ali lastnostmi grafa — glej tabelo 7.1.

Naloga 7.13. Dokaži, da so vse karakterizacije v vsaki vrstici tabele 7.1 res ekvivalentne!

Marsikdaj imamo sledeči problem: za določene pare elementov $(x_i, y_i)_{i \in I}$ hočemo, da so v neki relaciji in relacija mora zadoščati predpisani lastnosti. Kako definirati takšno relacijo? Smiselna izbira je vzeti najmanjšo relacijo s predpisano lastnostjo, ki vsebuje vse (x_i, y_i). V ta namen definiramo pojem ogrinjače relacij.

Definicija 7.14. Naj bo $\mathscr{R} \subseteq X \times X$ relacija in $\mathscr{L}$ lastnost relacij na X. Najmanjša relacija na X, ki vsebuje $\mathscr{R}$ in ima lastnost $\mathscr{L}$, se imenuje ***$\mathscr{L}$-ogrinjača*** ali ***$\mathscr{L}$-ovojnica*** relacije $\mathscr{R}$.

Ogrinjača relacije je dobro definirana (v smislu, da je enolično določena): če imamo dve relaciji $\mathscr{R}$ in $\mathscr{S}$, ki obe vsebujeta dano relacijo in imata lastnost $\mathscr{L}$ ter sta najmanjši taki, mora potem veljati, da sta vsebovani ena v drugi, tj. $\mathscr{R} \subseteq \mathscr{S}$ in $\mathscr{S} \subseteq \mathscr{R}$, kar pomeni, da sta enaki.

Ni pa nujno, da ogrinjača dane relacije za dano lastnost sploh obstaja — na primer, irefleksivna ogrinjača ne obstaja za nobeno relacijo, ki ni že sama po sebi irefleksivna (premisli, zakaj). Seveda, če relacija je irefleksivna, tedaj je svoja lastna irefleksivna ogrinjača. To očitno velja v splošnem: če ima relacija lastnost $\mathscr{L}$, je enaka svoji $\mathscr{L}$-ogrinjači.

Premislimo, kdaj smo lahko gotovi, da ogrinjača obstaja.

Definicija 7.15. Naj bo X množica in $\mathscr{L}$ lastnost relacij na X. Rečemo, da je $\mathscr{L}$ ***presečno dedna***, kadar velja: poljuben presek relacij na X z lastnostjo $\mathscr{L}$ prav tako ima lastnost $\mathscr{L}$.

Naloga 7.16. Dokaži: konjunkcija končno mnogo presečno dednih lastnosti relacij na dani množici je presečno dedna.

Trditev 7.17. *Če je $\mathscr{L}$ presečno dedna lastnost relacij na X, tedaj za vsako relacijo $\mathscr{R}$ na X obstaja njena $\mathscr{L}$-ogrinjača, in sicer je enaka preseku vseh relacij na X, ki vsebujejo $\mathscr{R}$ in imajo lastnost $\mathscr{L}$.*

Dokaz. Naj bo $\mathscr{S}$ presek vseh relacij na X, ki vsebujejo $\mathscr{R}$ in imajo lastnost $\mathscr{L}$. Posledično je $\mathscr{S}$ vsebovana v vseh relacijah na X z lastnostjo $\mathscr{L}$, ki vsebujejo $\mathscr{R}$. Ker je $\mathscr{L}$ presečno dedna lastnost, jo ima tudi $\mathscr{S}$. Prav tako $\mathscr{S}$ vsebuje $\mathscr{R}$. Torej je $\mathscr{S}$ $\mathscr{L}$-ogrinjača $\mathscr{R}$. □

Kako pa vemo, kdaj je lastnost presečno dedna? Včasih lahko to razberemo kar iz oblike logične formule, s katero je lastnost podana.

Izrek 7.18. *Naj bo $\mathscr{L}$ lastnost relacij na množici X, ki jo lahko za poljubno relacijo $\mathscr{R}$ podamo z zapisom oblike*

$$\forall x_1, x_2, \ldots, x_n \in X. (\phi(\mathscr{R}, x_1, x_2, \ldots, x_n) \implies \psi(\mathscr{R}, x_1, x_2, \ldots, x_n)),$$

kjer sta $\phi(\mathscr{R}, x_1, x_2, \ldots, x_n)$ in $\psi(\mathscr{R}, x_1, x_2, \ldots, x_n)$ konjunkciji končno mnogo členov oblike $x_i \mathscr{R} x_j$ — v posebnem primeru je lahko $\phi(\mathscr{R}, x_1, x_2, \ldots, x_n)$ konjunkcija nič členov in potem je $\mathscr{L}$ podana z zapisom oblike

$$\forall x_1, x_2, \ldots, x_n \in X. \psi(\mathscr{R}, x_1, x_2, \ldots, x_n).$$

Tedaj je $\mathscr{L}$ presečno dedna lastnost in torej ima vsaka relacija na X $\mathscr{L}$-ogrinjačo.

Dokaz. Naj bo $(\mathscr{R}_i)_{i \in I}$ poljubna družina relacij na X z lastnostjo $\mathscr{L}$ in naj bo $\mathscr{R} := \bigcap_{i \in I} \mathscr{R}_i$ njen presek. Dokazujemo, da $\mathscr{L}$ velja za $\mathscr{R}$.

Vzemimo poljubne $x_1, x_2, \ldots, x_n \in X$, za katere velja $\phi(\mathscr{R}, x_1, x_2, \ldots, x_n)$. Ker je $\phi(\mathscr{R}, x_1, x_2, \ldots, x_n)$ konjunkcija členov oblike $x_i \mathscr{R} x_j$, velja tudi $\phi(\mathscr{R}_i, x_1, x_2, \ldots, x_n)$ za vsak $i \in I$. Po predpostavki torej velja $\psi(\mathscr{R}_i, x_1, x_2, \ldots, x_n)$ za vsak $i \in I$.

Vzemimo poljuben člen $x_a \mathscr{R} x_b$ iz $\psi(\mathscr{R}, x_1, x_2, \ldots, x_n)$. Videli smo, da velja $x_a \mathscr{R}_i x_b$ za vsak $i \in I$, torej velja $x_a \mathscr{R} x_b$.

Vidimo, da pod našimi predpostavkami velja $\psi(\mathscr{R}, x_1, x_2, \ldots, x_n)$. Sklenemo, da velja lastnost $\mathscr{L}$ za relacijo $\mathscr{R}$. □

Posledica 7.19. *Za naslednje lastnosti relacij (in njihovo poljubno konjunkcijo) vselej obstaja ogrinjača: refleksivnost, simetričnost, tranzitivnost.*

Dokaz. Vse izmed naštetih lastnosti se po definiciji dajo zapisati v obliki iz izreka 7.18. Za njihovo konjunkcijo glej še vajo 7.16 in trditev 7.17. □

Naloga 7.20. Dokaži, da za poljubno relacijo $\mathscr{R}$ na množici X velja spodnja tabela!

Lastnost	**Ogrinjača relacije $\mathscr{R}$**
refleksivnost	$\mathscr{R} \cup =_X$
simetričnost	$\mathscr{R} \cup \mathscr{R}^{-1}$
tranzitivnost	$\bigcup_{n \in \mathbb{N}_{\geq 1}} \mathscr{R}^n$

(ena izmed nalog: Za relacijo $n \mathscr{R} (n+1)$ na $\mathbb{N}$ (ali $\mathbb{Z}$) preveri, da je njena tranzitivna ogrinjača $<$.)

7.4 Izpeljava preslikav iz relacij

Ko definiramo temeljne matematične pojme, imamo določeno mero izbire, kaj vzamemo za izvoren pojem, kaj pa definiramo s pomočjo drugih pojmov. V tej knjigi smo od začetka vzeli preslikave za bolj osnoven pojem in relacije lahko definiramo s pomočjo preslikav (kot omenjeno v opombi 7.2, relacijo lahko definiramo kot družino preslikav), lahko pa postopamo tudi obratno — pojem preslikave izpeljemo iz pojma relacije. Kako to gre, si bomo ogledali v tem razdelku.

Definicija 7.21. ***Delna preslikava*** (ali ***delna funkcija*** ali ***parcialna funkcija***) je enolična dvomestna relacija.

Kot dvomestna relacija ima vsaka delna preslikava določeno domeno, kodomeno, nosilec in zalogo vrednosti. Če je f delna preslikava z domeno X in kodomeno Y, to zapišemo kot $f \colon X \rightharpoonup Y$.

V primeru delne preslikave podmnožico produkta domene in kodomene, ki določa relacijo, označimo z Γ_f in imenujemo ***graf*** delne preslikave f (ne zamešaj tega s prej definiranim pojmom grafa relacije — prejšnji pojem je pomenil graf v smislu teorije grafov, sedanji pojem pa graf v smislu preslikav). Delna preslikava je torej v celoti podana z informacijo o domeni, kodomeni in grafu.

Ideja je, da za delno preslikavo $f \colon X \rightharpoonup Y$ za vsak $x \in D_f$ obstaja natanko en $y \in Y$, s katerim je x v relaciji. To potem zapišemo $f(x) = y$. Torej, če je x v definicijskem območju, rečemo, da je $f(x)$ definiran, kar zapišemo $f(x)\downarrow$, in v tem primeru je $f(x)$ enak vrednosti, s katero je x v relaciji. V nasprotnem primeru rečemo, da $f(x)$ ni definiran.

Če imamo dve vrednosti, ki morda nista definirani, ni posebej smiselno pisati enakosti med njima. Smiselna relacija med njima je ***Kleenejeva enakost***, kar pišemo $f(x) \simeq g(y)$, kar pomeni naslednje: leva stran $f(x)$ je definirana natanko tedaj, ko je definirana desna stran $g(y)$, in če sta obe definirani, sta enaki.

Zgled 7.22. Deljenje na realnih številih lahko obravnavamo kot delno preslikavo $/ \colon \mathbb{R} \times \mathbb{R} \rightharpoonup \mathbb{R}$; njen nosilec je $D_/ = \mathbb{R} \times \mathbb{R}_{\neq 0}$. Za vsak $x \in \mathbb{R}$ velja $\frac{x}{x^2} \simeq \frac{1}{x}$, ne pa tudi $\frac{x^2}{x} \simeq x$ (premisli, zakaj).

Zgled 7.23. Delne preslikave so zelo uporabne v računalništvu. Za algoritme pričakujemo, da jim podamo vhodne podatke in bodo potem vrnili želene izhodne podatke. Zgodi se pa lahko, da se algoritem pri nekaterih vhodnih podatkih nikoli ne ustavi (ali javi napako), se pravi, ne

dobimo rezultata. Če je P množica možnih podatkov, lahko poljuben algoritem obravnavamo kot delno preslikavo $P \rightharpoonup P$.[1]

Izkaže se, da za nekatere probleme ne obstaja računski postopek, ki bi pri vseh možnih vnosih vrnil pravilen odgovor. Primer tega je ***problem zaustavitve***: želimo algoritem, ki kot vhodna podatka sprejme poljuben algoritem in poljuben vnos ter se odloči, ali se dani algoritem pri danem vnosu ustavi. Kakršenkoli program, ki sprejme takšna podatka in nikoli ne vrne napačnega rezultata, nujno določa delno preslikavo, ki ni povsod definirana. (Verjetno bomo nekje hoteli imeti razdelek o diagonalizaciji; morda lahko tja dodamo dokaz te trditve. –Davorin)

Definicija 7.24. ***Preslikava*** (ali ***funkcija***) je celovita (z drugimi besedami, povsod definirana) delna preslikava. Če je domena preslikave f množica X in kodomena množica Y, to zapišemo kot $f\colon X \to Y$.

Seveda lahko vsako delno preslikavo zožimo do preslikave: delna preslikava $f\colon X \rightharpoonup Y$ porodi preslikavo $f|_{D_f} : D_f \to Y$.

Naloga 7.25. Operacijo sklapljanja $\circ$ smo definirali za splošne relacije (razdelek 7.2). Preveri, da se ta definicija ujema z običajno definicijo sklapljanja preslikav. Premisli še, kaj je sklop delnih preslikav.

7.5 Relacije urejenosti

Že od začetka tega poglavja kot klasične primere relacij podajamo razne urejenosti, kot $\leq$ in $<$. V tem razdelku si bomo ogledali, kakšne lastnosti morajo imeti relacije, da na določen način "urejajo" množico.

Sledeča definicija povzame štiri tipične primere relacij urejenosti.

Definicija 7.26. Naj bo X množica in $\preceq$ relacija na X. Tedaj:

- relacija $\preceq$ je ***šibka urejenost***, kadar je refleksivna in tranzitivna,
- relacija $\preceq$ je ***delna urejenost***, kadar je antisimetrična šibka urejenost (tj. refleksivna, tranzitivna, antisimetrična),
- relacija $\preceq$ je ***linearna urejenost***, kadar je strogo sovisna delna urejenost (tj. refleksivna, tranzitivna, antisimetrična, strogo sovisna),
- relacija $\preceq$ je ***stroga linearna urejenost***, kadar je irefleksivna, tranzitivna in sovisna.

(Poimenovanja v zvezi s sovisnostjo in strogostjo sem povzel po trenutnih predavanjih iz Logike in množic, ampak mislim, da bi se strogost lahko naredila bolj konsistentna. –Davorin)

V tej definiciji smo uporabili znak $\preceq$ za relacijo. Pogosto uporabimo kakšen takšen znak, če hočemo sugerirati, da gre za relacijo urejenosti.

Tipična primera linearne oz. stroge linearne urejenosti sta relaciji $\leq$ in $<$ na številskih množicah $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. Tipičen primer delne urejenosti je relacija inkluzije $\subseteq$ na katerikoli potenčni množici $\mathcal{P}(X)$ (če ima X vsaj dva elementa, ta relacija ne bo linearna).

[1] Natančneje, to velja za deterministične algoritme (takšne, ki se pri enakih vhodnih podatkih vedno enako obnašajo). V primeru nedeterminističnih algoritmov dobimo splošno relacijo na P.

Primere šibkih urejenosti pogosto dobimo na sledeči način. Naj bo $f\colon X \to Y$ preslikava in $\preceq_Y$ neka relacija urejenosti na Y. Za poljubna $a, b \in X$ definirajmo

$$a \preceq_X b := f(a) \preceq_Y f(b).$$

Tudi če je $\preceq_Y$ močnejše vrste relacija — delna ali linearna urejenost — je relacija $\preceq_X$ v splošnem zgolj šibka urejenost na X.

(še več primerov)
(razlaga imen relacij)
(najmanjši/največji, minimalni/maksimalni elementi, natančne meje)

7.6 Ekvivalenčne relacije in kvocientne množice

Ena temeljnih matematičnih dejavnosti je ***abstrakcija*** (pojmovanje? –Davorin), tj. iz posamičnih primerov izluščimo njihovo temeljno, bistveno lastnost in potem delamo s to lastnostjo. (To je pomembna stvar. Dajmo to razlago čimbolj izboljšati. –Davorin) Na primer, vemo, kaj pomeni "pet rac", "pet avtov", "pet sekund", ampak kaj pomeni "pet"?

V tem razdelku si bomo ogledali, kako lahko formalno abstrahiramo pojme s posamičnih primerov s pomočjo ekvivalenčnih relacij.

Definicija 7.27. ***Ekvivalenčna relacija*** je relacija, ki je refleksivna, simetrična in tranzitivna.

Ekvivalenčne relacije tipično označimo z $\sim$ (obstaja več načinov, kako to preberemo: vijuga, tilda, kača...) ali čim podobnim.

Zgled 7.28. Vsaka množica X ima najmanjšo ekvivalenčno relacijo — enakost $=_X$ — in največjo — polno relacijo $X \times X$.

Zgled 7.29. Za poljubni celi števili $a, b \in \mathbb{Z}$ definiramo: a je v relaciji z b, kadar sta a in b iste parnosti. To določa ekvivalenčno relacijo na $\mathbb{Z}$.

Za poljubno relacijo $\mathscr{R} \subseteq X \times X$ in poljuben $a \in X$ lahko definiramo

$$[a]_{\mathscr{R}} := \{x \in X \mid a \mathscr{R} x\}.$$

Torej, $[a]_{\mathscr{R}}$ sestoji iz vseh elementov, s katerimi je a v relaciji. V primeru, da imamo ekvivalenčno relacijo $\sim$, imenujemo množico $[a]_\sim$ ***ekvivalenčni razred*** elementa a. Kadar je jasno, za katero ekvivalenčno relacijo gre, pogosto ekvivalenčne razrede krajše označujemo kar z $[a]$.

Bistvo ekvivalenčne relacije je, da ekvivalenčni razredi tvorijo razdelitev množice.

(Razdelitev množice bomo verjetno definirali že prej, najbrž pri vsotah množic. Če ne, potem na tem mestu pride še definicija razdelitve. –Davorin)

Izrek 7.30 (ekvivalenčne relacije natanko ustrezajo razdelitvam)**.** *Naj bo X poljubna množica.*

1. *Naslednji trditvi sta ekvivalentni za vsako relacijo $\mathscr{R}$ na X.*
   (a) *$\mathscr{R}$ je ekvivalenčna relacija.*
   (b) *$\{[a]_{\mathscr{R}} \mid a \in X\}$ je razdelitev množice X.*
2. *Za vsako razdelitev množice X obstaja enolično določena ekvivalenčna relacija $\sim$ na X, tako da je razdelitev enaka $\{[a]_\sim \mid a \in X\}$.*

Dokaz. 1. $(\boldsymbol{a} \Rightarrow \boldsymbol{b})$

$(\boldsymbol{b} \Rightarrow \boldsymbol{a})$

2.
(dokončaj dokaz) □

Če je $\sim$ ekvivalenčna relacija na množici X, tedaj množico vseh njenih ekvivalenčnih razredov označimo z

$$X/_\sim := \{[a] \mid a \in X\}$$

in imenujemo ***kvocientna množica*** množice X po relaciji $\sim$.
(kvocientna množica kot množica abstrahiranih pojmov)

Naloga 7.31. Iz posledice 7.19 sklepamo, da za vsako relacijo na katerikoli množici obstaja njena ekvivalenčna ogrinjača. Dokaži: če je $\mathscr{R}$ relacija na množici X, tedaj je njena ekvivalenčna ogrinjača enaka

$$\bigcup_{n\in\mathbb{N}} (\mathscr{R} \cup \mathscr{R}^{-1})^n.$$

Naloga 7.32. Naj bo $(X, \preceq)$ šibka urejenost. Za poljubna $a, b \in X$ definiramo

$$a \approx b := a \preceq b \wedge b \preceq a.$$

1. Preveri, da je $\approx$ ekvivalenčna relacija na množici X.
2. Na kvocientni množici $X/_\approx$ definiramo relacijo $\leq$ na sledeči način: za poljubna $a, b \in X$ naj velja
$$[a] \leq [b] := a \preceq b.$$
Dokaži, da ta predpis podaja dobro definirano relacijo na $X/_\approx$.
3. Dokaži: $(X/_\approx, \leq)$ je delna urejenost.

To je kanoničen način, kako šibko urejenost okrepimo do delne urejenosti.

(Kakšen zanimiv zgled uporabe te vaje?)

Ko smo obravnavali bijekcije v razdelku 6.3, smo omenili, zakaj je uporabno imeti obrate preslikav. Težava je seveda, da imajo samo bijekcije obrate (v smislu, da so tudi obrati preslikave — kot relacije seveda imajo obrate), medtem ko včasih želimo obrniti tudi druge preslikave.

Vzemimo na primer eksponentno funkcijo $\lambda x.\, e^x$. Če jo obravnavamo kot preslikavo $\mathbb{R} \to \mathbb{R}$, seveda nima obrata, saj ni surjektivna. Ideja je, da zožimo kodomeno do zaloge vrednosti — preslikava $(\lambda x.\, e^x) : \mathbb{R} \to \mathbb{R}_{>0}$ je bijektivna in posledično lahko definiramo njen obrat (naravni logaritem) $\ln : \mathbb{R}_{>0} \to \mathbb{R}$.

To je standarden trik, če preslikava ni surjektivna. Kaj pa, če ni injektivna? Pogosto v tem primeru zožimo še domeno na območje, na katerem je preslikava injektivna. Na primer, preslikavo $(\lambda x.\, x^2) : \mathbb{R} \to \mathbb{R}$ zožimo do bijekcije $(\lambda x.\, x^2) : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, kjer imamo obrat $(\lambda x.\, \sqrt{x}) : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$.

Ima pa ta pristop težave. Prvič, v nasprotju z zožanjem kodomene pri zožitvi domene izgubimo določeno količino informacije o preslikavi (kam so se preslikale vrednosti, ki so prej bile v domeni, zdaj pa niso več?). Drugič, izbira zožene domene ni kanonična. Preslikavo $\lambda x.\, x^2$ bi ravno tako lahko zožili na $\mathbb{R}_{\leq 0} \to \mathbb{R}_{\geq 0}$ ali na $\mathbb{Q}_{\geq 0} \cup (\mathbb{R} \setminus \mathbb{Q})_{\leq 0} \to \mathbb{R}_{\geq 0}$ ali celo do $\emptyset \to \emptyset$ ali še neskončno drugih možnosti, pri katerih dobimo bijekcijo.

S pomočjo kvocientov lahko rešimo te probleme in najdemo kanoničen način, kako preslikavo popraviti do injektivne (in če dodamo še zožitev kodomene, do surjektivne in torej v celoti do bijektivne). Vemo že, da sta injektivnost in surjektivnost dualni (razdelek 6.2). Kaj je dualno zožitvi kodomene? Odgovor: kvocient domene. Namreč, če zožimo množico, je tako, kot da jo zdaj gledamo od precej bliže — vidimo samo manjše območje okoli sebe. Kvocienti počnejo obratno — tako je, kot če bi množico pogledali od precej daleč. Ne vidimo več posamičnih potez, pač pa se te združijo v bolj splošne oblike. (Seveda se ta dualnost, tako kot pri injektivnosti in surjektivnosti, da utemeljiti tudi formalno matematično. (Bomo govorili o zožkih in kozožkih? –Davorin))

Izrek 7.33 (naravna razčlenitev preslikave)**.** *Za vsako preslikavo $f\colon X \to Y$ obstaja (kanonična) razčlenitev*

$$f = i \circ \tilde{f} \circ q,$$

kjer je q surjekcija, $\tilde{f}$ bijekcija in i injekcija. Konkretno, $q\colon X \to X/_\sim$ je naravna kvocientna preslikava $q(x) = [x]$, pri čemer je ekvivalenčna relacija $\sim$ na X definirana kot

$$a \sim b := f(a) = f(b),$$

preslikava $i\colon Z_f \hookrightarrow Y$ je vključitev zaloge vrednosti v kodomeno, preslikava $\tilde{f}\colon X/_\sim \to Z_f$ pa je v celoti določena s pogojem

$$\tilde{f}([x]) = f(x)$$

(med drugim to pomeni, da sta množici $X/_\sim$ in $\operatorname{im}(f)$ v bijektivni korespondenci). (To je vir raznih izrekov o izomorfizmih v algebri. A povemo kaj na to temo? –Davorin)

Za ponazoritev, imamo spodnji diagram.
(diagram s tikz)

Dokaz. (napiši dokaz) □

7.7 Vaje

Poglavje 8

Strukture

Informacija, ki jo posamična množica podaja, je zgolj, katere elemente vsebuje. Izkušnje hitro pokažejo, da ta informacija ni najbolje naravnana za matematično delo. Po eni strani je del te informacije pogosto odveč: tipično si lahko z neko množico pomagamo enako, če njene elemente preimenujemo, tj. če obravnavamo izomorfno množico. Po drugi strani pa je te informacije premalo: ni dovolj, da vemo, katere elemente imamo na voljo, želimo vedeti tudi, kaj lahko s temi elementi počnemo. Podatek o tem imenujemo ***struktura*** množice.

Vzemimo za primer množico realnih števil $\mathbb{R}$. Njene elemente lahko poljubno seštevamo, odštevamo in množimo, tj. izvajamo določene operacije na njih (seveda imamo še cel kup drugih operacij, vključno z delnimi, kot so deljenje, potenciranje, logaritmiranje…). Strukturo, ki je dana z operacijami, imenujemo ***algebrska*** (ali ***algebrajska*** ali ***algebraična***).

Množico lahko opremimo tudi z raznimi relacijami, tipično z relacijami urejenosti. Na primer, na $\mathbb{R}$ imamo relaciji $\leq$ in $<$. To imenujemo ***struktura urejenosti*** (ali ***urejenostna struktura***).

Realna števila si lahko predstavljamo kot točke na številski premici. Vidimo, da lahko potem računamo razdaljo med njimi. Pravimo, da realna števila tvorijo ***metrični prostor*** oziroma da imajo realna števila ***metrično strukturo***.

Za realne intervale tudi znamo povedati, kdaj so odprti oz. zaprti. Kadar imamo pojem odprtosti oz. zaprtosti, to imenujemo ***topološka struktura***. Prav tako znamo povedati dolžino intervalov. Kadar imamo pojem velikosti podmnožic, to imenujemo ***merska struktura***.

Te in še nadaljnje strukture boste podrobneje spoznavali pri raznih matematičnih predmetih, v tej knjigi pa se bomo osredotočili zgolj na nekatere osnovne algebrske in urejenostne strukture.

Tipično velja: več kot imamo strukture na neki množici, bolj uporabna je (še zlasti, kadar se strukture med sabo prepletajo — na primer, dejstvo, da je seštevanje na $\mathbb{R}$ monotono, povezuje algebrsko in urejenostno strukturo na $\mathbb{R}$). Ker imajo realna števila tako bogato strukturo, ni presenetljivo, da jih kar naprej uporabljamo. Za primerjavo: množico vseh permutacij n elementov, ki se imenuje simetrična grupa in označi z S_n, uporabljate redkeje (je pa še vedno uporabna, saj premore nekaj operacij — permutacije lahko sklapljamo in obračamo).

Množico, opremljeno z neko strukturo, imenujemo ***strukturirana množica***. V tem kontekstu golo množico (brez njene dodatne strukture) imenujemo ***nosilna množica*** (te strukture).

Proučevanje struktur je ena temeljnih matematičnih dejavnosti. Na primer, pri predmetu Algebra spoznavate algebrske strukture, pri Topologiji topološke strukture, pri Analizi metrične in gladke strukture itd.

Za proučevanje strukture pa ne zadostuje opazovati zgolj množic, opremljenih s to struk-

turo, pač pa tudi preslikave med njimi, ki to strukturo na smiseln način ohranjajo. Tovrstnim preslikavam rečemo ***homomorfizmi***. Kaj točno to pomeni, bomo spoznali pri konkretnih strukturah v nadaljevanju tega poglavja.

(nekje (ne nujno tu) debata, kako strukturirano množico podamo preko njene karakterizacije — potrebna obstoj in enoličnost do izomorfizma)

8.1 Algebrske strukture

Kot rečeno, algebrska struktura je struktura, dana z operacijami. Operacije, na katere ste navajeni, imajo ***mestnost***, tj. koliko podatkov (ki jih imenujemo ***argumenti*** ali ***operandi***) sprejmejo, da vrnejo rezultat. Na primer, seštevanje vzame dva podatka (seštevanca ali sumanda), ki ju zapišemo na levo in desno stran plusa, da dobimo rezultat (vsoto). Seštevanje je torej dvomestna operacija.

Odštevanje je prav tako dvomestna operacija — od zmanjševanca odštejemo odštevanec in dobimo razliko. To je dvomestni minus, imamo pa tudi enomestni minus, ki vzame število in vrne njegovo nasprotno število. To sta dve različni operaciji in posledično imate zanju tudi dve različni tipki na kalkulatorju. Dvomestni minus je običajno označen kot $-$, enomestni pa kot ${}^{+}/_{-}$.

Še en primer enomestne operacije je faktoriela: za vsak $n \in \mathbb{N}$ lahko naračunamo $n!$, kar je spet naravno število. Primer tromestne operacije je mešani produkt vektorjev v trorazsežnem prostoru: za poljubne tri vektorje je njihov mešani produkt število, katerega absolutna vrednost pove prostornino paralelepipeda, ki ga ti vektorji razpenjajo, predznak pa pove orientacijo tega paralelepipeda.

V splošnem je n-mestna operacija na množici A dana kot preslikava $A^n \to A$, vsaj ko gre za operacijo, ki tako vzame kot vrne podatke iz množice A — taki operaciji rečemo ***notranja***. Če to ne velja, je operacija ***zunanja***. Vektorji lepo ponazorijo razliko. Seštevanje vektorjev v prostoru je preslikava $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$, torej dvomestna notranja operacija. Množenje vektorjev s skalarji $\mathbb{R} \times \mathbb{R}^3 \to \mathbb{R}^3$ je dvomestna zunanja operacija, kjer enega od argumentov vzamemo iz neke druge množice (v tem primeru iz $\mathbb{R}$). Skalarno množenje $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$ je prav tako dvomestna zunanja operacija, le da je tokrat rezultat iz druge množice. Prej omenjeni mešani produkt je tromestna zunanja operacija $\mathbb{R}^3 \times \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$.

V definiciji n-mestne operacije lahko vzamemo tudi $n = 0$. Ničmestna (notranja) operacija je torej preslikava $\mathbf{1} \to A$, se pravi izbira elementa iz A.

Obstajajo še splošnejše vrste operacij (npr. takšne, ki so odvisne od neskončno argumentov), ampak v tej knjigi se ne bomo ukvarjali z njimi.

8.1.1 Magme

Operacije, s katerimi imamo najpogosteje opravka, so tipično dvomestne. Če želimo obravnavati takšne operacije na splošno, si definiramo strukturo, ki zajema zgolj eno tako operacijo.

Definicija 8.1. ***Magma*** je množica, opremljena z dvomestno notranjo operacijo.

Strukturirano množico običajno zapišemo tako, da znotraj okroglih oklepajev najprej zapišemo simbol za nosilno množico, nato pa naštejemo vse sestavne dele strukture (ločene z vejicami). Če imamo strukturo magme na množici A in dano operacijo označimo z $\circledast$, tedaj to magmo zapišemo kot $(A, \circledast)$. Če hočemo poudariti, da je $\circledast$ dvomestna notranja operacija, lahko še natančneje zapišemo $(A,\ \circledast\colon A \times A \to A)$.

Imejmo magmi $(A, \circledast_A)$ in $(B, \circledast_B)$. Za preslikavo $f\colon A \to B$ rečemo, da je ***homomorfizem magem***, kadar ohranja magemsko strukturo v naslednjem smislu: za vse $x, y \in A$ mora veljati

$$f(x \circledast_A y) = f(x) \circledast_B f(y).$$

Z drugimi besedami, vseeno mora biti, če najprej izvedemo magemsko operacijo in nato izvrednotimo preslikavo ali obratno.

Če imamo magmo $(A, \circledast)$, lahko posamične elemente množice A povezujemo z operacijo in na ta način generiramo nove. Na primer, iz $x \in A$ lahko sestavimo izraze $x \circledast x$, $(x \circledast x) \circledast x$, $x \circledast (x \circledast x)$ itd. Če začnemo z večimi elementi, recimo $x, y, z \in A$, lahko dobimo bolj raznotere izraze, npr. $(x \circledast y) \circledast z$, $z \circledast ((y \circledast x) \circledast z)$ in tako naprej. Vsi ti izrazi so med sabo različni, njihove vrednosti pa so lahko bodisi enake bodisi različne. Na primer, v magmi $(\mathbb{N}, +)$ so $2 + 5$, $5 + 2$, $4 + 3$ in $(1 + 2) + (2 + 2)$ različni izrazi, ki pa imajo iste vrednosti.

Magemske izraze smo pisali kot zaporedja znakov, ki so vključevala elemente nosilne množice, simbol za operacijo in oklepaje (slednji so pomembni, saj v splošni magmi operacija ni družilna). Primernejši način podajanja takih izrazov so pa pravzaprav dvojiška drevesa. Vsakemu magemskemu izrazu ustreza neprazno dvojiško drevo, katerega listi so opremljeni z oznakami za elemente nosilne množice.

(nekaj primerov magemskih izrazov, podanih tako z dvojiškim drevesom kot z oklepajnim nizom)

Namen teh slikic pa ni zgolj ličen način, kako podati računanje neke operacije, pač pa se zadaj skrivajo vsaj tri temeljne ideje, ki so zelo pomembne za algebrske strukture in ki si jih bomo za začetek ogledali na preprostem primeru magem. Te tri ideje so:

- prosta struktura,
- homomorfizem kot preslikava, ki ohranja izraze,
- podajanje algebrske strukture z generatorji in relacijami.

Začnimo s pojmom proste strukture. Če imamo katerokoli množico A (ki jo v tem kontekstu običajno imenujemo ***baza***), jo lahko razširimo do magme na kanoničen način. Naj $T(A)$ označuje množico vseh magemskih izrazov, ki jih lahko dobimo iz elementov množice A, tj. množico vseh neprazniih dvojiških dreves, katerih listi so opremljeni z elementi množice A. Množico $T(A)$ opremimo z naslednjo dvojiško operacijo: če imamo izraza T_1 in T_2, tvorimo drevo, ki sestoji iz korena, katerega levo poddrevo je T_1, desno pa T_2.

Vsak element množice A lahko predstavimo z elementom množice $T(A)$: elementu $x \in A$ pripišemo drevo, ki vsebuje zgolj koren, ki je že kar list in je označen z x. Po domače povedano: vsaka vrednost je na trivialen način tudi izraz. To preslikavo $\eta_A\colon A \to T(A)$ imenujemo ***vložitev baze*** oz. ***vložitev generatorjev***. Izraz 'vložitev' je primeren, saj je ta preslikava očitno injektivna — izvorni element lahko preberemo z edinega lista v njegovi sliki.

Množico $T(A)$ skupaj z dano operacijo imenujemo ***prosta magma*** nad množico A (razlog za to poimenovanje bo postal jasen kasneje, ko si bomo ogledali podajanje algebrske strukture z generatorji in relacijami), kar označimo z $F(A)$. Ker lahko A vložimo v $T(A)$, smo v tem smislu dejansko razširili poljubno množico do magme.

Poglavje 9

Številske množice

Številske množice (naravna števila, cela števila, ...) poznate že od nekdaj. O njih imate zadosti občutka oz. intuitivne predstave, da jih lahko uporabljate in pridete do pravilnih rezultatov. Tudi v tej knjigi smo jih že kar naprej izkoriščali za razne primere.

Ampak intuitivna predstava je tudi vse, kar zaenkrat imamo o številskih množicah. Nismo še podali natančne matematične definicije zanje, na osnovi katere bi lahko neizpodbitno dokazovali izreke o njih.

Za vajo lahko sami premislite, ali bi znali na tem mestu podati natančno definicijo, kaj pomeni biti naravno, celo, racionalno oz. realno število. Definicija seveda mora biti natančna — npr. reči, da so realna števila tista, ki ležijo na številski premici, ni zadovoljiva definicija (vsaj ne, če ne pojasnite nedvoumno, kaj pomeni "številska premica" in kaj pomeni "ležati" na njej).

V tem poglavju se bomo sistematično lotili obravnave najpogosteje uporabljanih številskih množic. Podali bomo njihove konstrukcije, karakterizacije in temeljne lastnosti.

9.1 Naravna števila

9.1.1 Peanovi aksiomi

Če vas kdo vpraša, kako dobiti vsa naravna števila, verjetno odgovorite nekaj v naslednjem smislu: naravna števila so 0 in vsa tista števila, ki jih dobite s prištevanjem enice, tj. jemanjem naslednika. Torej, začnemo z 0, vzamemo naslednika in dobimo 1, nato še enkrat vzamemo naslednika in dobimo 2 itd.

Prvi, ki je znal to intuitivno predstavo preliti v natančno matematično definicijo, je bil Peano[1] komaj dobro stoletje nazaj. Pogoje, ki jih zahtevamo za neko množico, da jo lahko imenujemo "množica naravnih števil", po njem imenujemo ***Peanovi aksiomi***. (Nekje bomo predebatirali, kaj je aksiom in zakaj jih uporabljamo. Peanove aksiome povežimo s tem. –Davorin)

Če boste brskali po literaturi, boste naleteli na mnogo različnih inačic Peanovih aksiomov. Mi bomo izbrali sledečo jedrnato različico.

Definicija 9.1 (Peano)**.** ***Množica naravnih števil*** je množica (običajno označena z $\mathbb{N}$), skupaj z izbranim njenim elementom (običajno označenim z 0, kar beremo "ničla" ali "nič") in preslikavo na tej množici (običajno označeno z $\mathtt{S}\colon \mathbb{N} \to \mathbb{N}$, ki jo imenujemo "naslednik"), kadar veljajo naslednje lastnosti:

[1] Giuseppe Peano (1858 – 1932) je bil italijanski matematik.

- $\mathtt{S}$ je injektivna preslikava,
- $0 \notin Z_{\mathtt{S}}$,
- velja načelo ***matematične indukcije***: če je ϕ predikat na $\mathbb{N}$, za katerega velja

$$\phi(0) \qquad \text{in} \qquad \forall n \in \mathbb{N}.\, (\phi(n) \implies \phi(\mathtt{S}(n))),$$

  tedaj ϕ velja za vse elemente $\mathbb{N}$.

Poskusimo si zdaj natančno pojasniti pomen teh pogojev.

S pomočjo elementa 0 in preslikave $\mathtt{S}$ lahko v nedogled generiramo elemente množice $\mathbb{N}$. Začnemo z 0, nato vzamemo naslednika in dobimo $\mathtt{S}(0)$, nato vzamemo naslednika tega elementa in dobimo $\mathtt{S}(\mathtt{S}(0))$, nato naslednika $\mathtt{S}(\mathtt{S}(\mathtt{S}(0)))$ itd. Takšen zapis je sicer precej nepraktičen — si predstavljate, da rečete "dobimo se čez naslednika od naslednika od naslednika od naslednika od naslednika ničle ur" (namesto "dobimo se čez pet ur")? Zato sprejmemo dogovor: $\mathtt{S}(0)$ označimo krajše z 1 in preberemo "ena", $\mathtt{S}(\mathtt{S}(0))$ označimo z 2 in preberemo "dve" in tako naprej.[2]

Smo na ta način dobili neskončno različnih elementov $\mathbb{N}$? Če ne bi zahtevali zgornjih pogojev, to ne bi bilo nujno. Lahko bi se namreč zaciklali (v smislu, da je naslednik nekega elementa element, ki smo ga že prej navedli).

Včasih je takšno zaciklanje nekaj, kar dejansko hočemo. Na primer, pri algebri boste spoznali tako imenovane ***ciklične grupe***. Ciklično grupo z n elementi označimo $\mathbb{Z}_n$, njene elemente pa kar z $0, 1, \ldots, n-1$. Spodaj je slika ciklične grupe $\mathbb{Z}_5$.

(slika usmerjenega grafa, ki predstavlja $\mathbb{Z}_5$)

Puščice označujejo, kako slika naslednik v tej grupi: naslednik 0 je 1, naslednik 1 je 2, naslednik 2 je 3, naslednik 3 je 4, nato pa se zacikla in naslednik 4 je 0.

Pogoj $0 \notin Z_{\mathtt{S}}$ reče, da nič ni naslednik nobenega naravnega števila. Na ta način se izognemo, da bi naravna števila tvorila ciklično grupo.

Obstaja pa še en način, kako se lahko jemanje naslednika zacikla. Vzemimo spodnji primer.

(slike polgrupe $\{0, \ldots, 4\}$, ki se zacikla $4 \to 2$)

Nasledniki se lahko zaciklajo tudi pri elementu, ki ni 0. V danem primeru je naslednik 0 element 1, naslednik 1 je 2, naslednik 2 je 3, naslednik 3 je 4, naslednik 4 pa je 2.

Zakaj naravna števila niso taka? Ker v danem primeru $\mathtt{S}$ ni injektivna preslikava. Pogoj o injektivnosti nam v bistvu pove sledeče: naravna števila se ne morejo zaciklati pri nobenem nasledniku.

Vidimo, da se naravna števila ne morejo zaciklati niti na začetku (pri 0) niti nekje vmes v verigi naslednikov — torej gredo v nedogled, kot želimo. Z drugimi besedami, $0, \mathtt{S}(0), \mathtt{S}(\mathtt{S}(0)), \mathtt{S}(\mathtt{S}(\mathtt{S}(0))), \ldots$ so medsebojno različni elementi množice $\mathbb{N}$ in naravnih števil je posledično neskončno.

Čemu pa služi zadnji pogoj iz definicije 9.1, tj. načelo o indukciji? Že brez tega pogoja vemo, da so $0, \mathtt{S}(0), \mathtt{S}(\mathtt{S}(0)), \mathtt{S}(\mathtt{S}(\mathtt{S}(0))), \ldots$ naravna števila, česar pa ne vemo, je, da so to *vsa* naravna števila — da torej ni nobenih drugih.

[2] Trenutno dogovorjena sistematična imena za števila gredo do ***centiljona***, ki ga zapišemo z enico, ki ji sledi 600 ničel (vsaj pri nas; ponekod po svetu centiljon pomeni enica s 303 ničlami). To pomeni, da lahko sistematično izrazimo števila do $10^{606} - 1$ (= devetsto devetindevetdeset centiljard devetsto devetindevetdeset centiljonov devetsto devetindevetdeset novemnonagintiljard...). Nekateri razširijo to lestvico še z nadaljnjimi latinskimi izpeljankami, obstajajo pa tudi posebna imena za nekatera posamična velika števila, na primer ***gugol*** za 10^{100} (od tod izhaja ime spletnega brskalnika Google).

Naloga 9.2. Premisli, da množica $\mathbb{R}_{>-1}$ z naslednikom $\mathtt{S}(x) := x + 1$ zadošča vsem pogojem iz definicije 9.1, razen načelu indukcije.

Vidimo, da bi brez načela indukcije lahko imeli v množici $\mathbb{N}$ odvečna števila (takšna, ki jih ne štejemo kot naravna). S predpostavko o indukciji se to ne more zgoditi. Ta namreč pravi: če neka lastnost velja za začetni element verige $0, \mathtt{S}(0), \mathtt{S}(\mathtt{S}(0)), \mathtt{S}(\mathtt{S}(\mathtt{S}(0))), \ldots$ in če lahko sklepamo, da kakor hitro ta lastnost velja za določen element verige, velja tudi za naslednjega, potem ta lastnost velja za vsa naravna števila. Če za lastnost vzamemo "biti element te verige", iz načela o indukciji sklenemo, da se vsako naravno število nahaja nekje v tej verigi. Peanovi aksiomi torej podajajo strukturo, ki ustreza naši intuitivni predstavi množice naravnih števil.

Glede na to, da je načelo o matematični indukciji eden od osnovnih aksiomov, s katerimi so naravna števila podana, ne preseneča, da je indukcija eden najpogostejših načinov, kako dokazujemo izjave na naravnih številih. Natančneje rečeno, z matematično indukcijo dokazujemo univerzalno kvantificirane izjave na naravnih številih, torej izjave oblike

$$\forall n \in \mathbb{N}. \phi(n).$$

Po načelu indukcije za dokaz take izjave zadostuje narediti naslednje. Najprej dokažemo

$$\phi(0)$$

(da torej lastnost ϕ velja za začetno naravno število). To imenujemo ***temelj*** ali ***osnova*** ali ***baza*** indukcije. Nato dokažemo izjavo

$$\forall n \in \mathbb{N}. \phi(n) \implies \phi(\mathtt{S}(n));$$

to imenujemo ***indukcijski korak***. Z besedami, dokažemo, da kakor hitro velja lastnost ϕ za neko naravno število, mora veljati ta lastnost tudi za naslednje.

Intuitivno je jasno, da to mora delovati. Temelj indukcije nam pove, da dana lastnost velja za 0. Ker zdaj vemo, da velja za 0, mora po indukcijskem koraku veljati za naslednika ničle, torej za 1. Zdaj vemo, da velja za 1, torej mora po indukcijskem koraku veljati tudi za 2. Tako nadaljujemo: sklepamo, da lastnost velja za 3, nato za 4 in tako naprej. Ker se vsa naravna števila pojavijo v verigi naslednikov ničle, mora z indukcijo dokazana lastnost dejansko veljati za vsa naravna števila.

V poglavju 10 se bomo vrnili k indukciji, jo natančneje preučili in si ogledali primere dokazovanja z njo. Na tem mestu pa jo bomo uporabili za izpeljavo *rekurzije*, ki nam bo služila za definicijo nadaljnje strukture na naravnih številih.

9.1.2 Rekurzija

Poenostavljeno povedano, rekurzija pomeni, da določimo vrednost preslikave pri nekem argumentu iz (že prej naračunanih) vrednosti pri manjših argumentih. Tipičen primer rekurzivno podane preslikave je faktoriela: če zapišemo $0! := 1$ in $n! := (n+1) \cdot n!$ za vse $n \in \mathbb{N}$, smo s tem enolično podali preslikavo $! : \mathbb{N} \to \mathbb{N}$.

Naračunajmo nekaj vrednosti te preslikave. Neposredno iz definicije dobimo $0! = 1$ — to je ***temelj*** oz. ***osnova*** oz. ***baza*** rekurzije. Od tod s pomočjo ***rekurzijskega koraka*** izpeljemo

$$1! = 1 \cdot 0! = 1 \cdot 1 = 1.$$

S pomočjo te vrednosti in z rekurzijskim korakom lahko naračunamo vrednost faktoriele pri naslednjem naravnem številu.

$$2! = 2 \cdot 1! = 2 \cdot 1 = 2$$

In tako naprej.

$$3! = 3 \cdot 2! = 3 \cdot 2 = 6$$

$$4! = 4 \cdot 3! = 4 \cdot 6 = 24$$

$$5! = 5 \cdot 4! = 5 \cdot 24 = 120$$

$$\vdots$$

Vidimo, da lahko po tem postopku prej ali slej naračunamo $n!$ za poljuben $n \in \mathbb{N}$.

V primeru faktoriele smo neko vrednost naračunali iz predhodne, uporabljajo se pa tudi splošnejše rekurzivne definicije, kjer vrednost naračunamo iz večih prejšnjih. Slovit primer je ***Fibonaccijevo zaporedje*** $F\colon \mathbb{N} \to \mathbb{N}$, podano kot $F_0 := 0$, $F_1 := 1$ in $F_{n+2} := F_{n+1} + F_n$ za vse $n \in \mathbb{N}$. Od tod lahko naračunamo:

$$\begin{aligned}
F_0 &= 0,\\
F_1 &= 1,\\
F_2 &= F_1 + F_0 = 1 + 0 = 1,\\
F_3 &= F_2 + F_1 = 1 + 1 = 2,\\
F_4 &= F_3 + F_2 = 2 + 1 = 3,\\
F_5 &= F_4 + F_3 = 3 + 2 = 5,\\
F_6 &= F_5 + F_4 = 5 + 3 = 8,\\
&\vdots
\end{aligned}$$

Bo pa za naše potrebe zaenkrat zadostovala oblika rekurzije, kjer se skličemo samo na en predhodni člen, in na tako se bomo v tej knjigi tudi omejili. (Lahko pa vseeno v kakšni vaji zahtevamo od študentov, da zapišejo in dokažejo splošnejše načelo rekurzije. –Davorin)

Zakaj bi pa sploh podajali preslikave rekurzivno namesto z izrecnim (eksplicitnim) predpisom? Včasih to sledi iz narave problema. Na primer, imamo stanje, ki se razvija korak za korakom, kjer je trenutno stanje odvisno od prejšnjega. Zanima nas, kako se naš sistem razvija, in v tem primeru je naravno podati trenutno stanje sistema kot rekurzivno preslikavo. (ponazorimo s primerom)

Včasih preslikavo podamo rekurzivno, ker je rekurzivni predpis mnogo enostavnejši kot izrecni. Na primer, izrecna predpisa za faktorielo in Fibonaccijevo zaporedje sta

$$n! = \int_0^\infty x^n e^{-x}\, dx$$

in

$$F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}.$$

Odvisno od tega, katera vrednost vas zanima, utegneta biti ta dva predpisa mnogo bolj okorna za računanje, kot pa rekurzivna. Pravzaprav nekaj časa traja, da sploh dokažete, da so rezultati teh predpisov naravna števila!

Včasih pa preslikavo podamo rekurzivno preprosto zato, ker nimamo druge možnosti. Zgornja predpisa sicer podajata preslikavi izrecno, ampak cena za to je uporaba zapletenih operacij na realnih številih, kot so integral, eksponentna funkcija z naravno osnovo in korenjenje. Strogo vzeto smo zaenkrat od številskih množic definirali samo naravna števila, pa še zanje znamo povedati zgolj, kaj je 0 in kaj je naslednik. V bistvu še ne "znamo" niti seštevati!

S pomočjo rekurzije bomo lahko definirali ostalo strukturo, ki jo poznamo na naravnih številih: seštevanje, množenje in tako naprej. Za začetek pa natančno izoblikujmo in dokažimo načelo o rekurziji na naravnih številih. Iz zgornje razprave je jasno, da je rekurzija tesno povezana z indukcijo, od koder jo bomo tudi izpeljali.

Izrek 9.3 (Načelo rekurzije)**.** *Imejmo poljubni množici X in Y ter preslikavi $b\colon X \to Y$ in $r\colon X \times Y \times \mathbb{N} \to Y$. Tedaj obstaja natanko ena preslikava $f\colon X \times \mathbb{N} \to Y$, za katero velja*

$$f(x,0) = b(x)$$

in

$$f\big(x,\mathtt{S}(n)\big) = r\big(x,f(n,x),n\big)$$

za vse $x \in X$ in $n \in \mathbb{N}$.

Temu natančneje rečemo **načelo parametrizirane rekurzije***, ker pri preslikavi f na naravnih številih dopuščamo še poljuben parameter iz množice X. Če za X vzamemo enojec, se zgornja izjava reducira na sledeče* **načelo neparametrizirane rekurzije***.*

Če imamo množico Y, element $b \in Y$ in preslikavo $r\colon Y \times \mathbb{N} \to Y$, tedaj obstaja natanko ena preslikava $f\colon \mathbb{N} \to Y$, za katero velja

$$f(0) = b$$

in

$$f\big(\mathtt{S}(n)\big) = r\big(f(n),n\big)$$

za vse $n \in \mathbb{N}$.

Dokaz. □

Rekurzijo smo na ta način izpeljali iz indukcije, poudarimo pa, da je možen tudi obraten pristop: načelo o rekurziji vzamemo kot osnoven aksiom naravnih števil *namesto* indukcije, nato pa od tod izpeljemo načelo o indukciji. Poglejmo, kako to storimo.

Vzemimo poljuben predikat $\phi\colon \mathbb{N} \to \Omega$, za katerega velja $\phi(0)$ in $\forall n \in \mathbb{N}.\,(\phi(n) \implies \phi(\mathtt{S}(n)))$. Po načelu rekurzije obstaja natanko ena preslikava $f\colon \mathbb{N} \to \Omega$, za katero velja $f(0) = \top$ in $f\big(\mathtt{S}(n)\big) = f(n) \vee \phi\big(\mathtt{S}(n)\big)$ za vse $n \in \mathbb{N}$. Ampak predikat ϕ sam zadošča tema pogojema, saj lahko izjavo $\phi(n) \implies \phi\big(\mathtt{S}(n)\big)$ enakovredno zapišemo kot $\phi\big(\mathtt{S}(n)\big) = \phi(n) \vee \phi\big(\mathtt{S}(n)\big)$. Očitno pa tudi povsod resničen predikat zadošča danima pogojema, od koder zaključimo $\phi = \lambda n \in \mathbb{N}.\,\top$.

V tem smislu sta načeli rekurzije in indukcije enakovredni. Kot vidimo, lahko pravzaprav na indukcijo gledamo kot na poseben primer rekurzije, konkretno za preslikave oblike $\mathbb{N} \to \Omega$. To nam pove, da je ta primer tako generičen, da je iz njega možno dobiti načelo za poljubne preslikave oblike $X \times \mathbb{N} \to Y$.

(Premislek, da sta parametrizirano in neparametrizirano načelo rekurzije ekvivalentna (zaradi eksponentov). Rekurzor kot preslikava. Morda pripomba, ki zgornjo diskusijo poveže s primitivno rekurzijo iz teorije izračunljivosti.)

9.1.3 Računske operacije

Uporabimo zdaj izpeljano rekurzijo za natančno matematično definicijo strukture na naravnih številih, ki jo neformalno poznate že od malih nog. Začnimo z osnovnimi računskimi operacijami.

Seštevanje želimo definirati kot preslikavo $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Da ga definiramo rekurzivno, moramo povedati, kaj pomeni prišteti ničlo in kaj pomeni prišteti naslednika nekega števila (izraženo z vsoto, ki jo dobimo iz prištetja tega števila samega). Smiselno je podati naslednje.

$$m + 0 := m$$
$$m + \mathtt{S}(n) := \mathtt{S}(m + n)$$

V tej definiciji m nastopa kot parameter — se pravi, uporabili bomo načelo parametrizirane rekurzije. Glede na oznake iz izreka 9.3 smo vzeli $X = \mathbb{N}$, $Y = \mathbb{N}$, $b(m) = m$ (torej je b identiteta na $\mathbb{N}$) in $r(m, v, n) = \mathtt{S}(v)$ (se pravi, r je kompozicija projekcije na drugo komponento in preslikave naslednika). Po tem izreku dobimo enolično določeno preslikavo $+ \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ (ki igra vlogo preslikave f iz izreka).

Dokažimo, da pravkar definirano seštevanje zadošča zakonom, na katere smo navajeni. Začnimo s tem, da preverimo, da je 0 enota za seštevanje.

Seveda velja $a + 0 = a$ za vse $a \in \mathbb{N}$ — to je del definicije seštevanja. Od tod pa ne smemo takoj sklepati na $0 + a = a$, saj še nismo dokazali izmenljivosti seštevanja. Lahko bi na tem mestu začeli z dokazom izmenljivosti, ampak kot bomo videli, bomo za to že potrebovali dejstvo, da je 0 enota. Dokažimo torej $0 + a = a$ za vse $a \in \mathbb{N}$ neposredno.

Trditev dokazujemo z indukcijo. Najprej dokažemo trditev za $a = 0$, torej $0 + 0 = 0$. To je res po definiciji.

Privzemimo, da velja $0 + a = a$ za neki $a \in \mathbb{N}$. Dokazujemo $0 + \mathtt{S}(a) = \mathtt{S}(a)$. Preverimo:

$$0 + \mathtt{S}(a) = \mathtt{S}(0 + a) = \mathtt{S}(a).$$

Kaj pa, če namesto 0 prištejemo 1? Takrat seveda pričakujemo, da dobimo naslednika. Preverimo.

Za poljuben $a \in \mathbb{N}$ dobimo $a + 1 = a + \mathtt{S}(0) = \mathtt{S}(a + 0) = \mathtt{S}(a)$. Tukaj sploh nismo potrebovali indukcije. Jo pa potrebujemo za dokaz, da za vsak $a \in \mathbb{N}$ velja $1 + a = \mathtt{S}(a)$. Za $a = 0$ je to definicija oznake 1. Recimo, da za neki $a \in \mathbb{N}$ velja $1 + a = \mathtt{S}(a)$. Tedaj $1 + \mathtt{S}(a) = \mathtt{S}(1 + a) = \mathtt{S}(\mathtt{S}(a))$.

Prepričajmo se zdaj o družilnosti (asociativnosti) seštevanja. Dokazati želimo izjavo

$$\forall a \in \mathbb{N}. \forall b \in \mathbb{N}. \forall c \in \mathbb{N}. (a + b) + c = a + (b + c).$$

Vzemimo poljubna $a, b \in \mathbb{N}$, notranjo univerzalno kvantificirano izjavo pa dokažimo z indukcijo (po spremenljivki c). Če vzamemo $c = 0$, izjava velja: $(a + b) + 0 = a + b = a + (b + 0)$. Privzemimo zdaj, da pri nekem $c \in \mathbb{N}$ velja $(a + b) + c = a + (b + c)$. Poračunamo

$$(a + b) + \mathtt{S}(c) = \mathtt{S}\big((a + b) + c\big) = \mathtt{S}\big(a + (b + c)\big) = a + \mathtt{S}(b + c) = a + \big(b + \mathtt{S}(c)\big).$$

Zdaj lahko dokažemo izmenljivost (komutativnost) seštevanja. Dokazati želimo izjavo

$$\forall a \in \mathbb{N}. \forall b \in \mathbb{N}. a + b = b + a.$$

Vzemimo poljuben $a \in \mathbb{N}$, nato pa nadaljujmo z indukcijo (po b). Za $b = 0$ trdimo $a + 0 = 0 + a$. To smo že dokazali — obe strani enakosti sta enaki a, saj vemo, da je 0 enota za seštevanje.

Predpostavimo zdaj, da velja $a + b = b + a$ za neki $b \in \mathbb{N}$. Izpeljati želimo $a + \mathtt{S}(b) = \mathtt{S}(b) + a$. Preverimo:

$$a + \mathtt{S}(b) = \mathtt{S}(a + b) = \mathtt{S}(b + a) = 1 + (b + a) = (1 + b) + a = \mathtt{S}(b) + a.$$

Na podoben način lahko definiramo množenje in dokažemo njegove lastnosti. Smiselna rekurzivna definicija množenja je sledeča.

$$\begin{aligned} m \cdot 0 &:= 0 \\ m \cdot \mathtt{S}(n) &:= m \cdot n + m \end{aligned}$$

Če primerjamo z izrekom 9.3, smo vzeli $X = Y = \mathbb{N}$, $b(m) = 0$ (torej je b konstantna ničelna preslikava) in $r(m, v, n) = v + m$ (to preslikavo lahko definiramo s pomočjo pravkar definiranega seštevanja). Izrek nam porodi enolično določeno preslikavo $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

Podobno kot prej pri seštevanju za začetek ugotovimo, kaj se zgodi, ko množimo z 0 oziroma 1. Po definiciji vemo $a \cdot 0 = 0$ za vse $a \in \mathbb{N}$. Dokažimo še $0 \cdot a = 0$ za vse $a \in \mathbb{N}$. Za $a = 0$ velja $0 \cdot 0 = 0$ po definiciji. Vzemimo, da velja $0 \cdot a = 0$ za neki $a \in \mathbb{N}$. Tedaj $0 \cdot \mathtt{S}(a) = 0 \cdot a + 0 = 0 + 0 = 0$.

Število 1 bi morala biti enota za množenje. Preverimo. Najprej $a \cdot 1 = a \cdot s(0) = a \cdot 0 + a = 0 + a = a$. Po drugi strani trditev, da za vse $a \in \mathbb{N}$ velja $1 \cdot a = a$, dokažemo z indukcijo. Enakost $1 \cdot 0 = 0$ je jasna. Recimo, da trditev velja za neki $a \in \mathbb{N}$. Tedaj $1 \cdot \mathtt{S}(a) = 1 \cdot a + 1 = a + 1 = \mathtt{S}(a)$.

Preden se lotimo družilnosti in izmenljivosti množenja, dokažimo, da je množenje razčlenitveno (distributivno) čez seštevanje. Se pravi, dokazati želimo izjavi

$$\forall a \in \mathbb{N}. \forall b \in \mathbb{N}. \forall c \in \mathbb{N}. (a + b) \cdot c = a \cdot c + b \cdot c$$

in

$$\forall a \in \mathbb{N}. \forall b \in \mathbb{N}. \forall c \in \mathbb{N}. a \cdot (b + c) = a \cdot b + a \cdot c.$$

Pri prvi od izjav (desni razčlenitvi) vzemimo poljubna $a, b \in \mathbb{N}$, nato pa se lotimo indukcije po c. Dobimo $(a + b) \cdot 0 = 0 = 0 + 0 = a \cdot 0 + b \cdot 0$. Če velja $(a + b) \cdot c = a \cdot c + b \cdot c$ za neki c, tedaj

$$(a + b) \cdot \mathtt{S}(c) = (a + b) \cdot c + (a + b) = a \cdot c + b \cdot c + a + b = a \cdot c + a + b \cdot c + b = a \cdot \mathtt{S}(c) + b \cdot \mathtt{S}(c).$$

Pri drugi izjavi (levi razčlenitvi) sklepamo podobno: $a \cdot (b + 0) = a \cdot b = a \cdot b + 0 = a \cdot b + a \cdot 0$. Nato privzamemo izjavo za neki c in poračunamo

$$a \cdot \big(b + \mathtt{S}(c)\big) = a \cdot \mathtt{S}(b + c) = a \cdot (b + c) + a = a \cdot b + a \cdot c + a = a \cdot b + a \cdot \mathtt{S}(c).$$

Preverimo zdaj družilnost množenja, torej izjavo

$$\forall a \in \mathbb{N}. \forall b \in \mathbb{N}. \forall c \in \mathbb{N}. (a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Vzemimo poljubna $a, b \in \mathbb{N}$ in se lotimo indukcije po c. Za $c = 0$ dobimo $(a \cdot b) \cdot 0 = 0 = a \cdot 0 = a \cdot (b \cdot 0)$. Predpostavimo izjavo za neki c in poračunamo

$$(a \cdot b) \cdot \mathtt{S}(c) = (a \cdot b) \cdot c + a \cdot b = a \cdot (b \cdot c) + a \cdot b = a \cdot (b \cdot c + b) = a \cdot \big(b \cdot \mathtt{S}(c)\big).$$

Naposled preverimo še izmenljivost množenja na naravnih številih, torej izjavo

$$\forall a \in \mathbb{N}. \forall b \in \mathbb{N}. a \cdot b = b \cdot a.$$

Vzemimo poljuben $a \in \mathbb{N}$. Za $b = 0$ dobimo $a \cdot 0 = 0 = 0 \cdot a$. Vzemimo, da izjava velja za neki b. Tedaj

$$a \cdot \mathtt{S}(b) = a \cdot b + a = b \cdot a + a = b \cdot a + 1 \cdot a = (b+1) \cdot a = \mathtt{S}(b) \cdot a.$$

Na kratko lahko to celotno razpravo povzamemo: množica naravnih števil $\mathbb{N}$ tvori izmenljiv polkolobar z enico. (ta pojem bo pojasnjen že v prejšnjem poglavju o strukturah –Davorin) Seveda pa ne tvori kolobarja; vemo, da naravnih števil ne moremo poljubno odštevati. Še vedno pa lahko odštevanje na naravnih številih podamo kot *delno* operacijo, torej kot delno preslikavo $- \colon \mathbb{N} \times \mathbb{N} \rightharpoonup \mathbb{N}$. Spomnimo se namreč (od polkolobarjev v prejšnjem poglavju), da je odštevanje delna preslikava natanko tedaj, ko je polkolobar krajšalen.

Dokažimo krajšalnost polkolobarja naravnih števil, torej izjavo

$$\forall a \in \mathbb{N}. \forall b \in \mathbb{N}. \forall x \in \mathbb{N}. \big(a + x = b + x \implies a = b\big).$$

Vzemimo poljubna $a, b \in \mathbb{N}$, nato pa se kot običajno poslužimo indukcije. Pri $x = 0$ smo takoj na koncu. Privzemimo izjavo $a + x = b + x \implies a = b$ za neki x in naj velja $a + \mathtt{S}(x) = b + \mathtt{S}(x)$. Tedaj $\mathtt{S}(a + x) = \mathtt{S}(b + x)$ in ker je $\mathtt{S}$ injektivna preslikava (eden od Peanovih aksiomov!), sklepamo $a + x = b + x$, od tod pa $a = b$.[3]

S pomočjo (delnega) odštevanja lahko definiramo ***predhodnika*** na naravnih številih, in sicer kot $\mathtt{P}(n) := n - 1$. Tudi to je zgolj delna preslikava $\mathtt{P} \colon \mathbb{N} \rightharpoonup \mathbb{N}$; ničla je edino naravno število, ki ni v njenem definicijskem območju.

Naloga 9.4. Dokaži $\forall n \in \mathbb{N}. \mathtt{P}\big(\mathtt{S}(n)\big) \simeq n$.

Včasih je pa uporabno imeti obliko predhodnika in odštevanja, ki sta celoviti preslikavi. Pri predhodniku se dogovorimo, da se pomaknemo za eno nazaj, če se le da (pri ničli torej ostanemo, kjer smo). To različico predhodnika lahko definiramo z rekurzijo na naslednji način.

$$\begin{aligned} \tilde{\mathtt{P}}(0) &:= 0 \\ \tilde{\mathtt{P}}\big(\mathtt{S}(n)\big) &:= n \end{aligned}$$

Po načelu o neparametrizirani rekurziji dobimo enolično določeno preslikavo $\tilde{\mathtt{P}} \colon \mathbb{N} \to \mathbb{N}$ (konkretno, v izreku 9.3 vzamemo $Y = \mathbb{N}$, $b = 0$ in $r(v, n) = n$).[4]

Od tod lahko definiramo tako imenovano ***prisekano odštevanje*** na naravnih številih. Simbol za to operacijo je $\dot{-}$, kar se prebere "monus" (torej: $1 + 2$ se bere "ena plus dve", $1 - 2$ se bere "ena minus dve" in $1 \dot{-} 2$ se bere "ena monus dve").

Ideja prisekanega odštevanja je, da zmanjševanec zmanjšamo za tolikšen del odštevanca, kolikor le lahko (tako da še ostanemo v okviru naravnih števil). Z drugimi besedami: če se običajno odštevanje izide v naravnih številih, velja $a \dot{-} b = a - b$, sicer pa velja $a \dot{-} b = 0$. Natančna rekurzivna definicija je sledeča.

$$\begin{aligned} m \dot{-} 0 &:= m \\ m \dot{-} \mathtt{S}(n) &:= \tilde{\mathtt{P}}(m \dot{-} n) \end{aligned}$$

[3] Injektivnost preslikave $\mathtt{S}$ je točno to, kar potrebujemo za krajšalnost. Velja namreč tudi obrat: če imamo $\mathtt{S}(a) = \mathtt{S}(b)$, tj. $a + 1 = b + 1$, in lahko krajšamo, potem $a = b$.

[4] Morda se vam zdi vprašljivo, če bi to definicijo sploh imenovali "rekurzivna", saj $\tilde{\mathtt{P}}\big(\mathtt{S}(n)\big)$ nismo izrazili s $\tilde{\mathtt{P}}(n)$ (ali z drugimi besedami, preslikava r ni odvisna od svojega prvega argumenta). Ampak izrek 9.3 za ta primer še vedno velja in zgornja definicija torej podaja dobro definirano preslikavo $\tilde{\mathtt{P}} \colon \mathbb{N} \to \mathbb{N}$.

Se pravi, če v izreku 9.3 vzamemo $X = Y = \mathbb{N}$, $b(m) = m$ in $r(m,v,n) = \tilde{\mathtt{P}}(v)$, dobimo preslikavo $\dot{-}\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$.

(Ko se dokončno dogovorimo, kako bomo prevajali precendenco in asociiranje, povejmo, da ima prisekano odštevanje isto precendenco kot navadno odštevanje in da se asociira z leve. –Davorin)

Oglejmo si nekaj lastnosti, ki veljajo za prisekano odštevanje. Po definiciji je 0 desna enota, ni pa leva enota, kot takoj sledi iz naslednje vaje (od tod je jasno tudi, da $\dot{-}$ ni izmenljiv).

Naloga 9.5. Dokaži $\forall n\in\mathbb{N}.\, 0\mathbin{\dot{-}} n = 0$.

Bolj zvito je preveriti, da za vse $n\in\mathbb{N}$ velja $n\mathbin{\dot{-}} n = 0$. Če poskusimo to neposredno dokazati z indukcijo, bomo hitro naleteli na oviro. Namesto tega se raje lotimo splošnejše trditve: dokažimo

$$\forall n\in\mathbb{N}.\,\forall a\in\mathbb{N}.\,(n+a)\mathbin{\dot{-}} n = a.$$

Dokažimo trditev za $n=0$. Vzemimo poljuben $a\in\mathbb{N}$ in poračunajmo $(0+a)\mathbin{\dot{-}} 0 = a\mathbin{\dot{-}} 0 = 0$. Predpostavimo zdaj, da velja trditev $\forall a\in\mathbb{N}.\,(n+a)\mathbin{\dot{-}} n = a$ za neki n. Dokazati želimo $\forall a\in\mathbb{N}.\,\big(\mathtt{S}(n)+a\big)\mathbin{\dot{-}}\mathtt{S}(n) = a$. Vzemimo poljuben $a\in\mathbb{N}$. Tedaj

$$\big(\mathtt{S}(n)+a\big)\mathbin{\dot{-}}\mathtt{S}(n) = \big(n+1+a\big)\mathbin{\dot{-}}\mathtt{S}(n) = \big(n+\mathtt{S}(a)\big)\mathbin{\dot{-}}\mathtt{S}(n) =$$

$$= \tilde{\mathtt{P}}\Big(\big(n+\mathtt{S}(a)\big)\mathbin{\dot{-}} n\Big) = \tilde{\mathtt{P}}\big(\mathtt{S}(a)\big) = a.$$

Razmisli natančno, zakaj velja predzadnji enačaj! Če zamenjamo univerzalna kvantifikatorja v začetni izjavi, da dobimo $\forall a\in\mathbb{N}.\,\forall n\in\mathbb{N}.\,(n+a)\mathbin{\dot{-}} n = a$, in uporabimo trditev za $a=0$, sklenemo naposled $n\mathbin{\dot{-}} n = 0$ za vse $n\in\mathbb{N}$.

Prisekano odštevanje seveda ni družilno (nič bolj kot navadno odštevanje). Kot nadomestek pa nam služi naslednja trditev:

$$\forall a\in\mathbb{N}.\,\forall b\in\mathbb{N}.\,\forall c\in\mathbb{N}.\,(a\mathbin{\dot{-}} b)\mathbin{\dot{-}} c = a\mathbin{\dot{-}}(b+c).$$

Dokažimo jo. Vzemimo poljubna $a,b\in\mathbb{N}$ in se lotimo indukcije po c. Pri $c=0$ dobimo $(a\mathbin{\dot{-}} b)\mathbin{\dot{-}} 0 = a\mathbin{\dot{-}} b = a\mathbin{\dot{-}}(b+0)$. Privzemimo zdaj enakost pri nekem c in jo preverimo pri nasledniku:

$$(a\mathbin{\dot{-}} b)\mathbin{\dot{-}}\mathtt{S}(c) = \tilde{\mathtt{P}}\big((a\mathbin{\dot{-}} b)\mathbin{\dot{-}} c\big) = \tilde{\mathtt{P}}\big(a\mathbin{\dot{-}}(b+c)\big) = a\mathbin{\dot{-}}\mathtt{S}(b+c) = a\mathbin{\dot{-}}\big(b+\mathtt{S}(c)\big).$$

Preden dokažemo še členjenje množenja čez prisekanego odštevanje, si pripravimo pomožno trditev.

Lema 9.6. *Velja sledeče.*

1. *Vsako naravno število je bodisi nič bodisi naslednik; se pravi, velja trditev*

$$\forall n\in\mathbb{N}.\, n = 0 \veebar \exists m\in\mathbb{N}.\, n = \mathtt{S}(m).$$

Lahko smo še natančnejši: če je število naslednik, je naslednik svojega predhodnika. Trdimo torej

$$\forall n\in\mathbb{N}.\, n = 0 \veebar n = \mathtt{S}\big(\tilde{\mathtt{P}}(n)\big).$$

2. *Velja*

$$\forall a\in\mathbb{N}.\,\forall b\in\mathbb{N}.\, a\cdot\tilde{\mathtt{P}}(b) = a\cdot b\mathbin{\dot{-}} a.$$

Dokaz. 1. Po Peanovih aksiomih velja $0 \notin Z_{\mathtt{S}}$, torej naravno število ne more biti hkrati nič in naslednik. Zadostuje potemtakem, da dokažemo samo še $\forall n \in \mathbb{N}.\, n = 0 \vee n = \mathtt{S}\big(\tilde{\mathtt{P}}(n)\big)$.

Preverimo z indukcijo. Trditev očitno velja za $n = 0$. Recimo, da velja za neki n, in se lotimo dokazovanja za $\mathtt{S}(n)$. Pri dokazovanju disjunkcije si izberimo, da dokazujemo drugi disjunkt. Z računom smo takoj konec: $\mathtt{S}\Big(\tilde{\mathtt{P}}\big(\mathtt{S}(n)\big)\Big) = \mathtt{S}(n)$ (uporabili smo družilnost sklapljanja preslikav in rekurzivno definicijo celovitega predhodnika).

2. Vzemimo poljubna $a, b \in \mathbb{N}$. Po prejšnji točki velja bodisi $b = 0$ bodisi $b = \mathtt{S}\big(\tilde{\mathtt{P}}(b)\big)$. V prvem primeru dobimo

$$a \cdot \tilde{\mathtt{P}}(0) = a \cdot 0 = 0 = 0 \dot{-} a = a \cdot 0 \dot{-} a.$$

Predpostavimo, da smo v drugem primeru, da torej velja $b = \mathtt{S}\big(\tilde{\mathtt{P}}(b)\big)$. Račun bo bolj očiten, če začnemo z druge strani:

$$a \cdot b \dot{-} a = a \cdot \mathtt{S}\big(\tilde{\mathtt{P}}(b)\big) \dot{-} b = \big(a \cdot \tilde{\mathtt{P}}(b) + a\big) \dot{-} a = a \cdot \tilde{\mathtt{P}}(b).$$

□

Zdaj smo naposled pripravljeni, da dokažemo členjenje množenja čez prisekano odštevanje v naravnih številih. Ker že vemo, da je množenje izmenljivo, zadostuje preveriti členjenje samo na eni strani. Dokažimo torej $\forall a \in \mathbb{N}. \forall b \in \mathbb{N}. \forall c \in \mathbb{N}.\, a \cdot (b \dot{-} c) = a \cdot b \dot{-} a \cdot c$.

Vzemimo poljubna $a, b \in \mathbb{N}$ in nadaljujmo z indukcijo po c. Pri $c = 0$ takoj dobimo $a \cdot (b \dot{-} 0) = a \cdot b = a \cdot b \dot{-} 0 = a \cdot b \dot{-} a \cdot 0$. Recimo zdaj, da trditev velja za neki c. Dokažimo jo za $\mathtt{S}(c)$:

$$a \cdot \big(b \dot{-} \mathtt{S}(c)\big) = a \cdot \tilde{\mathtt{P}}(b \dot{-} c) = a \cdot (b \dot{-} c) \dot{-} a = (a \cdot b \dot{-} a \cdot c) \dot{-} a = a \cdot b \dot{-} (a \cdot c + a) = a \cdot b \dot{-} a \cdot \mathtt{S}(c).$$

9.1.4 Urejenost

V prejšnjem podrazdelku smo se posvetili algebrski strukturi naravnih števil. V tem podrazdelku dodajmo še urejenostno strukturo. Formalno bomo definirali $\leq$ in $<$ na $\mathbb{N}$ in preverili lastnosti teh relacij.

Obstaja sicer ogromno ekvivalentnih definicij relacij $\leq$ in $<$ na $\mathbb{N}$. (Mi si bomo izbrali sledeči, ekvivalenco z nekaterimi ostalimi pa preverite v tej in tej vaji.)

Definirajmo $\leq$ kot dvomestno relacijo na $\mathbb{N}$, dano s podmnožico

$$\big\{(a, b) \in \mathbb{N} \times \mathbb{N} \;\big|\; \exists x \in \mathbb{N}.\, a + x = b\big\}.$$

Preverimo, da je $\mathbb{N}$ linearno urejena z $\leq$.

Refleksivnost je preprosta, saj velja $a + 0 = a$. Tudi tranzitivnost takoj izpeljemo: če velja $a + x = b$ in $b + y = c$, tedaj $a + (x + y) = (a + x) + y = b + y = c$. To pomeni, da je $\leq$ (vsaj) šibka urejenost na $\mathbb{N}$.

Če natančneje pogledamo to izpeljavo, vidimo, da načeloma ni bilo pomembno, da smo jemali elemente iz množice naravnih števil. Uporabili smo zgolj družilnost seštevanja in obstoj enote za seštevanje. Z zgornjim predpisom torej lahko definiramo šibko urejenost $\leq$ na poljubni množici, opremljeni z družilno operacijo z enoto. Množicam s tako strukturo rečemo ***monoidi*** in tako definiran $\leq$ se imenuje ***naravna urejenost*** monoida.

V splošnem ta urejenost ni nič več kot šibka, konkretno na naravnih številih pa ima še več drugih lastnosti. Dokažimo, da je $\leq$ antisimetričen, torej delna urejenost na $\mathbb{N}$.

Vzemimo poljubna $a, b \in \mathbb{N}$, za katera obstajata $x, y \in \mathbb{N}$, tako da velja $a + x = b$ in $b + y = a$. Tedaj $a + x + y = b + y = a = a + 0$. Krajšamo a in dobimo $x + y = 0$.

Spomnimo se leme 9.6: za x se odločimo, ali je nič ali naslednik. Če $x = 0$, iz $a + x = b$ sledi $a = b$, kot želimo. Če je naslednik, pa dobimo $0 = x + y = y + x = y + \mathtt{S}\big(\tilde{\mathtt{P}}(x)\big) = \mathtt{S}\big(y + \tilde{\mathtt{P}}(x)\big)$. To bi pomenilo, da je 0 v zalogi vrednosti preslikave $\mathtt{S}$, kar je v protislovju s Peanovimi aksiomi in ta primer torej ne more nastopiti.

Dokažimo še strogo sovisnost relacije $\leq$ in s tem sklenimo, da je linearna urejenost na $\mathbb{N}$. Dokazujemo $\forall a \in \mathbb{N}. \forall b \in \mathbb{N}. a \leq b \vee b \leq a$.

Izvedimo indukcijo po a. Začnimo z $a = 0$ in vzemimo poljuben $b \in \mathbb{N}$. Velja $0 \leq b$, saj $0 + b = b$. Predpostavimo zdaj, da velja $\forall b \in \mathbb{N}. a \leq b \vee b \leq a$ za neki a, in dokažimo to trditev za $\mathtt{S}(a)$. Vzemimo poljuben $b \in \mathbb{N}$. Po lemi 9.6 je b bodisi nič bodisi naslednik. V prvem primeru velja $b \leq \mathtt{S}(a)$. V drugem primeru uporabimo predpostavko, da dobimo $a \leq \tilde{\mathtt{P}}(b) \vee \tilde{\mathtt{P}}(b) \leq a$. Če velja $a \leq \tilde{\mathtt{P}}(b)$, torej če obstaja $x \in \mathbb{N}$, tako da $a + x = \tilde{\mathtt{P}}(b)$, tedaj $\mathtt{S}(a) + x = a + 1 + x = a + \mathtt{S}(x) = \mathtt{S}(a + x) = \mathtt{S}\big(\tilde{\mathtt{P}}(b)\big) = b$, torej $\mathtt{S}(a) \leq b$. Če velja $\tilde{\mathtt{P}}(b) \leq a$, potem pa imamo $x \in \mathbb{N}$, za katerega $\tilde{\mathtt{P}}(b) + x = a$. Tedaj $b + x = \mathtt{S}\big(\tilde{\mathtt{P}}(b)\big) + x = \mathtt{S}\big(\tilde{\mathtt{P}}(b) + x\big) = \mathtt{S}(a)$, od koder sklenemo $b \leq \mathtt{S}(a)$.

Oglejmo si zdaj strogo urejenost $<$ na naravnih številih. (A imamo kako ime za "nestrogo" urejenost $\leq$? Recimo "ohlapna"? –Davorin) Definirajmo jo kot dvomestno relacijo na $\mathbb{N}$, dano s podmnožico

$$\big\{(a, b) \in \mathbb{N} \times \mathbb{N} \;\big|\; \exists x \in \mathbb{N}. a + \mathtt{S}(x) = b\big\}.$$

Očitno velja $a < b \implies a \leq b$ za vse $a, b \in \mathbb{N}$ — se pravi, $a < b$ je strožji pogoj od $a \leq b$ (od tod ime "stroga urejenost").

Oglejmo si povezavo med $<$ in $\leq$ podrobneje.

Trditev 9.7. *Velja sledeče za vse $a, b \in \mathbb{N}$.*

1. *$a < b$ je ekvivalentno tako $\neg(b \leq a)$ kot tudi $a \leq b \wedge a \neq b$.*
2. *$a \leq b$ je ekvivalentno tako $\neg(b < a)$ kot tudi $a < b \vee a = b$.*

Dokaz. 1. Privzemimo $a < b$, torej imamo $x \in \mathbb{N}$, tako da $a + \mathtt{S}(x) = b$. Od tod izpeljimo $\neg(b \leq a)$. Recimo, da velja $b \leq a$, da torej obstaja $y \in \mathbb{N}$, tako da $b + y = a$. Potem $b + \mathtt{S}(y + x) = b + y + \mathtt{S}(x) = a + \mathtt{S}(x) = b = b + 0$. Krajšamo b in dobimo $\mathtt{S}(y + x) = 0$. Izpeljali smo neresnico, saj po Peanovih aksiomih 0 ni v zalogi vrednosti preslikave $\mathtt{S}$. Sklenemo $\neg(b \leq a)$.

   Predpostavimo $\neg(b \leq a)$ in dokažimo $a \leq b \wedge a \neq b$. Vemo že, da je relacija $\leq$ strogo sovisna, torej velja $a \leq b \vee b \leq a$. Ker po predpostavki ne velja $b \leq a$, mora veljati $a \leq b$. Preverimo še $a \neq b$, kar je okrajšava za $\neg(a = b)$. Recimo, da velja $a = b$. Tedaj velja tudi $b \leq a$, kar je v nasprotju s predpostavko.

   Privzemimo zdaj $a \leq b \wedge a \neq b$ in izpeljimo $a < b$. Po predpostavki obstaja $x \in \mathbb{N}$, tako da velja $a + x = b$. Po lemi 9.6 velja $x = 0 \vee x = \mathtt{S}\big(\tilde{\mathtt{P}}(x)\big)$. Če $x = 0$, potem $a = b$, kar je v nasprotju s predpostavko. Torej $a + \mathtt{S}\big(\tilde{\mathtt{P}}(x)\big) = b$, kar pomeni $a < b$.

2. Iz ekvivalence iz prejšnje točke po zakonu o dvojni negaciji sledi ekvivalenca $a \leq b \iff \neg(b < a)$.

   Predpostavimo $a \leq b$ in izpeljimo $a < b \vee a = b$. Po zakonu o izključenem tretjem lahko ločimo primera $a = b$ in $a \neq b$. V prvem primeru smo takoj končali. V drugem primeru dobimo $a < b$ po ekvivalenci iz prejšnje točke.

Predpostavimo $a < b \vee a = b$ in izpeljimo $a \leq b$. Vemo že, da iz $a < b$ sledi $a \leq b$. Po refleksivnosti $\leq$ seveda tudi iz $a = b$ sledi $a \leq b$.

□

Iz te trditve lahko takoj izpeljemo nekaj lastnosti relacije $<$. Relacija je asimetrična: če bi hkrati veljalo $a < b$ in $b < a$, bi veljalo tudi $a < b$ in $b \leq a$, za kar pa že vemo, da se ne more zgoditi. Posledično je relacija $<$ tudi antisimetrična in irefleksivna. (Pri relacijah imejmo vajo, kjer se dokaže asimetričnost $\iff$ antisimetričnost $\wedge$ irefleksivnost. –Davorin)

Preverimo tranzitivnost relacije $<$. Pravzaprav lahko to lastnost okrepimo: ne samo, da lahko $a < c$ izpeljemo iz $a < b \wedge b < c$, pač pa lahko to izpeljemo tudi v primeru, ko naredimo enega od konjunktov ohlapnejšega. Dokažimo, da za vse $a, b, c \in \mathbb{N}$ velja $a \leq b \wedge b < c \implies a < c$, drugo obliko "krepke" tranzitivnosti pa prepustimo za vajo.

Vzemimo poljubne $a, b, c \in \mathbb{N}$, za katere velja $a \leq b$ in $b < c$, torej imamo $x, y \in \mathbb{N}$, tako da $a + x = b$ in $b + \mathtt{S}(y) = c$. Potem $a + \mathtt{S}(x + y) = a + x + \mathtt{S}(y) = b + \mathtt{S}(y) = c$, torej $a < c$.

Naloga 9.8. Dokaži $\forall a, b, c \in \mathbb{N}. a < b \wedge b \leq c \implies a < c$. Premisli, zakaj takoj sledi tranzitivnost relacije $<$.

Tudi sovisnost $<$ takoj dobimo iz zgornje trditve. Vzemimo poljubna $a, b \in \mathbb{N}$, za katera velja $a \neq b$. Gotovo velja $a \leq b \vee b \leq a$, kar je ekvivalentno $(a < b \vee a = b) \vee (b < a \vee b = a)$ ali krajše $a < b \vee b < a \vee a = b$. Zadnji disjunkt po predpostavki ne pride v poštev, torej smo izpeljali $a < b \vee b < a$.

Če povzamemo: relacija $<$ na $\mathbb{N}$ je stroga linearna urejenost.

Ker je relacija $<$ asimetrična in sovisna, zadošča tako imenovanemu ***zakonu trodelitve*** (s tujko ***zakon trihotomije***): za vsaka $a, b \in \mathbb{N}$ velja natanko ena izmed možnosti $a < b$, $a = b$ oz. $b < a$.

Naloga 9.9. Za poljubno dvomestno relacijo na neki množici formuliraj zakon trodelitve in dokaži, da mu relacija zadošča natanko tedaj, ko je asimetrična in sovisna.

(mrežna strukturo množice $\mathbb{N}$, tj. min in max (Pri mrežah (v poglavju o strukturah) že povejmo, da je vsaka linearna urejenost mreža. –Davorin), monotonost operacij)

Povežimo urejenostno strukturo s prisekanim odštevanjem in si pripravimo trditev, ki nam bo kasneje prišla prav v razdelku o celih številih.

Trditev 9.10. *Za vse $a, b \in \mathbb{N}$ veljata sledeči izjavi.*

1. $a \leq b \iff a \dot{-} b = 0$
2. $a \dot{-} b + b = \max\{a, b\}$

Dokaz. 1. Vzemimo poljubna $a, b \in \mathbb{N}$. Predpostavimo $a \leq b$, torej imamo $x \in \mathbb{N}$, tako da $a + x = b$. Z upoštevanjem lastnosti, ki smo jih izpeljali za $\dot{-}$, poračunamo: $a \dot{-} b = a \dot{-} (a + x) = (a \dot{-} a) \dot{-} x = 0 \dot{-} x = 0$.

Za dokaz obratne smeri predpostavimo $a \dot{-} b = 0$. Ker je $\leq$ strogo sovisna relacija, velja $a \leq b \vee b \leq a$. V prvem primeru smo z dokazom končali. Predpostavimo, da smo v drugem primeru, da torej imamo $x \in \mathbb{N}$, za katerega velja $b + x = a$. Tedaj $0 = a \dot{-} b = (b + x) \dot{-} b = x$, kar pomeni $a = b$ in posebej $a \leq b$.

2. Ponovno zaradi stroge sovisnosti ločimo primera $a \leq b$ in $b \leq a$. V prvem primeru trditev sledi iz prejšnje točke in enakosti $\max\{a,b\} = b$. Recimo zdaj, da velja $b \leq a$, torej $\max\{a,b\} = a$ in obstaja $x \in \mathbb{N}$, tako da $b + x = a$. Tedaj $a \dot{-} b + b = (b + x) \dot{-} b + b = x + b = a$.

□

9.1.5 Karakterizacija

Množico naravnih števil, skupaj z njeno strukturo, smo podali preko Peanovih aksiomov. Koliko pa pravzaprav je množic naravnih števil?

Namreč, naravnih števil nismo podali kot neke konkretne množice; Peanovi aksiomi jo zgolj karakterizirajo. (Ko bomo napisali razdelek o definicijah oziroma poglavje o strukturah, navežimo to diskusijo s tisto. Torej, če definicija podaja objekt preko karakterizacije njegove strukture, potem se pojavi vprašanje obstoja in enoličnosti do izomorfizma.)

Če obstaja vsaj ena množica naravnih števil, jih obstaja poljubno mnogo — elemente lahko namreč poljubno preimenujemo, pa bodo še vedno zadoščali Peanovim aksiomom. Z drugimi besedami, karkoli izomorfnega množici naravnih števil je spet množica naravnih števil. Še dobro, da je tako — bilo bi nadležno, če ne bi mogli vseh naslednjih zadev obravnavati kot množice naravnih števil: $\{0, \mathtt{S}(0), \mathtt{S}(\mathtt{S}(0)), \mathtt{S}(\mathtt{S}(\mathtt{S}(0))), \ldots\}$, $\{0,1,2,3,\ldots\}$, $\{0, \mathrm{I}, \mathrm{II}, \mathrm{III}, \ldots\}$, $\{\text{nič}, \text{ena}, \text{dve}, \text{tri}, \ldots\}$, $\{\text{zero}, \text{one}, \text{two}, \text{three}, \ldots\}$, $\{\text{null}, \text{eins}, \text{zwei}, \text{drei}, \ldots\}\ldots$

Kako pa vemo, da obstaja vsaj ena množica naravnih števil? Ne moremo preprosto reči, da jo lahko skonstruiramo recimo kot množico $\{0,1,2,3,\ldots\}$, saj tropičje nima natančnega matematičnega pomena.

Dokaz obstoja bi podajala konstrukcija množice $\mathbb{N}$ (skupaj z izbiro nekega njenega elementa, ki igra vlogo 0, in konstrukcijo ustrezne preslikave $\mathtt{S}\colon \mathbb{N} \to \mathbb{N}$). Taka konstrukcija bi iz določenih množic, za katere že vemo, da obstajajo, po določenih pravilih izpeljala $\mathbb{N}$. Seveda to vprašanje obstoja zgolj pomakne za en korak nazaj: kako vemo, da te določene množice obstajajo in katera pravila za konstrukcijo množic so dopustna?

Če hočemo karkoli izpeljati, moramo nekje začeti. Dogovoriti se torej moramo, katere *aksiome* bomo sprejeli za množice same. Obstoj nekaterih množic in dopustnost nekateri pravil za konstrukcije novih množic iz starih preprosto privzamemo.

Obstaja več različic aksiomov teorije množic. Na to temo bomo več povedali v (poglavju o hierarhiji množic). Nasplošno pa velja, da se množica naravnih števil šteje za tako osnovno, da je njen obstoj kar eden od aksiomov. (Odvisno od tega, kako točno bomo formulirali aksiom o neskončnosti, lahko ta stavek še popravimo. –Davorin) Z drugimi besedami, da množica naravnih števil obstaja, "vemo" zaradi tega, ker smo njen obstoj privzeli.

Kaj pa enoličnost do izomorfizma? No, struktura množice naravnih števil je podana z izbiro elementa, ki predstavlja nič, in preslikavo, ki predstavlja naslednika. Vzemimo poljubni dve taki strukturirani množici $(\mathbb{N}', 0', \mathtt{S}')$ in $(\mathbb{N}'', 0'', \mathtt{S}'')$ in skonstruirajmo bijekcijo med njima, ki ohranja vso strukturo (v obe smeri).

Za ti dve množici velja načelo o rekurziji, tako da lahko skonstruiramo preslikavi $f\colon \mathbb{N}' \to \mathbb{N}''$ in $g\colon \mathbb{N}'' \to \mathbb{N}'$ z rekurzivnima pogojema

$$\begin{aligned} f(0') &:= 0'', & g(0'') &:= 0', \\ f\big(\mathtt{S}'(x)\big) &:= \mathtt{S}''\big(f(x)\big), & g\big(\mathtt{S}''(y)\big) &:= \mathtt{S}'\big(g(y)\big). \end{aligned}$$

Po definiciji f in g ohranjata strukturo naravnih števil. Kakor hitro preverimo, da sta ti dve preslikavi druga drugi obratni, imamo željeni izormorfizem.

Dokažimo, da velja $g\big(f(x)\big) = x$ za vsak $x \in \mathbb{N}'$. To bomo seveda dokazali z indukcijo. Po definiciji velja $g\big(f(0')\big) = g(0'') = 0'$. Predpostavimo, da trditev drži za neki $x \in \mathbb{N}'$. Tedaj

$$g\Big(f\big(\mathtt{S}'(x)\big)\Big) = g\Big(\mathtt{S}''\big(f(x)\big)\Big) = \mathtt{S}'\Big(g\big(f(x)\big)\Big) = \mathtt{S}'(x).$$

Na enak način preverimo še, da $f\big(g(y)\big) = y$ za vse $y \in \mathbb{N}''$. Sklenemo, da so Peanovi aksiomi dopustna karakterizacija strukture, saj določajo množico naravnih števil enolično do izomorfizma.

Ni pa definicija 9.1 edina smiselna karakterizacija naravnih števil. V preostanku tega razdelka bomo omenili še nekaj drugih, ki se uporabljajo.

V razdelku o rekurziji smo že omenili, da lahko načelo indukcije izpeljemo iz rekurzije (in obratno). Peanovi aksiomi se potemtakem lahko podajo z rekurzijo namesto indukcijo.

V prejšnjih dveh razdelkih smo izpeljali običajno algebrsko in urejenostno strukturo naravnih števil. Včasih se del te strukture vključi v definicijo naravnih števil. Na primer, operacija seštevanja se vzame kot del osnovne strukture naravnih števil in enakosti $m + 0 = m$ ter $m + \mathtt{S}(n) = \mathtt{S}(m + n)$ se privzameta kot aksioma (ter podobno z ostalo strukturo).

Pravzaprav je možno podati strnjeno definicijo naravnih števil, ki že vključuje algebrsko strukturo, s pomočjo kategorij (spomni se jih iz (razdelka o kategorijah v poglavju o strukturah)). Na kratko: $\mathbb{N}$ je začetni polkolobar z enico.

Pojasnimo to definicijo natančneje. Naj $\mathbf{PKol}_1$ označuje kategorijo, katere objekti so polkolobarji z enico, morfizmi pa preslikave med njimi, ki ohranjajo seštevanje, množenje ter enoti zanju. Tedaj lahko $\mathbb{N}$ karakteriziramo kot začetni objekt v kategoriji $\mathbf{PKol}_1$.

Preverimo, da to drži. Zadostuje preveriti, da $\mathbb{N}$, dan z definicijo 9.1 in opremljen s polkolobarsko strukturo, izpeljano v podrazdelku 9.1.3, zadošča pogoju za začetni objekt. Namreč, vemo že, da Peanovi aksiomi določajo naravna števila do izomorfizma natančno, po drugi strani pa so tudi začetni objekti določeni do izomorfizma. Strogo gledano sicer gre tu za dve različni strukturi (in posledično načeloma različna pojma izomorfizma), ampak polkolobarsko strukturo na naravnih številih smo izpeljali iz ničle in naslednika, po drugi strani pa lahko ničlo in naslednika izpeljemo iz polkolobarske strukture: 0 je enota za seštevanje, 1 je enota za množenje in naslednik je dan s predpisom $x \mapsto x + 1$. Posledično se pojma izomorfizmov ujemata v smislu, da določata isti razpon objektov.

Naj bo X poljuben objekt v $\mathbf{PKol}_1$. Za lažje razumevanje označimo operacije, ki so del njegove strukture, z X v indeksu, torej $+_X$, 0_X, $\cdot_X$, 1_X. Če je $f\colon \mathbb{N} \to X$ poljuben morfizem v $\mathbf{PKol}_1$, mora zaradi ohranjanja operacij veljati $f(0) = 0_X$ in $f\big(\mathtt{S}(n)\big) = f(n+1) = f(n) +_X f(1) = f(n) +_X 1_X$. Ampak pogoja

$$\begin{aligned} f(0) &:= 0_X \\ f\big(\mathtt{S}(n)\big) &:= f(n) +_X 1_X \end{aligned}$$

po načelu o rekurziji enolično določata preslikavo $f\colon \mathbb{N} \to X$. Če preverimo, da je ta preslikava homomorfizem polkolobarjev z enico, lahko zaključimo, da je $\mathbb{N}$ res začetni objekt v $\mathbf{PKol}_1$.

Enota za seštevanje se ohranja po definiciji. Preverimo, da se ohranja seštevanje kot celota: dokazujemo $\forall a \in \mathbb{N}.\, \forall b \in \mathbb{N}.\, f(a+b) = f(a) +_X f(b)$. Vzemimo poljuben $a \in \mathbb{N}$ in se lotimo indukcije po b. Pri $b = 0$ velja $f(a+0) = f(a) = f(a) +_X 0_X = f(a) +_X f(0)$. Recimo, da trditev velja za neki $b \in \mathbb{N}$. Tedaj $f\big(a + \mathtt{S}(b)\big) = f\big(\mathtt{S}(a+b)\big) = f(a+b) +_X 1_X = f(a) +_X f(b) +_X 1_X = f(a) + f\big(\mathtt{S}(b)\big)$.

Kar se ohranjanja enice tiče, lahko poračunamo $f(1) = f\big(\mathtt{S}(0)\big) = f(0) +_X 1_X = 0_X +_X 1_X = 1_X$. Preverimo, da se ohranja množenje, da torej velja $\forall a \in \mathbb{N}.\, \forall b \in \mathbb{N}.\, f(a \cdot b) = f(a) \cdot_X f(b)$.

Vzemimo poljuben $a \in \mathbb{N}$ in se poslužimo indukcije po b. Najprej $f(a \cdot 0) = f(0) = 0_X = f(a) \cdot_X 0_X = f(a) \cdot_X f(0)$, nato pa predpostavimo trditev za neki $b \in \mathbb{N}$. Dobimo $f\big(a \cdot \mathtt{S}(b)\big) = f(a \cdot b + a) = f(a \cdot b) +_X f(a) = f(a) \cdot_X f(b) +_X f(a) \cdot_X 1_X = f(a) \cdot_X \big(f(b) +_X 1_X\big) = f(a) \cdot_X f\big(\mathtt{S}(b)\big)$.

Naloga 9.11. Premisli, da lahko $\mathbb{N}$ okarakteriziramo tudi kot začetni izmenljiv polkolobar z enico.

Karakterizacija "$\mathbb{N}$ je začetni polkolobar z enico" sicer uporablja seštevanje in množenje na naravnih številih. Možno je pa podati tudi kategorično definicijo naravnih števil, ki se sklicuje samo na ničlo in naslednika, tako kot Peanovi aksiomi (kot podani v definiciji 9.1).

Definirajmo kategorijo, katere objekti so diagrami oblike $\mathbf{1} \to X \to X$, kjer je X poljubna množica, puščici pa predstavljata poljubni preslikavi (z domeno in kodomeno, kot podano v diagramu). Dogovorimo se, da so morfizmi iz objekta $\mathbf{1} \xrightarrow{a} X \xrightarrow{t} X$ v objekt $\mathbf{1} \xrightarrow{b} Y \xrightarrow{u} Y$ preslikave $f\colon X \to Y$, za katere velja $f \circ a = b$ in $f \circ t = u \circ f$ — z drugimi besedami, komutirati mora sledeči diagram.

(diagram)

Naravna števila potem lahko definiramo kot začetni objekt v tej kategoriji.

Preverimo, da je to res. Trdimo, da je $\mathbf{1} \xrightarrow{\mathtt{N}} \mathbb{N} \xrightarrow{\mathtt{S}} \mathbb{N}$ začetni objekt dane kategorije, kjer $\mathbb{N}$ označuje množico naravnih števil, definirano s Peanovimi aksiomi, $\mathtt{N}$ označuje preslikavo, ki odbere element 0, $\mathtt{S}$ pa kot običajno označuje naslednika.

Vzemimo poljuben objekt $\mathbf{1} \xrightarrow{b} Y \xrightarrow{u} Y$. Preveriti želimo, da obstaja enolična preslikava $f\colon \mathbb{N} \to Y$, za katero komutira sledeči diagram.

(diagram)

To pomeni, da imamo dva pogoja na f. Za začetek mora veljati $f \circ \mathtt{N} = b$, kar je ekvivalentno $f\big(\mathtt{N}(())\big) = b(())$ oziroma $f(0) = b(())$. Drugi pogoj pravi $f \circ \mathtt{S} = u \circ f$, tj. za vsak $n \in \mathbb{N}$ mora veljati $f\big(\mathtt{S}(n)\big) = u\big(f(n)\big)$. Obstoj in enoličnost takšne preslikave f nam poda načelo o rekurziji.

Naravna števila (skupaj s podatkom o ničli in nasledniku) so torej res začetni objekt dane kategorije. Spomnimo se še, da tako Peanovi aksiomi kot začetnost objekta podajajo objekt do izomorfizma natančno. Bralcu prepuščamo, da preveri, da se pojma izomorfizma v obeh primerih ujemata.

Videli smo, da je kategorična definicija naravnih števil ekvivalentna Peanovi, je pa v določenem smislu splošnejša. Objekti dane kategorije so bili oblike $\mathbf{1} \to X \to X$, kjer sta bila $\mathbf{1}$ in X množici, puščici pa sta preslikavi (tj. objekte in morfizme smo jemali iz kategorije **Množ**). Takšne diagrame pa lahko tvorimo tudi v splošnejših kategorijah — za $\mathbf{1}$ vzamemo končni objekt, X je poljuben objekt, puščici pa poljubna morfizma (z ustrezno domeno in kodomeno). Zgornja definicija naravnih števil nam v bistvu da načelo neparametrizirane rekurzije in če imamo eksponente, lahko izpeljemo še načelo parametrizirane rekurzije (kot v podrazdelku 9.1.2). Torej nam kategorična definicija poda pojem naravnih števil v poljubni kartezično zaprti kategoriji! (Obstaja način, kako prilagoditi to definicijo, da že od začetka vključuje parametre; v tem primeru deluje celo za poljubno kategorijo s končnimi produkti.) To je uporabno, kadar želimo za temelje matematike vzeti kaj drugega kot običajne množice.

9.2 Cela števila

Zdaj ko imamo množico naravnih števil, lahko skonstruiramo nadaljnje številske množice. Naslednji korak so cela števila.

9.2.1 Konstrukcija

Težava z naravnimi števili je, da je odštevanje zgolj delna preslikava. Namen konstrukcije celih števil je razširiti množico naravnih števil ravno za toliko, da lahko neomejeno odštevamo (in ostale računske operacije še vedno imajo smisel ter zadoščajo običajnim zakonom).

Kako to doseči? Za vsak par naravnih števil $a, b \in \mathbb{N}$ želimo imeti element, ki predstavlja njuno razliko. Pretkana ideja, kako to doseči, je: razliko teh elementov predstavimo kar z elementoma samima, tj. njuno razliko naj predstavlja par (a, b). V tem kontekstu takemu paru zaradi tega rečemo ***formalna razlika*** elementov a in b.

Ti pari so elementi množice $\mathbb{N} \times \mathbb{N} = \mathbb{N}^2$, ki jo lahko opremimo z operacijami in urejenostjo, če premislimo, kako se pri računanju obnašajo razlike. Na primer, pričakujemo, da velja $(a - b) + (c - d) = (a + c) - (b + d)$, zato definiramo seštevanje $+ \colon \mathbb{N}^2 \times \mathbb{N}^2 \to \mathbb{N}^2$ s predpisom

$$(a, b) + (c, d) := (a + c, b + d)$$

(se pravi, seštevamo po komponentah). Pri tem smo si privoščili zlorabo oznak: plusa na desni predstavljata v podrazdelku 9.1.3 definirano seštevanje na naravnih številih, isti simbol $+$ na levi pa pravkar definirano operacijo na $\mathbb{N}^2$.

Kaj bi bilo smiselno množenje formalnih razlik? Pričakujemo $(a - b) \cdot (c - d) = a \cdot c - a \cdot d - b \cdot c + b \cdot d = (a \cdot c + b \cdot d) - (a \cdot d + b \cdot c)$, zato definiramo operacijo $\cdot \colon \mathbb{N}^2 \times \mathbb{N}^2 \to \mathbb{N}^2$ s predpisom

$$(a, b) \cdot (c, d) := (a \cdot c + b \cdot d, a \cdot d + b \cdot c).$$

Preverimo lahko, da ti dve operaciji zadoščata običajnim lastnostim.

Naloga 9.12. Preveri, da sta podani seštevanje in množenje na $\mathbb{N}^2$ izmenljivi in družilni, da se množenje člení čez seštevanje, seštevanje je krajšalno ter da je $(0, 0)$ enota za seštevanje, $(1, 0)$ pa enota za množenje.

Sklenemo: $\mathbb{N}^2$ je s podano algebrsko strukturo izmenljiv krajšalen polkolobar z enico, podobno kot naravna števila. Pravzaprav lahko naravna števila vložimo ta polkolobar.

Naloga 9.13. Preveri, da je preslikava $\mathbb{N} \to \mathbb{N}^2$, dana z $n \mapsto (n, 0)$, injektiven homomorfizem polkolobarjev z enico.

V tem smislu lahko naravna števila obravnavamo kot podpolkolobar polkolobarja formalnih razlik naravnih števil. To ni presenetljivo; $(n, 0)$ predstavlja razliko $n - 0$, ki jo seveda poistovetimo z n.

Razširimo pa lahko ne samo algebrske operacije, pač pa tudi urejenost. Kdaj velja $a - b \leq c - d$? Natanko tedaj, ko $a + d \leq b + c$. Vpeljimo torej urejenost na $\mathbb{N}^2$ s predpisom

$$(a, b) \leq (c, d) := a + d \leq b + c.$$

Enako sklepamo za strogo urejenost, zato dodajmo še

$$(a, b) < (c, d) := a + d < b + c.$$

Ta dva predpisa dejansko razširjata definicijo urejenosti z naravnih števil, saj velja $(m,0) \leq (n,0) \iff m+0 \leq n+0 \iff m \leq n$ in podobno za $<$.

Naloga 9.14. Preveri, da je $\leq$ na $\mathbb{N}^2$ šibka urejenost (refleksivna in tranzitivna).

Ni pa $\leq$ delna urejenost na $\mathbb{N}^2$, saj ni antisimetrična. Velja na primer tako $(2,1) \leq (5,4)$ kot $(5,4) \leq (2,1)$. To je smiselno, saj bi razliki $2-1$ in $5-4$ morali biti enaki. Vidimo: če želimo dobiti dejanski pojem celih števil, moramo poistovetiti formalne razlike, ki so obojestransko primerljive in bi posledično morale predstavljati isto vrednost.

Spomnimo se (od relacij urejenosti), da vsaka šibka urejenost $\leq$ določa ekvivalenčno relacijo, dano z $x \approx y := x \leq y \wedge y \leq x$. V našem primeru to pomeni $(a,b) \approx (c,d) \iff a+d = b+c$. Definirajmo množico celih števil kot $\mathbb{Z} := \mathbb{N}^2/_{\approx}$. Elementi množice $\mathbb{Z}$ so torej ekvivalenčni razredi $[(a,b)]_{\approx}$, ki jih bomo pa zavoljo lažje berljivosti pisali kar kot $[a,b]$.

Po konstrukciji šibka urejenost $\leq$ na $\mathbb{N}^2$ porodi delno urejenost na kvocientu $\mathbb{Z}$, ki jo bomo spet označili z $\leq$. Premisli, da tudi $<$ na $\mathbb{N}^2$ porodi dobro definirano relacijo na $\mathbb{Z}$.

Ne velja pa samo za urejenost, da jo lahko prenesemo z $\mathbb{N}^2$ na kvocient $\mathbb{Z}$ — to lahko storimo tudi z algebrskimi operacijami.

Naloga 9.15. Preveri, da je $\approx$ kongruenca za polkolobar $\mathbb{N}^2$. Sklepaj, da je s porojenimi operacijami tudi $\mathbb{Z}$ izmenljiv krajšalen polkolobar z enico.

Kot smo omenili, lahko $\mathbb{N}$ vložimo v $\mathbb{N}^2$. Če to vložitev sklopimo z naravno kvocientno preslikavo, dobimo homomorfizem polkolobarjev z enico $\mathbb{N} \to \mathbb{Z}$. Trdimo, da je tudi ta injektiven. Namreč, za poljubna $m,n \in \mathbb{N}$ velja

$$[m,0] = [n,0] \iff (m,0) \approx (n,0) \iff m+0 = 0+n \iff m = n.$$

V tem smislu je $\mathbb{N}$ podpolkolobar polkolobarja $\mathbb{Z}$. Vse omenjene operacije in relacije so uslajene med $\mathbb{N}$ in $\mathbb{Z}$, zato ni problema, če prenalagamo (naj popravi, kdor se spomni, kako se v tem kontekstu prevaja izraz 'overload' –Davorin) simbole zanje.

Zaenkrat smo izpeljali polkolobarsko strukturo celih števil, ampak te celotne konstrukcije smo se lotili, ker dodatno hočemo še odštevanje. Premislimo, da so cela števila pravzaprav kolobar.

Kaj bi naj bila nasprotna vrednost razlike? Navajeni smo na $-(a-b) = b-a$, torej pričakujemo, da dobimo nasprotno vrednost para z zamenjavo komponent. Preverimo, da se to dejansko izide v celih številih:

$$[a,b] + [b,a] = [a+b, b+a] = [0,0],$$

pri čemer zadnja enakost velja, ker $a+b+0 = b+a+0$ (vemo pa že tudi, da je $[0,0]$ enota za seštevanje v $\mathbb{Z}$).

Naloga 9.16. Vpeljava ekvivalenčne relacije je bistvena za konstrukcijo *kolobarja*, ki razširja naravna števila. Premisli namreč, da polkolobar formalnih razlik $\mathbb{N}^2$ *ni* kolobar: z izjemo enote za seštevanje $(0,0)$ noben par (a,b) nima nasprotnega elementa (ne (b,a) niti kateregakoli drugega).

Torej, $\mathbb{Z}$ je izmenljiv kolobar z enico. Kar se tiče njegove urejenostne strukture, smo že definirali $\leq$ in $<$ ter izpeljali nekaj njunih lastnosti. Za vajo prepuščamo še naslednje.

Naloga 9.17. Preveri, da je $\leq$ linearna urejenost na $\mathbb{Z}$ (posledično je $\mathbb{Z}$ tudi mreža), $<$ pa stroga linearna urejenost na $\mathbb{Z}$ (in posledično zadošča zakonu trodelitve).

Naloga 9.18. Razmisli, kako je z monotonostjo algebrskih operacij na polkolobarju formalnih razlik $\mathbb{N}^2$ in kolobarju celih števil $\mathbb{Z}$.

Morda se vam sicer zdi predstavitev celih števil s formalnimi razlikami nekoliko nenavadna; povečini nismo navajeni nanjo. Vsekakor niste celih števil podali na ta način v osnovni šoli. Običajno pišemo cela števila kot naravna z ustreznim predznakom. Preverimo, da zgornja definicija celih števil dopušča takšen zapis.

Trditev 9.19. *Vsak ekvivalenčni razred $[a, b] \in \mathbb{Z}$ vsebuje natanko enega predstavnika, ki ima vsaj eno komponento enako* 0*, in sicer velja $[a, b] = [a \dot{-} b, b \dot{-} a]$.*

Dokaz. Preverimo najprej enoličnost. Naj bosta $m, n \in \mathbb{N}$ poljubni naravni števili. Vemo že, da iz $[m, 0] = [n, 0]$ sledi $m = n$ — to je ravno injektivnost vložitve naravnih števil v cela. Na podoben način izpeljemo $[0, m] = [0, n] \implies (0, m) = (0, n)$. Recimo še, da velja $[m, 0] = [0, n]$, torej $m + n = 0$. V podrazdelku 9.1.4 smo že izpeljali, da potem velja $m = n = 0$, torej se predstavnika spet ujemata.

S pomočjo trditve 9.10(2) izpeljemo

$$a + (b \dot{-} a) = \max\{b, a\} = \max\{a, b\} = b + (a \dot{-} b),$$

torej res velja $[a, b] = [a \dot{-} b, b \dot{-} a]$. Upoštevajmo še trditev 9.10(1) in sovisnost relacije $\leq$ na naravnih številih ter zaključimo, da je vsaj ena od komponent $a \dot{-} b$, $b \dot{-} a$ enaka 0. □

Vsako celo število torej lahko predstavimo v obliki $[n, 0]$ ali $[0, n]$. V prvem primeru je celo število v zalogi vrednosti vložitve $\mathbb{N}$ v $\mathbb{Z}$ in ga zato pišemo kar kot n (ali če hočemo poudariti predznak, kot $+n$). V drugem primeru pa lahko upoštevamo $[0, n] = -[n, 0]$ in ga zato pišemo kot $-n$. V vsakem primeru ga lahko zapišemo kot predznačeno naravno število. V mejnem primeru, ko sta obe komponenti enaki 0, gre za enoto za seštevanje, tj. ničlo v celih številih, ki jo seveda lahko zapišemo s poljubnim predznakom.

Načeloma bi lahko cela števila skonstruirali tudi na tovrsten način — recimo kot $\{+, -\} \times \mathbb{N}_{>0} + \{0\}$ ali kot kvocient vsote $\mathbb{N} + \mathbb{N}$, kjer poistovetimo obe ničli, je pa potem bolj nadležno uvesti strukturo na cela števila, ker je kar naprej potrebno ločevati primere. Spomnite se definicije operacij in urejenosti na $\mathbb{Z}$ iz osnovne šole — za vsa števila ste ločili primere glede na njihov predznak.

9.2.2 Karakterizacija

Naravna števila smo v prejšnjem razdelku karakterizirali s Peanovimi aksiomi, preverili, da so s tem določena do izomorfizma natančno, njihov obstoj pa smo privzeli. Pri celih številih smo zaenkrat ubrali drugačno strategijo — zanje smo podali izrecno konstrukcijo.

Pri naravnih številih smo že omenili, da je smiselno, da so določena le do izomorfizma: če števila zgolj preimenujemo, še vedno ohranijo strukturo, ki jo želimo. Enak argument velja tudi za druge številske množice. Spremenimo torej definicijo celih števil tako, da bodo podana s karakterizacijo, ki jih bo določala do izomorfizma natančno.

Spomnimo se, da je ena od karakterizacij naravnih števil bila "začetni polkolobar z enico". Da dobimo cela števila, moramo dodati še neomejeno odštevanje, kar nam da idejo: definirajmo cela števila $\mathbb{Z}$ kot *začetni kolobar z enico*.

Če to natančneje pojasnimo: naj $\mathbf{Kol}_1$ označuje kategorijo, katere objekti so kolobarji z enico, morfizmi pa homomorfizmi kolobarjev, ki ohranjajo tudi enico. Tedaj je $\mathbb{Z}$ po definiciji začetni objekt kategorije $\mathbf{Kol}_1$.

Kot začetni objekt je $\mathbb{Z}$ seveda določen do izomorfizma natančno. Konstrukcijo iz prejšnjega podrazdelka lahko potem obravnavamo kot en konkreten primerek $\mathbb{Z}$-ja, kar dokaže obstoj množice celih števil. Preverimo, da je kvocient množice formalnih razlik z danimi operacijami res začetni kolobar z enico.

Vemo že, da je kolobar z enico. Naj bo X z operacijami $+_X$, 0_X, $-_X$, $\cdot_X$, 1_X poljuben kolobar z enico. Dokažimo, da obstaja natanko en homomorfizem kolobarjev z enico $\mathbb{N}^2/_\approx \to X$.

Vsak kolobar z enico je tudi polkolobar z enico, torej imamo enolično določen homomorfizem polkolobarjev z enico $v\colon \mathbb{N} \to X$. Definirajmo preslikavo $f\colon \mathbb{N}^2/_\approx \to X$ s predpisom

$$f\big([a,b]\big) := v(a) -_X v(b).$$

Preverimo, da je f dobro definirana. Naj velja $(a,b) \approx (c,d)$, torej $a+d = b+c$. Posledično $v(a) +_X v(d) = v(a+d) = v(b+c) = v(b) +_X v(c)$. Odštejmo $v(b)$ in $v(d)$ na obeh straneh enačbe, da dobimo $v(a) -_X v(b) = v(c) -_X v(d)$, torej $f\big([a,b]\big) = f\big([c,d]\big)$, kot želeno.

Dokaz, da je podani f homomorfizem kolobarjev z enico, prepuščamo bralcu. Preverimo pa njegovo enoličnost.

Naj bo $g\colon \mathbb{N}^2/_\approx \to X$ poljuben homomorfizem kolobarjev z enico. Označimo z $i\colon \mathbb{N} \to \mathbb{N}^2/_\approx$ vložitev naravnih števil v cela, tj. $i(n) = [n,0]$. Tedaj je $g \circ i\colon \mathbb{N} \to X$ homomorfizem polkolobarjev z enico in je torej enak zgoraj omenjenemu v. Za poljubna $a, b \in \mathbb{N}$ velja $[a,b] = [a,0] + [0,b] = [a,0] - [b,0] = i(a) - i(b)$, kar pomeni

$$g\big([a,b]\big) = g\big(i(a) - i(b)\big) = g\big(i(a)\big) -_X g\big(i(b)\big) = v(a) -_X v(b).$$

Torej je g enak zgornjemu f.

Seveda karakterizacija celih števil kot začetni kolobar z enico ni edina možna. S pomočjo teorije kategorij lahko neposredno izrazimo, kaj pomeni "zapreti objekt za neko dodatno strukturo" (v našem primeru želimo polkolobar $\mathbb{N}$ zapreti za odštevanje). Pojem, ki formalno zajame tovrstna zaprtja, se imenuje kategorična ***refleksija***. Natančen opis tega pojma je precej abstrakten in onkraj ciljev te knjige (tako da bomo, kar se celih števil tiče, ostali pri definiciji "začetni kolobar z enico"), lahko pa ga vsaj v grobem opišemo v našem primeru.

Kategorijo kolobarjev **Kol** lahko vložimo v kategorijo polkolobarjev **PKol**. Refleksija je preslikava v nasprotni smeri, ki polkolobar razširi za najmanj, kolikor lahko, da postane kolobar. Formalno se to izrazi na naslednji način: če je X poljuben polkolobar, tedaj je refleksija $R(X)$ polkolobarja X določena s pogoji, da je $R(X)$ kolobar, da se X vloži v $R(X)$ in da se mora vsak homomorfizem polkolobarjev $X \to Y$, kjer je Y kolobar, enolično razširiti do homomorfizma kolobarjev $R(X) \to Y$.

Našo definicijo celih števil lahko izpeljemo iz tega splošnejšega pogleda. Velja namreč, da refleksije slikajo začetne objekte v začetne objekte. Če se z refleksijo omejimo na (pol)kolobarje z enico in že vemo, da so naravna števila začetni polkolobar z enico, tedaj mora njihova refleksija $\mathbb{Z} = R(\mathbb{N})$ biti začetni kolobar z enico.

Mimogrede: tudi refleksije so določene do izomorfizma natančno. (komentar o splošnosti konstrukcije s formalnimi razlikami)

9.3 Racionalna števila

Kar se številskih množic tiče, smo začeli z naravnimi števili, ki jih lahko poljubno seštevamo in množimo (tj. tvorijo polkolobar). Želeli smo še neomejeno odštevati (tj. imeti kolobar), zato

smo jih razširili do celih števil. Naslednji korak je seveda, da želimo še neomejeno deliti (razen z 0, tj. dobiti obseg), in jih zato razširimo do racionalnih števil.

Ta razdelek bomo zastavili podobno kot prejšnji: podajmo konkretno konstrukcijo racionalnih števil, nato pa splošno karakterizacijo racionalnih števil in preverimo, da ji dana konstrukcija zadošča.

9.3.1 Konstrukcija

Ideja za konstrukcijo racionalnih števil je podobna, kot za cela števila: količnike predstavimo kar kot pare $(\text{deljenec}, \text{delitelj})$. Deljenci so lahko poljubna cela števila, delitelji pa morajo biti neničelni. Načeloma bi torej začeli z uvedbo operacij in urejenosti na $\mathbb{Z} \times \mathbb{Z}_{\neq 0}$, ampak to vodi do nadležnih ločevanj primerov pri urejenosti. Lahko se znajdemo in se omejimo na delitelje, ki so pozitivni: vemo namreč, da lahko minus "nesemo" iz imenovalca v števec.

Definirajmo torej množico ***formalnih količnikov*** kot $\mathbb{Z} \times \mathbb{Z}_{>0}$. Opremimo jo s strukturo. Če se spomnimo, kako računamo s količniki, pridemo do naslednjih definicij.

$$(a,b) + (c,d) := (a \cdot d + b \cdot c, b \cdot d) \qquad (a,b) \cdot (c,d) := (a \cdot c, b \cdot d)$$

Seštevanje in množenje sta na ta način dobro definirani, saj je zmnožek dveh pozitivnih celih števil spet pozitivno celo število. (če ne bo to že kje prej omenjeno, se na tem mestu preveri) Hitro vidimo, da je $(0,1)$ enota za seštevanje in $(1,1)$ enota za množenje.

Naloga 9.20. Prepričaj se, da je $\mathbb{Z} \times \mathbb{Z}_{>0}$ z danima operacijama izmenljiv krajšalen polkolobar z enico in da predpis $a \mapsto (a,1)$ podaja homomorfizem polkolobarjev z enico, če ga obravnavamo kot preslikavo $\mathbb{N} \to \mathbb{Z} \times \mathbb{Z}_{>0}$ oziroma $\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}_{>0}$.

Uvedimo še urejenost: definirajmo

$$(a,b) \leq (c,d) := a \cdot d \leq b \cdot d \qquad \text{in} \qquad (a,b) < (c,d) := a \cdot d < b \cdot c.$$

Naloga 9.21. Preveri, da je $\leq$ šibka urejenost na $\mathbb{Z} \times \mathbb{Z}_{>0}$ (refleksivna in tranzitivna).

Tako kot prej pri celih številih bomo dobili željeno šele, ko naredimo kvocient po ekvivalenčni relaciji $\approx$, dani z $(a,b) \approx (c,d) := (a,b) \leq (c,d) \wedge (c,d) \leq (a,b)$, kar pomeni $(a,b) \approx (c,d) \iff a \cdot d = b \cdot c$. Definirajmo torej množico racionalnih števil kot $\mathbb{Q} := (\mathbb{Z} \times \mathbb{Z}_{>0})/_{\approx}$.

Elementi tega kvocienta so ekvivalenčni razredi $[(a,b)]_{\approx}$, ki pa jih raje pišemo kot $\frac{a}{b}$. Na primer, ker velja $2 \cdot 3 = 6 \cdot 1$, dobimo $[(2,6)]_{\approx} = [(1,3)]_{\approx}$ oziroma $\frac{2}{6} = \frac{1}{3}$. (Če te razprave ne bo že prej (ob debati o razliki med izrazom in vrednostjo, ki jo izraz predstavlja), tu pojasnimo razliko med ulomkom in racionalnim številom, vključno s tem, kaj pomeni enakost v enem oz. drugem primeru.)

Naloga 9.22. Preveri, da je $\approx$ kongruenca na polkolobarju $\mathbb{Z} \times \mathbb{Z}_{>0}$ in da je potem tudi $\mathbb{Q}$ izmenljiv krajšalen polkolobar z enico za porojene operacije. Preveri tudi, da je porojena $\leq$ linearna urejenost na $\mathbb{Q}$ (torej je $\mathbb{Q}$ mreža), porojena $<$ pa je stroga linearna urejenost na $\mathbb{Q}$ (ki posledično zadošča zakonu trodelitve).

Trdimo: za poljuben $\frac{a}{b} \in \mathbb{Q}$ je $\frac{-a}{b}$ njegov nasprotni element. Res: $\frac{a}{b} + \frac{-a}{b} = \frac{a \cdot b + b \cdot (-a)}{b^2} = \frac{0}{b^2} = \frac{0}{1}$, kar je enota za seštevanje v $\mathbb{Q}$. Sklenemo, da je $\mathbb{Q}$ kolobar.

Naloga 9.23. Preveri, da je preslikava $\mathbb{N} \to \mathbb{Q}$, $a \mapsto \frac{a}{1}$ homomorfizem polkolobarjev z enico, preslikava $\mathbb{Z} \to \mathbb{Q}$, $a \mapsto \frac{a}{1}$ pa homomorfizem kolobarjev z enico. V tem smislu obravnavamo $\mathbb{N}$ in $\mathbb{Z}$ kot pomnožici množice $\mathbb{Q}$.

Ostane še preveriti, da je $\mathbb{Q}$ obseg, da torej ima vsak neničelni element obrat. Očitno velja $\frac{a}{b} = \frac{0}{1} \iff a = 0$. Po zakonu trodelitve za cela števila lahko ločimo primere $a < 0$, $a = 0$, $a > 0$, pri čemer primer $a = 0$ odpade, če se omejimo na neničelna racionalna števila. V primeru $a > 0$ lahko zapišemo $(\frac{a}{b})^{-1} = \frac{b}{a}$, v primeru $a < 0$ pa $(\frac{a}{b})^{-1} = \frac{-b}{-a}$.

Naloga 9.24. Preveri, da na ta način dejansko dobimo obrat poljubnega neničelnega racionalnega števila.

Vidimo, da smo si pri računanju obratov nekoliko zakomplicirali življenje s tem, da smo za množico formalnih količnikov vzeli $\mathbb{Z} \times \mathbb{Z}_{>0}$ namesto $\mathbb{Z} \times \mathbb{Z}_{\neq 0}$ — v slednjem primeru bi namreč za obrat zadostovala zgolj formula $(\frac{a}{b})^{-1} = \frac{b}{a}$. Bi pa potem imeli več ločevanja primerov pri $\leq$ in $<$.

Naloga 9.25. Za primerjavo konstruiraj racionalna števila kot $(\mathbb{Z} \times \mathbb{Z}_{\neq 0})/_{\approx}$. Zapiši vse podrobnosti, predvsem definicijo in lastnosti relacij urejenosti. Dokaži, da sta obe konstrukciji izomorfni kot obsega in kot urejenosti.

V prejšnjem razdelku smo videli: če cela števila predstavimo s formalnimi razlikami naravnih števil, ima sicer vsako celo število mnogo predstavnikov, ampak eden izmed njih, dan v trditvi 9.19, je "najboljši", v smislu, da je z njim najlažje računati. Podobno trditev imamo tudi za racionalna števila: vsako racionalno število je možno predstaviti z okrajšanim ulomkom. Ker to že zelo dobro poznate, te trditve ne bomo izrecno dokazovali, lahko pa za vajo sami natančno formulirate trditev in jo skrbno dokažete.

9.3.2 Karakterizacija

9.4 Realna števila

9.5 Kompleksna števila

(Se ustavimo že pri realnih številih? Gremo še dlje do kvaternionov? –Davorin)

9.6 Vaje

Vaja 9.1. Potenciranje na naravnih številih (torej kot preslikavo $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$) lahko definiramo rekurzivno z naslednjim predpisom.

$$m^0 := 1$$
$$m^{\mathrm{S}(n)} := m^n \cdot m$$

Premisli, da načelo o rekurziji zagotavlja dobro definiranost te preslikave, in izpelji sledeče znane zakone potenciranja.

1. $a^1 = a$
2. $1^n = 1$
3. $a^{m+n} = a^m \cdot a^n$
4. $a^{m \cdot n} = (a^m)^n$

5. $(a \cdot b)^n = a^n \cdot b^n$

6. $\vdots$

Poglavje 10

Indukcija

(Razlaga imena ‘indukcija’.)

10.1 Indukcija na $\mathbb{N}$

10.2 Indukcija na $\mathbb{Z}_{\geq n}$

(za začetek na $\mathbb{N}_{\geq n}$)

10.3 Indukcija na $\mathbb{Z}$

10.4 Gnezdena indukcija

(za začetek dvojna indukcija na $\mathbb{N} \times \mathbb{N}$, nato splošnejša gnezdena na $\mathbb{N}^k$)

10.5 Indukcija s parametrom

(indukcija na $\mathbb{N}$ se posploši na $\mathbb{N} \times X$; podobno z ostalimi primeri)

10.6 Krepka indukcija

(tj. indukcija, kjer v indukcijskem koraku sklepamo z vseh manjših elementov, ne le predhodnika (pomembno kasneje za posplošitev na dobro osnovano urejene množice))

10.7 Strukturna indukcija

(tj. indukcija po kompleksnosti izrazov, generiranih iz signature strukture)

10.8 Dobro osnovane urejenosti

(Zaenkrat bom “well-founded” prevajal kot “dobro osnovan”, ker je ta izraz uporabljal Marko pri LMN. Ampak dobro bi bilo, da bi ta prevod še predebatirali. –Davorin)

V prejšnjih razdelkih smo si ogledali mnogo različic indukcij. Čas je, da vse te različice pripeljemo pod isto streho: da najdemo splošni pojem indukcije, ki zajema prejšnje kot posebne primere. To nam omogočajo tako imenovane dobro osnovano urejene množice.

Na kratko rečeno, dobro osnovano urejene množice so množice s toliko strukture, da lahko na njih izvajamo indukcijo — konkretno, indukcijo v krepkem smislu, kot podano v razdelku 10.6. Natančna definicija je sledeča.

Definicija 10.1. Naj bo X množica in $\prec$ relacija na njej.

- Za predikat ϕ na X rečemo, da je ***$\prec$-induktiven***, kadar za vsak $a \in X$ velja: če ϕ velja za vse $x \in X_{\prec a}$, tedaj velja tudi za a. Simbolno zapisano:

$$\forall a \in X. (\forall x. X_{\prec a}\phi(x)) \implies \phi(a).$$

- Množica X, skupaj z relacijo $\prec$, je ***dobro osnovano urejena***, kadar je posod resničen predikat edini $\prec$-induktiven predikat na X.

Torej: če želimo dokazati, da neka lastnost ϕ velja za vse elemente dobro osnovano urejene množice, dokažemo indukcijski korak za ϕ (v smislu: če lastnost velja za vse elemente, "manjše" od a, potem velja tudi za a).

Zgornja definicija dobro osnovane urejenosti je neposredno naravnana na indukcijo. To je njena prednost, je pa tudi njena slabost: kako vemo, da neka relacija $\prec$ dejansko dobro osnovano ureja dano množico? Neposredno preveriti definicijo je lahko težje, kot pa neposredno preveriti željeno univerzalno kvantificirano lastnost; v tem primeru nismo nič pridobili. Zato je dobro imeti alternativne karakterizacije dobro osnovane urejenosti.

Izrek 10.2. *Naslednje izjave so ekvivalentne za poljubno množico X in relacijo $\prec$ na njej.*

- *$\prec$ dobro osnovano ureja X.*
- *Ne obstaja neskončna padajoča veriga v X. Natančneje: ne obstaja zaporedje $a\colon \mathbb{N} \to X$, za katerega velja $a_{n+1} \prec a_n$ za vse $n \in \mathbb{N}$.*
- *Vsaka nahajajoča podmnožica $S \subseteq X$ ima minimalni element v naslednjem smislu: obstaja $a \in S$, tako da za noben $x \in S$ ne velja $x \prec a$.*

Dokaz. □

Splošne dobro osnovane urejenosti so lahko precej razvejane (kot bomo kasneje videli iz primerov). Včasih se zato želimo omejiti na tako imenovane dobre urejenosti

Definicija 10.3. Množica X, opremljena z relacijo $\prec$, je ***dobra urejena***, kadar je dobro osnovano urejena in relacija $\prec$ je stroga linearna urejenost.

Tudi za dobre urejenosti imamo karakterizacijo.

Izrek 10.4. *Naslednji izjavi sta ekvivalentni za poljubno množico X in relacijo $\prec$ na njej.*

- *$\prec$ dobro ureja X.*
- *Vsaka nahajajoča podmnožica $S \subseteq X$ ima najmanjši element v naslednjem smislu: obstaja $a \in S$, tako da za vsak $x \in S \setminus \{a\}$ velja $a \prec x$.*

Dokaz. □

(Razlaga, v kakšnem smislu so različice indukcij iz prejšnjih razdelkov posebni primeri indukcije na dobro (osnovano) urejenih množicah. Primeri indukcije na dobro (osnovano) urejenih množicah, ki niso oblike, kot podane v prejšnjih razdelkih. Omemba, da bomo kasneje (pri ordinalnih številih) spoznali še pojem transfinitne indukcije.)

10.9 Vaje

Poglavje 11

Kumulativna hierarhija

11.1 Aksiomi teorije množic

(Zagotovo pa ne ZFC, ampak neka aksiomatizacija, ki ima razrede, recimo BGN ali MK. –Andrej)

Poglavje 12

Kardinalna števila

12.1 Končnost in neskončnost

12.2 Števnost

12.3 Kardinalnost množice

Poglavje 13

Ordinalna števila

(Mogoče združimo kardinalna in ordinalna števila v eno poglavje? –Davorin)

Poglavje 14

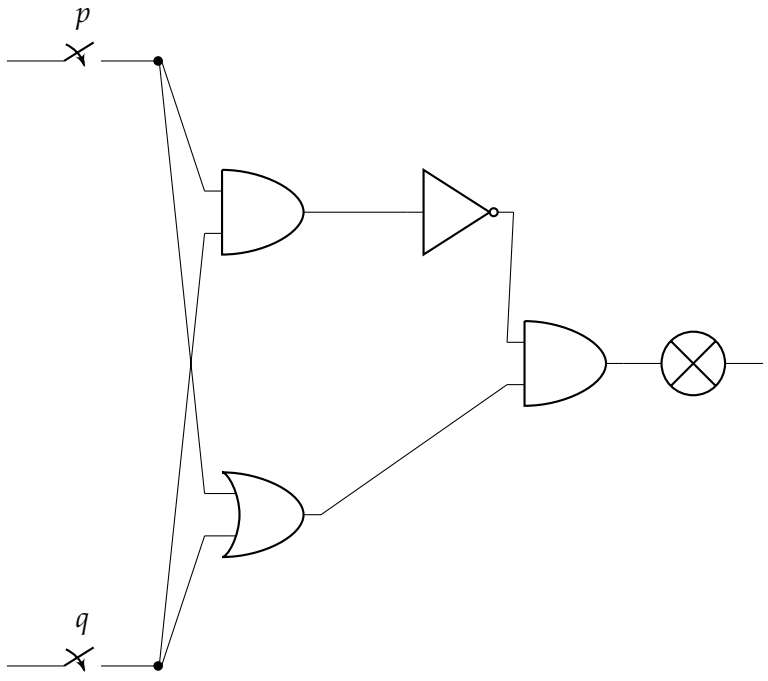
Rešitve vaj

Rešitev 2.1 Množica A ima kvečjemu en element, tj. množica A je bodisi prazna bodisi enojec. Tudi: množica A je podmnožica kakega enojca oz. edina preslikava $A \to \mathbf{1}$ je injektivna.

Rešitev 3.8 Imamo dve stikali, imenujmo ju p in q. Opazujemo, kdaj luč sveti. Na začetku sta obe stikali ugasnjeni in luč ne sveti. Če prižgemo eno stikalo, mora luč zasvetiti. Če prižgemo nato še drugo stikalo mora luč ugasniti. Ugotovimo, da je luč prižgana, ko je prižgano natanko eno stikalo. To ponazorimo v naslednji tabeli:

p	q	luč sveti
$\top$	$\top$	$\bot$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\bot$

Opazimo, da ima to enako tabelo, kot izjava $p \veebar q$. Torej moramo to izjavo izraziti z izjavnimi vezniki $\wedge, \vee$ in $\neg$. En način, kako to naredimo je, da zapišemo $p \veebar q \equiv (p \vee q) \wedge \neg(p \wedge q)$, in tako konstruiramo vezja z vrati "in", "ali" in negacijo takole:



Le z veznikoma $\wedge$ in $\vee$ tega ne moremo storiti, saj veznika ne predstavljata polnega nabora. Z uporabo zgolj Łukasiewiczevega veznika pa je to mogoče, saj predstavlja poln nabor.

Dodatek A

Pomembnejši makroji (razlaga uporabe)

(To poglavje je namenjeno zgolj za nas pisce, ne pa za bralce. Tu razložim uporabo nekaterih latexovskih makrojev, ki sem jih definiral. Če dodate svoje, katerih uporaba ni očitna, njihovo razlago prosim dodajte sem. –Davorin)

Nekateri zapisi

Za podajanje latexovskih ukazov uporabimo `\ltc`. (Okolje `verbatim` ne deluje dobro znotraj makrojev, ampak če kdo ve, kako to razrešiti, naj popravi. –Davorin)

Koda: `\ltc{sqrt\{2\}}`

Prikaz: `\sqrt{2}`

Narekovaje pišemo tako, kot je to običajno v LaTeXu, saj lahko kasneje določimo, kako se jih dejansko prikazuje.

Včasih bomo želeli podati stavek v naravnem jeziku (namesto v simbolnem matematičnem).

Koda: `\nls{Stavek v naravnem jeziku.}`

Prikaz: "*Stavek v naravnem jeziku.*"

Za definirani izraz uporabimo `\df`.

Koda: `Funkcija je \df{zvezna}, kadar\ldots`

Prikaz: Funkcija je ***zvezna***, kadar...

Za definicijsko enakost uporabimo `\dfeq` oz. za enakost v nasprotni smeri `\revdfeq`.

Koda: `$f(x,y) \dfeq x + y$`

Prikaz: $f(x,y) := x + y$

Koda: `$e^2 + \pi \revdfeq a$`

Prikaz: $e^2 + \pi =: a$

Množice

Za množice uporabimo ukaz `\set`. Podamo lahko enega ali dva argumenta.

Koda: `$\set{1,2,3}$`

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

Koda: `$\set{x \in \RR}{x > 1}$`

Prikaz: $\{x \in \mathbb{R} \mid x > 1\}$

Zaviti oklepaji se samodejno prilagajajo velikosti besedila.

Koda: `$\set{1, \displaystyle{\frac{3}{4}}} \cup \set{x \in \NN}{x > 2^{2^{`

Prikaz: $\left\{1, \frac{3}{4}\right\} \cup \left\{x \in \mathbb{N} \,\middle|\, x > 2^{2^{100}}\right\}$

Če nam privzeta velikost oklepajev ni všeč, jo lahko spremenimo z izbirnim parametrom, ki je število od 0 do 4.

Koda: `$\set[0]{0}, \set[1]{1}, \set[2]{2}, \set[3]{3}, \set[4]{4}$`

Prikaz: $\{0\}, \{1\}, \left\{2\right\}, \left\{3\right\}, \left\{4\right\}$

Za generični enojec uporabimo ukaz `\one`, za njegov element pa `\unit`.

Koda: `$\one = \set{\unit}$`

Prikaz: $\mathbf{1} = \{()\}$

Intervali

(Glej diskusijo, ki se trenutno nahaja v razdelku 2.1 (ampak to se bo spremenilo). –Davorin)

Za intervale uporabljamo ukaze `\intoo`, `\intoc`, `\intco`, `\intcc`, kjer `o` označuje odprtost, `c` pa zaprtost intervala. Krajišči intervala podamo kot argumenta.

Koda: `$\intoo{0}{1}, \intoc{2}{3}, \intco{4}{5}, \intcc{6}{7}$`

Prikaz: $\mathbb{R}_{(0,1)}, \mathbb{R}_{(2,3]}, \mathbb{R}_{[4,5)}, \mathbb{R}_{[6,7]}$

Če želimo interval na neki drugi množici kot $\mathbb{R}$, podamo to množico kot izbirni argument.

Koda: `$\intco[\NN]{1}{5} = \set{1,2,3,4}$`

Prikaz: $\mathbb{N}_{[1,5)} = \{1,2,3,4\}$

Kvantifikatorji, λ- in ι-izrazi

Vsi kvantifikatorji imajo enako obliko, ponazorimo jo z univerzalnim kvantifikatorjem:

- Koda: `\all{x \in A} \Phi`
- Prikaz: $\forall x \in A. \Phi$

Če želimo oklepaje okoli Φ, jih enostavno napišemo. Če želimo imeti neomejen kvantifikator, lahko napišemo `\all{x} \Phi` itd.

Ostali kvantifikatorji si:

- eksistenčni: `\some{x \in A} \Phi`, dobimo $\exists x \in A. \Phi$
- enolični obtoj: `\exactlyone{x \in A} \Phi`, dobimo $\exists! x \in A. \Phi$
- funkcija: `\lam{x \in A} e`, dobimo $\lambda x \in A. e$
- opis: `\that{x \in A} \Phi`, dobimo $\iota x \in A. \Phi$

Kanonične projekcije in injekcije

Nismo še sprejeli odločitve, kako bomo označevali projekcije oz. injekcije pri dvojiških produktih oz. vsotah. Tudi ko jo bomo, bomo verjetno šli skozi več iteracij. Imejmo torej makroje zanje, ki jih bomo lahko na koncu poljubno spreminjali.

(Projekcije in injekcije so naravne preslikave. Tega verjetno ne bomo omenjali študentom, dobro pa bi bilo, da se sami tega zavedamo in izrecno pišemo indekse komponent. Na ta način se izognemo zmedi v situacijah, kjer obravnavamo več kot en (ko)produkt. –Davorin)

Ukazi za leve oz. desne projekcije oz. injekcije so sledeči.

	leva	desna
projekcija	`\fst`	`\snd`
injekcija	`\inl`	`\inr`

Tem ukazom kot izbirna parametra podamo faktorja oz. sumanda.

Koda: `$X \stackrel{\fst[X][Y]}{\longleftarrow} X \times Y \stackrel{\snd[X`

Prikaz: $X \stackrel{\pi_1^{X,Y}}{\longleftarrow} X \times Y \stackrel{\pi_2^{X,Y}}{\longrightarrow} Y$

Koda: `$X \stackrel{\inl[X][Y]}{\longrightarrow} X + Y \stackrel{\inl[X][Y]`

Prikaz: $X \stackrel{\iota_1^{X,Y}}{\longrightarrow} X + Y \stackrel{\iota_2^{X,Y}}{\longleftarrow} Y$