Logika in množice
ZAPISKI V NASTAJANJU

Andrej Bauer

13. november 2022

Kazalo

Predgovor

Glavni namen predmet Logika in množice v prvem letniku študija matematike je študente naučiti osnov matematičnega izražanja: kako beremo in pišemo matematično besedilo, kako uporabljamo simbolni zapis, kako zapišemo in preberemo dokaz itd. Drugi poglavitni namen predmeta je spoznavanje osnov matematične logike in teorije množic.

Za semesterski predmet z dvema urama predavanj in dvema urama vaj ima predmet zelo ambiciozen program. Najučinkovitejši recept za uspeh je tisti, ki ga študenti ne marajo: učite se sproti, sprašujte predavatelja in asistente, trkajte na vrata njihovih pisarn tudi takrat, ko nimajo govorilnih ur.

Ti zapiski s predavanj nastajajo sproti. Prvotno sem jih zapisoval v formatu Markdown, a napočil je čas, da jih prenesem v LaTeX in nato izboljšujem. Opozarjam vas, da zapiski vsebujejo napake, ker so le grob zapis vsebine predavanj. Odkrivanje napak je sestavni del učnega procesa, čeprav si ne želim, da bi bi bilo napak toliko, da bi motile učenje. Zelo vam bom hvaležen, če mi boste odkrite napake sporočili, da jih popravim. Asistentom pri predmetu se zahvaljujem za skrbno odpravljanje napak. Vse ki so ostale, so moja last.

Andrej Bauer

Zahvala. Pri urejanju zapiskov so pomagali:

- šolsko leto 2021/22: Luka Debevc, Matija Fajfar, Miha Gyergyek, Jan Kastelic, Jan Malej, Matej Marinko, Jan Pantner, Lev Rus, Jakob Schrader, Matija Sirk, Matej Šafarič, Gal Zmazek, Marjetka Zupan, Patrik Žnidaršič.
- šolsko leto 2022/23: Leila Mokrovič, Luka Ponikvar, Vesna Poznič, Jaka Prevorčnik, Anja Rupnik, Andraž Ziherl.

Vsem se najlepše zahvaljujem.

Osnovni podatki o predmetu

Gradivo: Osnovni podatki o predmetu in gradivo je na spletni učilnici, kjer najdete:

- povezavo do video posnetkov predavanj in zapiskov s table,
- naloge z vaj, ki so objavljenje v naprej,
- prejšnje kolokvije in izpite,
- povezo na Discord server za predmet.

Izpitni režim. Predmet opravite z izpitom, ki ima dva dela:

1. **pisni izpit**
2. **ustni izpit**

Namesto pisnega izpita lahko opravite dva kolokvija (s povprečno oceno obeh kolokvijev skupaj vsaj 50%). Na ustni izpit pridete šele, ko ste opravili pisni izpit. Če ustnega izpita ne opravite, vam pisni izpit propade in ga morate ponovno opravljati.

Poglavje 1

Množice in preslikave

Pri predmetu Logika in množice se bomo učili, kako matematiki komuniciramo in razmišljamo. Spoznali bomo osnove logike in teorije množic, tako iz povsem praktičnega vidika kot tudi matematičnega. Pri tem predmetu cenimo ne le matematično razmišljanje, ampak tudi razmišljanje o matematiki.

Za uvod povejmo nekaj osnovnega o množicah in spoznajmo nekatere osnovne konstrukcije.

1.1 Osnovno o množicah

1.1.1 Množice kot skupki elementov, relacija $\in$

Naivno bi rekli, da je množica kakršnakoli zbirka ali skupek matematičnih objektov. Le-ti so lahko števila, funkcije, množice, množice števil ipd., skratka karkoli. Najbolj preprosti primeri množic so končne množice, katerih elemente naštejemo. Zapišemo jih na primer takole:

$$\{1, 2, 3\}$$
$$\{\sin, \cos, \tan\}$$
$$\{\{1\}, \{2\}, \{3\}\}.$$

Objektom, ki tvorijo množico, pravimo **elementi**. Na primer, elementi množice $\{1, \{4\}, 7/3\}$ so število 1, množica $\{4\}$, in število $7/3$.

Kadar je a element množice M, to zapišemo $a \in M$ in beremo »a je element M«.

Ali sta množici $\{1, 4, 10\}$ in $\{4, 10, 1, 10\}$ enaki? Da, saj množice obravnavamo kot *neurejene* skupke, v katerih ni pomembno, kolikokrat se pojavi kak element. Da vrstni red in število pojavitev nista pomembna, sledi iz **aksioma ekstenzionalnosti**. Aksiom je matematična izjava, ki jo vzamemo za osnovno, se pravi, da je ne dokazujemo. Aksiomi opredeljujejo matematično teorijo, ki jo želimo študirati. Tako bomo pri tem predmetu spoznali aksiome teorije množic, pri algebri aksiome za vektorski prostor in grupo itd.

Aksiom 1.1 (Ekstenzionalnost množic) *Množici sta enaki, če imata iste elemente.*

Povedano drugače: če je vsak element množice A tudi element množice B in je vsak element množice B tudi element množice A, potem velja $A = B$.

Z uporabo ekstenzionalnosti, lahko *dokažemo*, da sta $\{1, 4, 10\}$ in $\{4, 10, 1, 10\}$ enaki:

1. Vsak element $\{1, 4, 10\}$ je tudi element $\{4, 10, 1, 10\}$:
   (a) velja $1 \in \{4, 10, 1, 10\}$
   (b) velja $4 \in \{4, 10, 1, 10\}$
   (c) velja $10 \in \{4, 10, 1, 10\}$
2. Vsak element $\{4, 10, 1, 10\}$ je tudi element $\{1, 4, 10\}$:
   (a) velja $4 \in \{1, 4, 10\}$
   (b) velja $10 \in \{1, 4, 10\}$
   (c) velja $1 \in \{1, 4, 10\}$
   (d) velja $10 \in \{1, 4, 10\}$

Iz zgornjih dveh preverjanj z uporabo ekstenzionalnosti sledi, da $\{1, 4, 10\} = \{4, 10, 1, 10\}$.

Naloga 1.2 Zapišite podroben dokaz, da sta množici $\{x, y\}$ in $\{y, x\}$ enaki.

Opomba 1.3 Poznamo tudi skupke, pri katerih je pomembno, kolikokrat se pojavi vsak element. Imenujejo se **multimnožice**.

Opozorimo takoj, da v praksi pogosto uporabljamo zapise, ki niso povsem natančni. Takrat se zanašamo, da bodo ostali pravilno uganili, kaj imamo v mislih. Na primer, katere elemente vsebuje množica

$$\{1, 2, 3, ..., 1000\} \ ?$$

Verjetno bi vsi »uganili«, da so mišljena vsa naravna števila med 1 in 1000, ali ne? Zavedati se je treba, da zgornji zapis tega ne določa! Morda smo imeli v mislih vsa števila med 1 in 1000, ki pri deljenju s 5 ne dajo ostanka 4.

Pri tem predmetu bomo pogosto opozarjali na razne nejasnosti in nenatančne zapise, ki jih uporabljajo matematiki v praksi. Ni mišljeno, da bi se pretvarjali, da je kaj narobe s »človeško matematiko«. Želimo se predvsem zavedati, kje se nejasnosti v praksi pojavljajo in kako bi jih lahko odpravili (tudi če jih v praksi dejansko ne odpravimo). Ko bo torej asistent pri analizi na tablo napisal

$$1, 2, 4, 8, \ldots$$

imate tri možnosti:

1. Ste zmedeni.
2. Uganete, da ima v mislih potence števila 2.
3. Vprašate, ali je n-ti člen število regij, na katerega lahko razdelimo prostor z $(n-1)$ ravninami?

Sami se odločite, kakšen odnos želite vzpostaviti z asistentom.

1.1.2 Prazna množica $\emptyset$

Verjetno ni treba izgubljati besed o prazni množici. To je množica, ki nima nobenega elementa. Zapišemo jo $\emptyset$ ali $\{\}$.

Naloga 1.4 Ali je kakšna razlika med $\{\}$ in $\{\emptyset\}$?

1.1.3 Standardni enojec $\mathbb{1}$

Množici, ki ima natanko en element, pravimo **enojec**.

Ali znamo pojasniti, kaj pomeni, da ima množica natanko en element, ne da bi pri tem omenili število 1 ali katerokoli drugo število? Takole: množica A ima natanko en element če velja:

1. obstaja $x \in A$ in
2. če je $x \in A$ in $y \in A$, potem $x = y$.

Naloga 1.5 Kako bi opredelili »množica ima natanko dva elementa« brez uporabe števil?

Pogosto bomo potrebovali kak enojec (že na naslednjih predavanjih). Seveda se ni težko domisliti enojca, na primer $\{42\}$ ali $\{\sin\}$. Da pa ne bomo vedno znova izgubljali časa z izbiro enojca, se dogovorimo da je **standardni enojec** $\mathbb{1}$ množica $\{()\}$. To je zelo čudno, ker smo označili množico s številko[1] 1 in ker je element standardnega enojca $()$, česar še nikoli nismo videli.

Glede oznake $\mathbb{1}$ povejmo, da imamo kot matematiki *načelno svobodo* pri izbiri zapisa, a je smiselno in vljudno, da se ne zafrkavamo. Ali se torej predavatelj zafrkava, ko standardni enojec označi s številko $\mathbb{1}$? Ne, saj gresta »ena« in »enojec« lepo skupaj, poleg tega pa bomo na naslednjih predavanjih spoznali tudi matematične razloge za tak zapis.

Glede oznake $()$ se bo kmalu izkazalo, da je zapis smiseln, ker je $()$ pravzaprav »urejena ničterica«.

1.1.4 Številske in ostale množice

Seveda si bomo privoščili uporabo raznih množic, ki jih že poznate, kot so na primer številske množice $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ itd. Opozorimo pa na naslednjo dilemo: v osnovni in srednji šoli z $\mathbb{N}$ označimo množico celih števil, ki so večja ali enaka 1, vendar pa pogosto v matematiki, še posebej pa v logiki, tudi število 0 obravnavamo kot naravno število. V takih primerih $\mathbb{N}$ označuje množico celih števil, ki so večja ali enaka 0.

Kaj je torej prav $\mathbb{N} = \{0, 1, 2, \ldots\}$ ali $\mathbb{N} = \{1, 2, 3, \ldots\}$? To je napačno vprašanje! Lahko vprašamo le »kako se bomo dogovorili?«. Pri tem predmetu se dogovorimo, da je 0 naravno število, ker vadimo »matematično svobodo«, imamo dobre matematične razloge, da 0 uvrstimo med naravna števila, in ker je predavatelj tako zapovedal.

Naloga 1.6 Zberite pogum in predavatelja vprašate, kakšni so ti dobri matematični razlogi, zaradi katerih je zapovedal, da je 0 naravno število, bo sledila filozofska razprava, ki vam bo pokvarila odmor.

1.2 Konstrukcije množic

Ena od osnovnih matematičnih aktivnosti so **konstrukcije**. Poznamo na primer geometrijske konstrukcije z ravnilom in šestilom. Ko rešujemo enačbo, bi lahko rekli, da konstruiramo število, ki zadošča enačbi. Ko pišemo dokaz, konstruiramo objekt, iz katerega je razvidna resničnost neke izjave. Tudi računalniški programi so le matematični konstrukti.

[1] Ali ločite med »števka«, »številka« in »število«?

Spoznajmo nekatere osnovne konstrukcije množic, se pravi, načine, kako iz množic naredimo nove množice.

1.2.1 Zmnožek ali kartezični produkt

Urejeni par (x, y) je matematični objekt, ki da dobimo tako, da združimo dva matematična objekta x in y. V srednji šoli ste večinoma pisali urejene pare števil (ki ste jih imenovali »koordinate«). V urejenem paru je vrstni red *pomemben*: urejena para $(1, 3)$ in $(3, 1)$ *nista* enaka. (Množici $\{1, 3\}$ in $\{3, 1\}$ sta enaki.)

Urejeni par (x, y) ima **prvo komponento** x in **drugo komponento** y. Če imamo neki urejeni par u, njegovi komponenti pišemo tudi $\mathsf{pr}_1(u)$ in $\mathsf{pr}_2(u)$. Velja torej:

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

Simboloma pr_1 in pr_2 pravimo **prva** in **druga projekcija**. Običajne oznake za projekciji so tudi π_1 in π_2, v programiranju `fst` in `snd`, lahko pa tudi π_0 in π_1.

Spoznajmo sedaj **zmnožek** ali **kartezični produkt** množic A in B. Navesti moramo zapis za konstruirano množico, katere elemente ima, in kdaj sta elementa konstruirane množice enaka:

1. Zmnožek množic A in B zapišemo $A \times B$.
2. Elementi množice $A \times B$ so urejeni pari (x, y), pri čemer je $x \in A$ in $y \in B$.
3. Enakost elementov (princip ekstenzionalnosti za pare): $u \in A \times B$ in $v \in A \times B$ sta enaka, če velja $\mathsf{pr}_1(u) = \mathsf{pr}_1(v)$ in $\mathsf{pr}_2(u) = \mathsf{pr}_2(v)$.

Primer 1.7 Zmnožek množic $\{1, 2, 3\}$ in $\{\square, \diamond\}$ je

$$\{1, 2, 3\} \times \{\square, \diamond\} = \{(1, \square), (2, \square), (3, \square), (1, \diamond), (2, \diamond), (3, \diamond)\}.$$

Iz principa ekstenzionalnosti za pare sledi, da je vrstni red v urejenem paru pomemben, saj $(1, 3) \neq (3, 1)$, ker $\mathsf{pr}_1(1, 3) = 1 \neq 3 = \mathsf{pr}_1(3, 1)$.

Zmnožek več množic

Tvorimo lahko tudi zmnožek več množic. Na primer, zmnožek množic A, B in C je množica $A \times B \times C$, katerih elementi so **urejene trojke** (x, y, z), kjer je $x \in A$, $y \in B$ in $z \in C$. V tem primeru imamo tri projekcije pr_1, pr_2 in pr_3. Podobno lahko tvorimo zmnožek štirih, petih, šestih, ... množic.

Naloga 1.8 Ali lahko tvorimo zmnožek ene množice? Kaj pa zmnožek nič množic?

1.2.2 Vsota ali koprodukt

Naslednja osnovna konstrukcija je **vsota** ali **koprodukt** množic A in B:

1. vsoto množic A in B označimo z $A + B$,
2. elementi množice $A + B$ so $\mathsf{in}_1(x)$ za $x \in A$ in $\mathsf{in}_2(y)$ za $y \in B$,
3. elementa $u \in A + B$ in $v \in A + B$ sta enaka, kadar velja
   (a) bodisi za neki $a \in A$ velja $u = \mathsf{in}_1(a) = v$,
   (b) bodisi za neki $b \in B$ velja $u = \mathsf{in}_2(b) = v$.

Primer 1.9 Primeri vsote množic:

1. $\{1,2,3\} + \{\square, \diamond\} = \{\mathsf{in}_1(1), \mathsf{in}_1(2), \mathsf{in}_1(3), \mathsf{in}_2(\square), \mathsf{in}_2(\diamond)\}$
2. $\{a,b\} + \{b,c\} = \{\mathsf{in}_1(a), \mathsf{in}_1(b), \mathsf{in}_2(b), \mathsf{in}_2(c)\}$
3. Vsota *ni* unija! Po eni strani je $\{3,5\} \cup \{3,5\} = \{3,5\}$ in po drugi $\{3,5\} + \{3,5\} = \{\mathsf{in}_1(3), \mathsf{in}_1(5), \mathsf{in}_2(3), \mathsf{in}_2(5)\}$.

Vsoti pravimo tudi »disjunktna unija«, a se bomo temu izrazu izogibali, ker obravnavamo vsoto kot osnovno operacijo in ne kot poseben primer unije.

Oznakama in_1 in in_2 pravimo **prva in druga injekcija**. Uporabljajo se tudi oznake ι_1 in ι_2, v funkcijskem programiranju `inl` in `inr`, pa tudi ι_0 in ι_1. Pravzaprav ni pomembno, kakšne oznake uporabimo, poskrbeti moralo le, da sta to različna simbola, s katerima razločimo elemente prvega in drugega sumanda.

Tvorimo lahko vsoto več množic, na primer $A + B + C$. V tem primeru imamo tri injekcije in_1, in_2 in in_3.

1.3 Preslikave ali funkcije

Poleg množic so preslikave še en osnovni matematični pojem, ki mu bomo posvetili veliko pozornosti. **Preslikava** ali **funkcija** sestoji iz treh sestavin:

- množice, ki ji pravimo **domena**,
- množice, ki ji pravimo **kodomena**,
- **prirejanja**, ki vsakemu elementu domene priredi natanko en element kodomene.

Če je f funkcija z domeno A in kodomeno B, to zapišemo

$$f : A \to B$$

ali

$$A \xrightarrow{\quad f \quad} B$$

Rišemo lahko tudi diagrame, ki prikazujejo več funkcij hkrati, na primer

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ & & & & \downarrow{\scriptstyle h} \\ & & & & D \end{array}$$

Ta diagram prikazuje tri preslikave: $f : A \to B$, $g : B \to C$ in $h : C \to D$.

V srednji šoli ste spoznavali posamične zvrsti funkcij, na primer linearne funkcije, trigonometrične funkcije, eksponentno funkcijo itd. Le-te so običajno slikale števila v števila, bile so *številske funkcije*. Mi se bomo ukvarjali s preslikavami na splošno, se pravi s poljubnimi preslikavami med poljubnimi množicami.

Princip ekstenzionalnosti preslikav

Princip ekstenzionalnosti za preslikave, pove, kdaj sta dve funkciji enaki, namreč takrat, ko prirejata enake vrednosti: če za preslikavi $f : A \to B$ in $g : C \to D$ velja $A = C$, $B = D$ in $f(x) = g(x)$ za vse $x \in A$, potem velja $f = g$.

Kasneje bomo videli, da princip ekstenzionalnosti za preslikave sledi iz principa ekstenzionalnosti za množice.

1.3.1 Prirejanje in funkcijski predpisi

Dejstvo, da mora prirejanje vsakemu elementu domene prirediti »natanko en« element kodomene, lahko izrazimo tako, da se izognemo uporabi števila »ena« ali kateregakoli števila. Poglejmo kako.

Prirejanje z domeno A in kodomeno B mora biti:

1. **celovito:** vsakemu $x \in A$ je prirejen vsaj en $y \in B$ (priredimo vsaj en element),
2. **enolično:** če sta $x \in A$ prirejena $y \in B$ in $z \in B$, potem velja $y = z$ (priredimo največ en element).

Res, celovitost zagotavlja, da vsakemu elementu domene priredimo *vsaj en* element kodomene, enoličnost pa zagotavlja, da priredimo *kvečjemu enega*.

Opomba 1.10 Pozor, celovitost *ni* surjektivnost in enoličnost *ni* injektivnost!

Kako pravzaprav podamo prirejanje? Kaj to pravzaprav je? Čez kak mesec bomo znali odgovoriti na to vprašanje natančno, zaenkrat pa le povejmo, da je prirejanje kakršnakoli metoda, tabela, postopek, prikaz, ali konstrukcija, ki zagotavlja celovitost in enoličnost prirejanja elementov kodomene elementom domene.

Običajni način za podajanje prirejanja je **funkcijski predpis**, ki ga pišemo

$$x \mapsto \cdots$$

Pri čemer za $\cdots$ na desni postavimo neki smiseln izraz, ki določa enolično vrednost za vsak x iz domene. Spremenljivki x na levi pravimo **parameter**, izrazu $\cdots$ na desni pa **prirejena vrednost**.

Primer 1.11 Primeri prirejanj:

- prirejanje »prištej 7 in kvadriraj« zapišemo s funkcijskim predpisom $x \mapsto (x+7)^2$,
- prirejanje »kvadriraj in prištej 7« zapišemo s funkcijskim predpisom $x \mapsto x^2 + 7$,
- prirejanje »prištej kvadrat 7« zapišemo s funkcijskim predpisom $x \mapsto x + 7^2$.

Opomba 1.12 Pozor: če podamo *samo* funkcijski predpis brez domene in kodomene, še nismo podali preslikave! Preslikava sestoji iz *treh* delov: domena, kodomena in prirejanje. Torej zgornji trije primeri *ne* podajajo preslikav, ker nismo podali domen in kodomen.

Domeno, kodomeno in funkcijski predpis lahko zapišemo na različne načine:

$$\begin{aligned} f &: \mathbb{Z} \to \mathbb{N} \\ f &: x \mapsto x^2 + 7 \end{aligned}$$

ali

$$\begin{aligned} f &: \mathbb{Z} \to \mathbb{N} \\ f(x) &:= x^2 + 7 \end{aligned}$$

ali

$$\begin{aligned} f &: \mathbb{Z} \to \mathbb{N} \\ f &= (x \mapsto x^2 + 7) \end{aligned}$$

Simbol x je **vezana spremenljivka**, če jo preimenujemo, se predpis ne spremeni. Naslednji funkcijski predpisi so *enaki*:

$$x \mapsto x^2 + 7$$
$$y \mapsto y^2 + 7$$
$$banana \mapsto banana^2 + 7$$

Funkcijski predpis $x \mapsto 5+x\cdot x+2$ pa *ni enak* zgornjim trem, čeprav vrača enake vrednosti in torej določa *enako* funkcijo.

Aplikacija ali uporaba

Preslikavo $f : A \to B$ **uporabimo** ali **apliciramo** na elementu $a \in A$, da dobimo **vrednost** $f(a) \in B$. V izrazu $f(a)$ se imenuje a **argument** Kadar je f podana s predpisom, izračunamo vrednost $f(a)$ tako, da a vstavimo v predpis (vezano spremenljivo zamenjamo z argumentom A). O zamenjavi vezane spremenljivke z argumentom bomo več povedali v razdelku 5.7.2 o substituciji.

Primer 1.13 Če je $f : \mathbb{N} \to \mathbb{N}$ podana s predpisom $f = (x \mapsto x^3 + 4)$, tedaj je $f(5)$ enako $5^3 + 4$. Lahko bi celo pisali

$$(x \mapsto x^3 + 4)(5) = 5^3 + 4.$$

1.3.2 Eksponentna množica

Tretja konstrukcija množic, ki jo bomo spoznali v uvodnem poglavju, je **eksponent** ali **eksponentna množica**:

1. eksponent množic A in B označimo B^A, in preberemo »B na A«,
2. elementi B^A so preslikave z domeno A in kodomeno B,
3. preslikavi $f : A \to B$ in $g : A \to B$ sta enaki, če imate enake vrednosti: za vse $x \in A$ velja $f(x) = g(x)$, potem je $f = g$.

Eksponent B^A pišemo tudi $A \to B$. To pomeni, da bi lahko namesto $f : A \to B$ pisali tudi $f \in B^A$ ali celo $f \in A \to B$, vendar je ta zadnji zapis neobičajen.

Primer 1.14 Eksponent $\{1, 2\}^{\{a,b\}}$ ima štiri elemente:

$$\{1, 2\}^{\{a,b\}} = \{(a \mapsto 1, b \mapsto 1), (a \mapsto 1, b \mapsto 2), (a \mapsto 2, b \mapsto 1), (a \mapsto 2, b \mapsto 2)\}.$$

Poglavje 2

Aritmetika množic

Nadaljujmo s študijem splošnih preslikav.

2.1 Preslikave in prazna množica

Naj bo A množica. Kaj vemo povedati o preslikavah $\emptyset \to A$? Čez nekaj tednov bomo spoznali naslednji dejstvi, ki ju zaenkrat vzemimo v zakup:

- Vsaka izjava oblike »za vsak element $\emptyset$ ...« je resnična.
- Vsaka izjava oblike »obstaja element $\emptyset$ ...« je neresnična.

Primeri resničnih izjav:

1. »Vsak element prazne množice je sodo število«
2. »Vsak element prazne množice je liho število«
3. »Vsak element prazne množice je hkrati sodo in liho število«
4. »Vsak element prazne množice . . . «

Primeri neresničnih izjav:

1. »Obstaja element prazne množice, ki je sodo število«
2. »Obstaja element prazne množice, ki je enak sam sebi«
3. »Obstaja element prazne množice, ki . . . «

Denimo, da imamo preslikavi $f : \emptyset \to A$ in $g : \emptyset \to A$. Tedaj sta enaki, saj velja: »za vsak element $x \in \emptyset$ velja $f(x) = g(x)$«. Torej imamo kvečjemu eno preslikavo $\emptyset \to A$. Ali pa imamo sploh kakšno? Da, pravimo ji **prazna preslikava**, ker je njeno prirejanje »prazno«, oziroma ga sploh ni treba podati (saj ni nobenega elementa domene $\emptyset$, ki bi mu morali prirediti kak element kodomene A).

Kaj pa preslikave $A \to \emptyset$? Če je $A = \emptyset$, potem imamo natanko eno preslikavo $A \to \emptyset$, namreč prazno preslikavo, $\emptyset^A = \{\text{prazna-preslikava}\}$. Če A vsebuje kak element, potem ni nobene preslikave $A \to \emptyset$, se pravi $\emptyset^A = \emptyset$.

Zakaj ni preslikave $A \to \emptyset$, kadar A vsebuje kak element? Denimo da je $x \in A$. Če bi bila kaka preslikava $f : A \to \emptyset$, bi veljalo $f(x) \in \emptyset$, kar pa ni res. Torej take preslikave ni.

Naloga 2.1 Koliko je preslikav $1 \to A$ in koliko je preslikav $A \to 1$? Ali je odgovor odvisen od A?

2.2 Identiteta in kompozicija

Spoznajmo nekaj osnovnih preslikav in operacij na preslikavah.

Identiteta na A je preslikava $\mathrm{id}_A : A \to A$, podana s predpisom $x \mapsto x$.

Kompozitum preslikav

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

je preslikava $g \circ f : A \to C$, podana s predpisom $x \mapsto g(f(x))$.

Kompozitum je asociativen: za preslikave

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

velja $(h \circ g) \circ f = h \circ (g \circ f)$. Res, za vsak $x \in A$ velja

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

torej želena[1] enačba sledi iz principa ekstenzionalnosti za funkcije.

Identiteta je nevtralni element za kompozitum: za vsako preslikavo $f : A \to B$ velja

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

To preverimo z uporabo ekstenzionalnosti za funkcije: za vsak $x \in A$ velja

$$(\mathrm{id}_B \circ f)(x) = \mathrm{id}_B(f(x)) = f(x)$$

in

$$(f \circ \mathrm{id}_A)(x) = f(\mathrm{id}_A(x)) = f(x).$$

Kompozicija $\circ$ in identiteta id se torej obnašata podobno kot nekatere operacije v algebri, na primer $+$ in 0 ter $\times$ in 1.

Naloga 2.2 Seštevanje je komutativno, velja $a + b = b + a$. Ali je kompozicija preslikav tudi komutativna?

2.3 Funkcijski predpisi na zmnožku in vsoti

Pogosto želimo definirati preslikavo, katere kodomena je zmnožek množic, denimo $f : A \times B \to C$. V takem primeru lahko podamo funkcijski predpis takole:

$$(x, y) \mapsto \cdots$$

pri čemer je $x \in A$ in $y \in B$. To je dovoljeno, ker je vsak element domene $A \times B$ urejeni par (x, y) za natanko določena $x \in A$ in $y \in B$.

[1] Piše se »želen« in ne »željen«, ker je »želen« deležnik na »n« glagola »želeti«. V slovenščini ni glagola »željeti«. Hitro boste spoznali, da na FMF profesorji za matematiko radi popravljajo slovnico.

Primer 2.3 Preslikavo

$$\begin{aligned} \mathbb{R} \times \mathbb{R} &\to \mathbb{R} \\ u &\mapsto \mathsf{pr}_1(u)^2 + 3 \cdot \mathsf{pr}_2(u) \end{aligned}$$

lahko bolj čitljivo podamo s predpisom

$$\begin{aligned} \mathbb{R} \times \mathbb{R} &\to \mathbb{R} \\ (x, y) &\mapsto x^2 + 3 \cdot y \end{aligned}$$

Primer 2.4 Seveda lahko podobno podajamo tudi preslikave na zmnožkih več množic, denimo

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

in

$$\begin{aligned} X \times (Y \times Z) &\to (X \times Y) \times Z \\ (x, (y, z)) &\mapsto ((x, y), z). \end{aligned}$$

Kako pa zapišemo funkcijski predpis funkcije z domeno $A + B$? V tem primeru je vsak element domene bodisi oblike $\mathsf{in}_1(x)$ za enolično določeni $x \in A$, bodisi oblike $\mathsf{in}_2(y)$ za enolično določeni $y \in B$, zato funkcijski predpis podamo v dveh vrsticah:

$$\begin{aligned} A + B &\to C \\ \mathsf{in}_1(x) &\mapsto \cdots \\ \mathsf{in}_2(y) &\mapsto \cdots \end{aligned}$$

Primer 2.5 Primer take preslikave je

$$\begin{aligned} \mathbb{R} + \mathbb{Z} &\to \mathbb{R} \\ \mathsf{in}_1(x) &\mapsto x \\ \mathsf{in}_2(y) &\mapsto y + 3 \end{aligned}$$

Seveda lahko podobno podajamo tudi preslikave na vsotah več množic:

$$\begin{aligned} A + B + C &\to \{u, v\} \\ \mathsf{in}_1(x) &\mapsto u \\ \mathsf{in}_2(y) &\mapsto u \\ \mathsf{in}_3(z) &\mapsto v \end{aligned}$$

in

$$\begin{aligned} A + (B + C) &\to \{u, v\} \\ \mathsf{in}_1(x) &\mapsto u \\ \mathsf{in}_2(\mathsf{in}_1(y)) &\mapsto u \\ \mathsf{in}_2(\mathsf{in}_2(y)) &\mapsto v \end{aligned}$$

Zapisa za zmnožek in vsoto lahko tudi kombiniramo:

$$\begin{aligned}(A \times B \times C) + (D \times E) &\to \{0,1,2\}\\ \mathsf{in}_1((a,b,c)) &\mapsto 1\\ \mathsf{in}_2((d,e)) &\mapsto 2\end{aligned}$$

in

$$\begin{aligned}(A + B) \times C &\to \{0,1,2\}\\ (\mathsf{in}_1(a), c) &\mapsto 0\\ (\mathsf{in}_2(b), c) &\mapsto 1\end{aligned}$$

Izraz na levi strani $\mapsto$ sestoji iz vezanih spremenljivk in operacij, s katerimi gradimo elemente množic (urejeni par, kanonična injekcija). Imenuje se tudi **vzorec**. Predpis je podan pravilno, če so vzorci napisani tako, da vsak element domene ustreza natanko enemu vzorcu. S tem zagotovimo, da predpis obravnava vse možne primere (celovitost) in da ne obravnava nobenega primera večkrat (enoličnost).

2.3.1 Funkcijski predpis, podan po kosih

Omenimo še en pogost način podajanja funkcij, namreč s predpisom po kosih.

Primer 2.6 Preslikava »absolutno« je definirana po kosih za negativna in nenegativna števila:

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

Primer 2.7 Preslikava »predznak« je definirana po kosih:

$$\begin{aligned}&\mathbb{R} \to \mathbb{R}\\ &x \mapsto \begin{cases} -1 & \text{če } x < 0,\\ 0 & \text{če } x = 0,\\ 1 & \text{če } x > 0.\end{cases}\end{aligned}$$

Pri takem zapisu moramo paziti, da kosi skupaj pokrivajo domeno (vsi elementi domene so obravnavani) in da se kosi ne prekrivajo (vsak element domene je obravnavan natanko enkrat). Pravzaprav se smejo kosi prekrivati, a moramo v tem primeru preveriti, da se na skupnih delih skladajo, se pravi, da vsi kosi podajajo enake vrednosti na preseku.

Primer 2.8 Preslikavo »absolutno« bi lahko podali takole:

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

Kosa se prekrivata pri $x = 0$, vendar to ni težava, ker je $-0 = 0$.

2.4 Nekatere preslikave na eksponentnih množicah

Poglejmo si nekaj preslikav, ki slikajo iz in v eksponente množice.

Evalvacija ali **aplikacija** ali **uporaba** je preslikava, ki sprejme preslikavo in argument, ter preslikavo uporabi na argumentu:

$$\begin{aligned}\mathsf{ev} &: B^A \times A \to B\\ \mathsf{ev} &: (f, x) \mapsto f(x)\end{aligned}$$

Pravimo, da je ev **preslikava višjega reda**, ker slika preslikave v vrednosti.

Primer 2.9 Določeni integral $\int_0^1$ je funkcija višjega reda, ker sprejme funkcijo $[0,1] \to \mathbb{R}$ in vrne realno število. Je torej preslikava $\mathbb{R}^{[0,1]} \to \mathbb{R}$, če se pretvarjamo, da lahko integriramo vsako funkcijo. Bolj pravilno bi bilo reči, da je $\int_0^1$ preslikava iz množice *integrabilnih funkcij* $[0,1] \to \mathbb{R}$ v realna števila.

Kompozitum preslikav je tudi preslikava višjega reda:

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

Tretja splošna preslikava višjega reda je »currying« (ali zna kdo to prevesti v slovenščino?):

$$\begin{aligned}A^{(B\times C)} &\to (A^B)^C\\ f &\mapsto (c \mapsto (b \mapsto f(b,c))).\end{aligned}$$

Pravzaprav je to izomorfizem, katerega inverz je »uncurrying«:

$$\begin{aligned}(A^B)^C &\to A^{B\times C}\\ g &\mapsto ((b,c) \mapsto g(c)(b)).\end{aligned}$$

Zapis $g(c)(b)$ beremo kot $(g(c))(b)$.

2.5 Izomorfizmi in aritmetika množic

2.5.1 Inverz

Definicija 2.10 Preslikava $f : A \to B$ je **inverz** preslikave $g : B \to A$, če velja $f \circ g = \mathrm{id}_B$ in $g \circ f = \mathrm{id}_A$.

Naloga 2.11 Utemelji: če je f inverz g, potem je g inverz f.

Primer 2.12 Kub in kubični koren sta inverza

$$\begin{aligned}&\mathbb{R} \to \mathbb{R} && \mathbb{R} \to \mathbb{R}\\ &x \mapsto x^3 && y \mapsto \sqrt[3]{y}\end{aligned}$$

Naloga 2.13 Naj bo S množica nenegativnih realnih števil, se pravi, $\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} \mid x \geq 0\}$. Ali sta kvadriranje in kvadratni koren inverza?

$$\begin{aligned} \mathbb{R} &\to \mathbb{R}_{\geq 0} \\ x &\mapsto x^2 \end{aligned} \qquad\qquad \begin{aligned} \mathbb{R}_{\geq 0} &\to \mathbb{R} \\ y &\mapsto \sqrt[2]{y} \end{aligned}$$

Izjava 2.14 *Če sta $f : A \to B$ in $g : A \to B$ oba inverza preslikave $h : B \to A$, potem je $f = g$.*

Dokaz. Denimo, da sta $f : A \to B$ in $g : A \to B$ inverza preslikave $h : B \to A$. Tedaj velja

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

■

Ali znate utemeljiti vsakega od zgornjih korakov?

Definicija 2.15 Preslikava, ki ima inverz, se imenuje **izomorfizem**.

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

Primer 2.16 Identiteta $\mathrm{id}_A : A \to A$ je izomorfizem, saj je sama sebi inverz. Torej ${\mathrm{id}_A}^{-1} = \mathrm{id}_A$.

Primer 2.17 Eksponentna preslikava $\exp : \mathbb{R} \to \mathbb{R}_{>0}$, $\exp : x \mapsto e^x$ je izomorfizem, njen inverz je naravni logaritem $\ln : \mathbb{R}_{>0} \to \mathbb{R}$, torej $\exp^{-1} = \ln$.

Primer 2.18 Eksponentna preslikava $\exp : \mathbb{R} \to \mathbb{R}$ *ni* izomorfizem.

Izjava 2.19 *Če sta $f : A \to B$ in $g : B \to C$ izomorfizma, potem je tudi $g \circ f : A \to C$ izomorfizem. Velja torej $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Dokaz. Dokazati moramo, da ima $g \circ f$ inverz. Trdimo, da je $f^{-1} \circ g^{-1} : C \to A$ inverz preslikave $g \circ f$. Računajmo:

$$\begin{aligned} (g \circ f) \circ (f^{-1} \circ g^{-1}) & \\ &= ((g \circ f) \circ f^{-1}) \circ g^{-1} \\ &= (g \circ (f \circ f^{-1})) \circ g^{-1} \\ &= (g \circ \mathrm{id}_B) \circ g^{-1} \\ &= g \circ g^{-1} \\ &= \mathrm{id}_C. \end{aligned}$$

Doma sami preverite, da velja tudi $(f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathrm{id}_A$. ■

2.5.2 Izomorfne množice

Definicija 2.20 Množici A in B sta **izomorfni**, če obstaja izomorfizem $f : A \to B$. Kadar sta A in B izomorfni, to zapišemo $A \cong B$.

Izjava 2.21 *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 $A \to A$,
2. če je $f : A \to B$ izomorfizem, potem je tudi $f^{-1} : B \to A$ izomorfizem,
3. če je $f : A \to B$ izomorfizem in $g : B \to C$ izomorfizem, potem je $g \circ f : A \to C$ izomorfizem.

■

Primer 2.22 $A \times B \cong B \times A$, ker imamo izomorfizem in njegov inverz

$$\begin{array}{cc} A \times B \to B \times A & B \times A \to A \times B \\ (x, y) \mapsto (y, x) & (b, a) \mapsto (a, b) \end{array}$$

2.5.3 Aritmetika množic

Veljajo naslednji izomorfizmi, ki nas seveda spomnijo na zakone aritmetike, ki veljajo za števila. Ali gre tu za kako globljo povezavo?

1. Vsota in $\emptyset$:
   (a) $A + \emptyset \cong A$
   (b) $A + B \cong B + A$
   (c) $(A + B) + C \cong A + (B + C)$
2. Zmnožek in $\mathbb{1}$:
   (a) $A \times 1 \cong A$
   (b) $A \times B \cong B \times A$
   (c) $(A \times B) \times C \cong A \times (B \times C)$
3. Distributivnost:
   (a) $A \times (B + C) \cong (A \times B) + (A \times C)$
   (b) $A \times \emptyset \cong \emptyset$
4. Eksponenti:
   (a) $A^1 \cong A$
   (b) $1^A \cong 1$
   (c) $A^\emptyset \cong 1$
   (d) $\emptyset^A \cong \emptyset$, če $A \neq \emptyset$
   (e) $A^{(B \times C)} \cong (A^B)^C$
   (f) $A^{(B+C)} \cong A^B \times A^C$
   (g) $(A \times B)^C \cong A^C \times B^C$

Naloga 2.23 Zapišite vseh 15 izomorfizmov, ki potrjujejo pravilnost zgornjega seznama.

Poglavje 3

Simbolni zapis

V matematiki uporabljamo **simbolni zapis** – matematične objekte, konstrukcije in dokaze opišemo s pomočjo izrazov kot so

$$3 + 4$$
$$x \mapsto x^2 + 3$$
$$\forall x \in \mathbb{R} \,.\, x^2 + x + 1 \geq 1/4$$

Matematično besedilo je mešanica naravnega jezika (slovenščine) in simbolnega zapisa. Načeloma bi lahko pisali matematiko *samo* s simbolnim zapisom (kar dejansko počnemo, kadar matematiko *formaliziramo* z računalnikom, a o tem kdaj drugič), a bi bilo to ljudem preveč nerazumljivo. V starih časih so uporabljali samo naravni jezik (latinščino), kar je bilo tudi zelo nerazumljivo.

Spoznajmo pravila simbolnega zapisa in se učimo razumeti, brati in pisati logične formule (matematične izjave, izražene s simbolnim zapisom).

3.1 Izrazi

(Simbolni) izraz je zaporedje znakov, ki predstavlja neki matematični pojem, na primer

$$3 + 5$$
$$S \cap (T \cup V)$$
$$2xy \leq x^2 + y^2$$

Izraz je *pravilno formiran* ali *sintaktično pravilen*, če ustreza pravilom, ki določajo kako postavljamo oklepaje, vejice, pike, kako uporabljamo razne posebne simbole ($+$, $\vee$, $\int$) itd. Na primer, izraz $3+)x \cdot 4$ ni sintaktično pravilen, ker ima narobe postavljen zaklepaj.

Natančna sintaktična pravila za pisanje matematičnih izrazov so precej zapletena, ker je matematični zapis raznovrsten in se je razvijal skozi zgodovino. Na srečo skoraj vsa pravila že poznate (»vsak oklepaj mora imeti ustrezni zaklepaj«, »piše se $a + b$ in ne $ab+$« ipd). Tu se ne bomo ukvarjali s podajanjem vseh pravil – to je delo za računalničarje, ki želijo taka pravila naprogramirati. Kljub temu pa velja omeniti nekatere pojme.

3.1.1 Prefiksne, postfiksne in infiksne operacije

V simbolnem zapisu uporabljamo *operacije*, ki jih pišemo pred, za ali med argumente:

- **prefiksne operacije** so take, ki jih pišemo *pred* argument:
  - $-x$ za nasprotno vrednost x,
  - $\neg P$ za negacijo izjave P,
- **infiksne operacije** so take, ki jih pišemo *med* argumenta:
  - aritmetične operacije $x + y$, $x - y$, $x \cdot y$ itn.
  - logični vezniki $P \wedge Q$, $P \vee Q$, $P \Rightarrow Q$ itn.
- **postfiksne operacije** so take, ki jih pišemo *za* argument:
  - $n!$ za faktorielo števila n.

Včasih uporabljamo tudi druge oblike zapisa:

- *potenciranje* A^B
- *ulomki* $\frac{a}{b}$
- integrali $\int f(x)dx$ in vsote $\sum_{i=0}^{n} a_i$,
- zapis podmnožice $\{x \in \mathbb{R} \mid x^2 + x > 2\}$.

Operacija je lahko celo »nevidna«, oziroma jo pišemo kot presledek med argumentoma:

- $x\,y$ kot zmnožek x in y,
- $\sin x$ kot uporabe funkcije sin na argumentu x.

3.1.2 Oklepaji, prioriteta in asociiranost

Z oklepaji ponazorimo, katera operacija ima prednost. Na primer, če ne bi imeli dogovora, da ima množenje prednost pred seštevanjem, potem bi lahko izraz $3 + 4 \times 5$ razumeli kot $3 + (4 \times 5)$ ali kot $(3 + 4) \times 5$. Oklepajev ne smemo opustiti, kadar bi lahko prišlo do take zmede. Nikoli pa ne škodi, če zapišemo kak oklepaj več, kot je to potrebno (v mejah normale).

Da se izognemo pisanju oklepajev, se dogovorimo, da imajo nekatere operacije prednost pred ostalimi, kar so vas učili že v osnovni šoli. Pravimo, da imajo operacije **prioriteto**. Operacija z višjo prioriteto ima prednost pred operacijo z nižjo prioriteto.

Primer 3.1 Množenje $\times$ ima višjo prioriteto kot seštevanje $+$ (to je *dogovor* in ne matematično dejstvo). Podobno ima konjunkcija $\wedge$ višjo prioriteto kot disjunkcija $\vee$.

Poleg prioritete imajo nekatere operacije tudi **asociiranost**. Kako naj razumemo izraz $8 - 3 - 2$, kot $(8 - 3) - 2$ ali kot $8 - (3 - 2)$? V šoli so vas učili, da je

$$A - B - C = (A - B) - C$$

Pravimo, da $-$ veže na levo oziroma da ima **levo asociiranost**. Ker beremo z leve na desno, ima večina operacij levo asociiranost. Velja na primer

$$A + B + C = (A + B) + C$$
$$A \times B \times C = (A \times B) \times C.$$

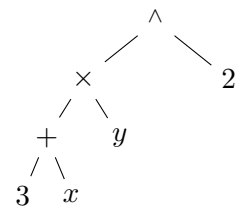
Morda bo kdo pripomnil, da itak velja $(A+B)+C = A+(B+C)$ in da zato ni pomembno, kako razumemo $A+B+C$. To je res v preprostih primerih, ko vemo, da smo s $+$ označili seštevanje števil. Kaj pa, če s $+$ označimo kako drugo preslikavo? Ali $(A + B) + C =$

$A + (B + C)$ velja tudi v programskih jezikih, pri katerih lahko pride do prekoračitve največjega možnega števila?

Primer operacije z desno asociiranostjo je implikacija: $P \Rightarrow Q \Rightarrow R$ je enako $P \Rightarrow (Q \Rightarrow R)$.

3.1.3 Izrazi predstavljajo drevesa

Izrazi so zaporedja znakov, ki jih pišemo z leve na desno. A kje drugje bi jih morda pisali z desne na levo ali navpično. Izrazi so le *predstavitve* tako imenovanih **sintaktičnih dreves**. Na primer $((3 + x) \times y)^2$ predstavlja sintaktično drevo, pri čemer potenciranje predstavimo z znakom $\hat{}$:



O sintaktičnih drevesih ne bomo govorili, a jih omenimo, ker so pomembna iz dveh razlogov: sintaktična drevesa so *podatkovni tip*, s katerim v programu dejansko obdelujemo izraze; s pomočjo sintaktičnih dreves lahko simbolni zapis predstavimo kot posebno vrsto algebre, ki omogoča matematično obravnavo izrazov.

3.1.4 Ostala sintaktična pravila

Sintaktičnih pravil je še več, od katerih omenimo le nekatera.

Podnapisi in nadnapisi

Argumente operacije ali funkcije včasih zapišemo v **podnapis** ali **nadnapis**. Na primer, če je $a : \mathbb{N} \to \mathbb{R}$ preslikava, pogosto pišemo a_i namesto $a(i)$.

Implicitni argumenti

Argumente operacije lahko opustimo in od bralca pričakujemo, da bo pravilno uganil, kaj smo mislili. Pravimo, da so to **implicitni argumenti**. Primer implicitnih argumentov smo že videli, ko smo zapisali prvo in drugo projekcijo pr_1 in pr_2:

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

Če bi bili zelo natančni, bi morali pri projekcijah zapisati tudi množici A in B, ki tvorita kartezični produkt, na primer nekaj takega kot $\mathsf{pr}_1^{A,B} : A \times B \to A$. Ko torej vpeljemo nov zapis, lahko nekatere argumente razglasimo za **implicitne**, kar pomeni, da jih bomo opuščali, kadar to ne pripelje do zmede.

Naloga 3.2 Ali ima kompozicija preslikav $\circ$ implicitne argumente? Katere?

Privzete vrednosti

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

Preobteževanje

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

3.2 Logične formule

Izrazi, ki označujejo števila, se imenujejo **aritmetični izrazi**.

Izrazi, ki označujejo matematične izjave, se imenujejo **logični izrazi** ali **logične formule**. Razumevanje, branje in pisanje le-teh zahteva kar nekaj treninga, zato se mu bomo posvetili tu in na vajah. Pravzaprav ne bomo vadili le razumevanja zapisa, ampak tudi, kako matematiki razmišljajo in razumejo drug drugega.

Tu o dokazih in pravilih dokazovanja še ne bomo govorili, bomo pa pojasnili intuitivni pomen logičnih operacij.

Računanje z logičnimi formulami delimo na:

- **izjavni račun** zaobjema logične veznike $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$,
- **predikatni račun** zaobjema izjavni račun ter kvantifikatorja $\forall$ in $\exists$.

3.2.1 Izjavni račun

Izjavni vezniki so naslednje operacije:

- **resničnostni konstanti** $\bot$ in $\top$: beremo ju »neresnica» in »resnica«,
- **negacija** $\neg$: izjavo $\neg A$ beremo »A ne velja« ali »ni res, da A«,
- **konjunkcija** $\wedge$: izjavo $A \wedge B$ beremo »A in B«,
- **disjunkcija** $\vee$: izjavo $A \vee B$ beremo »A ali B«,
- **implikacija** $\Rightarrow$: izjavo $A \Rightarrow B$ lahko beremo na več načinov:
  - »Iz A sledi B.«
  - »Če A, potem B.«
  - »A samo če B.«
  - »B sledi iz A.«
  - »A je zadosten pogoj za B.«
  - »B je potreben pogoj za A.«
- **ekvivalenca** $\Leftrightarrow$: izjavo $A \Leftrightarrow B$ beremo
  - »A je ekvivalentno B.«
  - »A, če in samo če B.«
  - »A natanko tedaj, ko B.«

– »A je zadosten in potreben pogoj za B.«

Malo bolj neobičajna je:

- **ekskluzivna disjunkcija** $\oplus$: izjava $A \oplus B$ beremo »bodisi A bodisi B« ali »A ali B, vendar ne oba hkrati«.

Prioriteta veznikov, od najvišje do najnižje:

- $\neg$,
- $\wedge$,
- $\vee$, $\oplus$,
- $\Rightarrow$, $\Leftrightarrow$.

Primer 3.3 Izraz $\neg A \wedge B \Rightarrow C \vee D$ beremo kot $((\neg A) \wedge B) \Rightarrow (C \vee D)$.

Asociiranost veznikov:

- leva asociiranost: $\wedge$, $\vee$, $\oplus$,
- desna asociiranost: $\Rightarrow$.

Ekvivalenca $\Leftrightarrow$ nima asociiranosti, zato je zapis $A \Leftrightarrow B \Leftrightarrow C$ načeloma dvoumen, a v praksi pomeni $(A \Leftrightarrow B) \wedge (B \Leftrightarrow C)$.

Opomba 3.4 Tudi zapis $x = y = z$ pravzaprav ni smiseln, saj sta $(x = y) = z$ in $x = (y = z)$ oba nesmiselna. V praksi $x = y = z$ pomeni $(x = y) \wedge (y = z)$. Pa še to: koliko enačb je izraženih z $a = b = c = d$? Tri! Toliko kot je enačajev.

Opomba 3.5 Zapis $x \neq y \neq z$ je nejasen in se mu je bolje izogibati, saj zlahka pripelje do pomote, ker iz $x \neq y$ in $y \neq z$ ne sledi nujno $x \neq z$.

Glede razumevanja veznikov, omenimo:

- disjunkcija je *inkluzivna*, kar pomeni, da je $A \vee B$ resnična izjava, če sta A in B resnični,
- v implikaciji $A \Rightarrow B$ se A imenuje **antecedent** in B **konsekvent**. Implikacija je veljavna, če je antecedent neveljaven,
- ekvivalenco $A \Leftrightarrow B$ lahko razumemo kot okrajšavo za $(A \Rightarrow B) \wedge (B \Rightarrow A)$.

3.2.2 Kvantifikatorja

Matematične izjave vsebujejo fraze, kot so »za vse«, »za neki«, »obstaja vsaj en«, »za natanko enega« ipd. Le-te izrazimo s **kvantifikatorji**. Osnovna kvantifikatorja sta **univerzalni** in **eksistenčni**.

Univerzalni kvantifikator $\forall$

Formulo $\forall x \in A \,.\, \phi$ beremo:

- »Za vsak x iz A velja ϕ.«,
- »Vsi x iz A zadoščajo ϕ.«,
- »ϕ za vse x iz A.«

Pika pri tem nima nobenega posebnega pomena, pogosti so tudi zapisi

$$\forall x \in A \,,\, \phi \qquad \text{ali} \qquad \forall x : A \,,\, \phi \qquad \text{ali} \qquad (\forall x : A)\phi.$$

Nekateri matematiki pišejo po principu »piši kao što govoriš«

$$\phi, \forall x \in A \qquad (\text{»}\phi \text{ za vse } x \text{ iz } A\text{«})$$

Ta zapis odsvetujemo, ker ne deluje, ko kombiniramo več kvantifikatorjev hkrati.

Omenili smo že, da $\forall x \in \emptyset \,.\, \phi$ vedno velja. To bomo utemeljili v poglavju o pravilih sklepanja.

Eksistenčni kvantifikator $\exists$

Formulo $\exists x \in A \,.\, \phi$ beremo:

- »Obstaja x iz A velja ϕ.«
- »Obstaja vsaj en x iz A velja ϕ.«
- »Za neki x iz A velja ϕ.«
- »ϕ za neki x iz A.«

S tem povemo, da obstaja *eden ali več* takih x. Na primer, izjava $\exists x \in \mathbb{N} \,.\, x < 3$ je veljavna, saj je 2 naravno število, ki je manjša od 3.

Prioriteta $\forall$ in $\exists$

Prioriteta kvantifikatorjev $\forall$ in $\exists$ je nižja od prioritete veznikov. Na primer:

- $\forall x \in A \,.\, \phi \wedge \psi$ je enako $\forall x \in A \,.\, (\phi \wedge \psi)$,
- $\forall x \in \mathbb{R} \,.\, x > 0 \Rightarrow \phi$ je enako $\forall x \in \mathbb{R} \,.\, (x > 0 \Rightarrow \phi)$.

Kvantifikator vedno zaobjame vse, kar zmore:

- $\forall x \in A \,.\, \phi \wedge \exists y \in B \psi$ je enako $\forall x \in A \,.\, (\phi \wedge (\exists y \in B . \psi))$ in *ni* enako $(\forall x \in A \,.\, \phi) \wedge (\exists y \in B \psi)$,
- $(P \wedge \forall x \in A \,.\, Q \Rightarrow R) \Rightarrow \exists y \in B \,.\, S$ je enako $(P \wedge \forall x \in A \,.\, (Q \Rightarrow R)) \Rightarrow (\exists y \in B \,.\, S)$ in *ni* enako $(P \wedge (\forall x \in A \,.\, Q) \Rightarrow R) \Rightarrow (\exists y \in B \,.\, S)$

Kombinacija $\forall$ in $\exists$

Pozor, vrstnega reda kvantifikatorjev ne smemo mešati:

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

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

Kvantifikator z dodatnim pogojem

Pogosto kvantifikacijo kombiniramo z dodatnim pogojem, na primer:

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

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

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

In še druga izjava:

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

Zapomnimo si: **dodatni pogoj pri $\exists$ izrazimo $\wedge$** in **dodatni pogoj pri $\forall$ izrazimo $\Rightarrow$**.

Poglejmo še en primer, ko imamo več možnosti za zapis s formulo:

> »Za vsako pozitivno realno število x obstaja tako naravno število n, da je $x < n$.«

Začetni del »za vsako pozitivno realno število« lahko zapišemo na več načinov:

- $\forall x \in \mathbb{R}_{>0} \,.\, \exists n \in \mathbb{N} \,.\, x < n$,
- $\forall x \in \{y \in \mathbb{R} \mid y > 0\} \,.\, \exists n \in \mathbb{N} \,.\, x < n$,
- $\forall x \in \mathbb{R} \,.\, x > 0 \Rightarrow \exists n \in \mathbb{N} \,.\, x < n$,
- $\forall x > 0 \,.\, \exists n \in \mathbb{N} \,.\, x < n$.

Pri prvem načinu moramo biti v naprej dogovorjeni, da $\mathbb{R}_{>0}$ označuje množico pozitivnih realnih števil. Pri drugem načinu smo vstavili definicijo $\mathbb{R}_{>0}$, zato dogovor ni več potreben, a je zapis bolj nečitljiv. Pri tretjem načinu smo predstavili pozitivnost kot dodatni pogoj. Četrti način je najbolj čitljiv in se pogosto uporablja, a nam ne pove, ali je x realno, celo, ali racionalno število.

Vezane in proste spremenljivke

V nekaterih izrazih nastopajo spremenljivke, ki so **vezane**. To pomeni, da je njihovo območje veljavnosti omejeno, oziroma da so neke vrste »lokalne spremenljivke«. Spremenljivka, ki ni vezana, je **prosta**. Primeri:

- V funkcijskem predpisu $x \mapsto x^2 + y$ je x vezan in y prost.
- V funkcijskem predpisu $(x, y) \mapsto x^2 + y$ sta x in y vezana.
- V integralu $\int (x + a)^2 dx$ je x vezan in a prost.
- V vsoti $\sum_{i=0}^{n} (i^2 + 1)$ je i vezan in n prost.
- V formuli $\forall x \in \mathbb{R} \,.\, x^3 + 3x < 7$ je x vezana spremenljivka.

Če vezano spremenljivko preimenujemo, se izraz ne spremeni. Funkcijska predpisa $x \mapsto a \cdot x^2 + 1$ in $y \mapsto a \cdot y^2 + 1$ sta *enaka*. Vendar pozor, če vezano spremenljivko preimenujemo, za novo ime *ne* smemo izbrati spremenljivke, ki se že pojavlja. Na primer, v integralu

$$\int_0^1 (a + x)^2 \, dx$$

smemo x preimenovati v t, zato sta integrala enaka izraza (in imata tudi enako vrednost):

$$\int_0^1 (a+x)^2\,dx = \int_0^1 (a+t)^2\,dt$$

Ne bi pa smeli x preimenovati v a, saj bi dobili

$$\int (a+a)^2\,da.$$

Pravimo, da se je prosta spremenljivka a *ujela* v integral.

Poglavje 4

Definicije in dokazi

4.1 Enolični obstoj

4.1.1 Kvantifikator enoličnega obstoja $\exists!$

S kvantifikatorjema $\forall$ in $\exists$ lahko izrazimo tudi druge kvantifikatorje. Na primer, »obstajata vsaj dva elementa x in y iz A, da velja $\phi(x, y)$« zapišemo

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

Kako pa izrazimo »obstaja natanko en x iz A, da velja $\phi(x)$«? Takole:

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

ali ekvivalentno

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

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

4.1.2 Operator enoličnega opisa

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

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

Proti-primeri:

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

To je lahko zelo koristen način za opredelitev matematičnih objektov, zato uvedemo zanj simbolni zapis. Če dokažemo

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

potem lahko pišemo

$$\iota x \in A \,.\, \phi(x), \qquad \text{»tisti } x \in A, \text{ za katerega velja } \phi(x)\text{«}$$

Torej velja

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

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

Primer 4.1 Denimo, da še ne bi poznali simbola $\sqrt{}$ za kvadratne korene. Tedaj bi lahko kvadratni koren iz 2 zapisali kot

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

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

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

Naloga 4.2 Zapišite »limita zaporedja $a : \mathbb{N} \to \mathbb{R}$« z operatorjem ι, pod predpostavko, da je a konvergentno zaporedje. Najprej povejte z besedami »limita zaporedja a je tisti $x \in \mathbb{R}$, ki . . . «, nato pa zapišite še v obliki $\iota x \in \mathbb{R} \,.\, \ldots$.

Opomba 4.3 Ne pozabite: zapis $\iota x \in A \,.\, \phi(x)$ je veljaven samo v primeru, da velja $\exists! x \in A \,.\, \phi(x)$.

4.2 Spremenljivke in definicije

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

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

V obeh primerih dodamo simbol s v **kontekst**, se pravi v spisek znanih simbolov. Če smo simbol uvedli le začasno (na primer v enem poglavju, ali v delu dokaza), ga iz konteksta odstranimo, ko ni več veljaven.

Matematiki zapisujejo definicije in vpeljujejo spremenljivke na razne načine.

4.2.1 Vpeljava spremenljivke

Če želimo vpeljati spremenljivko x, ki predstavlja neki poljuben ali neznani element množice A, zapišemo

> Naj bo $x \in A$.

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

- »Naj bo $x \in A$ poljuben.«
- »Obravnavajmo poljuben $x \in A$.«
- »Izberimo poljuben $x \in A$.«
- »Denimo, da imamo poljuben $x \in A$.«

Pozor, beseda »izberimo« bi komu dala misliti, da si lahko izbere neki konkretni x, a to preprečuje beseda »poljuben«, ki jo matematik uporabi, kadar želi povedati, da je x neznana ali nedoločena (poljubna) vrednost.

Naloga 4.4 Denimo, da učitelj reče »Naj bo n (poljubno) naravno število«, nato pa vas vpraša »Ali je n sodo število?«, kako boste odgovorili?

4.2.2 Definicija simbola

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

$$s := \dots$$

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

- $s = \sqrt{\log_2 7 + \pi/6}$ (namesto := uporabimo =)
- $s \cong \sqrt{\log_2 7 + \pi/6}$ (namesto := uporabimo $\cong$)
- $s \triangleq \sqrt{\log_2 7 + \pi/6}$ (namesto := uporabimo $\triangleq$)

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

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

to raje zapišemo kot

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

Kadar definiramo simbol s pomočjo enoličnega obstoja, recimo

$$r := \iota x \in \mathbb{R} \,.\, x^3 = 2$$

to raje zapišemo z besedami:

$$\text{Naj bo } r \text{ tisto realno število, ki zadošča } r^3 = 2.$$

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

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

ali

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

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

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

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

4.2.3 Definicije novih matematičnih pojmov

Kaj pa definicije novih pojmov, ki jih srečujete pri predavanjih, denimo pri analizi?

Definicija 4.5 Zaporedje števil $a : \mathbb{N} \to \mathbb{R}$ je **neomejeno**, če za vsak $x \in \mathbb{R}$ obstaja $i \in \mathbb{N}$, da je $a_i > x$.

S stališča simbolnega zapisa, je to le uvedba novega simbola $\mathsf{neomejeno}$:

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

Seveda bistvo take definicije ni le krajši zapis izjave $\forall x \in \mathbb{R} \,.\, \exists i \in \mathbb{N} \,.\, a_i > x$, ampak uporabna vrednost pojma »neomejeno zaporedje«.

4.3 Konstrukcije in dokazi

Matematiki v sklopu svojih aktivnosti *konstruiramo* matematične objekte:

- v geometriji so znane konstrukcije z ravnilom in šestilom,
- računanje števk števila π je konstrukcija približka,
- reševanje enačbe, je konstrukcija števila z želeno lastnostjo,
- konstruiramo lahko elemente množice, pogosto kar tako, da jih zapišemo, na primer $(2, \mathsf{in}_1(3)) \in \mathbb{N} \times (\mathbb{Z} + \mathbb{Z})$.

Poleg tega *dokazujemo* matematične izjave. Na dokaz lahko gledamo kot na konstrukcijo, saj je to le še ena zvrst matematičnega objekta. Ker pa so dokazi skoraj vedno zapisani v naravnem jeziku, jih matematiki pogosto dojemajo ločeno od ostalih matematičnih objektov (števila, preslikave, množice, ploskve, ...).

Kaj pravzaprav je dokaz? V prvi vrsti je dokaz utemeljitev matematične izjave. Zgrajen je po točno določenih *pravilih sklepanja*, ki jih lahko podamo formalno in jih tudi implementiramo na računalniku.[1]

V praksi ljudje ne pišejo vseh podrobnosti v dokazu, ker bi bil tak dokaz nečitljiv in nerazumljiv. Pogosto podajo samo glavno idejo, iz katere lahko izkušeni matematik sam rekonstruira dokaz. Iz dobro napisanega dokaza se lahko naučimo marsikaj novega, poleg gole veljavnosti izjave.

Mi bomo vadili podrobno pisanje dokazov. Pri ostalih predmetih boste videli »žive dokaze«, ki imajo manj podrobnosti in so zapisani manj formalno. A vsi pravilni matematični dokazi se dajo zapisati na način, kot ga bomo predstavili mi (in celo zapisati povsem formalno z dokazovalnim pomočnikom).

4.3.1 Kako pišemo dokaze

Pravila sklepanja so kot pravila igre. Ne povedo, kako dobro igrati, samo kaj je dovoljeno. Seveda bomo hkrati s pravili sklepanja povedali nekaj namigov in nasvetov, kako dokaz poiščemo. A kot pri vsaki igri velja, da vaja dela mojstra.

Dokaz ima ugnezdeno strukturo: sestoji iz delov in pod-dokazov, ki sestoje iz nadaljnjih pod-dokazov itn., ki se zaključijo z osnovnimi dejstvi. Vsi ti kosi so s pomočjo pravil sklepanja zloženi v dokazno »drevo«.

Ko pišemo dokaz, moramo v vsakem trenutku poznati

[1] Kogar to zanima, si lahko ogleda »The dawn of formalized mathematics« (prosojnice) in se nauči uporabljati kak dokazovalni pomočnik (v zadnjem času hitro napreduje Lean).

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

Ko napravimo korak v dokazu, mora biti utemeljen z enim od pravil sklepanja. Dokaz je popoln, ko smo utemeljili vse pod-dokaze, ki ga sestavljajo. Kot primer si poglejmo zelo podroben dokaz izjave $(p \vee q) \wedge r \Rightarrow (p \wedge r) \vee (q \wedge r)$.

Dokažimo $(p \vee q) \wedge r \Rightarrow (p \wedge r) \vee (q \wedge r)$.
(1) Predpostavimo $(p \vee q) \wedge r$.
(2) Zaradi (1) velja $p \vee q$.
(3) Zaradi (1) velja r.
Zaradi (2) lahko obravnavamo dva primera:

(a) če velja p:
Dokažimo $(p \wedge r) \vee (q \wedge r)$.
Dokažimo levi disjunkt $p \wedge r$:
(i) p velja zaradi (a)
(ii) r velja zaradi (3).

(b) če velja q:
Dokažimo $(p \wedge r) \vee (q \wedge r)$.
Dokažimo desni disjunkt $q \wedge r$:
(i) q velja zaradi (b)
(ii) r velja zaradi (3).

Dokaz bi bolj po človeško napisali takole:

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

Ali pa kar takole:

> Očitno.

Pravila sklepanja delimo na:

- **pravila vpeljave**, ki povedo, kako dokažemo izjavo, ter
- **pravila uporabe**, ki povedo, kako lahko že znano izjavo uporabimo.

Poleg tega poznamo še pravila o zamenjavi:

- **zamenjava enakih izrazov**: izraz lahko vedno zamenjamo z njim enakim,
- **zamenjava ekvivalentnih izjav**: izjavo vedno lahko zamenjamo z njej ekvivalentno.

Dokaz je skupek računskih korakov in sklepov, s katerimi utemeljimo izjavo. V vsakem trenutku mora biti jasno, kaj dokazujemo, katere spremenljivke so veljavne in katere predpostavke so na voljo. Nekateri deli dokaza so samostojni pod-dokazi pomožnih izjav. Vse spremenljivke in predpostavke, ki jih uvedemo v pod-dokazu, so na voljo izključno v pod-dokazu samem.

4.3.2 Pravila vpeljave

S pravilom za vpeljavo *neposredno* dokažemo izjavo. Za vsak veznik in kvantifikator ponazorimo, kako uporabimo pripadajoče pravilo vpeljave.

Konjunkcija

Dokažimo $\phi \wedge \psi$.

1. *Dokažimo ϕ:* $\ldots \langle \textit{dokaz } \phi \rangle \ldots$
2. *Dokažimo ψ:* $\ldots \langle \textit{dokaz } \psi \rangle \ldots$

Disjunkcija

Prvi način:

Dokažimo $\phi \vee \psi$.

Zadostuje dokazati levi disjunkt ϕ: $\ldots \langle \textit{dokaz } \phi \rangle \ldots$

Drugi način:

Dokažimo $\phi \vee \psi$.

Zadostuje dokazati desni disjunkt ψ: $\ldots \langle \textit{dokaz } \psi \rangle \ldots$

Implikacija

Dokažimo $\phi \Rightarrow \psi$:

Predpostavimo ϕ.
Dokažimo ψ: $\ldots \langle \textit{dokaz } \psi \rangle \ldots$

Ekvivalenca

Dokažimo $\phi \Leftrightarrow \psi$.

1. *Dokažimo $\phi \Rightarrow \psi$:* $\ldots \langle \textit{dokaz } \phi \Rightarrow \psi \rangle \ldots$
2. *Dokažimo $\psi \Rightarrow \phi$:* $\ldots \langle \textit{dokaz } \psi \Rightarrow \phi \rangle \ldots$

Resnica

Resnice $\top$ ni treba dokazovati, zapišemo »očitno«. [2]

Neresnica

Kadar dokazujemo $\bot$, pravimo, da "iščemo protislovje".

Poiščimo protislovje.

1. *Dokažimo ϕ:* $\ldots \langle \textit{dokaz } \phi \rangle \ldots$
2. *Dokažimo $\neg\phi$:* $\ldots \langle \textit{dokaz } \neg\phi \rangle \ldots$

[2] V praksi $\top$ nastopi kot izjava, ki jo želimo dokazati, ko neko drugo izjavo poenostavimo. Primer: ko dokazujemo $12^2 + 12^2 < 17^2$, najprej izračunamo, da je to ekvivalentno $288 < 289$, kar je ekvivalentno $\top$. S tem je dokaz zaključen, saj smo dobili $\top$.

Negacija

Dokažimo $\neg\psi$*:*

Predpostavimo ψ*.*
Poiščimo protislovje: ...

Opomba: ni nujno, da poiščemo protislovje med ψ in $\neg\psi$, vsako protislovje je sprejemljivo.

Univerzalna izjava

Dokažimo $\forall x \in A \,.\, \phi(x)$*.*

Naj bo $x \in A$*.*
Dokažemo $\phi(x)$*:* ... $\langle$*dokaz* $\phi(x)\rangle$ ...

Pozor: spremenljivka x mora biti *sveža*, se pravi, da je ne uporabljamo nikjer drugje. Če jo, najprej izberemo svežo spremenljivko y in x preimenujemo v y.

Eksistenčna izjava

Dokažimo $\exists x \in A \,.\, \phi(x)$*:*

Podamo $x := \langle$*izraz*$\rangle$*.*
Dokažemo $\langle$*izraz*$\rangle \in A$*:* ...
Dokažemo $\phi(\langle$*izraz*$\rangle)$*:* ...

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

4.3.3 Pravila uporabe

Pravila uporabe nam povedo, kako iz predpostavk in že znanih dejstev izpeljemo nova dejstva.

Konjunkcija

Vemo, da velja $\phi \wedge \psi$*.*
Torej velja ϕ*.*
Torej velja ψ*.*

Opomba: v praksi tega koraka ne delamo, ampak namesto predpostavke $\phi \wedge \psi$ kar takoj vpeljemo ločeni predpostavki ϕ in ψ.

Disjunkcija

Dokažimo ρ*.*
Vemo, da velja $\phi \vee \psi$*, torej obravnavamo primera:*

1. *Če velja* ϕ*:*
   Dokažemo ρ*:* ... $\langle$*dokaz* $\rho\rangle$ ...
2. *Če velja* ψ*:*
   Dokažemo ρ*:* ... $\langle$*dokaz* $\rho\rangle$ ...

Implikacija

Vemo, da velja $\phi \Rightarrow \psi$.

Dokažimo ϕ: $\ldots \langle \textit{dokaz } \phi \rangle \ldots$

Torej velja tudi ψ.

Resnica

Resnica ni uporabna kot predpostavka in jo lahko zavržemo.

Neresnica

Dokažimo ρ:

Ugotovimo, da velja $\bot$.
Ker iz neresnice sledi karkoli, velja ρ.

Negacija

Negacijo $\neg\phi$ uporabimo tako, da dokažemo ϕ in zaključimo dokaz.

Dokažimo ρ.
Vemo, da velja $\neg\phi$.

- *Dokažimo* ϕ: $\ldots \langle \textit{dokaz } \phi \rangle \ldots$

Torej velja ρ.

Univerzalna izjava

Vemo, da velja $\forall x \in A \,.\, \phi(x)$.
Vemo, da je $\langle \textit{izraz} \rangle \in A$.
Torej velja $\phi(\langle \textit{izraz} \rangle)$.

Eksistenčna izjava

Dokažimo ρ.
Vemo, da velja $\exists x \in A \,.\, \phi(x)$.

Imamo $x \in A$, *za katerega velja* $\phi(x)$.
Dokažemo ρ: $\ldots \langle \textit{dokaz } \rho \rangle \ldots$

Pozor: spremenljivka x mora biti sveža, se pravi, da se ne pojavlja v ρ ali kjerkoli drugje. Če se x pojavi kje drugje, ga moramo najprej nadomestiti s svežo spremenljivko y.

Izključena tretja možnost in dokaz s protislovjem

Pravilo izključene tretje možnosti pravi, da vedno velja $\phi \vee \neg\phi$ in ga uporabimo takole:

Dokažimo ρ.
Velja $\phi \vee \neg\phi$:

1. *Če velja ϕ:*
   Dokažemo ρ: ...
2. *Če velja $\neg\phi$.*
   Dokažemo ρ: ...

Dokaz s protislovjem poteka takole:

Dokažimo ρ. Dokazujemo s protislovjem:

Predpostavimo $\neg\rho$.
Poiščimo protislovje: ...

Opomba: dokaz s protislovjem in pravilo vpeljave za negacijo sta *različni* pravili!

Poglavje 5

Logika in pravila sklepanja (dodatno poglavje)

Opomba: To poglavje je del učbenika v nastajanju in ni povsem v skladu s predavanji. Kljub temu ga vključujem v te zapiske, ker vsebuje precej koristnih nasvetov in misli.

5.1 Kaj je matematični dokaz?

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

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

Izrek 5.1 *Za vsako naravno število n je $n^3 - n$ deljivo s 3.*

Po kratkem premisleku bi izkušeni matematik zapisal:

Dokaz. Očitno. ∎

To ni dokaz, izkušeni matematik nam le dopoveduje, da je (zanj) izrek zelo lahek in da nima smisla izgubljati časa s pisanjem dokaza. Začetnik, ki težko razume že sam izrek, bo

ob takem »dokazu« seveda zgrožen. Verjetno bo najprej preizkusil izrek na nekaj primerih:

$$\begin{aligned} 1^3 - 1 &= 0, \\ 2^3 - 2 &= 8 - 2 = 6, \\ 3^3 - 3 &= 27 - 4 = 24, \\ 4^3 - 4 &= 64 - 4 = 60. \end{aligned}$$

Res dobivamo večkratnike števila 3. Ali smo izrek s tem dokazali? Seveda ne! Preizkusili smo le štiri primere, ostane pa jih še neskončno mnogo. Kdor misli, da lahko iz nekaj primerov sklepa na splošno veljavnost, naj v poduk vzame naslednjo nalogo.

Naloga 5.2 Ali je $n^2 - n + 41$ praštevilo za vsako naravno število n?

Ko izkušenega matematika prosimo, da naj nam vsaj pojasni idejo dokaza, zapiše:

> *Dokaz.* Število $n^3 - n$ je zmnožek treh zaporednih naravnih števil. ∎

To še vedno ni dokaz, ampak samo namig. Starejši študenti matematike pa bi iz namiga morali znati sestaviti naslednji dokaz:

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

Mimogrede, znak ∎ označuje konec dokaza. Čeprav bi bila večina matematikov s tem dokazom zadovoljna, bi morali za popoln dokaz preveriti še nekaj podrobnosti:

1. Ali res velja $n^3 - n = (n-1) \cdot n \cdot (n+1)$?
2. Ali je res, da je izmed treh zaporednih naravnih števil eno vedno deljivo s 3?
3. Ali je res, da je zmnožek treh števil deljiv s 3, če je eno od števil deljivo s 3?

S srednješolskim znanjem algebre ugotovimo, da je odgovor na prvo vprašanje pritrdilen. Tudi odgovora na drugo in tretje vprašanje sta očitno pritrdilna, mar ne? To pa ne pomeni, da ju ni treba dokazati. Nasprotno, zgodovina matematike nas uči, da moramo prav »očitne« izjave še posebej skrbno preveriti.

Naloga 5.3 Kakšno je tvoje mnenje o resničnosti naslednjih izjav? Vprašaj starejše kolege, asistente in učitelje, kaj menijo oni. Ali znajo svoje mnenje utemeljiti z dokazi?

1. Sodih števil je manj kot naravnih števil.
2. Kroglo je mogoče razdeliti na pet delov tako, da lahko iz njih sestavimo dve krogli, ki sta enako veliki kot prvotna krogla.
3. Sklenjena krivulja v ravnini, ki ne seka same sebe, razdeli ravnino na dve območji, eno omejeno in eno neomejeno.
4. S krivuljo ne moremo prekriti notranjosti kvadrata.
5. Če ravnino razdelimo na tri območja, potem zagotovo obstaja točka, ki je dvomeja in ni tromeja med območji.

Vrnimo s k izreku 5.1. Če dokaz zapišemo preveč podrobno, postane dolgočasen in nerazumljiv:

Dokaz. Naj bo n poljubno naravno število. Tedaj velja

$$\begin{aligned} n^3 - n &= n \cdot n^2 - n \cdot 1 \\ &= n \cdot (n^2 - 1) \\ &= n \cdot ((n+1) \cdot (n-1)) \\ &= n \cdot ((n-1) \cdot (n+1)) \\ &= (n \cdot (n-1)) \cdot (n+1) \\ &= (n-1) \cdot n \cdot (n+1). \end{aligned}$$

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

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

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

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

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

Naloga 5.4 S kolegi se igraj naslednjo igro.[1] Prvi igralec v zgornjem dokazu poišče korak, ki ga je treba še dodatno utemeljiti. Drugi igralec ga utemelji. Nato drugi igralec poišče korak, ki ga mora utemeljiti prvi igralec. Nato se igra ponovi. Zgubi tisti, ki se prvi naveliča igrati. Ali lahko igra traja neskončno dolgo?

Matematični dokaz ima dvojno vlogo. Po eni strani je utemeljitev matematične izjave, zato mora biti čim bolj podroben. V idealnem primeru bi bil dokaz zapisan tako, da bi lahko njegovo pravilnost preverili mehansko, z računalnikom. Po drugi strani je dokaz sredstvo za komunikacijo idej med matematiki, zato mora vsebovati ravno pravo mero podrobnosti. Mera pa je odvisna od tega, komu je dokaz namenjen. Te socialne komponente se študenti učijo skozi prakso v toku študija. Dokazu kot povsem matematičnemu pojmu pa se bomo posvetili prav pri predmetu Logika in množice. Pojasnili bomo, kaj je dokaz kot matematični konstrukt in kako ga zapišemo tako podrobno, da je res mehansko

[1] Igranje odsvetujemo zunaj prostorov Fakultete za matematiko in fiziko.

preverljiv. Naučili se bomo tudi nekaj preprostih tehnik iskanja dokazov, ki pa še zdaleč ne bodo zadostovale za reševanje zares zanimivih matematičnih problemov, ki zahtevajo poglobljeno znanje, vztrajnost, kanček talenta in nekaj sreče.

5.2 Simbolni zapis matematičnih izjav

Matematična **izjava** je smiselno besedilo, ki izraža kako lastnost ali razmerje med matematičnimi objekti (števili, liki, funkcijami, množicami itn.). Primeri matematičnih izjav:

- $2 + 2 = 5$.
- Točke P, Q in R so kolinearne.
- Enačba $x^2 + 1 = 0$ nima realnih rešitev.
- $a > 5$.
- $\phi \vee \psi \Rightarrow (\neg\phi \Rightarrow \psi)$.

Vidimo, da je lahko izjava resnična, neresnična, ali pa je resničnost izjave *odvisna* od vrednosti spremenljivk, ki nastopajo v njej. Primeri besedila, ki niso matematične izjave:

- Ali je $2 + 2 = 5$?
- Za vsak $x > 5$.
- Študenti bi morali znati reševati diferencialne enačbe.
- Od nekdaj lepe so Ljubljanke slovele, al lepše od Urške bilo ni nobene.
- $\phi\vee)\psi \Rightarrow \psi$.

Matematične izjave običajno pišemo kombinirano v naravnem jeziku in z matematični simboli, saj so tako najlažje razumljive ljudem. Za potrebe matematične logike pa izjave pišemo *samo* z matematičnimi simboli. Tako zapisani izjavi pravimo **logična formula**. V ta namen moramo nadomestiti osnovne gradnike izjav, kot so »in«, »ali« in »za vsak«, z **logičnimi operacijami**. Le-te delimo na tri sklope. V prvi sklop sodita **logični konstanti**:

- resnica $\top$,
- neresnica $\bot$.

V računalništvu resnico $\top$ pogosto označimo z 1 ali `True` in neresnico $\bot$ z 0 ali `False`. Naslednji sklop so **logični vezniki**, s katerimi sestavljamo nove izjave iz že danih:

- konjunkcija $\phi \wedge \psi$, beremo »ϕ in ψ«,
- disjunkcija $\phi \vee \psi$, beremo »ϕ ali ψ«,
- implikacija $\phi \Rightarrow \psi$, beremo »če ϕ potem ψ«,
- ekvivalenca $\phi \Leftrightarrow \psi$, beremo »$\phi$ če, in samo če, ψ« ali pa »ϕ natanko tedaj, kadar ψ«,
- negacija $\neg\phi$, beremo »ne ϕ«,

V tretji sklop sodita **logična kvantifikatorja**:

- univerzalni kvantifikator $\forall x \in S\,.\,\phi$, beremo »za vse x iz S velja ϕ«,
- eksistenčni kvantifikator $\exists x \in S\,.\,\phi$, beremo »obstaja x v S, da velja ϕ«,

Pri tem je S množica, razred[2] ali tip spremenljivke x. V praksi se uporablja več inačic zapisa za kvantifikatorje, kot so »$\forall x : S.\,\phi$«, »$\forall x \in S : \phi$« in »$(\forall x \in S)\phi$«. Srečamo tudi zapis »$\phi, \forall x \in S$«, ki pa ga odsvetujemo.

Neomejena kvantifikatorja $\forall x\,.\,\phi$ in $\exists x\,.\,\phi$ se uporabljata, kadar je vnaprej znana množica S, po kateri teče spremenljivka x. V matematičnem besedilu je običajno razvidna iz spremnega besedila, včasih pa je treba upoštevati ustaljene navade: n je naravno ali celo število, x realno, f je funkcija ipd.

[2]Kasneje bomo spoznali razliko med množicami in razredi, zaenkrat si S predstavljamo kot množico.

V uporabi so nekatere ustaljene okrajšave:

$\exists x, y \in S \,.\, \phi,$	pomeni	$\exists x \,.\, S(\exists y \,.\, S\phi),$
$\forall x \in S, y \in T \,.\, \phi,$	pomeni	$\forall x \in S \,.\, (\forall y \in T \,.\, \phi),$
$\phi \Leftrightarrow \psi \Leftrightarrow \rho \Leftrightarrow \sigma$	pomeni	$(\phi \Leftrightarrow \psi) \wedge (\psi \Leftrightarrow \rho) \wedge (\rho \Leftrightarrow \sigma),$
$f(x) = g(x) = h(x) = i(x)$	pomeni	$f(x) = g(x) \wedge g(x) = h(x) \wedge h(x) = i(x),$
$a \leq b < c \leq d$	pomeni	$a \leq b \wedge b < c \wedge c \leq d.$

Nekatere okrajšave odsvetujemo. V nizu neenakosti naj gredo vse primerjave v isto smer. Torej ne pišemo $a \leq b < c \geq d$, ker se zlahka zmotimo in mislimo, da velja $a \geq d$. To bi morali zapisati ločeno kot $a \leq b < c$ in $c \geq d$. Prav tako ne nizamo neenakosti, saj premnogi iz $f(x) \neq g(x) \neq h(x)$ »sklepajo« $f(x) \neq h(x)$, čeprav neenakost *ni* tranzitivna relacija. Zapis $f(x) = g(x) \neq h(x) = i(x)$ je v redu, saj ena sama neenakost ne povzroči težav.

Naloga 5.5 Zapiši $f(x) = g(x) \neq h(x) = i(x)$ brez okrajšav.

Povejmo še nekaj o pisanju oklepajev. Oklepaji povedo, katera operacija ima prednost. Kadar manjkajo, moramo poznati dogovorjeno **prioriteto** operacij. Na primer, ker ima množenje višjo prioriteto kot seštevanje, je $5 \cdot 3 + 8$ enako $(5 \cdot 3) + 8$ in ne $5 \cdot (3 + 8)$. Tudi logične operacije imajo svoje prioritete, ki pa niso tako splošno znane kot prioritete aritmetičnih operacij. Zato bodite pazljivi, ko berete tuje besedilo.

Mi bomo privzeli naslednje prioritete logičnih operacij:

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

Na primer:

- $\neg\phi \vee \psi$ je isto kot $(\neg\phi) \vee \psi$,
- $\neg\neg\phi \Rightarrow \phi$ je isto kot $(\neg(\neg\phi)) \Rightarrow \phi$,
- $\phi \vee \psi \wedge \rho$ je isto kot $\phi \vee (\psi \wedge \rho)$,
- $\phi \wedge \psi \Rightarrow \phi \vee \psi$ je isto kot $(\phi \wedge \psi) \Rightarrow (\phi \vee \psi)$,
- $\forall x \in S \,.\, \phi \Rightarrow \psi$ je isto kot $\forall x \in S \,.\, (\phi \Rightarrow \psi)$,
- $\exists x \in S \,.\, \phi \wedge \psi$ je isto kot $\exists x \in S \,.\, (\phi \wedge \psi)$.

V aritmetiki poznamo poleg prioritete operacij tudi **levo** in **desno asociiranost**. Denimo, seštevanje je levo asociirano, ker beremo $5 + 3 + 7$ kot $(5 + 3) + 7$, saj najprej izračunamo $5 + 3$ in nato $8 + 7$. Pri seštevanju to sicer ni pomembno in bi lahko seštevali tudi $3 + 7$ in nato $5 + 10$. Drugače je z odštevanjem, kjer $5 - 3 - 7$ pomeni $(5 - 3) - 7$ in ne $5 - (3 - 7)$. Tudi za logične operacije velja dogovor o njihovi asociiranosti. Konjunkcija in disjunkcija sta levo asociirani:

$\phi \wedge \psi \wedge \rho$	pomeni	$(\phi \wedge \psi) \wedge \rho,$
$\phi \vee \psi \vee \rho$	pomeni	$(\phi \vee \psi) \vee \rho.$

Za disjunkcijo in konjunkcijo sicer ni pomembno, kako postavimo oklepaje, ker sta obe možnosti med seboj ekvivalentni, vendar je prav, da natančno določimo, katera od njiju

je mišljena. V logiki je implikacija desno asociirana:

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

Tu *ni* vseeno, kako postavimo oklepaje, saj $\phi \Rightarrow (\psi \Rightarrow \rho)$ in $(\phi \Rightarrow \psi) \Rightarrow \rho$ v splošnem nista ekvivalentna. Vendar pozor! Ko matematiki, ki niso logiki, v matematičnem besedilu zapišejo

$$\phi \Rightarrow \psi \Rightarrow \rho,$$

s tem skoraj vedno mislijo

$$(\phi \Rightarrow \psi) \wedge (\psi \Rightarrow \rho).$$

Zakaj? Zato ker je to priročen zapis, ki nakazuje zaporedje sklepov »iz ϕ sledi ψ in nato iz ψ sledi ρ«, še posebej, če je zapisan v več vrsticah. Recimo, za nenegativni števili x in y bi takole zapisali utemeljitev neenakosti med aritmetično in geometrijsko sredino:

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

Matematiki radi celo spustijo znak $\Rightarrow$ in preprosto vsak naslednji sklep napišejo v svojo vrstico. Ker torej velja tak ustaljen način pisanja zaporedja sklepov, je varneje pisati $\phi \Rightarrow (\psi \Rightarrow \rho)$ brez oklepajev, da ne povzročamo zmede.

5.3 Kako beremo in pišemo simbolni zapis

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

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

preberemo:

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

Več izkušenj pa je potrebnih, da *razumemo* matematični pomen take izjave, v tem primeru:

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

Začetnik potrebuje nekaj vaje, da se navadi brati simbolni zapis. Tudi prevod v obratno smer, iz besedila v simbolno obliko, ni enostaven, zato povejmo, kako se prevede nekatere standardne fraze.

»ϕ je zadosten pogoj za ψ.«

To pomeni, da zadošča dokazati ϕ zato, da dokažemo ψ, ali v simbolni obliki

$$\phi \Rightarrow \psi.$$

»ϕ je potreben pogoj za ψ.«

To pomeni, da ψ ne more veljati, ne da bi veljal ϕ. Z drugimi besedami, če velja ψ, potem velja tudi ϕ, kar se v simbolni obliki zapiše

$$\psi \Rightarrow \phi.$$

»ϕ je zadosten in potreben pogoj za ψ.«

To je kombinacija prejšnjih dveh primerov, ki trdi, da iz ϕ sledi ψ in iz ψ sledi ϕ, kar pa je ekvivalenca:

$$\phi \Leftrightarrow \psi.$$

Naloga 5.6 Je »n je sod in $n > 2$« **potreben** ali **zadosten** pogoj za »n ni praštevilo«?

»Naslednje izjave so ekvivalentne: ϕ, ψ, ρ in σ.«

To pomeni, da sta vsaki dve izmed danih izjav ekvivalentni, se pravi

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

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

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

To pišemo krajše kar kot

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

čeprav je formalno gledano tako zapis nepravilen. V razdelku 5.6.5 bomo spoznali, kako se tako zaporedje ekvivalenc dokaže s ciklom implikacij $\phi \Rightarrow \psi \Rightarrow \rho \Rightarrow \sigma \Rightarrow \phi$.

Naloga 5.7 Podaj konkretne primere izjav ϕ, ψ in ρ, iz katerih je razvidno, da izjava $(\phi \Leftrightarrow \psi) \wedge (\psi \Leftrightarrow \rho)$ *ni* ekvivalentna niti $(\phi \Leftrightarrow \psi) \Leftrightarrow \rho$ niti $\phi \Leftrightarrow (\psi \Leftrightarrow \rho)$.

»Za vsak x iz S, za katerega velja ϕ, velja tudi ψ.«

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

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

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

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

Naloga 5.8 V simbolni obliki zapiši »n je lih« in »n je praštevilo«. Namig: n je lih, kadar obstaja naravno število k, za katerega velja $n = 2k + 1$, in n je praštevilo, kadar *ni* zmnožek dveh naravnih števil, ki sta obe večji od 1.

»Enačba $f(x) = g(x)$ nima realne rešitve.«

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

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

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

Naloga 5.9 Zapiši v simbolni obliki: »Sistem enačb

$$a_1x + b_1y = c_1,$$
$$a_2x + b_2y = c_2$$

nima pozitivnih realnih rešitev x, y.«

Naloga 5.10 Zapiši v simbolni obliki:

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

»Brez izgube za splošnost.«

V matematičnih besedilih najdemo frazo »brez izgube za splošnost« kot v naslednjem primeru.

Izrek 5.11 *Za vsa cela števila a, b in c je $|a - b| + |b - c| + |c - a|$ sodo število.*

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

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

kar je sodo število. ∎

Fraza »brez izgube za splošnost« nakazuje, da dokaz obravnava le eno od večih možnosti. Načeloma bi morali obravnavati tudi ostale možnosti, ki pa jih je pisec dokaza opustil, ker so bodisi zelo lahke bodisi zelo podobne tisti, ki jo dokaz obravnava. Za začetnika je najtežje dognati, katere so preostale možnosti in zakaj se je pisec dokaza pravzaprav odločil zanje. Avtor zgornjega dokaza je verjetno opazil, da števila a, b in c v izrazu $|a - b| + |b - c| + |c - a|$ nastopajo *simetrično*: če jih premešamo, se izraz ne spremeni. Denimo, ko zamenjamo a in b, dobimo $|b - a| + |a - c| + |c - b|$, kar je enako prvotnemu izrazu $|a - b| + |b - c| + |c - a|$. Torej lahko izmed šestih možnosti

$$a \geq b \geq c, \qquad a \geq c \geq b, \qquad b \geq a \geq c,$$
$$b \geq c \geq a, \qquad c \geq a \geq b, \qquad c \geq b \geq a$$

obravnavamo le eno. Seveda pisanje dokazov, pri katerih večji del dokaza opustimo, zahteva pazljivost in nekaj izkušenj.

Naloga 5.12 Dokaži izrek 5.11 tako, da obravnavaš samo možnost $b \geq c \geq a$ in zraven dopišeš »brez izgube za splošnost«.

5.4 Definicije

Poznamo tri vrste definicij. Prva in najpreprostejša je definicija, ki služi kot **okrajšava** za daljši izraz. To smemo vedno nadomestiti s prvotnim izrazom. Na primer, funkcija »hiperbolični tangens« $\tanh(x)$ je definirana kot

$$\tanh(x) = \frac{e^{2x} - 1}{e^{2x} + 1}.$$

Lahko bi shajali tudi brez zapisa $\tanh(x)$, vendar bi morali potem povsod pisati daljši izraz $\frac{e^{2x}-1}{e^{2x}+1}$, kar bi bilo nepregledno.

Druga vrsta definicije je vpeljava novega matematičnega pojma. Študenti prvega letnika matematike spoznajo celo vrsto novih pojmov (grupa, vektorski prostor, limita, stekališče, metrika itn.), s katerimi si razširijo sposobnost matematičnega razmišljanja. Matematiki cenijo dobre definicije in vpeljavo novih matematičnih pojmov vsaj toliko, kot dokaze težkih izrekov.

Tretja vrsta definicije je **konstrukcija** matematičnega objekta s pomočjo dokaza o enoličnem obstoju. O tem bomo povedali več v razdelku 5.7.4.

5.5 Pravila sklepanja in dokazi

Povedali smo že, da je dokaz utemeljitev neke matematične izjave. V razdelku 5.1 smo govorili o tem, da so dokazi mešanica besedila in simbolov, ki jih matematiki uporabljajo tako za utemeljitev matematičnih izjav, kakor tudi za razlago in podajanje matematičnih idej. V tem razdelku se posvetimo **formalnim dokazom**, ki so logične konstrukcije namenjene mehanskemu preverjanju pravilnosti izjav.

Za vsako logično operacijo bomo podali **formalna pravila sklepanja**, ki jih smemo uporabljati v formalnem dokazu. Pravilo sklepanja shematsko zapišemo

$$\frac{\phi \qquad \psi \qquad \rho}{\sigma}$$

in ga preberemo: »Če smo dokazali ϕ, ψ in ρ, smemo sklepati σ.« Izjavam nad črto pravimo **hipoteze**, izjavi pod črto pa **sklep**. Hipotez je lahko nič ali več, sklep mora biti natanko en. Pravilo sklepanja brez hipotez se imenuje **aksiom**.

Da bomo lahko pojasnili, kaj je dokaz, podajmo pravila sklepanja za $\top$ in $\wedge$, ki jih bomo v naslednjem razdelku še enkrat bolj pozorno obravnavali:

$$\frac{}{\top} \qquad \frac{\phi \qquad \psi}{\phi \wedge \psi} \qquad \frac{\phi \wedge \psi}{\phi} \qquad \frac{\phi \wedge \psi}{\psi}$$

Po vrsti beremo:

- Velja $\top$.
- Če velja ϕ in ψ, smemo sklepati $\phi \wedge \psi$.
- Če velja $\phi \wedge \psi$, smemo sklepati ϕ.
- Če velja $\phi \wedge \psi$, smemo sklepati ψ.

Formalni dokaz ima drevesno obliko in prikazuje, kako iz danih **hipotez** dokažemo neko **sodbo**. Pri dnu je zapisana izjava, ki jo dokazujemo, nad njo pa dokaz. Vsako vejišče je eno od pravil sklepanja. Vsaka veja se mora zaključiti z aksiomom ali s hipotezo. Oglejmo si dokaz izjave $(\alpha \wedge \alpha) \wedge (\top \wedge \beta)$ iz hipoteze $\beta \wedge \alpha$:

$$\dfrac{\dfrac{\dfrac{\beta \wedge \alpha}{\alpha} \quad \dfrac{\beta \wedge \alpha}{\alpha}}{\alpha \wedge \alpha} \qquad \dfrac{\dfrac{}{\top} \quad \dfrac{\beta \wedge \alpha}{\beta}}{\top \wedge \beta}}{(\alpha \wedge \alpha) \wedge (\top \wedge \beta)}$$

Dokaz se razveji na dve veji, vsaka od njiju pa še na dve veji. Tako pri vrhu dobimo štiri liste, od katerih so trije izjava $\beta \wedge \alpha$ in en aksiom za $\top$.

Naloga 5.13 Preveri, da je vsako vejišče v zgornjem dokazu res uporaba enega od zgoraj podanih pravil sklepanja.

V praksi matematično besedilo bolj ali manj odraža strukturo formalnega dokaza, le da se besedilo ne veji, ampak so sestavni kosi dokaza zloženi v zaporedje. Formalni dokazi so uporabni, kadar želimo preveriti veljavnost najbolj osnovnih logičnih dejstev. Ni mišljeno, da bi matematiki pisali ali preverjali velike formalne dokaze pomembnih matematičnih izrekov, to je delo za računalnike. Formalna pravila sklepanja in formalni dokazi so za matematike pomembni, ker nam omogočajo, da natančno in v celoti povemo, kakšna so »pravila igre« v matematiki.

5.6 Izjavni račun

Izjavni račun je tisti del logike, ki govori o logičnih konstantah $\bot$, $\top$ in o logičnih operacijah $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\neg$. Za vsako od njih podamo formalna pravila sklepanja, ki so dveh vrst. Pravila **vpeljave** povedo, kako se izjave dokaže, pravila **uporabe** pa povedo, kako se že dokazane izjave uporabi.

5.6.1 Konjunkcija

Konjunkcija ima eno pravilo vpeljave in dve pravili uporabe:

$$\dfrac{\phi \qquad \psi}{\phi \wedge \psi} \qquad\qquad \dfrac{\phi \wedge \psi}{\phi} \qquad\qquad \dfrac{\phi \wedge \psi}{\psi}$$

Pravilo vpeljave pove, da konjunkcijo $\phi \wedge \psi$ dokažemo tako, da dokažemo posebej ϕ in posebej ψ. Pravili uporabe pa povesta, da lahko $\phi \wedge \psi$ »razstavimo« na izjavi ϕ in ψ.

V matematičnem besedilu je dokaz konjunkcije $\phi \wedge \psi$ zapisan kot zaporedje dveh podkazov:

Dokazujemo $\phi \wedge \psi$:

1. *(Dokaz ϕ)*
2. *(Dokaz ψ)*

Dokazali smo $\phi \wedge \psi$.

Manj podroben dokaz ne vsebuje začetnega in končnega stavka, ampak samo dokaza za ϕ in ψ. Bralec mora sam ugotoviti, da je s tem dokazana izjava $\phi \wedge \psi$.

5.6.2 Implikacija

Preden zapišemo pravila sklepanja za implikacijo, si oglejmo primer neformalnega dokaza.

Izrek 5.14 *Če je $x > 2$, potem je $x^3 + x + 7 > 16$.*

Dokaz. Predpostavimo, da velja $x > 2$. Tedaj je $x^3 > 2^3 = 8$, zato velja

$$x^3 + x + 7 > 8 + 2 + 7 = 17 > 16.$$

Dokazali smo $x > 2 \Rightarrow x^3 + x + 7 > 16$. ∎

Prvi stavek dokaza z besedico »predpostavimo« uvede **začasno hipotezo** $x > 2$, iz katere nato izpeljemo posledico $x^3 + x + 7 > 16$. Implikacijo $\phi \Rightarrow \psi$ torej dokažemo tako, da začasno predpostavimo ϕ in dokažemo ψ. Tako pravilo vpeljave zapišemo

$$\frac{\begin{array}{c}[\phi]\\ \vdots \\ \psi\end{array}}{\phi \Rightarrow \psi}$$

Zapis $[\phi]$ z oglatimi oklepaji pomeni, da ϕ ni prava, ampak samo začasna hipoteza. Zapis

$$\begin{array}{c}[\phi]\\ \vdots \\ \psi\end{array}$$

pomeni »dokaz izjave ψ s pomočjo začasne hipoteze ϕ.«

Pravilo uporabe za implikacijo se imenuje **modus ponens** in se glasi

$$\frac{\phi \Rightarrow \psi \qquad \phi}{\psi}$$

V matematičnem besedilu se modus ponens pojavi kot uporaba že prej dokazanega izreka izreka oblike $\phi \Rightarrow \psi$.

5.6.3 Disjunkcija

Disjunkcija ima dve pravili vpeljave in eno pravilo uporabe:

$$\frac{\phi}{\phi \vee \psi} \qquad \frac{\psi}{\phi \vee \psi} \qquad \frac{\phi \vee \psi \qquad \begin{array}{c}[\phi]\\ \vdots \\ \rho\end{array} \qquad \begin{array}{c}[\psi]\\ \vdots \\ \rho\end{array}}{\rho}$$

Pravili sklepanja povesta, da lahko dokažemo disjunkcijo $\phi \vee \psi$ tako, da dokažemo enega od disjunktov.

Pojasnimo še pravilo uporabe. Denimo, da bi radi dokazali ρ, pri čemer že vemo, da velja $\phi \vee \psi$. Pravilo uporabe pravi, da je treba obravnavati dva primera: iz začasne hipoteze ϕ je treba dokazati ρ in iz začasne hipoteze ψ je treba dokazati ρ.

Ponazorimo pravilo uporabe v dokazu izjave $(\alpha \vee \gamma) \wedge (\beta \vee \gamma)$ iz hipoteze $(\alpha \wedge \beta) \vee \gamma$. Dokazno drevo je precej veliko, v njem pa se dvakrat pojavi uporaba disjunkcije:

$$\dfrac{\dfrac{(\alpha \wedge \beta) \vee \gamma \qquad \dfrac{\dfrac{[\alpha \wedge \beta]}{\alpha}}{\alpha \vee \gamma} \qquad \dfrac{[\gamma]}{\alpha \vee \gamma}}{\alpha \vee \gamma} \qquad \dfrac{(\alpha \wedge \beta) \vee \gamma \qquad \dfrac{\dfrac{[\alpha \wedge \beta]}{\beta}}{\beta \vee \gamma} \qquad \dfrac{[\gamma]}{\beta \vee \gamma}}{\beta \vee \gamma}}{(\alpha \vee \gamma) \wedge (\beta \vee \gamma)}$$

Poglejmo na primer levo vejo tega dokaza, desna je podobna:

$$\dfrac{(\alpha \wedge \beta) \vee \gamma \qquad \dfrac{\dfrac{[\alpha \wedge \beta]}{\alpha}}{\alpha \vee \gamma} \qquad \dfrac{[\gamma]}{\alpha \vee \gamma}}{\alpha \vee \gamma}$$

Res je to uporaba disjunkcije $\phi \vee \psi$, kjer smo vzeli $\phi = \alpha \wedge \beta$ in $\psi = \gamma$, dokazali pa smo izjavo $\rho = \alpha \vee \gamma$.

Naloga 5.15 Iz hipoteze $(\alpha \vee \gamma) \wedge (\beta \vee \gamma)$ dokaži $(\alpha \wedge \beta) \vee \gamma$.

V besedilu dokažemo disjunkcijo s pravilom za vpeljavo takole:

Dokazujemo $\phi \vee \psi$. Zadostuje dokazati ϕ:

(Dokaz ϕ.)

Dokazali smo $\phi \vee \psi$.

Pravilo uporabe disjunkcije se v besedilu zapiše kot obravnava primerov:

Dokazujemo ρ. To bomo dokazali z obravnavo primerov ϕ in ψ:

1. *(Dokaz $\phi \vee \rho$)*
2. *Predpostavimo, da velja ϕ. (Dokaz ρ)*
3. *Predpostavimo, da velja ψ. (Dokaz ρ)*

Dokazali smo ρ.

Še primer konkretnega dokaza, ki je tako napisan.

Izrek 5.16 *Naj bo x realno število. Če je $|x-3| > 5$, potem je $x^4 > 15$.*

Dokaz. Dokazujemo $|x-3| > 5 \Rightarrow x^4 > 15$. Predostavimo $|x-3| > 5$ in dokažimo $x^4 > 15$. To bomo dokazali z obravavo primerov $x \leq 3$ in $x \geq 3$:

1. $x \leq 3 \vee x \geq 3$ velja, ker so realna števila linearno urejena z relacijo $\leq$.
2. Predpostavimo $x \leq 3$. Tedaj je $x - 3 \leq 0$ in zato $|x-3| = 3 - x$, od koder sledi $3 - x = |x-3| > 5$, oziroma $x < -2$. Tako dobimo
$$x^4 > (-2)^4 = 16 > 15.$$
3. Predpostavimo $x \geq 3$. Tedaj je $x - 3 \geq 0$ in zato $|x-3| = x - 3$, od koder sledi $x - 3 = |x-3| > 5$, oziroma $x > 8$. Tako dobimo
$$x^4 > 8^4 = 4096 > 15.$$

Iz predpostavke $|x-3| > 5$ smo izpeljali $x^4 > 15$. S tem smo dokazali $|x-3| > 5 \Rightarrow x^4 > 15$. ∎

Težji del tega dokaza se skriva v izbiri disjunkcije. Kako je pisec uganil, da je treba obravnavati primera $x \leq 3$ in $x \geq 3$? Zakaj ni raje obravnaval $x < 3$ in $x \geq 3$, ali morda $x \leq 17$ in $x \geq 17$? Odgovor se skriva v definiciji absolutne vrednosti:

$$|a| = \begin{cases} a & \text{če je } a \geq 0, \\ -a & \text{če je } a \leq 0. \end{cases}$$

Ker v izreku nastopa izraz $|x-3|$, bo obravnava primerov $x-3 \geq 0$ in $x-3 \leq 0$ omogočila, da $|x-3|$ poenostavimo enkrat v $x-3$ in drugič v $3-x$. Seveda pa je $x-3 \geq 0$ ekvivalentno $x \geq 3$ in $x - 3 \leq 0$ ekvivalentno $x \leq 3$.

Naloga 5.17 Ali bi lahko izrek 5.16 dokazali tudi z obravnavo primerov $x < 3$ in $x \geq 3$?

5.6.4 Resnica in neresnica

Logična konstanta $\top$ označuje resnico. Kar je res, je res, in tega ni treba posebej dokazovati. To dejstvo izraža aksiom

$$\frac{}{\top}$$

Logična konstanta $\top$ nima pravila uporabe, ker iz $\top$ ne moremo sklepati nič koristnega.

Logična konstanta $\bot$ označuje neresnico. Ker se tega, kar ni res, ne more dokazati, $\bot$ nima pravila vpeljave. Pravilo uporabe je

$$\frac{\bot}{\phi}$$

se imenuje **ex falso (sequitur) quodlibet**, kar pomeni »iz neresnice sledi karkoli«.

V matematičnem besedilu se $\top$ in $\bot$ ne pojavljata pogosto, ker matematiki izraze, v katerih se $\top$ in $\bot$ pojavita, vedno poenostavijo s pomočjo ekvivalenc:

$$\top \wedge \phi \Leftrightarrow \phi \qquad \top \vee \phi \Leftrightarrow \top \qquad \bot \wedge \phi \Leftrightarrow \bot \qquad \bot \vee \phi \Leftrightarrow \phi$$

$$(\top \Rightarrow \phi) \Leftrightarrow \phi \qquad (\bot \Rightarrow \phi) \Leftrightarrow \top \qquad (\phi \Rightarrow \top) \Leftrightarrow \top$$

5.6.5 Ekvivalenca

Logična ekvivalenca $\phi \Leftrightarrow \psi$ je okrajšava za

$$(\phi \Rightarrow \psi) \wedge (\psi \Rightarrow \phi).$$

Ker je to konjunkcija (dveh implikacij), so pravila za vpeljavo in uporabo ekvivalence samo poseben primer pravil sklepanja za konjunkcijo:

$$\frac{\phi \Rightarrow \psi \qquad \psi \Rightarrow \phi}{\phi \Leftrightarrow \psi} \qquad \frac{\phi \Leftrightarrow \psi}{\phi \Rightarrow \psi} \qquad \frac{\phi \Leftrightarrow \psi}{\psi \Rightarrow \phi}$$

V matematičnem besedilu ekvivalenco dokažemo takole:

Dokazujemo $\phi \Leftrightarrow \psi$:

1. *(Dokaz $\phi \Rightarrow \psi$)*
2. *(Dokaz $\psi \Rightarrow \phi$)*

Dokazali smo $\phi \Leftrightarrow \psi$.

Če sta izjavi ϕ in ψ logično ekvivalentni, lahko eno zamenjamo z drugo. To matematiki s pridom uporabljajo pri dokazovanju izjav, čeprav pogosto sploh ne omenijo, katero ekvivalenco so uporabili.

Kadar dokazujemo medsebojno ekvivalenco večih izjav ϕ_1, ϕ_2, …, ϕ_n, zadostuje dokazati cikel implikacij

$$\phi_1 \Rightarrow \phi_2 \Rightarrow \cdots \Rightarrow \phi_{n-1} \Rightarrow \phi_n \Rightarrow \phi_1.$$

(Ne spreglejte zadnje implikacije $\phi_n \Rightarrow \phi_1$, ki zaključi cikel). V besedilu to dokažemo:

Dokazujemo, da so izjave $\phi_1, \phi_2, \ldots, \phi_n$ ekvivalentne:

1. *(Dokaz $\phi_1 \Rightarrow \phi_2$)*
2. *(Dokaz $\phi_2 \Rightarrow \phi_3$)*
3. *…*
4. *(Dokaz $\phi_{n-1} \Rightarrow \phi_n$)*
5. *(Dokaz $\phi_n \Rightarrow \phi_1$)*

Seveda smemo pred samim dokazovanjem izjave $\phi_1, \ldots, \phi_n$ preurediti tako, da je zahtevane implikacije kar najlažje dokazati. Dokaz lahko tudi razdelimo na dva ločena cikla implikacij

$$\phi_1 \Rightarrow \cdots \Rightarrow \phi_k \Rightarrow \phi_1$$

in

$$\phi_{k+1} \Rightarrow \cdots \Rightarrow \phi_n \Rightarrow \phi_{k+1}$$

in nato dokažemo še eno ekvivalenco $\phi_i \Leftrightarrow \phi_j$, pri čemer je ϕ_i iz prvega in ϕ_j iz drugega cikla.

5.6.6 Negacija

Negacija $\neg\phi$ je definirana kot okrajšava za $\phi \Rightarrow \bot$. Iz pravil sklepanja za $\Rightarrow$ in $\bot$ tako izpeljemo pravili sklepanja za negacijo:

$$\dfrac{\begin{array}{c}[\phi]\\ \vdots \\ \bot\end{array}}{\neg\phi} \qquad\qquad \dfrac{\neg\phi \qquad \phi}{\psi}$$

V besedilu dokazujemo $\neg\phi$ takole:

Dokazujemo $\neg\phi$.

> *Predpostavimo ϕ.*
> *(Dokaz $\bot$.)*

Dokazali smo $\neg\phi$.

Tu »Dokaz $\bot$« pomeni, da iz danih predpostavk izpeljemo protislovje. Mnogi matematiki menijo, da se takemu dokazu reče »dokaz s protislovjem«, vendar to ni res. To je samo navaden dokaz negacije. Dokazovanje s protislovjem bomo obravnavali v razdelku 5.6.7.

Pravilo uporabe za $\neg\phi$ v besedilu ni eksplicitno vidno, ampak ga matematiki uporabijo, ko sredi dokaza, da velja ψ, izpeljejo protislovje:

Dokazujemo ψ.

(Dokaz ϕ.)
(Dokaz $\neg\phi$.)

To je nesmisel, in ker iz nesmisla sledi karkoli, sledi ψ.

5.6.7 Aksiom o izključenem tretjem

Aksiom o izključenem tretjem se glasi

$$\frac{}{\phi \vee \neg\phi}$$

Povedano z besedami, vsaka izjava je bodisi resnična bodisi neresnična. Torej ni »tretje možnosti« za resničnostno vrednost izjave ϕ, od koder izhaja tudi ime aksioma.

Aksiom o izključenem tretjem omogoča *posredne* dokaze izjav, od katerih je najbolj znano **dokazovanje s protislovjem**: pri tem ne utemeljimo izjave ϕ, ampak utemeljimo, zakaj $\neg\phi$ *ne* velja. Natančneje povedano, izjavo ϕ zamenjamo z njej ekvivalentno izjavo $\neg\neg\phi$ in dokažemo $\neg\neg\phi$. Dokaz ekvivalence $\phi \Leftrightarrow \neg\neg\phi$ sestoji iz dokazov dveh implikacij:

$$\dfrac{\dfrac{\dfrac{[\neg\phi] \qquad [\phi]}{\bot}}{\neg\neg\phi}}{\phi \Rightarrow \neg\neg\phi} \qquad\qquad \dfrac{\dfrac{\dfrac{}{\phi \vee \neg\phi} \qquad [\phi] \qquad \dfrac{\dfrac{[\neg\neg\phi] \qquad [\neg\phi]}{\bot}}{\phi}}{\phi}}{\neg\neg\phi \Rightarrow \phi}$$

V dokazu $\neg\neg\phi \Rightarrow \phi$ smo uporabili aksiom o izključenem tretjem. V matematičnem besedilu se dokaz s protislovjem glasi:

Dokažimo ϕ s protislovjem.

Predpostavimo, da bi veljalo $\neg\phi$.
(Dokaz neresnice $\bot$.)

Ker torej $\neg\phi$ pripelje do protislovja, velja ϕ.

Praviloma izvemo o vsebini matematične izjave ϕ več, če jo dokažemo neposredno. Dokazovanja s protislovjem zato ni smiselno uporabljati vsepovprek, ampak le takrat, ko je zares potreben ali ko nam zelo olajša dokazovanje.

Ostali načini za sestavljanje posrednih dokazov slonijo na ekvivalencah

$$(\phi \vee \psi) \Leftrightarrow \neg(\neg\phi \wedge \neg\psi), \qquad (\phi \vee \psi) \Leftrightarrow (\neg\phi \Rightarrow \psi), \qquad (\phi \Rightarrow \psi) \Leftrightarrow (\neg\psi \Rightarrow \neg\phi),$$

$$(\forall x \in S \,.\, \phi) \Leftrightarrow \neg\exists x \in S \,.\, \neg\phi, \qquad (\exists x \in S \,.\, \phi) \Leftrightarrow \neg\forall x \in S \,.\, \neg\phi.$$

V vseh petih primerih implikacija $\Rightarrow$ iz leve na desno velja brez uporabe aksioma o izključenem tretjem. Za dokaz implikacij $\Leftarrow$ iz desne na levo pa potrebujemo aksiom o izključenem tretjem.

Naloga 5.18 Sestavi formalne dokaze za zgornjih pet ekvivalenc. Pri dokazovanju ekvivalenc za $\forall$ in $\exists$ si pomagaj s pravili sklepanja iz razdelkov 5.7.3 in 5.7.4.

Povejmo, kako zgornje ekvivalence uporabimo v besedilu za posredni dokaz izjave:

- $(\phi \vee \psi) \Leftrightarrow \neg(\neg\phi \wedge \neg\psi)$ uporabimo takole:

  Dokazujemo $\phi \vee \psi$.

  > *Predpostavimo, da velja $\neg\phi$ in $\neg\psi$.*
  > *(Dokaz neresnice $\bot$.)*

  Ker torej nista ϕ in ψ oba neresnična, je eden od njiju resničen. Dokazali smo $\phi \vee \psi$.

- $(\phi \vee \psi) \Leftrightarrow (\neg\phi \Rightarrow \psi)$ uporabimo takole:

  Dokazujemo $\phi \vee \psi$.

  > *Predpostavimo $\neg\phi$.*
  > *(Dokaz ψ.)*

  Če torej ne velja $\neg\phi$, velja ψ. Torej velja vsaj eden, zato smo dokazali $\phi \vee \psi$.

- $(\phi \Rightarrow \psi) \Leftrightarrow (\neg\psi \Rightarrow \neg\phi)$ uporabimo takole:

  Dokazujemo $\phi \Rightarrow \psi$.

  1. *Predpostavimo $\neg\psi$.*
  2. *(Dokaz $\neg\psi$.)*

  Dokazali smo, da iz ϕ sledi ψ.

- $(\forall x \in S\,.\,\phi) \Leftrightarrow \neg\exists x \in S\,.\,\neg\phi$ uporabimo takole:

  Dokazujemo, da za vsak $x \in S$ velja ϕ.

  1. *Predpostavimo, da obstaja $x \in S$, za katerega ϕ* ne *velja.*
  2. *(Dokaz neresnice $\bot$.)*

  Predpostavka, da obstaja $x \in S$, za katerega ϕ ne velja, pripelje do protislovja. Torej za vsak $x \in S$ velja ϕ.

- $(\exists x \in S\,.\,\phi) \Leftrightarrow \neg\forall x \in S\,.\,\neg\phi$ uporabimo takole:

  Dokazujemo, da obstaja tak $x \in S$, za katerega velja ϕ.

  1. *Predpostavimo, da bi veljalo $\neg\phi$ za vse $x \in S$.*
  2. *(Dokaz neresnice $\bot$.)*

  Predpostavka, da velja $\neg\phi$ za vse $x \in S$, pripelje do protislovja. Torej obstaja $x \in S$, za katerega velja ϕ.

Negacijo poljubne izjave ϕ tvorimo preprosto tako, da pred njo postavimo $\neg$. Vendar nam to ne pove dosti o matematični vsebini negirane izjave. V večini primerov je negacijo lažje razumeti, če simbol $\neg$ »porinemo« navznoter do osnovnih izjav z uporabo naslednjih

ekvivalenc:

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

Primer 5.19 Denimo, da bi radi ovrgli izjavo

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

Da izjavo ovržemo, moramo dokazati njeno negacijo. Načeloma lahko negacijo tvorimo tako, da pred izjavo napišemo »ni res, da velja . . . «, a nam to ne pove, kako bi negacijo dokazali. Zapišimo prvotno izjavo v delni simbolni obliki:

$$\forall a \in \mathbb{R}^{\mathbb{N}} \,.\, (a_n)_n \text{ pozitivno zaporedje} \Rightarrow 0 \text{ je limita zaporedja } (a_n)_n. \tag{5.1}$$

Zgornja pravila za računanje negacije nam povedo, da se $\neg\forall$ spremeni v $\exists\neg$ in da se nato implikacija oblike $\phi \Rightarrow \psi$ spremeni v $\phi \wedge \neg\psi$. Tako izrazimo negacijo izjave (5.1):

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

To preberemo z besedami:

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

Če se še malo potrudimo, preberemo bolj razumljivo:

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

S tem še nismo končali, saj je tudi »Število 0 ni limita zaporedja $(a_n)_n$« negacija. Izjavo »0 je limita zaporedja $(a_n)_n$« najprej zapišemo simbolno:

$$\forall \epsilon > 0 \,.\, \exists m \,.\, \mathbb{N} \forall n \geq m \,.\, |a_n - 0| < \epsilon. \tag{5.2}$$

Z zgornjimi pravili za negiranje izračunamo negacijo izjave (5.2). Operacijo $\neg$ postopoma »porivamo« navznoter:

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

V zadnjem koraku smo upoštevali, da za pozitivno število a_n velja $|a_n - 0| = |a_n| = a_n$. Tako smo dobili podrobno zapisano negacijo prvotne izjave

»Obstaja tako zaporedje pozitivnih števil $(a_n)_n$ in obstaja tak $\epsilon > 0$, da za vsak $m \in \mathbb{N}$ obstaja $n \geq m$, za katerega velja $a_n > \epsilon$.«

To izjavo pa znamo dokazati tako, da podamo konkreten primer zaporedja $(a_n)_n$ in konkretno vrednost ϵ, ki zadoščata pogoju, denimo $a_n = 2 + n$ in $\epsilon = 1$. Res, če je $m \in \mathbb{N}$ poljuben, lahko vzamemo kar $n = m$, saj potem velja $a_n = a_m = 2 + m > 1 = \epsilon$.

Pričujoči primer smo zapisali zelo podrobno. Izkušeni matematik tega seveda ne bo pisal, saj bo izračunal negacijo prvotne izjave kar v glavi in takoj podal primer zaporedja, ki dokazuje, da prvotna izjava ne velja.

5.7 Predikatni račun

Predikatni račun je tisti del logike, ki obravnava predikate ter kvantifikatorja $\forall$ in $\exists$.

Predikate tvorimo z logičnimi operacijami in kvantifikatorji iz **osnovnih predikatov**. Katere osnovne predikate imamo na voljo, je odvisno od snovi, ki jo obravnavamo.[3] Vedno imamo na voljo tudi **enakost** $x = y$, ki jo bomo obravnavali v razdelku 5.7.5.

V osnovnih predikatih nastopajo **izrazi** ali **termi**. Katere izraze lahko tvorimo je spet odvisno od tega, katere konstante in operacije imamo na voljo. Na primer, če obravnavamo aritmetiko celih števil, so na voljo operacije $+$, $-$, $\times$, če pa obravnavamo realna števila, so na voljo operacije $+$, $-$, $\times$, $/$. V izrazih vedno lahko nastopajo **spremenljivke**. Kadar uporabimo spremenljivko, moramo povedati njen **tip** oziroma **množico** vrednosti, ki jih lahko zavzame spremenljivka. Pogosto je tip spremenljivke razviden iz spremnega besedila ali iz ustaljene uporabe: n se uporablja za naravno število, x za realno, f za funkcijo ipd.

Ponazorimo pravkar definirane pojme s primerom. Predikat

$$0 < f(x) \wedge f(x) < \pi/4 \Rightarrow \sin(2f(x)) = 1/3$$

je sestavljen s pomočjo logičnih operacij $\wedge$ in $\Rightarrow$ iz treh osnovnih predikatov, zgrajenih iz osnovnih relacij $<$ in $=$,

$$0 < f(x) \qquad f(x) < \pi/4 \qquad \sin(2f(x)) = 1/3,$$

v katerih nastopa pet izrazov:

$$0 \qquad f(x) \qquad \pi/4 \qquad \sin(2f(x)) \qquad 1/3$$

V teh izrazih nastopa spremenljivka x, katere tip je množica realnih števil (to moramo uganiti) in spremenljivka f, ki označuje funkcijo iz realnih v realna števila (tudi to moramo uganiti). Nadalje, v izrazih nastopajo konstante 0, π, 4, 2, 1 in 3, operacija sin in operacija množenja.

5.7.1 Proste in vezane spremenljivke

V predikatih in izrazih se pojavljajo spremenljivke. Pri tem moramo ločiti med **prostimi** in **vezanimi** spremenljivkami. Oglejmo si naslednja izraza in predikat:

$$\sum_{i=0}^{n} a_i, \qquad \int_0^1 f(t)\,dt, \qquad \forall x \in A.\, \phi(x)\ .$$

[3] Na primer, če obravnavamo ravninsko geometrijo, potem so osnovni predikati »točka x leži na premici y«, »premici p in q se sekata« itn.

V vsoti je vezana spremenljivka i, spremenljivki n in a sta prosti. To pomeni, da je i neke vrste »lokalna spremenljivka«,[4] katere veljavnost je samo znotraj vsote, medtem ko sta spremenljiki n in a veljavni tudi zunaj samega izraza. Podobno je v integralu t vezana spremenljivka in f prosta, v izjavi na desni pa je vezana spremenljivka x, spremenljivki A in ϕ sta prosti.

Vezane spremenljivke so »nevidne« zunaj izraza in jih lahko vedno preimenujemo, ne da bi spremenili pomen izraza (seveda se novo ime ne sme mešati z ostalimi spremenljivkami, ki nastopajo v izrazu): izraza $\int_0^1 f(t)\,dt$ in $\int_0^1 f(x)\,dx$ štejemo za *enaka*, ker se razlikujeta le v imenu vezane spremenljivke. Spremenljivki, ki ni vezana, pravimo **prosta**. Izrazu, v katerem ni prostih spremenljivk, pravimo **zaprt izraz**. Zaprta logična izjava se imenuje **stavek**.

Pomembno se je zavedati, da vezana spremenljivka »zunaj« svojega območja ne obstaja. Matematiki so glede tega precej površni in na primer pišejo

$$\int x^2\,dx = x^3/3 + C,$$

kar je strogo gledano nesmisel. Na levi strani v integralu stoji vezana spremenljivka x, ki je na desni »pobegnila« iz integrala. Še več, če je $x \in \mathbb{R}$ in $C \in \mathbb{R}$, potem je izraz $x^3/3 + C$ *število* (odvisno od vrednosti x in C), saj je vsota dveh realnih števil. Na desni strani bi morala stati oznaka za *funkcijo*, recimo

$$\int x^2\,dx = (x \mapsto x^3/3 + C),$$

vendar tega v praksi nihče ne piše. Seveda pri vsem tem ostane še vprašanje, kakšno vlogo ima v zgornjem izrazu C. Pri analizi se učimo, da je C »poljubna konstanta«. Poskusimo to razumeti natančno s stališča logike. Besedico »poljubno« ponavadi razumemo kot »za vsak«, vendar to ne gre, saj je

$$\forall C \in \mathbb{R}\,.\, \int x^2\,dx = (x \mapsto x^3/3 + C)$$

nesemisel. Če bi to bilo res, bi veljalo za $C = 1$ in za $C = 2$, od koder bi dobili

$$(x \mapsto x^3/3 + 1) = \int x^2\,dx = (x \mapsto x^3/3 + 2).$$

Potemtakem bi morali biti funkciji $(x \mapsto x^3/3 + 1)$ in $(x \mapsto x^3/3 + 1)$ enaki, od koder sledi nesmisel $1 = 2$. Težave nastopajo iz dejstva, da poskušamo nedoločeni integral razumeti kot operacijo, ki slika funkcije v funkcije, kar ni. Nedoločeni integral preslika funkcijo f v *množico* vseh funkcij F, za katere velja $F' = f$. Če bi to želeli zapisati zares pravilno, bi dobili

$$\int x^2\,dx = \left\{ (x \mapsto x^3/3 + C) \;\middle|\; C \in \mathbb{R} \right\}.$$

Ali naj torej sklepamo, da so matematiki pravzaprav zelo površni pri pisanju integralov? Da, s stališča formalne logike prav gotovo. Vendar to ni nujno slabo: matematični zapis v praksi služi ljudem za sporazumevanje in prav je, da si izberejo tak zapis, s katerim najbolj učinkovito komunicirajo drug z drugim. Kljub temu pa se je treba zavedati, kdaj gredo matematiki »po bližnjici« in ne zapišejo ali povedo vsega dovolj natančno, da bi to bilo sprejemljivo za standarde, ki jih postavlja formalna logika.

[4] Podobnost z lokalnimi spremenljivkami v programskih jezikih ni zgolj naključje. Lokalna spremenljivka in števec v zanki sta tudi primera vezanih spremenljivk v teoriji programskih jezikov.

5.7.2 Substitucija

Substitucija je osnovna sintaktična operacija, v kateri *proste* spremenljivke zamenjamo z izrazi. Zapis

$$e[x_1 \mapsto e_1, \ldots, x_n \mapsto e_n]$$

pomeni: »v izrazu e *hkrati* zamenjaj proste spremenljivke x_1 z e_1, x_2 z e_2, ... in x_n z e_n.« Na primer,

$$(x^2 + y)[x \mapsto 3, y \mapsto 5, z \mapsto 12]$$

je enako $3^2 + 5$. Nič hudega ni, če se v substituciji omenja spremenljivko z, ki se v izrazu $x^2 + y$ ne pojavi.

Ko naredimo substitucijo, moramo paziti, da se proste spremenljivke ne »ujamejo«. Denimo, da želimo v integralu

$$\int_0^1 \frac{x}{a - x^2}\, dx$$

parameter a zamenjati z y^2. To naredimo s substitucijo

$$\left(\int_0^1 \frac{x}{a - x^2}\, dx\right)[a \mapsto y^2] = \int_0^1 \frac{x}{y^2 - x^2}\, dx.$$

Vse lepo in prav. Kaj pa, če želimo a zamenjati z $1 + x$? Ker je spremenljivka x vezana v integralu, *ne smemo* delati takole:

$$\left(\int_0^1 \frac{x}{a - x^2}\, dx\right)[a \mapsto x^2] = \int_0^1 \frac{x}{x^2 - x^2}\, dx?!$$

Ker vstavljamo v integral spremenljivko x, moramo vezano spremenljivko x najprej preimenovati v kaj drugega, na primer t, šele nato vstavimo:

$$\left(\int_0^1 \frac{x}{a - x^2}\, dx\right)[a \mapsto x^2] = \left(\int_0^1 \frac{t}{a - t^2}\, dx\right)[a \mapsto x^2] = \int_0^1 \frac{t}{x^2 - t^2}\, dt.$$

Podajmo še nekaj primerov substitucij:

$$\begin{aligned}
(x + y + 1)[x \mapsto 2] &= 2 + y + 1,\\
(x + y^2 + 1)[x \mapsto y, y \mapsto x] &= y + x^2 + 1,\\
((x + y^2 + 1)[x \mapsto y])[y \mapsto x] &= x + x^2 + 1,\\
(x + \textstyle\int_0^1 x \cdot y\ , dx)[x \mapsto 2] &= 2 + \textstyle\int_0^1 x \cdot y\, dx,\\
(\textstyle\int_0^1 x \cdot y\ dx)[y \mapsto x^2] &= \textstyle\int_0^1 t \cdot x^2\, dt.
\end{aligned}$$

Ločiti je treba med hkratno in zaporedno substitucijo:

$$\begin{aligned}
(x + y^2)[x \mapsto y, y \mapsto x] &= y + x^2,\\
((x + y^2)[x \mapsto y])[y \mapsto x] &= (y + y^2)[y \mapsto x] = x + x^2,\\
((x + y^2)[y \mapsto x])[x \mapsto y] &= (x + x^2)[x \mapsto y] = y + y^2.
\end{aligned}$$

V nadaljevanju bomo obravnavali pravila sklepanja za univerzalne in eksistenčne kvantifkatorje, v katerih se pojavi substitucija. Ker je sam zapis za substitucijo nekoliko nepregleden, bomo uporabili nekoliko manj pravilen, a bolj praktičen zapis. Denimo, da imamo

logično formulo ϕ, v kateri se morda pojavi spremenljivka x, ni pa to nujno. Tedaj pišemo $\phi(x)$. Če želimo zamenjati x z izrazom e, zapišemo $\phi(e)$. To je pravzaprav običajni zapis, kot ga uporabljajo matematiki za zapis funkcij, mi pa smo ga uporabili za zapis logičnih formul. Če bi uporabili zapis s substitucijo, bi formulo označili samo s ϕ namesto s $\phi(x)$ in zamenjavo s $\phi[x \mapsto e]$ namesto s $\phi(e)$. Zakaj je ta bolj priročen zapis hkrati manj pravilen? V formalni logiki strogo ločimo med *simbolnim zapisom* matematičnega pojma, ki je zaporedje znakov na papirju, in njegovim *pomenom*, ki je matematična abstrakcija. Substitucija $\phi[x \mapsto e]$ nam pove, kako niz znakov ϕ predelamo v novi niz znakov, torej deluje na nivoju simbolnega zapisa. Ko pišemo $\phi(x)$ pa si že predstavljamo, da je ϕ matematična funkcija, ki deluje na argumentu x. S tem nastopi zmešnjava med simbolnim zapisom in pomenom. Dokler se zmešnjave zavedamo, je vse v redu.

5.7.3 Univerzalni kvantifikator

Univerzalna kvantifikacija $\forall x \in S \,.\, \phi$ se prebere »Za vse x iz S velja ϕ.« Pravili sklepanja sta

$$\dfrac{\begin{array}{c}[x \in S] \\ \vdots \\ \phi(x)\end{array}}{\forall x \in S \,.\, \phi(x)}\ (x \text{ svež}) \qquad\qquad \dfrac{\forall x \in S \,.\, \phi(x) \qquad e \in S}{\phi(e)}$$

pri čemer je x spremenljivka, $\phi(x)$ logična formula in e poljuben izraz.

V besedilu se pravilo vpeljave zapiše:

> *Dokazujemo* $\forall x \in S \,.\, \phi(x)$*:*
>
> > *Naj bo* $x \in S$ *poljuben.*
> > *(Dokaz, da velja* $\phi(x)$*).*
>
> *Dokazali smo* $\forall x \in S \,.\, \phi(x)$*.*

Pravilo uporabe v besedilu ponavadi ni eksplicitno navedeno, če pa bi ga že zapisali, bi šlo takole:

> *Dokazujemo, da velja* $\phi(e)$*:*
>
> > *(Dokaz, da velja* $\forall x \in S \,.\, \phi(x)$*.)*
> > *(Dokaz, da velja* $e \in S$*.)*
>
> *Torej velja* $\phi(e)$*.*

Ob pravilu vpeljave stoji stranski pogoj, da mora biti spremenljivka x »sveža«. To pomeni, da se x ne sme pojavljati drugje v dokazu, saj bi sicer lahko prišlo do zmešnjave med vezanimi in prostimi spremenljivkami. V besedilu se dejstvo, da je x svež izraža z besedico »poljuben« ali »katerikoli«. Primer, kako gredo stvari narobe, če ne pazimo in pomešamo spremenljivke:

Izrek 5.20 (z napako v dokazu) *Če je* x *večji od* 42*, so vsa realna števila večja od* 23*.*

Dokaz. Denimo, da bi nekoliko nerodno zapisali izrek simbolno takole:

$$x > 42 \Rightarrow \forall x \in \mathbb{R} \,.\, x > 23.$$

To je sicer dovoljeno, saj se prosti x, ki stoji zunaj $\forall$ ni ujel, ni pa preveč smotrno, ker smo na dobri poti, da bomo zunanji prosti x in vezanega znotraj $\forall$ pomešali. Res, če ne upoštevamo pravila, da mora biti x svež, dobimo tale nepravi »dokaz«:

$$\dfrac{\dfrac{\dfrac{[x > 42] \qquad 42 > 23}{x > 23}}{\forall x \in \mathbb{R} \,.\, x > 23}}{x > 42 \Rightarrow \forall x \in \mathbb{R} \,.\, x > 23}$$

Pri pravilu za vpeljavo $\forall$ smo uporabili spremenljivko x, ki pa je že nastopala v začasni hipotezi $x > 42$. Z besedilom bi se isti dokaz glasil takole:

> »Dokazujemo $x > 42 \Rightarrow \forall x \in \mathbb{R} \,.\, x > 23$. Predpostavimo, da velja $x > 42$ in dokažimo $\forall x \in \mathbb{R} \,.\, x > 23$. Naj bo $x \in \mathbb{R}$. Po predpostavki je $x > 42$ in ker je $42 > 23$, od tod sledi $x > 23$.«

Če bi izrek zapisali bolje kot $x > 42 \Rightarrow \forall y \in \mathbb{R} \,.\, y > 23$, težav ne bi bilo, saj bi se prejšnji dokaz »zataknil«:

> »Dokazujemo $x > 42 \Rightarrow \forall y \in \mathbb{R} \,.\, y > 23$. Predpostavimo, da velja $x > 42$ in dokažimo $\forall y \in \mathbb{R} \,.\, y > 23$. Naj bo $y \in \mathbb{R}$. (Kaj zdaj? Lahko sicer dokažemo $x > 23$, a zares bi morali dokazati $y > 23$, kar ne gre.)«

■

Pogoj, da mora biti spremenljivka x v pravilu za vpeljavo »sveža«, se v praksi kaže v tem, da pri uvajanju nove spremenljivke izberemo zanjo novo ime, ki se še ni pojavilo v dokazu.

5.7.4 Eksistenčni kvantifikator

Eksistenčna kvantifikacija $\exists x \in S \,.\, \phi$ se prebere »obstaja x iz S, za katerega velja ϕ« ali »za neki x iz S velja ϕ.« Pravili sklepanja za eksistenčni kvantifikator se glasita

$$\dfrac{\phi(e) \qquad e \in S}{\exists x \in S \,.\, \phi(x)} \qquad\qquad \dfrac{\exists x \in S \,.\, \phi(x) \qquad \begin{array}{c}[x \in S \wedge \phi(x)] \\ \vdots \\ \psi\end{array}}{\psi} \ (x \text{ svež})$$

kjer je e poljuben izraz in x spremenljivka. Pri tem mora biti x v pravilu uporabe svež. V besedilu pravilo vpeljave uporabimo takole:

> *Dokazujemo $\exists x \in S \,.\, \phi(x)$:*
>
> 1. *(Skonstruiramo element $e \in S$.)*
> 2. *(Dokažemo, da velja $\phi(e)$.)*
>
> *Dokazali smo $\exists x \in S \,.\, \phi(x)$.*

Pravilo uporabe pa se v besedilu izraža takole:

Dokazujemo ψ:

1. *(Dokaz izjave $\exists x \in S \,.\, \phi(x)$.)*
2. *Predpostavimo, da za $x \in S$ velja $\phi(x)$:*
   (Dokaz izjave ψ.)

Dokazali smo ψ.

Enolični obstoj

Poleg običajnega eksistenčnega kvantifikatorja $\exists$ poznamo tudi *enolični* eksistenčni kvantifikator $\exists!$. Izjavo $\exists! x \in S \,.\, \phi(x)$ preberemo »obstaja natanko en $x \in S$, za katerega velja $\phi(x)$«.

Enolični eksistenčni kvantifikator ni osnovni logični operator, ampak je $\exists! x \in S \,.\, \phi(x)$ le okrajšava za

$$\exists x \in S \,.\, \phi(x) \wedge (\forall y \in S \,.\, \phi(y) \Rightarrow x = y). \tag{5.3}$$

Z besedami preberemo to izjavo takole: »obstaja x iz S, za katerega velja $\phi(x)$ in za vsak $y \in S$ za katerega velja $\phi(y)$ sledi $x = y$«. To je samo zapleten način, kako povedati, da obstaja natanko en element množice S, ki zadošča pogoju ϕ.

Pravilo sklepanja za vpeljavo enoličnega obstoja izpeljemo iz (5.3):

$$\frac{e \in S \qquad \phi(e) \qquad \begin{array}{c} y \in S \wedge \phi(y) \\ \vdots \\ y = e \end{array}}{\exists! x \in S \,.\, \phi(x)}$$

V besedilu dokažemo enolični obstoj takole:

Dokazujemo, da obstaja natanko en $x \in S$, za katerega velja $\phi(x)$:

1. *Obstoj: (Konstrukcija elementa $e \in S$ in dokaz, da velja $\phi(e)$.)*
2. *Enoličnost: denimo da za $y \in S$ velja $\phi(y)$:a*
   (Dokaz, da je $y = e$).

Dokazali smo $\exists! x \in S \,.\, \phi(x)$.

Če dokažemo enolični obstoj $\exists! x \in S \,.\, \phi(x)$, lahko vpeljemo novo konstanto c, ki označuje tisti element iz S, ki zadošča pogoju ϕ, pri čemer moramo seveda paziti, da znaka c nismo že prej uporabili za kak drug pomen. Nova konstanta c je opredeljena s praviloma

$$\frac{}{\phi(c)} \qquad\qquad \frac{y \in S \qquad \phi(y)}{y = c}$$

Če v formuli ϕ poleg spremenljivke x nastopajo še druge proste spremenljivke, denimo $y_1, \ldots, y_n$, potem je nova konstanta c v resnici *funkcija* parametrov $y_1, \ldots, y_n$.

5.7.5 Enakost in reševanje enačb

Enakost $=$ je osnovna relacija, ki zadošča naslednjim aksiomom in pravilom sklepanja:

$$\frac{}{a = a} \qquad \frac{a = b}{b = a} \qquad \frac{a = b \qquad b = c}{a = c} \qquad \frac{\phi(a) \qquad a = b}{\phi(b)}$$

Po vrsti se imenujejo: *refleksivnost*, *simetrija*, *tranzitivnost* in *zamenjava*. Zaenkrat enakosti ne bomo posvečali posebne pozornosti, saj jo v praksi študenti dobro obvladajo.

V osnovni iz srednji šoli se učimo pravil za reševanje enačb: enačbi smemo na obeh straneh prišteti ali odšteti poljuben izraz, pomnožiti ali deliti smemo s poljubnim *neničelnim* izrazom, ipd. Od kod izhajajo ta pravila? Kaj sploh pomeni, da smo enačbo »rešili«? Ko rešimo kvadratno enačbo

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

običajno zapišemo rešitev takole:

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

Kako naj to razumemo iz stališča matematične logike? Treba je pojasniti dvoje: kaj pomenita x_1 in x_2, saj v prvotni enačbi nastopa spremenljivka x, ter kako naj razumemo vejico med izjavama $x_1 = 2$ in $x_2 = 3$. Z indeksoma 1 in 2 štejemo rešitve enačbe in sta v resnici nepotrebna,[5] na kar kaže tudi dejstvo, da pišemo $x = \ldots$ in ne $x_1 = \ldots$, kadar je rešitev ena sama. Torej bi lahko rešitev zapisali kot

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

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

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

Začetna enačba in tako zapisana rešitev sta logično ekvivalentni:

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

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

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

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

medtem ko obratna implikacija

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

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

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

Naloga 5.21 Kako bi srednješolcem pojasnil, od kod izvira pravilo za množenje enačbe z neničelnim številom?

Naloga 5.22 Enačbo $f(x) = g(x)$ smo »rešili« z zaporedjem korakov

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

kjer smo v k-tem koraku namesto ekvivalence pomotoma naredili implikacijo. Smo s tem dobili preveč ali premalo rešitev prvotne enačbe?

Poglavje 6

Boolova algebra

6.1 Resničnostne tabele

Vsaka izjava ima **resničnostno vrednost**. Resničnostni vrednosti sta $\bot$ (neresnica) in $\top$ (resnica). Na primer, izjava $\bot \vee (\top \Rightarrow \top)$ je resnična, njena resničnostna vrednost je $\top$. Izjava $2 + 2 = 5$ je neresnična, njena resničnostna vrednost je $\bot$.

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

x	y	$x + 2y < 3$
0	0	$\top$
0	1	$\top$
1	0	$\top$
2	0	$\top$
1	1	$\bot$
0	2	$\bot$
$\vdots$	$\vdots$	$\vdots$

Kot vidimo, je lahko resničnostna tabela neskončna. Bolj uporabne so končne resničnostne tabele, v katerih parametri zavzemajo vrednosti iz končne množice.

V izjavi lahko nastopajo tudi **izjavne spremenljivke** ali **izjavni simboli**, to se spremenljivke, ki zavzamejo vrednosti $\bot$ in $\top$. Na primer, naj bo $\mathbb{2} = \{\bot, \top\}$ in $p, q \in \mathbb{2}$. Tedaj je $\neg p \vee q$ izjava, katere resničnostna tabela je

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

Izjava $\phi(p_1, \ldots, p_n)$, v kateri nastopajo izjavne spremenljivke $p_1, \ldots, p_n$ (in nobeni drugi parametri) določa preslikavo

$$\mathbb{2} \times \cdots \times \mathbb{2} \to \mathbb{2}$$

s predpisom

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

Preslikavi, ki slika iz produkta $\mathbb{2} \times \cdots \times \mathbb{2}$ v $\mathbb{2}$ pravimo **Boolova preslikava**. Prikažemo jo lahko z resničnostno tabelo. Če ima preslikava n argumentov, ima tabela 2^n vrstic.

6.1.1 Tavtologije

Izjava je **tavtologija**, če je njena resničnostna vrednost $\top$ ne glede na vrednosti parametrov. Premisli: kako iz resničnostne tabele razberemo, ali je izjava tavtologija?

Izrek 6.1 *Naj bo ϕ izjava, v kateri nastopajo le izjavni simboli $p_1, \ldots, p_n$. Tedaj je ϕ tavtologija, če in samo če ima dokaz.*

Dokaz. Dokaz najdete v [Pri92]. ∎

Izrek je pomemben, ker nam pove, da lahko dokazovanje izjav nadomestimo s preverjanjem resničnostnih tabel.

Opomba 6.2 Izrek velja samo za izjave, ki jih sestavimo iz izjavnih simbolov, $\bot$, $\top$ in logičnih veznikov $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$. Za splošne izjave, ki vsebujejo tudi $\forall$ in $\exists$ izrek *ne* velja. Lahko se namreč zgodi, da ima izjava neskončno resničnostni tabelo, v kateri so vse resničnostne vrednosti $\top$, a izjava nima dokaza.

6.1.2 Polni nabori

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

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

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

Disjunktivna oblika

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

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

Nato tvorimo disjunkcijo tako dobljenih konjunkcij:

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

Dobljena formula ima želeno resničnostno tabelo.

Konjuktivna oblika

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

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

Nato tvorimo konjunkcijo tako dobljenih disjunkcij:

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

Zgornjo tabelo bi lahko dobili tudi kot resničnostno tabelo formule

$$p \Leftrightarrow q$$

6.1.3 Polni nabori

Vidimo, da lahko vsako resničnostno tabelo dobimo z uporabo veznikov $\neg$, $\vee$ in $\wedge$. **Polni nabor** je tak izbor veznikov, k katerim lahko dobimo vsako resničnostno tabelo.

Torej je $\neg$, $\vee$, $\wedge$ poln nabor. Lahko bi ga še zmanjšali na $\neg$, $\wedge$, saj lahko $p \vee q$ izrazimo kot $\neg p \wedge \neg q$.

Nabor $\wedge$, $\vee$ pa *ni* poln, saj ne moremo dobiti resničnostne tabele

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

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

6.2 Boolova algebra

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

Opomba 6.3 Ekvivalentni izjavi imata lahko različen *pomena*. Na primer, $\forall x, y \in R\,.\, x + y = y + x$ in $\forall \alpha \in R\,.\, \sin(2\alpha) = 2 \cdot \cos\alpha \cdot \sin\alpha$ sta ekvivalentni, saj sta obe resnični, a ne moremo reči, da je njun pomen enak. (Predstavljate si, da bi bi vas v srednji šoli profesorica matematike vprašala adicijski izrek za sin, vi pa bi odgovorili »vrstni red seštevanja realnih števil ne vpliva na vrednost vsote«.)

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

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

Pravila za konjunkcijo:

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

Pravila za disjunkcijo:

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

Pravila za implikacijo:

$$\begin{aligned}
(p \Rightarrow q) &= (\neg q \Rightarrow \neg p) && \text{(kontrapozitivna oblika } \Rightarrow) \\
(p \Rightarrow q) &= \neg p \vee q \\
(\bot \Rightarrow q) &= \top \\
(\top \Rightarrow q) &= q \\
(p \Rightarrow \bot) &= \neg p \\
(p \Rightarrow \top) &= \top
\end{aligned}$$

Kombinirana pravila:

$$\begin{aligned}
\neg(p \wedge q) &= \neg p \vee \neg q && \text{(de Morganovo pravilo za } \wedge) \\
\neg(p \vee q) &= \neg p \wedge \neg q && \text{(de Morganovo pravilo za } \vee) \\
\neg(p \Rightarrow q) &= p \wedge \neg q \\
p \wedge (p \vee q) &= p && \text{(absorbcijsko pravilo za } \wedge) \\
p \vee (p \wedge q) &= p && \text{(absorbcijsko pravilo za } \vee) \\
p \wedge (q \vee r) &= (p \wedge q) \vee (p \wedge r) && \text{(distributivnost } \wedge) \\
p \vee (q \wedge r) &= (p \vee q) \wedge (p \vee r) && \text{(distributivnost } \vee)
\end{aligned}$$

Pravila za negacijo:

$$\begin{aligned}
\neg\top &= \bot \\
\neg\bot &= \top \\
\neg\neg p &= p && \text{(negacija je involucija)} \\
p \vee \neg p &= \top && \text{(izključena tretja možnost)} \\
p \wedge \neg p &= \bot
\end{aligned}$$

Zapišimo še uporabna logična pravila za kvantifikatorje. Tokrat uporabimo $\Leftrightarrow$ namesto $=$, ker je to bolj običajno:

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

Te ekvivalence je treba preveriti tako, da jih dokažemo.

Poglavje 7

Podmnožice in potenčne množice

7.1 Podmnožice

Pojem podmnožice že poznamo, a ga kljub temu ponovimo.

7.1.1 Definicija relacije $\subseteq$

Pravimo, da je množica S **podmnožica** množice T, pišemo $S \subseteq T$, ko velja $\forall x \in S \,.\, x \in T$. Pravimo tudi, da je S **vsebovana** v T in da je T **nadmnožica** S.

Vedno velja $\emptyset \subseteq S$ in $S \subseteq S$.

Princip ekstenzionalnosti za množice pravi:

$$S = T \iff (\forall x \in S \,.\, x \in T) \wedge (\forall y \in T \,.\, y \in S)$$

kar lahko zapišemo s podmnožicami:

$$S = T \iff S \subseteq T \wedge T \subseteq S.$$

Vsaka podmnožica $S \subseteq A$ opredeljuje neko lastnost elementov iz A: tisti elementi, ki imajo opredeljeno lastnost, so v S, ostali pa ne.

Primer 7.1 Naj bo P množica vseh praštevil, torej je $P \subseteq N$. Podmnožica P opredeljuje lastnost »je praštevilo«.

7.1.2 Kako tvorimo podmnožice

Če je $\phi(x)$ logična formula, v kateri nastopa spremenljivka $x \in A$, lahko tvorimo množico

$$\{x \in A \mid \phi(x)\}\,.$$

Pri tem je x vezana spremenljivka. Za to množico velja:

$$a \in \{x \in A \mid \phi(x)\} \iff a \in A \wedge \phi(a).$$

Povedano z besedami: elementi množice $\{x \in A \mid \phi(x)\}$ so tisti elementi iz A, ki zadoščajo pogoju ϕ. Velja $\{x \in A \mid \phi(x)\} \subseteq A$, prav tako pa

$$\{x \in A \mid \phi(x)\} \subseteq \{x \in A \mid \psi(x)\} \iff \forall x \in A \,.\, \phi(x) \Rightarrow \psi(x).$$

7.1.3 Kanonična inkluzija

Za podmnožico $S \subseteq T$ definiramo **kanonično inkluzijo** ali **kanonično vključitev** $i_S : S \to T$, s predpisom $i_S : x \mapsto x$. Pozor, to ni identiteta, razen v primeru $S = T$. Oznaka i_S ni standardna, pravzaprav standardne oznake ni.

Če je $f : T \to U$ in $S \subseteq T$, pravimo kompozitumu $f \circ i_S$ **zožitev** preslikave f na S, pišemo $f|_S$.

7.2 Potenčna množica

7.2.1 Definicija potenčne množice

Za vsako množico A tvorimo množico $\mathcal{P}(A)$, ki ji pravimo **potenčna množica**. Elementi potenčne množice $\mathcal{P}(A)$ so natanko podmnožice množice A:

$$S \in \mathcal{P}(A) \iff S \subseteq A$$

Na primer $\mathcal{P}(\emptyset) = \{\emptyset\}$ in

$$P(\{a, b, c\}) = \{\{\}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

7.2.2 Karakteristične funkcije

Karakteristična funkcija na množici A je funkcija z domeno A in kodomeno $\mathbb{2}$. Tu je $\mathbb{2} = \{\bot, \top\}$ množica resničnostnih vrednosti.

Eksponentna množica 2^A je torej množica vseh karakterističnih funkcij na A.

Opomba 7.2 Karakteristične funkcije se uporabljajo tudi v analizi, kjer jih običajno razumemo kot preslikave $A \to \{0, 1\}$ namesto $A \to \{\bot, \top\}$. Ker sta množici $\{\bot, \top\}$ in $\{0, 1\}$ izomorfni, to ni bistvena razlika.

Karakteristično funkcijo si lahko predstavljamo kot preslikavo, ki opredeljuje neko lastnost elementov A: tisti elementi, ki imajo opredeljeno lastnost, se slikajo v $\top$, ostali pa v $\bot$.

Primer 7.3 Preslikava $p : \mathbb{N} \to \mathbb{2}$, definirana s predpisom

$$p(n) = \begin{cases} \top & \text{če je } n \text{ praštevilo,} \\ \bot & \text{če } n \text{ ni praštevilo.} \end{cases}$$

je karakteristična preslikava lastnosti »je praštevilo«. Lahko bi jo zapisali tudi takole:

$$p(n) = (n > 1 \wedge \forall k, m \,.\, n = k \cdot m \Rightarrow k = 1 \vee m = 1).$$

7.2.3 Izomorfizem $\mathcal{P}(A) \cong 2^A$

Videli smo, da lahko neko lastnost elementov množice A predstavimo bodisi s podmnožico bodisi s karakteristično preslikavo. To nam da idejo, da med podmnožicami A in karakterističnimi preslikavami na A obstaja neka zveza.

Izrek 7.4 $\mathcal{P}(A) \cong 2^A$.

Dokaz. Definirajmo preslikavi

$$\chi : \mathcal{P}(A) \to 2^A \qquad\qquad \xi : 2^A \to \mathcal{P}(A)$$
$$\chi_S(x) := \begin{cases} \top & \text{če } x \in S, \\ \bot & \text{če } x \notin S, \end{cases} \qquad\qquad \xi_f := \{x \in A \mid f(x) = \top\}.$$

Ta predpisa bi lahko krajše zapisali tudi takole:

$$\chi_S(x) := (x \in S), \qquad\qquad \xi_f := \{x \in A \mid f(x)\}.$$

Preslikavi χ_S pravimo **karakteristična funkcija podmnožice** S. Trdimo, da sta χ in ξ inverza:

1. Dokažimo $\chi \circ \xi = \mathrm{id}_{2^A}$. Uporabimo princip ekstenzionalnosti za preslikave. Naj bo $f \in 2^A$. Dokažimo, da je $\chi_{\xi_f} = f$. Uporabimo princip ekstenzionalnosti za preslikave. Naj bo $x \in A$:

$$\chi_{\xi_f}(x) = (x \in \xi_f) = f(x).$$

2. Dokažimo $\xi \circ \chi = id_{\mathcal{P}(A)}$. Uporabimo princip ekstenzionalnosti za preslikave. Naj bo $S \in \mathcal{P}(A)$. Dokažimo, da je $\xi_{\chi_S} = S$:

$$\xi_{\chi_S} = \{x \in A \mid \chi_S(x)\} = \{x \in A \mid x \in S\} = S.$$

■

7.2.4 Boolova algebra podmnožic

Podmnožice množice A tvorijo Boolovo algebro za operacije presek $\cap$, unija $\cup$ in relativni komplement. Nevtralni element za unijo je $\emptyset$ in nevtralni element za presek je A.

Definirajmo tudi operacijo **simetrična razlika** $\oplus$, ki podmnožicama $S, T \in A$ priredi podmnožico

$$S \oplus T := (S \setminus T) \cup (T \setminus S) = (S \cup T) \setminus (S \cap T).$$

Potenčna množica $\mathcal{P}(A)$ je za operacijo $\oplus$ Abelova grupa.

Poglavje 8

Razredi in družine

8.1 Russellov paradoks

V prejšnji lekciji smo spoznali zapis podmnožice

$$\{x \in A \mid \phi(x)\},$$

ki tvori podmnožico A vseh elementov, ki zadoščajo pogoju x. Ko je bila teorija množic še v povojih, se je sama po sebi ponujala ideja, da bi lahko opisali množice kot kakršnokoli zbirko stvari. Torej bi lahko pisali

$$\{x \mid \phi(x)\}$$

za množico vseh tistih stvari (objektov, matematičnih entitet), ki zadoščajo pogoju ϕ. Se pravi, da bi veljalo

$$a \in \{x \mid \phi(x)\} \iff \phi(a)$$

A izkaže se, da ne moremo kar tako tvoriti povsem poljubnih množic objektov. To je odkril znameniti filozof, logik in matematik Betrand Russell. Razmislek se po njem imenuje **Russellov paradoks**. Le-ta je v matematiko vnesel pravo »krizo temeljev«, iz katere se je v prvi polovici 20. stoletja razvila logika in temelji matematike, kot jih poznamo danes.

Russellov paradoks gre takole. Denimo, da bi lahko tvorili poljubne množice objektov. Tedaj bi lahko tvorili tudi množico vseh množic, ki niso element same sebe:

$$R := \{S \mid S \notin S\}$$

Sedaj bomo izpeljali protislovje tako, da bomo dokazali $R \notin R$ in $R \in R$:

1. Dokažimo $R \notin R$. Denimo, da bi veljalo $R \in R$. Potem po definiciji R velja $R \notin R$, kar je v protislovju s predpostavko $R \in R$.
2. Dokažimo $R \in R$. V prvem koraku smo že dokazali $R \notin R$, torej po definiciji R velja $R \in R$.

Kaj lahko storimo? Očitno je treba pazljivo nadzorovati dopustne konstrukcije množic.

8.2 Množice in razredi

V sodobni teoriji množic Russellov paradoks razrešimo tako, da ločimo med dvema različnima zvrstema zbirk ali skupkov elementov, namreč **množicami** in **razredi**.

Torej imamo opravka s tremi zvrstmi matematičnih objektov:

1. Elementi, ki niso množice (na primer naravna števila), pravimo jim **urelementi**.
2. Zbirke elementov, ki se imenujejo **množice**.
3. Zbirke elementov, ki se imenujejo **razredi**.

Elementi množic so urelementi in množice. Enako velja za razrede. V čem je torej razlika med množicami in razredi? *Množica je lahko element (druge množice ali razreda). Razred ne more biti element (druge množice ali razreda).* S tem želimo povedati, da je zapis

$$x \in Y$$

neveljaven, če je x razred. Se pravi, če je x razred, potem sploh ne moremo govoriti o tem, ali je $x \in Y$ resnična izjava, saj ni izjava, ker ni izraz.

Vsaka množica je hkrati razred. Ni pa vsak razred tudi množica.

Razred je množica, če ga lahko skonstruiramo še na kak drug način s pomočjo pravil za konstrukcije množic (kartezični produkti, vsote, eksponenti, unije, preseki, podmnožice in vse ostale konstrukcije množic, ki jih bomo še spoznali).

Pravi razred je tak razred, ki ni množica. Z zapisom

$$\{x \mid \phi(x)\}$$

definiramo **razred** vseh objektov, ki zadoščajo pogoju ϕ. Se pravi, da velja

$$a \in \{x \mid \phi(x)\} \iff \phi(a).$$

Poglejmo nekaj primerov.

Primer 8.1 Russellov razred $R := \{S \mid S \notin S\}$ vsebuje vse množice, ki niso element same sebe. Paradoks smo razrešili, saj je nesmiselno zapisati $R \in R$.

Primer 8.2 Razred vseh množic

$$V := \{S \mid S \text{ je množica}\},$$

ki ga označimo tudi s Set. To je pravi razred. Res, če bi bil V množica, potem bi lahko tvorili podmnožico

$$\{S \in V \mid S \notin S\},$$

ki ni nič drugega kot Russellov R. Tako bi spet dobili protislovje. Torej V ni množica.

Primer 8.3 Razred vseh enojcev $E := \{S \mid \exists! x \in S \,.\, \top\}$ je pravi razred. Res, če bi bil množica, potem bi bila množica tudi njegova unija $\bigcup E$, ki pa je enaka V.

Primer 8.4 Zbirke vseh matematičnih struktur dane vrste pogosto tvorijo prave razrede. Na primer, razred vseh grup, razred vseh kolobarjev, vseh vektorskih prostorov itd.

Z razredi lahko delamo tako kot z množicami: tvorimo unije, preseke in produkte razredov, govorimo o podrazredih. Pri tem uporabljamo enake oznake za operacije kot pri množicah. Paziti moramo le, da razreda nikoli ne uporabimo kot element kake množice ali razreda. Na primer, če je C razred, lahko tvorimo »potenčni razred« $\mathcal{P}(C)$, ki vsebuje vse *podmnožice* C:

$$\mathcal{P}(C) := \{S \mid S \in \mathsf{Set} \wedge S \subseteq C\}.$$

Ne smemo pa tvoriti $\{D \mid D \subseteq C\}$, ker bi s tem C postal element razreda $\{D \mid D \subseteq C\}$.

8.3 Družine množic

Pogosto imamo opravka z zbirko množic. Če je zbirka končna, lahko množice preprosto naštejemo in vsako od njih poimenujemo

$$\begin{aligned} A &= \cdots \\ B &= \cdots \\ C &= \cdots \end{aligned}$$

Če je množic neskončno, jih morda lahko oštevilčimo:

$$\begin{aligned} A_1 &= \cdots \\ A_2 &= \cdots \\ A_3 &= \cdots \\ A_4 &= \cdots \\ &\vdots \end{aligned}$$

A tu se zadeve še ne končajo, saj lahko v splošnem obravnavamo poljubno zbirko množic. Takim zbirkam pravimo **družine množic**. Družina množic je **indeksirana** z elementi neke množice I, ki ji pravimo **indeksna množica**. Za vsak $i \in I$ imamo množico A_i, kar lahko izrazimo tudi z naslednjo definicijo.

Definicija 8.5 Družina množic je preslikava $I \to \mathsf{Set}$. Množici I pravimo **indeksna množica** in njenim elementov **indeksi**.

Primer 8.6 Končno zbirko množic lahko indeksiramo s končno množico. Denimo, da imamo množice A, B, C, D, E. Iz njih lahko tvorimo družino $S : I \to \mathsf{Set}$:

$$\begin{aligned} I &= \{1, 2, 3, 4, 5\}, \\ S_1 &= A, \\ S_2 &= B, \\ S_3 &= C, \\ S_4 &= D, \\ S_5 &= E. \end{aligned}$$

Primer 8.7 Nihče nas ne sili, da morajo biti indeksi števila. V prejšnjem primeru bi lahko uporabili $I = \left\{42, 13, \sqrt{2}, \emptyset, \mathbb{R}\right\}$ in definirali $S : I \to \mathsf{Set}$

$$\begin{aligned} S_{42} &= A, \\ S_{13} &= B, \\ S_{\sqrt{2}} &= C, \\ S_{\emptyset} &= D, \\ S_{\mathbb{R}} &= E. \end{aligned}$$

Primer 8.8 Množice v družini se lahko ponavljajo. Skrajni primer je **konstantna družina**, v kateri so vse množice med seboj enake.

Primer 8.9 Prazna družina je družina množic, ki je indeksirana z $\emptyset$.

Primer 8.10 Prazno družino moramo ločiti od **družine praznih množic**

$$\begin{aligned} I &\to \mathsf{Set} \\ i &\mapsto \emptyset \end{aligned}$$

Primer 8.11 Neprazna družina je družina indeksirana z neprazno množico. **Družina nepraznih množic** je družina, v kateri so vse množice neprazne. Torej velja:

- Prazna družina je družina nepraznih množic.
- Družina praznih množic je lahko prazna družina (ko je indeksna množica $\emptyset$).
- Družina praznih množic je lahko neprazna družina (ko je indeksna množica neprazna).

8.4 Konstrukcije in operacije z družinami množic

Operacije $\times$, $+$, $\cap$ in $\cup$ lahko posplošimo tako, da namesto z dvema množicama delujejo na poljubnem številu množic. V ta namen uporabimo družine množic.

8.4.1 Presek in unija družine

Presek in unija družine $A : I \to \mathsf{Set}$ sta definirana takole:

$$\begin{aligned} \bigcup_{i \in I} A_i &:= \{x \mid \exists i \in I \,.\, x \in A_i\}\,, \\ \bigcap_{i \in I} A_i &:= \{x \mid \forall i \in I \,.\, x \in A_i\}\,. \end{aligned}$$

Pozor! Na desni strani imamo razred! Res se lahko zgodi, da dobimo pravi razred, namreč kot presek prazne družine:

$$\begin{aligned} \bigcap_{i \in \emptyset} A_i &= \{x \mid \forall i \in \emptyset \,.\, x \in A_i\} \\ &= \{x \mid \top\} \\ &= V. \end{aligned}$$

Kdaj pa dobimo množico? Presek neprazne družine je vedno množica. Res, če imamo $k \in I$, potem velja

$$\bigcap_{i \in I} A_i = \{x \in A_k \mid \forall i \in I \,.\, x \in A_i\}\,.$$

Sedaj na desni ne stoji več razred, ampak podmnožica množice A_k.

Kaj pa unija družine množic? Ali je množica? Izkaže se, da za to potrebujemo aksiom:

Aksiom 8.12 *Unija družine množic je množica.*

8.4.2 Kartezični produkt družine

Definicija 8.13 Funkcija izbire za družino $A : I \to \mathsf{Set}$ je tako prirejanje, ki vsakemu indeksu $i \in I$ priredi natanko en element $f(i) \in A_i$.

Primer 8.14 Primer: funkcija izbire za družino

$$\begin{aligned} A &: \mathbb{N} \to \mathsf{Set} \\ A_n &:= \left\{ x \in R \mid 0 < x < 2^{-n} \right\} \end{aligned}$$

je na $f(n) := 2^{-n-1}$. To ni edina funkcija izbire za A, lahko bi vzeli tudi $f(n) = 2^{-n}/3$.

Definicija 8.15 Kartezični produkt družine $A : I \to \mathsf{Set}$ je množica vseh funkcij izbire družine A:

$$\prod_{i \in I} A_i := \{ f : I \to \textstyle\bigcup_{i \in I} A_i \mid \forall i \in I \,.\, f(i) \in A_i \} \,.$$

Za vsak $j \in I$ imamo **j-to projekcijo**

$$\begin{aligned} \mathsf{pr}_j &: (\textstyle\prod_{i \in I} A_i) \to A_j, \\ \mathsf{pr}_j &: f \mapsto f(j). \end{aligned}$$

Običajni kartezični produkt dveh množic je poseben primer produkta množic, namreč družine množic, ki je indeksirana z $I = \{1, 2\}$. Natančneje, velja

$$A \times B \cong \textstyle\prod_{i \in \{1,2\}} C_i,$$

kjer je $C_1 = A$ in $C_2 = B$.

Tudi eksponentna množica je poseben primer produkta množic, saj velja

$$B^A \cong \textstyle\prod_{a \in A} B$$

Na desni imamo produkt konstantne družine množic

$$\begin{aligned} A &\to \mathsf{Set}, \\ a &\mapsto B. \end{aligned}$$

8.4.3 Koprodukt ali vsota množic

Vsoto množic posplošimo na koprodukt družine.

Definicija 8.16 Koprodukt ali **vsota družine** $A : I \to \mathsf{Set}$ je množica $\sum_{i \in I} A_i$, katere elementi so $\mathsf{in}_i(a)$ za $i \in I$ in $a \in A_i$. Preslikavi $\mathsf{in}_k : A_k \to \sum_{i \in I} A_i$ pravimo **k-ta injekcija**.

Poleg tega definiramo še **projekciji**

$$\begin{aligned} \mathsf{pr}_1(\mathsf{in}_i(a)) &= i, \\ \mathsf{pr}_2(\mathsf{in}_i(a)) &= a. \end{aligned}$$

Namesto $\sum$ se piše tudi $\coprod$.

Poseben primer koprodukta je vsota $A + B$, saj velja

$$A + B \cong \sum_{k \in \{1,2\}} C_k$$

kjer je

$$\begin{aligned} C &: \{1, 2\} \to \mathsf{Set} \\ C_1 &:= A, \\ C_2 &:= B. \end{aligned}$$

Tudi kartezični produkt $A \times B$ je poseben primer koprodukta, saj velja

$$A \times B \cong \sum_{a \in A} B$$

Na desni imamo tokrat koprodukt konstantne družine množic

$$\begin{aligned} A &\to \mathsf{Set}, \\ a &\mapsto B. \end{aligned}$$

Poglavje 9

Lastnosti preslikav

Mnogi ste v srednji šoli že spoznali osnovne lastnosti preslikav, kot so injektivnost, surjektivnost in bijektivnost preslikave. V tej lekciji ponovimo te pojme in jih povežemo še s pojmoma monomorfizem in epimorfizem, ki sta pomembna v algebri

9.1 Osnovne lastnosti preslikav

9.1.1 Injektivna, surjektivna, bijektivna preslikava

Definicija 9.1 Preslikava $f : A \to B$ je
- **injektivna**, ko velja $\forall xy \in A \,.\, f(x) = f(y) \Rightarrow x = y$,
- **surjektivna**, ko velja $\forall y \in B \,.\, \exists x \in A \,.\, f(x) = y$,
- **bijektivna**, ko je surjektivna in injektivna.

Opomba 9.2 Pogosto vidimo definicijo injektivnosti, ki pravi, da f slika različne elemente v različne vrednosti, se pravi $\forall xy \in A \,.\, x \neq y \Rightarrow f(x) \neq f(y)$. Ta definicija je ekvivalentna naši, a jo ne priporočamo, ker je manj uporabna. Naša definicija namreč podaja recept, kako preverimo injektivnost: predpostavimo $f(x) = f(y)$ in od tod izpeljemo $x = y$ tako, da predelamo *enačbo* $f(x) = f(y)$ v enačbo $x = y$. To je v splošnem lažje kot predelava **neenačb**.

Naloga 9.3 Primerjaj definicijo injektivnosti in surjektivnosti z zahtevo, da mora biti prirejanje, ki določa preslikavo, enolično in celovito.

9.1.2 Monomorfizmi in epimorfizmi

Definicija 9.4 Preslikava $f : A \to B$ je
- **monomorfizem (mono)**, ko jo lahko krajšamo na levi:

$$\forall C \in \mathsf{Set} \,.\, \forall g, h : C \to A \,.\, f \circ g = f \circ h \Rightarrow g = h.$$

- **epimorfizem (epi)**, ko jo lahko krajšamo na desni:

$$\forall C \in \mathsf{Set} \,.\, \forall g, h : B \to C \,.\, g \circ f = h \circ f \Rightarrow g = h.$$

Pojma monomorfizem in epimorfizem sta uporabna, ker nam omogočata, da *krajšamo* funkcije, ki nastopajo v enačbah. Na vajah boste reševali naloge, kjer to pride prav.

Izrek 9.5 *Naj bosta $f : A \to B$ in $g : B \to C$ preslikavi. Tedaj velja:*

1. *Kompozicija monomorfizmov je monomorfizem.*
2. *Kompozicija epimorfizmov je epimorfizem.*
3. *Če je $g \circ f$ monomorfizem, je f monomorfizem.*
4. *Če je $g \circ f$ epimorfizem, je g epimorfizem.*

Dokaz.

1. Naj bosta $f : A \to B$ in $g : B \to C$ monomorfizma. Dokazujemo, da je $g \circ f$ tudi monomorfizem. Naj bosta $h, k : D \to A$ preslikavi, za kateri velja $(g \circ f) \circ h = (g \circ f) \circ k$. Dokazujemo $h = k$. Ker je kompozicija preslikav asociativna, velja $g \circ (f \circ h) = (g \circ f) \circ h = (g \circ f) \circ k = g \circ (f \circ k)$. Ker je g monomorfizem, ga smemo krajšati na levi, torej dobimo $f \circ h = f \circ k$. Ker je f monomorfizem, ga smemo krajšati in dobimo želeno enakost $h = k$.
2. Dokaz je podoben prejšnjemu, le vloga leve in desne strani se spremeni.
3. Dokaz je podoben naslednjemu, le vloga leve in desne strani se spremeni.
4. Naj bosta $f : A \to B$ in $g : B \to C$ preslikavi in $g \circ f$ epimorfizem. Dokazujemo, da je g epimorfizem. Naj bosta $h, k : C \to D$ taki preslikavi, da velja $h \circ g = k \circ g$. Dokazujemo, da je $h = k$. Iz $h \circ g = k \circ g$ sledi $(h \circ g) \circ f = (k \circ g) \circ f$. Če upoštevamo asociativnost kompozicije, dobimo $h \circ (g \circ f) = k \circ (g \circ f)$. Ker je $g \circ f$ epimorfizem, ga smemo krajšati na desni, od koder dobimo želeno enakost $h = k$.

■

Izrek 9.6 *Za preslikavo $f : A \to B$ velja:*

1. *f je monomorfizem, če in samo če je f injektivna.*
2. *f je epimorfizem, če in samo če je f surjektivna.*
3. *f je izomorfizem, če in samo če je f bijektivna.*

Dokaz.

1. ($\Rightarrow$) Če je f monomorfizem in $f(x) = f(y)$, tedaj je $(f \circ (u \mapsto x))() = f(x) = f(y) = (f \circ (u \mapsto y))()$, torej $(u \mapsto x) = (u \mapsto y)$ in sledi $x = y$.
   ($\Leftarrow$) Če je f injektivna in $f \circ g = f \circ h$, potem je za vsak x $f(g(x)) = f(h(x))$, torej $g(x) = h(x)$ za vsak x, torej $g = h$.
2. ($\Rightarrow$) Če je f epimorfizem: obravnavajmo množico

   $$S = \{z \in B \mid \exists x \in A \,.\, f(x) = z\}$$

   ter preslikavi $\chi_S : B \to 2$ in $(y \mapsto \top) : B \to 2$. Ker velja $\chi_S \circ f = (y \mapsto \top) \circ f$, sledi $\chi_S = (y \mapsto \top)$, torej $S = B$, kar je surjektivnost.
   ($\Leftarrow$) Če je f surjektivna in $g \circ f = h \circ f$: naj bo $y \in B$. Obstaja $x \in A$, da je $f(x) = y$. Torej je $g(y) = g(f(x)) = h(f(x)) = h(y)$. Torej je $g = h$.
3. ($\Rightarrow$) Če je f izomorfizem, potem: je f epi, ker je $\mathrm{id}_B = f \circ f^{-1}$ epi; je f mono, ker je $\mathrm{id}_A = f^{-1} \circ f$ mono.
   ($\Leftarrow$) Če je f bijektivna, potem je njen inverz f^{-1} definiran s predpisom

   $$f(y) = \iota x \in A \,.\, f(x) = y \qquad \text{»tisti } x\text{, ki ga } f \text{ slika v } y\text{«}$$

   Dokazati je treba $\exists! x \in A \,.\, f(x) = y$. To velja, saj $\exists x \in A \,.\, f(x) = y$ sledi iz surjektivnosti f in $\forall x_1, x_2 \,.\, f(x_1) = y \wedge f(x_2) = y \Rightarrow x_1 = x_2$ iz injektivnosti f.

■

9.1.3 Retrakcija in prerez

Spoznajmo še pojem retrakcije in prereza. Na predavanjih bomo s sliko pojasnili, zakaj se tako imenujeta.

Definicija 9.7 Če sta $f : A \to B$ in $g : B \to A$ taki preslikava, da velja $f \circ g = \mathrm{id}_B$, pravimo:

- f je **retrakcija** ali **levi inverz** g,
- g je **prerez** ali **desni inverz** f.

Naloga 9.8 Podajte primer retrakcije in prereza, ki *nista* izomorfizma.

Izrek 9.9 *Retrakcija je epimorfizem, prerez je monomorfizem.*

Dokaz. Denimo, da velja $f \circ g = \mathrm{id}$, torej je f retrakcija in g prerez. Ker je identiteta monomorfizem, je po izreku 9.5 tudi g monomorfizem. In ker je identiteta epimorfizem, je po istem izreku f epimorfizem. ∎

9.2 Slike in praslike

9.2.1 Izpeljane množice

Naj bo $f : A \to B$ preslikava. Tedaj definiramo **izpeljano množico**

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

ter **izpeljano množico s pogojem**

$$\{f(x) \mid x \in A \mid \phi(x)\} := \{y \in B \mid \exists x \in A \,.\, \phi(x) \wedge y = f(x)\}\,.$$

Običajno se piše izpeljano množico s pogojem kar

$$\{f(x) \mid x \in A \wedge \phi(x)\}\,.$$

Primer 9.10 Množica vseh kvadratov naravnih števil je izpeljana množica $\{n^2 \mid n \in \mathbb{N}\}$.

9.2.2 Slike in praslike

Definicija 9.11 Naj bo $f : A \to B$ preslikava:

- **Praslika** podmnožice $S \subseteq B$ je $f^*(S) := \{x \in A \mid f(x) \in S\}$.
- **Slika** podmnožice $T \subseteq A$ je $f_*(T) := \{y \in B \mid \exists x \in T \,.\, f(x) = y\}$.

Prasliki pravimo tudi **inverzna slika** in sliki tudi **direktna slika**.

Kot vidimo, lahko sliko zapišemo tudi kot izpeljano množico

$$f_*(T) := \{f(x) \mid x \in T\}\,.$$

Običajni zapis za prasliko $f^*(S)$ je tudi $f^{-1}(S)$, vendar tega zapisa mi ne bomo uporabljali, ker napačno namiguje, da ima f inverz. Boste pa ta zapis videli marsikje drugje, ker so matematiki konzervativni bitja, ki raje nekaj stoletij uporabljajo slab zapis, kot da bi spremenili svoje navade.

Običajni zapis za sliko $f_*(S)$ je tudi $f(S)$ ali $f[S]$. Predvsem $f(S)$ se uporablja v praksi, a tudi tega odsvetujemo. Kako naj pri takem zapisu ločimo med $f(x)$ in $f_*(\{x\})$?

Definicija 9.12 Zaloga vrednosti preslikave $f : A \to B$ je slika domene, torej $f_*(A)$.

9.2.3 Slike in praslike kot preslikave višjega reda

Naj bo $f : A \to B$. Tedaj sta tudi f^* in f_* preslikavi. Res, $f^* : \mathcal{P}(B) \to \mathcal{P}(A)$ je določena s predpisom $S \mapsto \{x \in A \mid f(x) \in S\}$, in $f_* : \mathcal{P}(A) \to \mathcal{P}(B)$ je določena s predpisom $T \mapsto \{f(x) \mid x \in T\}$

Še več, tudi »zgornja zvezdica *« in »spodnja zvezdica $_*$« sta preslikavi

$$^* : B^A \to \mathcal{P}(A)^{\mathcal{P}(B)} \qquad _* : B^A \to \mathcal{P}(B)^{\mathcal{P}(A)}$$

Ker slikata preslikave v preslikave, pravimo, da sta to **preslikavi višjega reda**. Primer preslikave višjega reda je tudi odvod, ki funkciji priredi njen odvod.

9.2.4 Lastnosti slike in praslike

Izrek 9.13 *Naj bo $f : A \to B$ preslikava:*

- *praslike so monotone: če je $S \subseteq T \subseteq A$, potem je $f^*(S) \subseteq f^*(T)$*
- *slike so monotone: če je $X \subseteq Y \subseteq B$, potem je $f_*(X) \subseteq f_*(Y)$.*

Dokaz. Dokaz pustimo za vajo. ∎

Izrek 9.14 *Praslike ohranjajo preseke in unije: za vse $f : A \to B$ in $S : I \to \mathcal{P}(B)$ velja*

$$f^*(\textstyle\bigcup_{i\in I} S_i) = \bigcup_{i\in I} f^*(S_i) \qquad \textit{in} \qquad f^*(\textstyle\bigcap_{i\in I} S_i) = \bigcap_{i\in I} f^*(S_i).$$

Dokaz. Dokažimo prvo izjavo, druga je zelo podobna, le da $\exists$ zamenjamo z $\forall$. Dokazujemo $f^*(\bigcup_{i\in I} S_i) \subseteq \bigcup_{i\in I} f^*(S_i)$. Naj bo $x \in f^*(\bigcup_{i\in I} S_i)$ in dokazujemo $x \in \bigcup_{j\in I} f^*(S_j)$. Ker je $f(x) \in \bigcup_{i\in I} S_i$ obstaja $k \in I$, da je $f(x) \in S_k$, torej je $x \in f^*(S_k) \subseteq \bigcup_{i\in I} f^*(S_i)$. ∎

Izrek 9.15 *Naj bo $f : A \to B$ in $T : I \to \mathcal{P}(A)$. Tedaj je*

$$f_*(\textstyle\bigcup_{i\in I} T_i) = \bigcup_{i\in I} f_*(T_i) \qquad \textit{in} \qquad f_*(\textstyle\bigcap_{i\in I} T_i) \subseteq \bigcap_{i\in I} f_*(S_i).$$

Dokaz. Dokaz prepustimo za vajo. ∎

Naloga 9.16 Iz zgornjih dveh izrekov izpeljite naslednja dejstva:

$$\begin{aligned} f^*(\emptyset) &= \emptyset, \\ f_*(\emptyset) &= \emptyset, \\ f^*(B) &= A, \\ f^*(S \cup T) &= f^*(S) \cup f^*(T), \\ f^*(S \cap T) &= f^*(S) \cap f^*(T). \end{aligned}$$

Poleg tega imamo za $S \subseteq B$ še $f^*(\complement S) = \complement(f^*(S))$.

Poglavje 10

Relacije

10.1 Predikati

Predikat na množici A opredeljuje kako lastnost elementov množice A. Če je P predikat na A in $x \in A$, potem se je smiselno vprašati, ali x zadošča predikatu P. Odgovor je resničnostna vrednost, ki jo označimo s $P(x)$.

Primer 10.1 Na množici naravnih števil $\mathbb{N}$ lahko obravnavamo predikat »je sodo število«. Tako na primer 4 zadošča predikatu »je sodo število«, 7 pa mu ne zadošča.

Predikat P na množici A lahko predstavimo na dva načina:
- kot preslikavo $P : A \to 2$, ki slika $x \in A$ v resničnostno vrednost $P(x)$,
- kot podmnožico $P \subseteq A$ tistih $x \in A$, za katere velja $P(x)$.

Oba načina predstavitve sta uporabna, spoznali pa smo že izomorfizem med njima, saj velja $P(A) \cong 2^A$.

10.2 Relacije

Relacije z večmestni predikati. Se pravi, relacija R opredeljujejo kako lastnost urejenih večteric kartezičnega produkta $A_1 \times A_2 \times \cdots \times A_n$. Pravimo, da je R **n-člena** ali **n-mestna relacija** na množicah $A_1, \ldots, A_n$.

Primer 10.2 Na množici točk v ravnini lahko obravnavamo relacijo kolinearnosti. To je trimestna relacija: točke A, B in C so kolinearne, kadar obstaja premica, ki vsebuje vse tri točke.

Relacijo R na množicah $A_1, \ldots, A_n$ lahko predstavimo na dva načina, podobno kot predikate:
- kot preslikavo $R : A_1 \times A_2 \times \cdots \times A_n \to 2$,
- kot podmnožico $R \subseteq A_1 \times A_2 \times \cdots \times A_n$.

Bolj običajna je predstavitev s podmnožicami, zato bomo dejstvo, da je R relacija na množicah $A_1, \ldots, A_n$ zapisali kar kot $R \subseteq A_1 \times A_2 \times \cdots \times A_n$. Za elemente $x_1 \in A_1, \ldots, x_n \in A_n$ dejstvo, da so v relaciji R zapišemo $R(x_1, \ldots, x_n)$, včasih pa tudi $(x_1, \ldots, x_n) \in R$.

Na množicah $A_1, \ldots, A_n$ lahko vedno definiramo:
- **prazno relacijo** $\emptyset$: nobeni elementi niso v prazni relaciji,

- **univerzalno relacijo** $A_1 \times A_2 \times \cdots \times A_n$: vsi elementi so v univerzalni relaciji.

Univerzalna relacija se imenuje tudi **polna relacija**.

V praksi so najbolj pogoste **dvomestna relacije**, se pravi relacije na dveh množicah, $R \subseteq A \times B$. V tem primeru pravimo množici A **domena** in B **kodomena** relacije R, relaciji R pa relacija med A in B.

Pomembna relacija na množici A je **enakost** ali **diagonala** na A:

$$\Delta_A := \{(x, y) \in A \times A \mid x = y\}$$

Zakaj ji pravimo diagonala?

Izmed dvočlenih relacij so najbolj pogoste relacije, pri katerih se domena in kodomena ujemata, torej $R \subseteq A \times A$. V tem primeru pravimo, da je R **relacija na množici** A.

Denimo, da je $R \subseteq A \times B$ relacija, $x \in A$ in $y \in B$. Dejstvo, da sta x in y v relaciji R zapišemo na enega od načinov

$$(x, y) \in R \qquad R(x, y) \qquad x \mathrel{R} y$$

Prvi zapis se uporablja, kadar je R podana kot podmnožica $A \times B$, drugi kadar podamo R z logično formulo. Tretji način je tudi pogost, še posebej kadar je relacija označena s simbolom kot je $=$, $\neq$, $<$, $>$, $\sqsubseteq$, $\sim$ ipd.

Relacijo lahko predstavimo na več načinov, na primer z logično formulo, z resničnostno tabelo, ali z usmerjenim grafom. Z grafom predstavimo $R \subseteq A \times A$ tako, da za vozlišča grafa vzamemo elemente množice A, nato pa narišemo puščico od x do y, kadar velja $x \mathrel{R} y$.

10.3 Osnovne lastnosti relacij

Relacije, ki so pomembne v matematični praksi imajo pogosto lastnosti, ki jih poimenujemo. Za relacijo $R \subseteq A \times A$ pravimo da je:

- **refleksivna:** $\forall x \in A \,.\, x \mathrel{R} x$,
- **simetrična:** $\forall x, y \in A \,.\, x \mathrel{R} y \Rightarrow y \mathrel{R} x$,
- **antisimetrična:** $\forall x, y \in A \,.\, x \mathrel{R} y \wedge y \mathrel{R} x \Rightarrow x = y$,
- **tranzitivna:** $\forall x, y, z \in A \,.\, x \mathrel{R} y \wedge y \mathrel{R} z \Rightarrow x \mathrel{R} z$,
- **irefleksivna:** $\forall x \in A \,.\, \neg(x \mathrel{R} x)$,
- **asimetrična:** $\forall x, y \in A \,.\, x \mathrel{R} y \Rightarrow \neg(y \mathrel{R} x)$,
- **sovisna:** $\forall x, y \in A \,.\, x \neq y \Rightarrow x \mathrel{R} y \vee y \mathrel{R} x$,
- **strogo sovisna:** $\forall x, y \in A \,.\, x \mathrel{R} y \vee y \mathrel{R} x$.

Naloga 10.3 Kako iz usmerjenega grafa relacije razberemo refleksivnost in simetričnost? Kaj pa ostale lastnosti?

10.4 Operacije na relacijah

10.4.1 Unija, presek in komplement relacij

Ker so relacije pravzaprav podmnožice, lahko na njih uporabljamo operacije unija $\cup$, presek $\cap$ in komplement $\square^{\mathsf{C}}$. Denimo, da sta $R, S \subseteq A \times B$ relaciji. Tedaj velja:

$$\begin{aligned} x\ (R \cup S)\ y &\iff x\ R\ y \vee x\ S\ y, \\ x\ (R \cap S)\ y &\iff x\ R\ y \wedge x\ S\ y, \\ x R^{\mathsf{C}} y &\iff \neg(x\ R\ y). \end{aligned}$$

Primer 10.4 Za relacije enakosti in urejenost na realnih številih velja:
- Komplement relacije enakosti $=$ je relacija neenakosti $\neq$.
- Unija relacij $<$ in $>$ na realnih številih je relacija $\neq$.
- Presek relacij $\leq$ in $\geq$ na realnih številih je relacija $=$.

10.4.2 Transponirana relacija

Dvojiške relacije lahko tudi **transponiramo**. Transponiranka relacije $R \subseteq A \times B$ je relacija $R^{\mathsf{T}} \subseteq B \times A$, definirana s predpisom

$$y R^{\mathsf{T}} x \quad :\iff \quad x\ R\ y$$

ali ekvivalentno

$$R^{\mathsf{T}} := \{(y, x) \in B \times A \mid x\ R\ y\}\,.$$

Očitno velja $(R^{\mathsf{T}})^{\mathsf{T}} = R$, torej je transponiranje *involucija*.

Primer 10.5 Transpozicija relacije $<$ na realnih številih $\mathbb{R}$ je relacija $>$ na $\mathbb{R}$. Komplement relacije $<$ na $\mathbb{R}$ je relacija $\geq$ na $\mathbb{R}$.

10.4.3 Kompozitum relacij

Nadalje definiramo **kompozitum** relacij $R \subseteq A \times B$ in $S \subseteq B \times C$ kot relacijo $S \circ R \subseteq A \times C$, s predpisom

$$x\ (S \circ R)\ z \quad :\iff \quad \exists y \in B\,.\, x\ R\ y \wedge y\ S\ z$$

ali ekvivalentno

$$S \circ R := \{(x, z) \in A \times C \mid \exists y \in B\,.\, (x, y) \in R \wedge (y, z) \in S\}\,.$$

Se pravi, da sta $x \in A$ in $z \in C$ v relaciji $S \circ R$, če sta preko S in R povezana s kakim elementom $y \in B$.

Primer 10.6 Kompozitum relacij »x je otrok od y« in »z je mati od y« je relacija »z je babica od x«.

Izrek 10.7 *Komponiranje relacij je asociativno in diagonala je enota.*

Naloga 10.8 Zgornji izrek zapiši bolj natančno, da bo razvidno, kaj so domene in kodomene relacij.

Dokaz. Najprej dokažimo asociativnost kompozicije. Naj bo $R \subseteq A \times B$, $S \subseteq B \times C$ in $T \subseteq C \times D$ ter $a \in A$ in $d \in D$. Tedaj velja

$$\begin{aligned} a\ (T \circ (S \circ R))\ d &\iff \\ \exists c \in C\,.\, a\ (S \circ R)\ c \wedge c\ T\ d &\iff \\ \exists c \in C\,.\, (\exists b \in B\,.\, a\ R\ b \wedge b\ S\ c) \wedge c\ T\ d & \end{aligned} \tag{10.1}$$

in

$$\begin{aligned} a\ ((T \circ S) \circ R)\ d &\iff \\ \exists b \in B\,.\, a\ R\ b \wedge b\ (T \circ S)\ d &\iff \\ \exists b \in B\,.\, a\ R\ b \wedge (\exists c \in C\,.\, b\ S\ c \wedge c\ T\ d) & \end{aligned} \tag{10.2}$$

Torej je treba dokazati ekvivalenco izjav (10.1) in (10.2), kar prepuščamo za vajo. Naj namignemo, da je treba pri dokazovanju ekvivalence uporabiti *Frobeniuseva pravilo*

$$(\exists x \in X\,.\, p \wedge q(x)) \Leftrightarrow p \wedge \exists x \in X\,.\, q(x).$$

V pravilu je p formula, v kateri x ne nastopa kot prosta spremenljivka.

Dokažimo še, da je diagonala enota za kompozicijo: naj bo $R \subseteq A \times B$ ter $x \in A$ in $y \in B$. Tedaj velja

$$\begin{aligned} x(\Delta_B \circ R)y &\iff \\ \exists z \in B\,.\, x\ R\ z \wedge z \Delta_B y &\iff \\ \exists z \in B\,.\, x\ R\ z \wedge z = y &\iff \\ x\ R\ y & \end{aligned}$$

V zadnjem koraku smo uporabili ekvivalenco $(\exists u \in U\,.\, u = v \wedge P(v)) \Leftrightarrow P(v)$. Podobno dokažemo, da je diagonala desna enota. ∎

Kompozitum relacij ima torej podobne lastnosti kot kompozitum funkcij.

10.4.4 Potenca relacije

Za $n \in \mathbb{N}$ definiramo **n-to potenco** relacije $R \subseteq A \times A$ kot relacijo $R^n \subseteq A \times A$ takole:

$$x R^n y \quad :\iff \quad \exists z_0, \ldots, z_n \in A\,.\, z_0 = x \wedge z_n = y \wedge \forall i \in 0, \ldots, n-1\,.\, z_i\ R\ z_{i+1}.$$

To je precej nečitljiva formula. Bolj razumljiva definicija je potenca kot n-kratni kompozitum relacije R same s sabo:

$$R^n := \underbrace{R \circ \cdots \circ R}_{n}$$

kjer se desni R ponovi n-krat. Kaj dobimo, ko za n vstavimo 0? Enoto za kompozitum:

$$R^0 = \Delta_A.$$

10.5 Funkcijske relacije

Funkcijo $f : A \to B$ smo definirali kot *prirejanje* med elementi A in B. A kaj pravzaprav je »prirejanje«? Je to funkcijski predpis, program, kaj drugega? Sedaj lahko povemo natančno: prirejanje, s katerim je podana funkcija, je *relacija* med elementi domene in kodomene.

Definicija 10.9 Naj bo $f : A \to B$ funkcija. **Graf** funkcije f je relacija $\Gamma_f \subseteq A \times B$, definirana s predpisom

$$x \,\Gamma_f\, y \Leftrightarrow f(x) = y$$

ali ekvivalentno

$$\Gamma_f := \{(x, y) \in A \times B \mid f(x) = y\}\,.$$

Skratka, graf funkcije ni nič drugega kot njeno prirejanje. Sedaj pa se vprašajmo: kakšnim pogojem mora zadoščati relacija $R \subseteq A \times B$, da je prirejanje za neko funkcijo? Odgovor poznamo: biti mora enolična in celovita.

Definicija 10.10 Relacija $R \subseteq A \times B$ je **funkcijska relacija**, če je

- **celovita:** $\forall x \in A\,.\,\exists y \in B\,.\,x\ R\ y$ in
- **enolična:** $\forall x \in A\,.\,\forall y_1, y_2 \in B\,.\,x\ R\ y_1 \wedge x\ R\ y_2 \Rightarrow y_1 = y_2$.

Ekvivalentno oba pogoja skupaj zapišemo: $\forall x \in A\,.\,\exists! y \in B\,.\,x\ R\ y$.

Graf $\Gamma_f \subseteq A \times B$ funkcije $f : A \to B$ je vedno funkcijska relacija. Funkcijska relacija $R \subseteq A \times B$ določa preslikavo $\phi_R : A \to B$ definirano s predpisom

$$\phi_R : x \mapsto \iota y \in B\,.\,x\ R\ y.$$

Če iz funkcije $f : A \to B$ tvorimo njen graf Γ_f, nato pa iz njega funkcijo $\phi_{\Gamma_f} : A \to B$ dobimo nazaj prvotno funkcijo f. Obratno, če je R funkcijska relacija, tedaj je Γ_{ϕ_R} enaka R. Torej imamo izomorfizem

$$B^A \cong \{R \in \mathcal{P}(A \times B) \mid \forall x \in A\,.\,\exists! y \in B\,.\,x\ R\ y\}\,.$$

Izjava 10.11 *Kompozitum funkcij se ujema s kompozitumom relacij:* $\Gamma_{g \circ f} = \Gamma_g \circ \Gamma_f$.

Dokaz. Dokaz prepustimo za vajo, še prej pa morate izjavo zapisati bolj natančno: od kod in kam slikata preslikavi f in g, kaj pomeni kompozitum na levi in kaj na desni? ∎

10.6 Ovojnice relacij

Pogosto imamo opravka z relacijo R, ki nima želene lastnosti (na primer ni tranzitivna) mi pa želimo relacijo, ki to lastnost ima. Ali lahko R kako spremenimo, da bo imela želeno lastnost? Če to lahko naredimo na več načinov, ali se eden od njih odlikuje?

Definicija 10.12 Naj bo $R \subseteq A \times A$ relacija. Tedaj pravimo, da je relacija $T \subseteq A \times A$ **tranzitivna ovojnica** relacije R, če velja:

1. T je tranzitivna,
2. $R \subseteq T$ in

3. če je $S \subseteq A \times A$ tranzitivna in velja $R \subseteq S$, tedaj je $T \subseteq S$.

Povedano drugače: tranzitivna ovojnica relacije R je najmanjša tranzitivna relacija, ki vsebuje R. Zaenkrat ne vemo, ali ima vsaka relacija tranzitivno ovojnico.

Izraz »ovojnica« uporabljamo, ker si lahko mislimo, da smo relacijo ovili s tranzitivno relacijo tako, da se ji slednja čim bolj prilega. Namesto »ovojnica« rečemo tudi **ogrinjača** ali **zaprtje**.

Poleg tranzitivne ovojnice lahko definiramo tudi druge ovojnice:

- **Refleksivna ovojnica** relacije $R \subseteq A \times A$ je najmanjša refleksivna relacija, ki vsebuje R.
- **Simetrična ovojnica** relacije $R \subseteq A \times A$ je najmanjša simetrična relacija, ki vsebuje R.
- **Refleksivna tranzitivna ovojnica** relacije $R \subseteq A \times A$ je najmanjša refleksivna in tranzitivna relacija, ki vsebuje R.

Ali take ovojnice sploh obstajajo? Obravnavajmo le tranzitivne ovojnice, saj so ostali dokazi zelo podobni. Ključno pri dokazu obstoja tranzitivne ovojnice je naslednje dejstvo.

Lema 10.13 *Naj bo A množica in $R : I \to P(A \times A)$ družina relacij na A. Če za vsak $i \in I$ velja, da je R_i tranzitivna relacija, potem je tudi presek $\bigcap R$ tranzitivna relacija.*

Dokaz. Iz definicije preseka družine množic (relacije so le posebne množice) sledi

$$x(\bigcap R)y \Leftrightarrow \forall i \in I \,.\, xR_iy.$$

Dokažimo, da je $\bigcap R$ tranzitivna. Naj bodo $x, y, z \in A$ in denimo, da velja $x(\bigcap R)y$ in $y(\bigcap R)z$, kar je ekvivalentno

$$\forall i \in I \,.\, xR_iy \qquad \text{in} \qquad \forall j \in I \,.\, yR_jz.$$

Dokazati moramo $x(\bigcap R)z$, kar je ekvivalentno $\forall k \in I \,.\, xR_kz$. Naj bo torej $k \in I$, dokazujemo xR_kz. Uporabimo $\forall i \in I \,.\, xR_iy$ pri $i = k$ in dobimo xR_ky. Uporabimo $\forall j \in I \,.\, yR_jz$ pri $j = k$ in dobimo yR_kz. Po predpostavki je R_k tranzitivna relacija, torej velja xR_kz. ∎

Izrek 10.14 *Vsaka relacija ima enolično tranzitivno ovojnico.*

Dokaz. Najprej premislimo, da ima R največ eno tranzitivno ovojnico: če sta S in T obe tranzitivni ovojnici R, potem iz definicije tranzitivne ovojnice sledi $S \subseteq T$ in $T \subseteq S$, torej velja $S = T$.

Sedaj pokažimo, da R ima tranzitivno ovojnico. Naj bo $R \subseteq A \times A$. Definirajmo množico relacij

$$D := \{S \subseteq A \times A \mid R \subseteq S \text{ in } S \text{ je tranzitivna}\}.$$

Trdimo, da je $\bigcap D$ tranzitivna ovojnica relacije R. Iz prejšnje leme sledi, da je $\bigcap D$ tranzitivna. Ker velja $R \subseteq S$ za vsak $S \in D$, seveda sledi $R \subseteq \bigcap D$. Če je $R \subseteq T$ in $T \subseteq A \times A$ tranzitivna relacija, tedaj velja $T \in D$, torej je $\bigcap D \subseteq T$. ∎

Po istem kopitu pokažemo, da ima vsaka relacija $R \subseteq A \times A$ tudi ostale ovojnice. Je pa zgornji izrek neroden, ker nam dokaz ne poda uporabnega opisa tranzitivne ovojnice. Povejmo, kako lahko razne ovojnice opišemo bolj eksplicitno:

1. Refleksivna ovojnica relacije R je relacija $R \cup \Delta_A$, se pravi, da relaciji R dodamo še diagonalo.
2. Simetrična ovojnica relacije R je relacija $R \cup R^{\mathsf{T}}$.
3. Tranzitivna ovojnica relacije R je relacija $R^+ := \bigcup_{n \geq 1} R^n$, se pravi
$$R^+ := R \cup (R \circ R) \cup (R \circ R \circ R) \cup \cdots$$
4. Refleksivna tranzitivna ovojnica relacije R je relacija $R^* := \bigcup_{n \geq 0} R^n$, se pravi
$$R^* := \Delta_A \cup R \cup (R \circ R) \cup (R \circ R \circ R) \cup \cdots$$

Poglavje 11

Ekvivalenčne relacije

11.1 Ekvivalenčne relacije

Definicija 11.1 Relacija $R \subseteq A \times A$ je **ekvivalenčna relacija**, če je refleksivna, tranzitivna in simetrična. Kadar velja $x \ R \ y$, pravimo, da sta x in y **ekvivalentna** glede na R.

Opomba 11.2 Kdor reče »ekvivalentna relacija«, je noob. Kdor reče, da sta »x in y ekvivalenčna«, je rookie.

Ekvivalenčne relacije se običajno označuje s simboli, ki so podobni znaku za enakost: $\equiv$, $\sim$, $\simeq$, $\cong$.

Primer 11.3 Primeri ekvivalenčnih relacij:
1. Relacija »vzporednost« med premicami v ravnini.
2. Relacija »skladnost« med trikotniki v ravnini.
3. Relacija »podobnost« med trikotniki v ravnini.
4. Relacija »isti ostanek pri deljenju s 7« na množici $\mathbb{N}$.
5. Prazna relacija $\emptyset \subseteq A \times A$ je ekvivalenčna le v primeru, da je $A = \emptyset$.
6. Polna relacija $A \times A$ je ekvivalenčna.
7. Diagonala (enakost) je ekvivalenčna relacija.

11.1.1 Ekvivalenčna relacija porojena s preslikavo

Posebej pomemben je primer ekvivalenčne relacije **porojene (ali inducirane) s preslikavo**: naj bo $f : A \to B$ preslikava in definirajmo relacijo $\sim_f$ na A s predpisom

$$x \sim_f y \Leftrightarrow f(x) = f(y)$$

Tedaj je $\sim_f$ ekvivalenčna relacija:
- refleksivnost: $x \sim_f x$ velja, ker velja $f(x) = f(x)$,
- tranzitivnost: če je $x \sim_f y$ in $y \sim_f z$, potem je $f(x) = f(y)$ in $f(y) = f(z)$, torej $f(x) = f(z)$ in $x \sim_f z$,
- simetričnost: če je $x \sim_f y$, potem je $f(x) = f(y)$, torej $f(y) = f(x)$ in $y \sim_f x$.

Ali je vsaka ekvivalenčna relacija porojena z neko preslikavo?

Primer 11.4 Premici sta vzporedni natanko tedaj, ko imata enaka smerna vektorja. Če je torej P množica vseh premic, $\mathbb{R}^2$ množica vektorjev v ravnini, in $s : P \to \mathbb{R}^2$ preslikava, ki premici P priredi njen enotski smerni vektor, ki leži v zgornji polravnini ali na pozitivnem delu osi x, tedaj velja

$$p \parallel q \Leftrightarrow s(p) = s(q).$$

Torej je vzporednost porojena s preslikavo s.

11.2 Ekvivalenčni razredi in kvocientne množice

Definicija 11.5 Naj bo $E \subseteq A \times A$ ekvivalenčna relacija. **Ekvivalenčni razred** elementa $x \in A$ je množica $[x]_E := \{y \in A \mid x \mathrel{E} y\}$. Z besedami: ekvivalenčni razred x je množica vseh elementov, ki so mu ekvivalentni.

Opomba 11.6 Kdor reče »ekvivalentni razred«, je newbie. Če pustimo šalo ob strani: ekvivalenčni razredi se tako imenujejo zaradi zgodovinskih razlogov. Beseda »razred« nakazuje dejstvo, da so imajo elementi ekvivalenčnega razredi vsi nekaj skupnega (»delavski razred«, »Tina Maze je razred zase«) in ne, da niso množice (saj očitno so).

Definicija 11.7 Naj bo $E \subseteq A \times A$ ekvivalenčna relacija. **Kvocientna ali faktorska množica** ali **kvocient** A/E je množica vseh ekvivalenčnih razredov:

$$A/E := \{\xi \in \mathcal{P}(A) \mid \exists x \in A \,.\, \xi = [x]_E\}\,.$$

Z izpeljanimi množicami lahko to zapišemo bolj razumljivo

$$A/E = \{[x]_E \mid x \in A\}\,.$$

Kanonična kvocientna preslikava $q_E : A \to A/E$ je preslikava, ki vsakemu elementu priredi njegov ekvivalenčni razred: $q_E(x) := [x]_E$.

Izrek 11.8 *Vsaka ekvivalenčna relacija je porojena z neko preslikavo.*

Dokaz. Dokažimo, da je ekvivalenčna relacija porojena s svojo kvocientno preslikavo.

Naj bo E ekvivalenčna relacija na A. Najprej ugotovimo naslednje: za vse $x, y \in A$ velja

$$x \mathrel{E} y \Leftrightarrow [x]_E = [y]_E.$$

($\Rightarrow$) Če je $x \mathrel{E} y$ potem je $[x]_E \subseteq [y]_E$, ker iz $z \mathrel{E} x$ in $x \mathrel{E} y$ sledi $z \mathrel{E} y$. Podobno dokažemo $[y]_E \subseteq [x]_E$.

($\Leftarrow$) Če je $[x]_E = [y]_E$ potem je $y \in [y]_E = [x]_E$, torej po definiciji $[x]_E$ dobimo $x \mathrel{E} y$.

Sedaj izrek sledi zlahka: $q_E(x) = q_E(y) \Leftrightarrow [x]_E = [y]_E \Leftrightarrow x \mathrel{E} y$. ∎

11.2.1 Razdelitev množice

Definicija 11.9 **Razdelitev** ali **particija** množice A je množica nepraznih, paroma disjunktnih množic, ki tvorijo pokritje A (kar pomeni, da je A enaka njihovi uniji). Se pravi, to je množica $S \subseteq \mathcal{P}(A)$, za katero velja:

1. Elementi razdelitve so neprazni: $\forall B \in S \,.\, B \neq \emptyset$.
2. Vsaka dva elementa razdelitve sta bodisi enaka bodisi disjunktna:

$$\forall B, C \in S \,.\, B = C \vee B \cap C = \emptyset.$$

3. Elementi razdelitve tvorijo pokritje A, se pravi $A = \bigcup S$.

Primer 11.10 Primeri razdelitev:

1. Navpične premice tvorijo razdelitev ravnine.
2. Množici sodih in lihih števil tvorita razdelitev naravnih števil.
3. Množica $\{\{1,2\},\{3,5\},\{4,6,7\}\}$ tvori razdelitev $\{1,2,3,4,5,6,7\}$.
4. Množica $\{\{1,2,3,4,5,6,7\}\}$ tvori razdelitev $\{1,2,3,4,5,6,7\}$.

Izrek 11.11 *Naj bo $E \subseteq A \times A$ ekvivalenčna relacija. Njeni ekvivalenčni razredi tvorijo razdelitev množice A.*

Dokaz. Dokažimo, da so ekvivalenčni razredi neprazni, paroma disjunktni in da tvorijo pokritje.

Naj bo $\xi \in \mathcal{P}(A)$ ekvivalenčni razred za E. Tedaj obstaja $x \in A$, da je $\xi = [x]_E$, torej je $x \in \xi$ in zato $\xi \neq \emptyset$.

Naj bosta $\zeta, \xi \in \mathcal{P}(A)$. Dokazali bomo $\zeta \cap \xi \neq \emptyset \Rightarrow \zeta = \xi$. Če je $x \in \zeta \cap \xi$, potem velja $\zeta \subseteq \xi$ ker: naj bo $y \in \zeta$, tedaj je $y \; E \; x$ in ker je $x \in \xi$ velja $y \in \xi$. Simetrično dokažemo $\xi \subseteq \zeta$.

Očitno je unija vseh ekvivalenčnih razredov podmnožica A, saj je vsak ekvivalenčni razred podmnožica A. Zagotovo pa je vsak $x \in A$ v kakem ekvivalenčnem razredu, namreč $x \in [x]_E$. ∎

Torej vsaka ekvivalenčna relacija na A določa razdelitev množice A, namreč na ekvivalenčne razrede. Velja pa tudi obrat: vsaka razdelitev $S \subseteq \mathcal{P}(A)$ določa ekvivalenčno relacijo na A, namreč $\simeq_S$ definiran s predpisom

$$x \simeq_S y \quad :\Longleftrightarrow \quad \exists B \in S \,.\, x \in B \wedge y \in B.$$

Z besedami: x in y sta ekvivalentna, kadar sta v istem elementu razdelitve. Pravzaprav smo ugotovili, da imamo izomorfizem množic

$$\{E \subseteq A \times A \mid E \text{ je ekvivalenčna relacija na } A\} \cong \{S \subseteq \mathcal{P}(A) \mid S \text{ je razdelitev } A\}.$$

V eno smer izomorfizem ekvivalenčni relaciji E priredi njeno razdelitev, v drugo pa razdelitvi priredimo ekvivalenčno relacijo, kakor smo to opisali zgoraj. (Premislite, da sta ti preslikavi inverza.)

11.2.2 Prerezi kvocientne preslikave in aksiom izbire

Ekvivalenčni razred je natanko določen že z enim od svojih elementov, zato pogosto želimo namesto ekvivalenčnih razredov navesti le njihove predstavnike.

Definicija 11.12 Naj bo E ekvivalenčna relacija na A. Množico $C \subseteq A$, ki vsak ekvivalenčni razred relacije E seka natanko enkrat, imenujemo **izbor predstavnikov** (ekvivalenčnih razredov) za relacijo E.

Izbor predstavnikov $C \subseteq A$ za E določa preslikavo $c : A/E \to A$, ki priredi ekvivalenčnemu razredu ξ tisti $x \in \xi$, ki je element C:

$$\begin{aligned} c &: A/E \to A \\ c &: \xi \mapsto \iota x \in \xi \,.\, x \in C \end{aligned}$$

Preslikava $c : A/E \to A$ je *prerez* kvocientne preslikave $q_E : A \to A/E$.

Izjava 11.13 *Če je $s : A/E \to A$ prerez kvocientne preslikave $q_E : A \to A/E$, potem je njegova slika $s_*(A/E) = \{c(\xi) \mid \xi \in A/E\}$ izbor predstavnikov za E.*

Dokaz. Vaja. ∎

Ker izbor predstavnikov in prerez kvocientne preslikave določata drug drugega, včasih tudi prerez imenujemo »izbor predstavnikov«.

Primer 11.14 Definirajmo $\sim$ na množici celih števil Z s predpisom

$$a \sim b \quad :\Longleftrightarrow \quad 7 \mid a - b.$$

Torej sta števili a in b ekvivalentni, če dasta enak ostanek pri deljenju s 7, na primer $13 \sim 20$ in $\neg(13 \sim 15)$. Ekvivalenčni razred števila a dobimo tako, da a prištejemo vse večkratnike števila 7:

$$[a]_\sim = \{a + 7 \cdot k \mid k \in \mathbb{Z}\}\,.$$

Na primer,

$$[13]_\sim = \{7 \cdot k + 13 \mid k \in \mathbb{Z}\} = \{\ldots, -22, -15, -8, -1, 6, 13, 20, 27, 34, 41, \ldots\}\,.$$

Koliko pa je ekvivalenčnih razredov? Toliko, kot je ostankov pri deljenju s 7, torej sedem. Množica $\{0, 1, 2, 3, 4, 5, 6\}$ je izbor predstavnikov za $\sim$, saj je vsako celo število ekvivalentno natanko enemu od teh števil po modulu 7. Ni pa to edini izbor! Tudi $\{0, 1, 2, 3, 4, 5, 13\}$ je izbor in prav tako $\{-7, -6, -5, -4, -3, -2, -1\}$.

Ali ima vsaka ekvivalenčna relacija izbor predstavnikov? Da to vprašanje ni tako enostavno, kot se zdi na prvi pogled, doma premislite o naslednji nalogi.

Naloga 11.15 Na množici realnih števil $\mathbb{R}$ definiramo relacijo E s predpisom

$$x \mathrel{E} y \quad :\Longleftrightarrow \quad x - y \in \mathbb{Q}.$$

Se pravi, da sta števili ekvivalentni, če je njuna razlika racionalno število. Podajte kak izbor predstavnikov za E.

Izrek 11.16 *Naslednje izjave so ekvivalentne:*

1. *Vsaka surjektivna preslikava ima desni inverz (prerez).*
2. *Vsaka ekvivalenčna relacija ima izbor predstavnikov.*
3. *Vsaka družina nepraznih množic ima funkcijo izbire.*
4. *Produkt družine nepraznih množic je neprazen.*

Dokaz. (1 ⇒ 2): Naj bo $E \subseteq A \times A$ ekvivalenčna relacija na A. Tedaj je $q_E : A \to A/E$ surjektivna, zato ima po predpostavki (1) prerez, ki določa izbor predstavnikov.

(2 ⇒ 3): Naj bo $A : I \to \mathsf{Set}$ družina nepraznih množic. Naj bo $\sim$ ekvivalenčna relacija na koproduktu $K := \sum_{i \in I} A_i$, porojena s prvo projekcijo $\mathsf{pr}_1 : S \to I$, t.j.,

$$\mathsf{in}_i(x) \sim \mathsf{in}_j(y) \Leftrightarrow i = j.$$

Po predpostavki (2) obstaja izbor predstavnikov za $\sim$, se pravi taka množica $C \subseteq K$, da za vsak $u \in K$ obstaja natanko en $v \in C$, da je $\mathsf{pr}_1(u) = \mathsf{pr}_1(v)$. Definirajmo $f : I \to \bigcup A$ s predpisom

$$f(i) := \iota x \in A_i \,.\, \mathsf{in}_i(x) \in C$$

Očitno je f funkcija izbire za družino A, če je izraz na desni veljaven:

- Enoličnost: iz $\mathsf{in}_i(x) \in C$ in $\mathsf{in}_i(y) \in C$ sledi $\mathsf{in}_i(x) = \mathsf{in}_j(y)$.
- Celovitost: ker je A_i neprazna, obstaja $z \in A_i$, torej obstaja $v \in C$, da je $i = \mathsf{pr}_1(\mathsf{in}_i(z)) = \mathsf{pr}_1(v)$, in je potemtakem $\mathsf{pr}_2(v) \in A_i$ element, za katerega velja $\mathsf{in}_i(\mathsf{pr}_2(v)) \in C$.

(3 ⇒ 4): Elementi produkta so funkcije izbire, zato je produkt res neprazen, če obstaja kaka funkcija izbire.

(4 ⇒ 1): Naj bo $f : X \to Y$ surjektivna. Definirajmo družino $A : Y \to \mathsf{Set}$ s predpisom $A_y = f^*(\{y\})$. Ker je f surjektivna, je A družina nepraznih množic. Po predpostavki (4) je produkt te družine neprazen, torej vsebuje neko funkcijo izbire $c : Y \to \bigcup A$, se pravi, da je $f(c(y)) = y$ za vsak $y \in Y$. Opazimo še, da je $\bigcup A = Y$, torej je c prerez f. ∎

Izbor predstavnikov je torej ekvivalenten še nekaterim drugim trditvam. Pa te veljajo? Za to potrebujemo aksiom.

Aksiom 11.17 (Aksiom izbire) *Vsaka družina nepraznih množic ima funkcijo izbire.*

Se pravi, če je $A : I \to \mathsf{Set}$ taka družina množica, da za vsak $i \in I$ velja $A_i \neq \emptyset$, tedaj obstaja $f : I \to \bigcup A$, za katerega je $f(i) \in A_i$ za vse $i \in I$. O aksiomu izbire bomo še govorili.

11.2.3 Univerzalna lastnost kvocientne množice

Naj bo E ekvivalenčna relacija na A in B množica. Pogosto želimo definirati preslikavo

$$f : A/E \to B$$

s pomočjo preslikave $A \to B$. Kdaj lahko to naredimo?

Izrek 11.18 *Naj bo E ekvivalenčna relacija na A in $g : A \to B$ preslikava, ki je* skladna *z E, kar pomeni da g slika ekvivalentne elemente v enake: $\forall x, y \in A \,.\, x \; E \; y \Rightarrow g(x) = g(y)$. Tedaj obstaja natanko ena preslikava $f : A/E \to B$, da je $f([x]_E) = g(x)$ za vse $x \in A$, ali drugače povedano, $f \circ q_E = g$.*

Dokaz. Dokažimo najprej, da imamo največ eno tako preslikavo. Denimo da za $f_1 : A/E \to B$ in $f_2 : A/E \to B$ velja $f_1 \circ q_E = f_2 \circ q_E$. Ker je q_E surjektivna, je epi in jo smemo krajšati na desni, od koder res sledi $f_1 = f_2$.

Sedaj dokažimo, da f obstaja. V ta namen naj bo $\phi \subseteq A/E \times B$ relacija

$$\phi(\xi, y) \quad :\Longleftrightarrow \quad \exists x \in A \,.\, x \in \xi \wedge g(x) = y.$$

Trdimo, da je ϕ funkcijska relacija:

- Enoličnost: če je $\phi(\xi, y_1)$ in $\phi(\xi, y_2)$, potem obstajata $x_1, x_2 \in \xi$, da je $g(x_1) = y_1$ in $g(x_2) = y_2$. Ker pa velja $x_1 \; E \; x_2$ in je g skladna z E, sledi $y_1 = g(x1) = g(x_2) = y_2$.
- Celovitost: naj bo $\xi \in A/E$. Tedaj obstaja $x \in \xi$. Očitno velja $g(\xi, g(x))$.

Naj bo $f : A/E \to B$ preslikava, ki je določena s funkcijsko relacijo ϕ. Za $x \in A$ velja $\phi([x]_E, f([x]_E))$, od tod pa iz definicije ϕ sledi tudi $g(x) = f([x]_E)$. ∎

Opomba 11.19 Profesorja prosite, da pojasni ali sem zapiše, zakaj se reče »univerzalna lastnost« kvocientne množice.

11.3 Kanonična razčlenitev preslikave

Naj bo $f : A \to B$ preslikava. Naj bo $\sim_f$ ekvivalenčna relacija na A, ki jo porodi f, in $q_f : A \to A/E$ kanonična kvocientna preslikava (morali bi jo pisati $q_{\sim_f}$, kar je nečitljivo). Naj bo $i : f_*(A) \to B$ kanonična inkluzija slike f v kodomeno. Preslikava $f : A \to f_*(A)$ je skladna s $\sim_f$, zato obstaja (natanko ena) preslikava $b_f : A/f \to f_*(A)$, da velja $b_f([x]_\sim) = f(x)$. Trdimo:

1. $f = i_f \circ b_f \circ q_f$ in
2. q_f je surjektivna, b_f je bijektivna in i_f je injektivna.

Računajmo: $f(x) = b_f([x]_\sim) = i_f(b_f([x]_\sim)) = i_f(b_f(q_f(x)))$, za vse $x \in A$, od koder sledi prva trditev.

Vemo že, da je kanonična kvocientna preslikava surjektivna in kanonična inkluzija injektivna. Ostane nam še bijektivnost preslikave b_f:

- b_f je injektivna: naj bosta $\xi, \zeta \in A/(\sim_f)$ in denimo, da velja $b_f(\xi) = b_f(\zeta)$. Obstajata $x, y \in A$, da je $\xi = [x]_\sim$ in $\zeta = [y]_\sim$. Velja

  $$f(x) = i_f(b_f(q_f(x))) = i_f(b_f(\xi)) = i_f(b_f(\zeta)) = i_f(b_f(q_f(y))) = f(y),$$

  torej je $x \sim_f y$ in zato $\xi = [x]_\sim = [y]_\sim = \zeta$.
- b_f je surjektivna: naj bo $u \in f_*(A)$. Tedaj obstaja $x \in A$, da je $u = f(x)$. Vzemimo $\xi = [x]_E$ in preverimo: $b_f(\xi) = b_f([x]_\sim) = f(x) = u$.

Poglavje 12

Relacije urejenosti

12.1 Relacije urejenosti

Definicija 12.1 Relacija $R \subseteq A \times A$ je:

1. **šibka urejenost**, ko je refleksivna in tranzitivna,
2. **delna urejenost**, ko je refleksivna, tranzitivna in antisimetrična,
3. **linearna urejenost**, ko je delna urejenost in je strogo sovisna ($\forall x, y \in A \,.\, x \; R \; y \vee y \; R \; x$).

Za relacije urejenosti ponavadi uporabljamo simbole, ki spominjajo na znak $\leq$, kot so $\preceq$, $\subseteq$, $\sqsubseteq$ ipd.

Primer 12.2 Primeri urejenosti:

1. Relacija deljivosti na naravnih številih je delna urejenost.
2. Relacija deljivosti na celih številih je šibka urejenost, ni pa delna urejenost.
3. Relacija $\leq$ na realnih številih je linearna urejenost.
4. Relacija $\subseteq$ na $\mathcal{P}(A)$ je delna urejenost. Za katere množice A je linearna?
5. Relacija $=$ je delna urejenost. Imenuje se tudi **diskretna urejenost**.

Definicija 12.3 V delni ureditvi $(P, \leq)$ je **veriga** taka podmnožica $V \subseteq P$, ki je linearno urejena z relacijo $\leq$, se pravi $\forall x, y \in V \,.\, x \leq y \vee y \leq x$. **Antiveriga** je taka podmnožica $A \subseteq P$, ki je diskretno urejena z relacijo $\leq$, se pravi $\forall x, y \in A \,.\, x \leq y \Rightarrow x = y$.

Primer 12.4

Primer 12.5 Primeri verig in antiverig:

- Če je $(P, \leq)$ linearno urejena, je vsaka njena podmnožica veriga. Na primer, vsaka podmnožica $\mathbb{N}$ je veriga glede na $\leq$.
- Potence števila 2 tvorijo verigo v $\mathbb{N}$ glede na relacijo deljivosti.
- Praštevila tvorijo antiverigo v $\mathbb{N}$ glede na relacijo deljivosti.
- V $(\mathcal{P}(\mathbb{Q}), \subseteq)$ imamo neštevno verigo $V = \{S \in \mathcal{P}(()\mathbb{Q}) \mid S \text{ je doljna množica}\}$. Množica $S \subseteq \mathbb{Q}$ je **doljna**, če velja $\forall xy \in \mathbb{Q} \,.\, x \leq y \wedge y \in \mathbb{Q} \Rightarrow x \in \mathbb{Q}$. Res, vsak Dedekindov rez je doljna množica, le-teh pa je neštevno mnogo.

12.1.1 Hassejev diagram

Končno delno ureditev $(A, \leq)$ lahko predstavimo s **Hassejevim diagramom**: elemente množice A narišemo tako, da je x pod y, kadar velja $x \leq y$. Nato povežemo vozlišči x in y, če je y neposredni naslednik x, se pravi, da velja $x \neq y$, $x \leq y$ in iz $x \leq z \leq y$ sledi $x = z \vee z = y$.

Naloga 12.6 Narišite Hassejev diagram relacije deljivosti na množici $\{0, 1, \ldots, 10\}$ ter Hassejev diagram relacije $\subseteq$ na množici $\mathcal{P}(()\{a, b, c\})$.

Naloga 12.7 Kako v Hassejevem diagramu prepoznamo verigo? In kako prepoznamo antiverigo?

12.1.2 Operacije na urejenostih

Obratna urejenost

Če je $\leq$ delna urejenost na P potem je tudi transponirana relacija $\geq$, definirana z

$$x \geq y \Leftrightarrow x \leq y,$$

delna urejenost na P. Če je $\leq$ linearna, je $\geq$ linearna.

Produktna in leksikografska urejenost

Naj bosta $(P, \leq_P)$ in $(Q, \leq_Q)$ delni urejenosti. Na kartezičnem produktu $P \times Q$ lahko definiramo dve urejenosti.

Prva je **produktna** urejenost

$$(x_1, y_1) \leq_\times (x_2, y_2) \quad :\Longleftrightarrow \quad x_1 \leq_P x_2 \wedge y_1 \leq_Q y_2$$

in druga **leksikografska** urejenost

$$(x_1, y_1) \preceq_{\text{lex}} (x_2, y_2) \quad :\Longleftrightarrow \quad (x_1 \neq x_2 \wedge x_1 \leq_P x_2) \vee (x_1 = x_2 \wedge y_1 \leq_Q y_2).$$

Naloga 12.8 Kako si predstavljamo produktno in leksikografsko ureditev na $[0, 1] \times [0, 1]$, če $[0, 1]$ uredimo z običajno relacijo $\leq$? Na sliki označite območji

$$\{(x, y) \in [0, 1] \times [0, 1] \mid (1/2, 1/3) \leq_\times (x, y)\}$$

in

$$\{(x, y) \in [0, 1] \times [0, 1] \mid (1/2, 1/3) \leq_{\text{lex}} (x, y)\}.$$

Izjava 12.9 *Produktna in leksikografska urejenosti sta delni urejenosti. Leksikografska urejenost linearnih urejenosti je linearna.*

Dokaz. Dejstvo, da je produktna urejenost refleksivna, tranzitivna in antisimetrična, pustimo za vajo. Preverimo, da je leksikografska urejenost $\leq_{\text{lex}}$ delna urejenost.

Dokaz, da je $\leq_{\text{lex}}$ je refleksivna: za vsak $(x, y) \in P \times Q$ velja $x = x \wedge y \sqsubseteq y$, torej velja $(x, y) \sqsubseteq (x, y)$.

Dokaz, da je $\leq_{\text{lex}}$ je antisimetrična: naj bosta $(x_1, y_1), (x_2, y_2) \in P \times Q$ in denimo, da velja

$$(x_1, y_1) \leq_{\text{lex}} (x_2, y_2) \wedge (x_2, y_2) \leq_{\text{lex}} (x_1, y_1)$$

To je ekvivalentno

$$\begin{aligned}
&(x_1 \neq x_2 \wedge x_1 \leq_P x_2 \wedge x_2 \neq x_1 \wedge x_2 \leq_P x_1) \vee \\
&(x_1 \neq x_2 \wedge x_1 \leq_P x_2 \wedge x_2 = x_1 \wedge y_2 \leq_Q y_1) \vee \\
&(x_1 = x_2 \wedge y_1 \leq_Q y_2 \wedge x_2 \neq x_1 \wedge x_2 \leq_P x_1) \vee \\
&(x_1 = x_2 \wedge y_1 \leq_Q y_2 \wedge x_2 = x_1 \wedge y_2 \leq_Q y_1).
\end{aligned}$$

Če v zgornji formuli upoštevamo, da je $x_1 \neq x_2 \wedge x_1 = x_2$, vidimo, da sta drugi in tretji disjunkt ekvivalentna $\bot$, zato je izjava ekvivalentna:

$$\begin{aligned}
&(x_1 \neq x_2 \wedge x_1 \leq_P x_2 \wedge x_2 \neq x_1 \wedge x_2 \leq_P x_1) \vee \\
&(x_1 = x_2 \wedge y_1 \leq_Q y_2 \wedge x_2 = x_1 \wedge y_2 \leq_Q y_1).
\end{aligned}$$

A tudi prvi disjunkt je ekvivalenten $\bot$, ker iz $x_1 \leq_P x_2 \wedge x_2 \leq_P x_1$ sledi $x_1 = x_2$, saj je $\leq_P$ po predpostavki antisimetrična. Torej ostane samo zadnji disjunkt, ki je ekvivalenten

$$x_1 = x_2 \wedge y_1 \leq_Q y_2 \wedge y_2 \leq_Q y_1.$$

Ker je $\leq_Q$ antisimetrična, sledi $x_1 = x_2$ in $y_1 = y_2$, kar smo želeli dokazati.

Dokaz, da je $\leq_{\text{lex}}$ tranzitivna: naj bodo $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in P \times Q$ in denimo, da velja

$$(x_1, y_1) \leq_{\text{lex}} (x_2, y_2) \wedge (x_2, y_2) \leq_{\text{lex}} (x_3, y_3).$$

To je ekvivalentno

$$\begin{aligned}
&(x_1 \neq x_2 \wedge x_1 \leq_P x_2 \wedge x_2 \neq x_3 \wedge x_2 \leq_P x_3) \vee \\
&(x_1 \neq x_2 \wedge x_1 \leq_P x_2 \wedge x_2 = x_3 \wedge y_2 \leq_Q y_3) \vee \\
&(x_1 = x_2 \wedge y_1 \leq_Q y_2 \wedge x_2 \neq x_3 \wedge x_2 \leq_P x_3) \vee \\
&(x_1 = x_2 \wedge y_1 \leq_Q y_2 \wedge x_2 = x_3 \wedge y_2 \leq_Q y_3)
\end{aligned}$$

Obravnavajmo štiri primere in v vsakem od njih dokažimo $(x_1, y_1) \leq_{\text{lex}} (x_3, y_3)$, se pravi $(x_1 \neq x_3 \wedge x_1 \leq_P x_3) \vee (x_1 = x_3 \wedge y_1 \leq_Q y_3)$:

1. Če velja $x_1 \neq x_2 \wedge x_1 \leq_P x_2 \wedge x_2 \neq x_3 \wedge x_2 \leq_P x_3$: ker je $\leq$ tranzitivna sledi $x_1 \leq_P x_3$, poleg tega pa velja $x_1 \neq x_3$: če bi veljalo $x_1 = x_3$, bi iz predpostavk dobili $x_3 \leq_P x_2 \wedge x_2 \leq_P x_3$, od koder bi sledilo $x_2 = x_3$, kar je v protislovju s predpostavko $x_2 \neq x_3$.
2. Če velja $x_1 \neq x_2 \wedge x_1 \leq_P x_2 \wedge x_2 = x_3 \wedge y_2 \leq_Q y_3$: ker je $x_2 = x_3$ iz prvih dveh predpostavk sledi $x_1 \neq x_3 \wedge x_1 \leq_P x_3$.
3. Če velja $x_1 = x_2 \wedge y_1 \leq_Q y_2 \wedge x_2 \neq x_3 \wedge x_2 \leq_P x_3$: ker je $x_1 = x_2$ iz zadnjih dveh predpostavk sledi $x_1 \neq x_3 \wedge x_1 \leq_P x_3$.

4. Če velja $x_1 = x_2 \wedge y_1 \leq_Q y_2 \wedge x_2 = x_3 \wedge y_2 \leq_Q y_3$: torej je $x_1 = x_3$ ker je $=$ tranzitivna in $y_1 \leq_Q y_3$ ker je $\leq_Q$ tranzitivna.

Nazadnje preverimo še, da je $\leq_{\text{lex}}$ linearna, če sta $\leq$ in $\leq_Q$ linearni. Naj bosta $(x_1, y_1), (x_2, y_2) \in P \times Q$. Dokazati želimo

$$(x_1, y_1) \preceq (x_2, y_2) \vee (x_2, y_2) \preceq (x_1, y_1).$$

To je ekvivalentno disjunkciji

$$\begin{aligned}
&(x_1 \neq x_2 \wedge x_1 \leq_P x_2) \vee \\
&(x_1 = x_2 \wedge y_1 \leq_Q y_2) \vee \\
&(x_2 \neq x_1 \wedge x_2 \leq_P x_1) \vee \\
&(x_2 = x_1 \wedge y_2 \leq_Q y_1),
\end{aligned}$$

kar je ekvivalentno

$$\begin{aligned}
&(x_1 \neq x_2 \wedge (x_1 \leq_P x_2 \vee x_2 \leq_P x_1)) \vee \\
&(x_1 = x_2 \wedge (y_1 \leq_Q y_2 \vee y_2 \leq_Q y_1)).
\end{aligned}$$

Ker sta $\leq_P$ in $\leq_Q$ linearni, je to ekvivalentno

$$(x_1 \neq x_2 \wedge \top) \vee (x_1 = x_2 \wedge \top),$$

kar je ekvivalentno

$$(x_1 \neq x_2) \vee (x_1 = x_2).$$

To pa drži po zakonu o izključeni tretji možnosti. S tem je linearnost $\leq_{\text{lex}}$, dokazana. ∎

Vsota urejenosti

Naj bosta $(P, \leq_P)$ in $(Q, \leq_Q)$ delni urejenosti. Na vsoti $P + Q$ lahko definiramo urejenost $\leq_+$ s predpisom:

$$\begin{aligned}
u \leq_+ v \quad :\Longleftrightarrow \quad &(\exists x, y \in P \,.\, u = \mathsf{in}_1(x) \wedge v = \mathsf{in}_1(y) \wedge x \leq_P y) \vee \\
&(\exists s, t \in Q \,.\, u = \mathsf{in}_2(s) \wedge v = \mathsf{in}_2(t) \wedge s \leq_Q t).
\end{aligned}$$

Zaporedna vsota urejenosti

Naj bosta $(P, \leq_P)$ in $(Q, \leq_Q)$ delni urejenosti. Na vsoti $P + Q$ lahko definiramo urejenost $\leq_\rightarrow$ s predpisom:

$$\begin{aligned}
u \leq_\rightarrow v \quad :\Longleftrightarrow \quad &(\exists x, y \in P \,.\, u = \mathsf{in}_1(x) \wedge v = \mathsf{in}_1(y) \wedge x \leq_P y) \vee \\
&(\exists x \in P \,.\, \exists s \in Q \,.\, u = \mathsf{in}_1(x) \wedge v = \mathsf{in}_2(s)) \vee \\
&(\exists s, t \in Q \,.\, u = \mathsf{in}_2(s) \wedge v = \mathsf{in}_2(t) \wedge s \leq_Q t).
\end{aligned}$$

Torej so vsi elementi P pred vsemi elementi Q. Zaporedna vsota linearnih urejenosti je linearna.

Potenca urejenosti

Naj bo $(P, \leq)$ delna urejenost in A množica. Na eksponentni množici P^A lahko definiramo urejenost $\preceq$ s predpisom:

$$f \preceq g \quad :\Longleftrightarrow \quad \forall x \in A \,.\, f(x) \leq g(x).$$

Naloga 12.10 Ali je $\preceq$ linearna, kadar je $\leq$ linearna?

Delna urejenost, inducirana s šibko ureditvijo

Naj bo $(P, \leq)$ šibka ureditev. Relacija $\sim$ na P, definirana s predpisom

$$x \sim y \quad :\Longleftrightarrow \quad x \leq y \wedge y \leq x,$$

je ekvivalenčna relacija. Na kvocientu $P/\!\sim$ lahko definiramo relacijo $\preceq$ s predpisom

$$[x] \preceq [y] \quad :\Longleftrightarrow \quad x \leq y.$$

Treba je preveriti, da je relacija dobro definirana, saj smo uporabili predstavnike ekvivalenčnih razredov. Se pravi, ali velja

$$x \sim x' \wedge y \sim y' \Rightarrow (x \leq y \Leftrightarrow x' \leq y')?$$

Pa preverimo. Denimo, da velja $x, y, x', y' \in P$ in $x \sim x'$ in $y \sim y'$. Torej velja

$$x \leq x' \wedge x' \leq x \wedge y \leq y' \wedge y' \wedge x.$$

Sedaj dokažimo $x \leq y \Leftrightarrow x' \leq y'$:

1. Če velja $x \leq y$ potem $x' \leq x \leq y \leq y'$.
2. Če velja $x' \leq y'$, potem $x \leq x' \leq y' \leq y$.

Torej je $\preceq$ dobro definirana.

Izjava 12.11 *Relacija, ki je inducirana s šibko ureditvijo, je delna ureditev.*

Dokaz. Refleksivnost in tranzitivnost $\preceq$ sledita iz refleksivnosti in tranzitivnosti $\leq$. Preverimo antisimetričnost: denimo, da velja $[x] \leq [y]$ in $[y] \leq [x]$. Tedaj velja $x \leq y$ in $y \leq x$, torej velja $x \sim y$ in $[x] = [y]$. ∎

Primer 12.12 Obravnavajmo cela števila $\mathbb{Z}$ in deljivost $|$, ki je šibka ureditev. Za vse $k, m \in \mathbb{Z}$ velja

$$k \sim m \Leftrightarrow k \mid m \wedge m \mid k \Leftrightarrow |k| = |m|.$$

Torej je $\mathbb{Z}/\!\sim \cong \mathbb{N}$, kjer izomorfizem preslika $[k] \mapsto |k|$. Delna ureditev na $\mathbb{Z}/\!\sim$ inducirana z deljivostjo je spet deljivost (ko jo prenesemo iz $\mathbb{Z}/\!\sim$ na $\mathbb{N}$ s pomočjo izomorfizma).

12.1.3 Monotone preslikave

Definicija 12.13 Preslikava $f : P \to Q$ med delnima urejenostma $(P, \leq_P)$ in $(Q, \leq_Q)$ je **monotona** (ali **naraščajoča**), ko velja $\forall x, y \in P \,.\, x \leq_P y \Rightarrow f(x) \leq_Q f(y)$.

Definicija 12.14 Preslikava $f : P \to Q$ med delnima urejenostma $(P, \leq_P)$ in $(Q, \leq_Q)$ je **antitona** (ali **padajoča**), ko velja $\forall x, y \in P \,.\, x \leq_P y \Rightarrow f(y) \leq_Q f(x)$.

Opomba 12.15 V analizi »monotona« pomeni »monotona ali antitona". To ni nič čudnega, ker »dan« tudi pomeni »dan in noč».

Izrek 12.16 *Kompozicija monotonih preslikav je monotona. Identiteta je monotona.*

Dokaz. Naj bosta $f : P \to Q$ in $g : Q \to R$ monotoni preslikavi med delnimi urejenostmi $(P, \leq_P)$, $(Q, \leq_Q)$ in $(R, \leq_R)$. Če je $x \leq_P y$, potem je zaradi monotonosti f tudi $f(x) \leq_Q f(y)$, nato pa je zaradi monotonosti g spet $g(f(x)) \leq_R g(f(y))$. Identiteta je očitno monotona. ∎

Primer 12.17 Primeri monotonih preslikav:
1. Konstantna preslikava je monotona.
2. Seštevanje $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ je monotona operacija glede na produktno ureditev na $\mathbb{R} \times \mathbb{R}$.
3. Množenje $\times : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ ni monotona operacija.

12.1.4 Meje

Definicija 12.18 Naj bo $(P, \leq)$ delna urejenost, $S \subseteq P$ in $x \in P$:
- x je **spodnja meja** podmnožice S, ko velja $\forall y \in S \,.\, x \leq y$,
- x je **zgornja meja** podmnožice S, ko velja $\forall y \in S \,.\, y \leq x$,
- x je **infimum** ali **največja spodnja meja** ali **natančna spodnja meja** podmnožice S, ko je spodnja meja S in velja: za vse $y \in P$, če je y spodnja meja S, potem je $y \leq x$,
- x je **supremum** ali **najmanjša zgornja meja** ali **natančna zgornja meja** podmnožice S, ko je zgornja meja S in velja: za vse $y \in P$, če je y zgornja meja S, potem je $x \leq y$,
- x je **minimalni element** podmnožice S, ko velja $x \in S$ in $\forall y \in S \,.\, y \leq x \Rightarrow x = y$,
- x je **maksimalni element** podmnožice S, ko velja $x \in s$ in $\forall x \in S \,.\, x \leq y \Rightarrow x = y$,
- x je **najmanjši** ali **prvi** element ali **minimum** podmnožice S, ko velja $x \in S$ in $\forall y \in S \,.\, x \leq y$,
- x je **največji** ali **zadnji** element ali **maksimum** podmnožice S, ko velja $x \in S$ in $\forall y \in S \,.\, y \leq x$.

Opomba 12.19 Minimalni element ni isto kot minimum (in maksimalni element ni isto kot maksimum).

Kadar govorimo o »prvem elementu« ali »maksimalnem elementu« in ne povemo, na katero podmnožico se nanaša element, imamo običajno v mislih kar celotno delno ureditev.

Izrek 12.20 *Naj bo $(P, \leq)$ delna urejenost in $S \subseteq P$. Tedaj ima S največ en infimum in največ en supremum, ki ju zapišemo* $\inf S$ *ter* $\sup S$*, kadar obstajata.*

Dokaz. Denimo, da sta x in y oba infimum S. Ker je y spodnja meja za S in x njen infimum, velja $y \leq x$. Podobno velja $x \leq y$, torej $x = y$. Za supremum je dokaz podoben. ∎

Primer 12.21 Supremum končne neprazne množice $S \subseteq \mathbb{N}$ za relacijo deljivosti $|$ je najmanjši skupni večkratnik elementov iz S. Infimum je največji skupni delitelj. Kaj pa, če je S prazna ali neskončna?

12.1.5 Mreže

Definicija 12.22 Naj bo $(P, \leq)$ delna urejenost:

1. $(P, \leq)$ je **mreža**, ko imata vsaka dva elementa $x, y \in P$ infimum in supremum.
2. $(P, \leq)$ je **omejena mreža**, ko ima vsaka končna podmnožica P infimum in supremum.
3. $(P, \leq)$ je **polna mreža**, ko ima vsaka podmnožica P infimum in supremum.

Infimum in supremum elementov x in y pišemo $x \wedge y$ in $x \vee y$.

Izrek 12.23 *Delna urejenost $(P, \leq)$ je omejena mreža natanko tedaj, ko ima najmanjši element in največji element, ter imata vsaka sva elementa infimum in supremum.*

Dokaz. Denimo, da je $(P, \leq)$ omejena mreža. Tedaj P ima najmanjši element, namreč $\sup \emptyset$, in največji element, namreč $\inf \emptyset$. Infimum in supremum x in y sta seveda $\inf \{x, y\}$ in $\sup \{x, y\}$.

Denimo, da ima P najmanjši element $\bot_P$ in največji element $\top_P$, vsaka dva elementa pa imata infimum in supremum. Naj bo $S \subseteq P$ končna množica:

1. če je $S = \emptyset$, potem je $\inf S = \top_P$ in $\sup S = \bot_P$,
2. če je $S = \{x_1, \ldots, x_n\}$ za $n > 0$, potem je $\inf S = \inf \{x_1, \ldots, x_{n-1}\} \vee x_n$ in $\sup S = \sup \{x_1, \ldots, x_{n-1}\} \vee x_n$.

∎

Primer 12.24 Primeri mrež:

1. Množica $\mathbb{2} = \{\bot, \top\}$ je omejena mreža za relacijo $\Rightarrow$.
2. Relacija deljivosti na množici pozitivnih naravnih števil je omejena mreža.
3. Potenčna množica $\mathcal{P}(A)$, urejena z $\subseteq$, je polna mreža.
4. Zaprti interval $[a, b]$, urejen z $\leq$, je polna mreža.
5. Realna števila R, urejena z $\leq$,

Poglavje 13

Indukcija in dobra osnovanost

13.1 Dobra osnovanost

13.1.1 Indukcija na naravnih številih

Poznamo že indukcijo na naravnih številih. Zapišemo jo lahko na dva načina, kjer naslednika števila n označimo n^+:

1. Kot aksiom o predikatih na naravnih številih:

$$\phi(0) \land (\forall n \in \mathbb{N} \,.\, \phi(n) \Rightarrow \phi(n^+)) \Rightarrow \forall m \in \mathbb{N} \,.\, \phi(m)$$

2. Kot lastnost podmnožic naravnih števil:

$$\forall S \in \mathcal{P}(\mathbb{N}) \,.\, 0 \in S \land (\forall k \in \mathbb{N} \,.\, k \in S \Rightarrow k^+ \in S) \Rightarrow S = \mathbb{N}$$

Uporabljali bomo verzijo s podmnožicami. Najprej jo predelajmo v ekvivalentno obliko:

$$\begin{aligned}
&\forall S \in \mathcal{P}(\mathbb{N}) \,.\, 0 \in S \land (\forall k \in \mathbb{N} \,.\, k \in S \Rightarrow k^+ \in S) \Rightarrow S = \mathbb{N} && (\Leftrightarrow)\\
&\forall S \in \mathcal{P}(\mathbb{N}) \,.\, 0 \in S \land (\forall m \in \mathbb{N} \,.\, (\forall k \in \mathbb{N} \,.\, k^+ = m \Rightarrow k \in S) \Rightarrow m \in S) \Rightarrow S = \mathbb{N} && (\Leftrightarrow)\\
&\forall S \in \mathcal{P}(\mathbb{N}) \,.\, (\forall m \in \mathbb{N} \,.\, (\forall k \in \mathbb{N} \,.\, k^+ = m \Rightarrow k \in S) \Rightarrow m \in S) \Rightarrow S = \mathbb{N}.
\end{aligned}$$

Kaj smo dosegli? Bazo indukcije in indukcijski korak smo združili v eno samo predpostavko

$$\forall m \in \mathbb{N} \,.\, (\forall k \in \mathbb{N} \,.\, k^+ = m \Rightarrow k \in S) \Rightarrow m \in S \tag{13.1}$$

Če vstavimo $m := 0$, dobimo:

$$\begin{aligned}
&(\forall k \in \mathbb{N} \,.\, k^+ = 0 \Rightarrow k \in S) \Rightarrow 0 \in S && (\Leftrightarrow)\\
&(\forall k \in \mathbb{N} \,.\, \bot \Rightarrow k \in S) \Rightarrow 0 \in S && (\Leftrightarrow)\\
&(\forall k \in \mathbb{N} \,.\, \top) \Rightarrow 0 \in S && (\Leftrightarrow)\\
&\top \Rightarrow 0 \in S && (\Leftrightarrow)\\
&0 \in S
\end{aligned}$$

Če vstavimo $m := n^+$ dobimo:

$$\begin{aligned}
&(\forall k \in \mathbb{N} \,.\, k^+ = n^+ \Rightarrow k \in S) \Rightarrow n^+ \in S && (\Leftrightarrow)\\
&(\forall k \in \mathbb{N} \,.\, k = n \Rightarrow k \in S) \Rightarrow n^+ \in S && (\Leftrightarrow)\\
&n \in S \Rightarrow n^+ \in S
\end{aligned}$$

To pa sta ravno običajna pogoja za indukcijo.

Ali lahko izrazimo indukcijo na naravnih številih tudi brez operacije naslednik? Da, s pomočjo relacije $<$:

$$\forall S \in \mathcal{P}(\mathbb{N}) \,.\, (\forall m \in \mathbb{N} \,.\, (\forall k \in \mathbb{N} \,.\, k < m \Rightarrow k \in S) \Rightarrow m \in S) \Rightarrow S = \mathbb{N}$$

Temu principu pravimo tudi **krepka indukcija**, z besedami jo povemo takole: za podmnožico $S \subseteq \mathbb{N}$ velja $S = \mathbb{N}$, če za vse $m \in \mathbb{N}$ velja »če so vsa števila manjša od m v S, potem je tudi m v S«.

Denimo, da S res ima dano lastnost. Ali je $0 \in S$? Da, ker za vse predhodnike 0 velja, da so S (saj jih ni). Ali je $1 \in S$? Da, saj za vse predhodnike 1 velja, da so v S. Ali je $2 \in S$? Da, saj za vse predhodnike 2 velja, da so v S. In tako naprej.

13.1.2 Dobra osnovanost

Princip indukcije na naravnih številih posplošimo, pri čemer izhajamo iz principa indukcije, izraženega s pomočjo lastnosti (13.1), v kateri relacijo »neposredni predhodnik« nadomestimo s splošno relacijo.

Definicija 13.1 Relacija $R \subseteq A \times A$ je **dobro osnovana**, kadar velja

$$\forall S \in P(A) \,.\, (\forall y \in A \,.\, (\forall x \in A \,.\, x \mathrel{R} y \Rightarrow x \in S) \Rightarrow y \in S) \Rightarrow S = A. \tag{13.2}$$

Množici $S \subseteq A$, ki zadošča pogoju

$$\forall y \in A \,.\, (\forall x \in A \,.\, x \mathrel{R} y \Rightarrow x \in S) \Rightarrow y \in S$$

pravimo R**-progresivna** množica ali, da je S **progresivna za** R.

Pogoj (13.2) je *indukcijski predpis* za dobro osnovano relacijo R. Nekatere relacije temu predpisu zadoščajo in druge ne. Na primer, relacija »neposredni predhodnik« na $\mathbb{N}$ mu zadošča, saj v tem primeru dobimo običajno indukcijo na $\mathbb{N}$.

Primer 13.2 Preverimo, da je relacija »neposredni predhodnik« P na množici $A = \{0, 1, \ldots, 42\}$ dobro osnovana. Natančneje, govorimo o relaciji

$$m \mathrel{P} n \quad :\Longleftrightarrow \quad m + 1 = n.$$

Naj bo $S \subseteq A$ progresivna množica, torej zadošča

$$\forall y \in A \,.\, (\forall x \in A \,.\, x + 1 = y \Rightarrow x \in S) \Rightarrow y \in S.$$

Če vstavimo $y = 0$, dobimo

$$(\forall x \in A \,.\, x + 1 = 0 \Rightarrow x \in S) \Rightarrow 0 \in S,$$

kar je ekvivalentno $0 \in S$. Torej je $0 \in S$. Nato vstavimo $y = 1$ in dobimo

$$(\forall x \in A \,.\, x + 1 = 1 \Rightarrow x \in S) \Rightarrow 1 \in S,$$

kar se poenostavi v $0 \in S \Rightarrow 1 \in S$. Ker smo že dokazali $0 \in S$, sledi tudi $1 \in S$. V naslednjem koraku vstavimo $y = 2$, poenostavimo in dobimo $1 \in S \Rightarrow 2 \in S$, torej $2 \in S$. Tako nadaljujemo do $y = 42$ in ugotovimo, da res velja $S = A$. S tem smo pokazali, da je P dobro osnovana. Seveda ni bistveno, da smo uporabili 42.

13.1.3 Dvojiška drevesa

Naravna števila $\mathbb{N}$ so **induktivno definirana množica**. To pomeni, da elemente $\mathbb{N}$ opredelimo s pravili, ki povedo, kako se gradi naravna števila:

- $0 \in \mathbb{N}$,
- če je $n \in \mathbb{N}$, potem je $n^+ \in \mathbb{N}$.

Množica $\mathbb{N}$ vsebuje natanko tiste elemente, ki jih lahko zgradimo s pomočjo teh pravil:

$$0, 0^+, 0^{++}, 0^{+++}, 0^{++++}, \ldots$$

Tu sta 0 in $^+$ mišljena kot simbolni oznaki, podobno kot in_1 in in_2 v definiciji vsote množic. Dejstvo, da $\mathbb{N}$ vsebuje natanko tiste elemente, ki jih lahko zgradimo s pomočjo 0 in $^+$ ni nič drugega kot indukcija na $\mathbb{N}$.

Podobno lahko definiramo tudi druge induktivne množice, ki tudi zadoščajo principu indukcije. Na primer, **dvojiška drevesa** so induktivno definirana množica Tree s predpisoma:

- $\mathsf{empty} \in \mathsf{Tree}$,
- če je $t_1 \in \mathsf{Tree}$ in $t_2 \in \mathsf{Tree}$, potem je $\mathsf{tree}(t_1, t_2) \in \mathsf{Tree}$

Z besedami: drevo je bodisi prazno, bodisi je sestavljeno iz dveh **poddreves**. Ali znamo našteti vsa drevesa, ali še bolje, jih narisati?

$$\begin{aligned}
&\mathsf{empty},\\
&\mathsf{tree}(\mathsf{empty}, \mathsf{empty})\\
&\mathsf{tree}(\mathsf{empty}, \mathsf{tree}(\mathsf{empty}, \mathsf{empty})),\\
&\mathsf{tree}(\mathsf{tree}(\mathsf{empty}, \mathsf{empty}), \mathsf{empty}),\\
&\mathsf{tree}(\mathsf{tree}(\mathsf{empty}, \mathsf{empty}), \mathsf{tree}(\mathsf{empty}, \mathsf{empty})),\\
&\vdots
\end{aligned}$$

Definirajmo relacijo $R \subseteq \mathsf{Tree} \times \mathsf{Tree}$ s predpisom:

$$t \; R \; s \quad :\Longleftrightarrow \quad \exists u \in \mathsf{Tree} \,.\, s = \mathsf{tree}(t, u) \vee s = \mathsf{tree}(u, t).$$

To je relacija »neposredno poddrevo«. Je dobro osnovana, česar ne bomo dokazali, porodi pa naslednji princip indukcije za dvojiška drevesa.

Izjava 13.3 (Indukcija za dvojiška drevesa) *Naj bo $S \subseteq \mathsf{Tree}$ podmnožica dreves, za katero velja:*

- *prazno drevo je v S,*
- *za vsa drevesa t_1 in t_2 velja: če je $t_1 \in S$ in $t_2 \in S$, potem je $\mathsf{tree}(t_1, t_2) \in S$.*

Tedaj je $S = \mathsf{Tree}$.

Princip povejmo še s pomočjo predikatov.

Izjava 13.4 (Indukcija za dvojiška drevesa) *Naj bo ϕ predikat na dvojiških drevesih, za katerega velja:*

- *baza indukcije: $\phi(\mathsf{empty})$*
- *indukcijski korak: za vsa drevesa t_1 in t_2, če velja $\phi(t_1)$ in $\phi(t_2)$, potem $\phi(\mathsf{tree}(t_1, t_2))$.*

Tedaj $\forall t \in \mathsf{Tree} \,.\, \phi(t)$.

Kot vidimo, imamo v indukcijskem koraku *dve* indukcijski predpostavki, ker ima vsako sestavljeno drevo dve poddrevesi.

Dobra osnovanost in padajoče verige

Kako pa bi dobili kak proti-primer, se pravi, relacijo, ki ni dobra osnovanost? Poiskati moramo kako lastnost, ki jo imajo vse dobre osnovanosti, nato pa relacijo, ki te lastnosti nima.

Definicija 13.5 Naj bo $R \subseteq A \times A$ relacija na A. **Padajoča veriga** za relacijo R je zaporedje $a : \mathbb{N} \to A$, za katerega velja $\forall i \in \mathbb{N} \,.\, a(i+1)\ R\ a(i)$.

Se pravi, da je padajoča veriga zaporedje, za katerega velja

$$\cdots a_4\ R\ a_3\ R\ a_2\ R\ a_1\ R\ a_0$$

Cikel za relacijo R je končna podmnožica $\{a_0, \ldots, a_n\} \subseteq A$ da velja

$$a_0\ R\ a_1\ R \cdots R\ a_n\ R\ a_0.$$

Iz cikla dobimo padajočo verigo, tako da cikel ponavljamo v nedogled:

$$\cdots R\ a_0\ R \cdots R\ a_n\ R\ a_0\ R \cdots R\ a_n\ R\ a_0.$$

Lema 13.6 *V dobri osnovanosti ni ciklov in ni padajočih verig.*

Dokaz. Dovolj je pokazati, da ni padajočih verig, saj iz cikla dobimo padajočo verigo. Denimo, da je $a : \mathbb{N} \to A$ padajoča veriga za $R \subseteq A \times A$. Dokazali bomo, da R ni dobro osnovana. Se pravi, da moramo poiskati R-progresivno podmnožico $S \subseteq A$, za katero velja $S \neq A$. Vzemimo $S := A \setminus \{a(i) \mid i \in \mathbb{N}\}$. Očitno velja $S \neq A$, saj $a(0) \notin S$. Preverimo, da je S progresivna, se pravi, da je

$$\forall y \in A \,.\, (\forall x \in A \,.\, x\ R\ y \Rightarrow x \in S) \Rightarrow y \in S.$$

Naj bo $y \in A$ in denimo, da velja

$$\forall x \in A \,.\, x\ R\ y \Rightarrow x \in S \tag{13.3}$$

Dokazati moramo $y \in S$. Obravnavamo dve možnosti:

- če $y \in S$, potem seveda sledi $y \in S$.
- če $y \notin S$, potem obstaja $i \in \mathbb{N}$, da je $y = a(i)$. Ker je $a(i+1)\ R\ a(i)$, iz predpostavke (13.3) sledi $y = a(i) \in S$.

Torej v vsakem primeru velja $y \in S$. ∎

Primer 13.7 Sedaj lahko zlahka priskrbimo kak proti-primer. Na primer, cela števila $\mathbb{Z}$ z relacijo $R \subseteq \mathbb{Z} \times \mathbb{Z}$

$$a\ R\ b \quad :\Longleftrightarrow \quad a + 1 = b$$

niso dobro osnovana, ker imajo padajočo verigo

$$\cdots R\ (-3)\ R\ (-2)\ R\ (-1)\ R\ 0$$

Prav tako ni dobro osnovana relacija $<$ na intervalu $[0, 1]$, ker imamo padajočo verigo $n \mapsto 2^{-n}$.

13.2 Dobra urejenost

Posplošimo sedaj še krepko indukcijo na naravnih številih. Tokrat bomo najprej posplošili strogo urejenost $<$.

13.2.1 Stroge urejenosti

Definicija 13.8 Relacija $R \subseteq A \times A$ je **stroga urejenost**, če je
- irefleksivna: $\forall x \in A \,.\, \neg(x \; R \; x)$ in
- tranzitivna: $\forall x, y, z \in A \,.\, x \; R \; y \wedge y \; R \; z \Rightarrow x \; R \; z$.

Stroga urejenost je **linearna**, če je še
- sovisna: $\forall x, y \in A \,.\, x \; R \; y \vee x = y \vee y \; R \; x$.

Za stroge urejenosti uporabljamo simbole $<$, $\subset$, $\prec$, $\sqsubset$ ipd.

Relaciji $<$ in $\leq$ na številih sta med seboj povezani, saj denimo za realna števila velja

$$x < y \iff x \leq y \wedge x \neq y$$

in

$$x \leq y \iff x < y \vee x = y \tag{13.4}$$

To velja v splošnem. Stroga urejenost $<$ na množici A porodi delno urejenost $\leq$ na A, definirano s predpisom:

$$x \leq y \quad :\iff \quad x = y \vee x < y.$$

V obratno smer, delna urejenost $\sqsubseteq$ določa strogo urejenost $\sqsubset$, definirano s predpisom

$$a \sqsubset b \quad :\iff \quad a \neq b \wedge a \sqsubseteq b. \tag{13.5}$$

Seveda je treba preveriti naslednja dejstva, ki jih pustimo za vajo:
- če je $<$ stroga urejenost, potem je $\leq$ definirana s (13.4) delna urejenost
- če je $\sqsubseteq$ delna urejenost, potem je $\sqsubset$ definirana s (13.5) stroga urejenost.

Tako lahko prehajamo med delno in strogo urejenostjo.

13.2.2 Dobra ureditev

Definicija 13.9 Relacija je **dobra ureditev**, če je dobro osnovana in stroga linearna ureditev.

Izrek 13.10 *Relacija je dobra ureditev natanko tedaj, ko je dobro osnovana in sovisna.*

Dokaz. V eno smer je ekvivalenca očitna, zato dokažimo samo obratno smer. Denimo, da je $R \subseteq A \times A$ dobro osnovana in sovisna relacija. Dokazujemo, da je dobra ureditev, se pravi, da potrebujemo še irefleksivnost in tranzitivnost R.

Relacija R je irefleksivna: če bi veljalo $x \; R \; x$ za $x \in A$, potem R ne bi bila dobro osnovana, ker bi vsebovala padajočo verigo $\cdots x \; R \; x \; R \; x$.

Relacija R je tranzitivna: denimo, da velja $x \; R \; y$ in $y \; R \; z$. Dokazujemo $x \; R \; z$. Ker je R sovisna, velja $x \; R \; z$ ali $x = z$ ali $z \; R \; x$. Pokažimo, da $x = z$ in $z \; R \; x$ nista možna:
- Če je $x = z$, potem velja $x \; R \; y$ in $y \; R \; x$, torej x in y tvorita cikel, a R je dobro osnovana, zato to ni možno.
- Če velja $z \; R \; x$, potem dobimo cikel $x \; R \; y \; R \; z \; R \; x$, kar spet ni možno.

∎

Lema 13.11 *Denimo, da je $<$ stroga urejenost na neprazni množici B. Če B nima $\leq$-minimalnega elementa, potem ima padajočo verigo.*

Dokaz. Denimo, da B nima minimalnega elementa, torej

$$\neg\exists x \in B\,.\,\forall y \in B\,.\,y \leq x \Rightarrow y = x.$$

To je ekvivalentno

$$\forall x \in B\,.\,\exists y \in B\,.\,y \leq x \wedge y \neq x$$

kar je ekvivalentno

$$\forall x \in B\,.\,\exists y \in B\,.\,y < x. \tag{13.6}$$

Padajočo verigo $b : \mathbb{N} \to B$ definiramo z zaporedjem izbir: ker je B neprazna, lahko izberemo neki element $b(0) \in B$. Denimo, da smo za neki $i \in \mathbb{N}$ že izbrali elemente $b(0), \ldots, b(i)$ tako, da velja

$$b(i) < b(i-1) < \ldots < b(1) < b(0).$$

Ker B nima minimalnega elementa, $b(i)$ ni minimalni, torej po (13.6) obstaja tak $y \in B$, da je $y < b(i)$. Torej lahko izberemo $b(i+1) \in B$, da velja $b(i+1) < b(i)$. ∎

Opomba 13.12 V zgornjem dokazu smo uporabili *aksiom odvisne izbire*, ki je poseben primer aksioma izbire in o katerem bomo še govorili.

Izrek 13.13 *Naj bo $\sqsubset$ relacija na A. Tedaj so ekvivalentne naslednje izjave:*

1. *$\sqsubset$ je dobro osnovana,*
2. *vsaka* neprazna *$S \subseteq A$ ima $\sqsubseteq$-minimalni element,*
3. *$\sqsubset$ nima padajoče verige.*

Dokaz. (1 $\Rightarrow$ 2) Denimo, da je $S \subseteq A$ neprazna. Če uporabimo (1) na $A \setminus S$ dobimo

$$(\forall y \in A\,.\,(\forall x \in A\,.\,x \sqsubset y \Rightarrow x \in A \setminus S) \Rightarrow y \in A \setminus S) \Rightarrow A \setminus S = A.$$

Ker je S neprazna, dobimo zaporedje ekvivalentnih izjav:

$$\begin{aligned}
&(\forall y \in A\,.\,(\forall x \in A\,.\,x \sqsubset y \Rightarrow x \in A \setminus S) \Rightarrow y \in A \setminus S) \Rightarrow \bot && (\Leftrightarrow)\\
&\neg(\forall y \in A\,.\,(\forall x \in A\,.\,x \sqsubset y \Rightarrow x \in A \setminus S) \Rightarrow y \in A \setminus S) && (\Leftrightarrow)\\
&\exists y \in A\,.\,(\forall x \in A\,.\,x \sqsubset y \Rightarrow x \in A \setminus S) \wedge y \notin A \setminus S && (\Leftrightarrow)\\
&\exists y \in A\,.\,(\forall x \in A\,.\,x \sqsubset y \Rightarrow x \notin S) \wedge y \in S && (\Leftrightarrow)\\
&\exists y \in S\,.\,\forall x \in A\,.\,x \sqsubset y \Rightarrow x \notin S && (\Leftrightarrow)\\
&\exists y \in S\,.\,(\forall x \in A\,.\,x \sqsubset y \Rightarrow x \notin S)
\end{aligned}$$

Torej obstaja element $y \in S$ z lastnostjo, da pod njim ni nobenega elementa iz S, kar pa pomeni, da je y iskani minimalni element.

(2 $\Rightarrow$ 3) Denimo, da je $a : \mathbb{N} \to A$ padajoča veriga. Tedaj slika $\{a(n) \mid n \in \mathbb{N}\}$ ne bi imela minimalnega elementa, v nasprotju z (2).

(3 $\Rightarrow$ 1) Denimo, da je $S \subseteq A$ progresivna. Trdimo, da množica $C := A \setminus S$ nima minimalnega elementa. Če bi bil $c \in C$ minimalni v C, bi to pomenilo

$$\forall x \in A\,.\,x \sqsubset c \Rightarrow x \notin C,$$

kar je ekvivalentno

$$\forall x \in A \,.\, x \sqsubset c \Rightarrow x \in S.$$

Ker je S progresivna, od tod sledi $c \in S$, kar ni mogoče. Dokazati moramo, da je C prazna. Če ne bi bila, bi lahko uporabili lemo 13.11 in dobili padajočo verigo v A, kar je v nasprotju s (3). ∎

Izrek 13.14 *Naj bo $\sqsubset$ stroga urejenost na A. Tedaj so ekvivalentne naslednje izjave:*
(1) $\sqsubset$ je dobro urejena,
(2) vsaka neprazna *množica $S \subseteq A$ ima $\sqsubset$-prvi element: to je tak $x \in S$, da velja $\forall y \in S \,.\, x \neq y \Rightarrow x \sqsubset y$.*
(3) A nima $\sqsubset$-padajoče verige in $\sqsubset$ je sovisna.

Dokaz. Za nalogo predelajte dokaz prejšnjega izreka v dokaz tega izreka. ∎

Primer 13.15 Primeri dobro urejenih množic:
1. Končna množica $\{0, \ldots, n\}$ urejena z relacijo $<$.
2. Naravna števila $\mathbb{N}$ urejena z relacijo $<$.
3. Če sta $(P, \leq_P)$ in $(Q, \leq_Q)$ dobri urejenosti, potem je dobro urejena tudi $P + Q$ z relacijo $\sqsubseteq$, ki P postavi pred Q:

$$\begin{aligned} u \sqsubseteq v \quad :\Longleftrightarrow \quad & (\exists x \in P \,.\, \exists y \in Q \,.\, u = \mathsf{in}_1(x) \wedge v = \mathsf{in}_2(y)) \vee \\ & (\exists x \in P \,.\, \exists y \in P \,.\, u = \mathsf{in}_1(x) \wedge v = \mathsf{in}_1(y) \vee x \leq_P y) \vee \\ & (\exists x \in Q \,.\, \exists y \in Q \,.\, u = \mathsf{in}_2(x) \wedge v = \mathsf{in}_2(y) \vee x \leq_Q y). \end{aligned}$$

4. S prejšnjim primerom lahko seštevamo dobre urejenosti, na primer $\mathbb{N} + \{0, 1, 2\}$ je dobra urejenost

$$\mathsf{in}_1 0 < \mathsf{in}_1 1 < \mathsf{in}_1 2 < \cdots < \mathsf{in}_2 0 < \mathsf{in}_2 1 < \mathsf{in}_2 2.$$

13.3 Ordinalna števila

Dobra urejenost na množici A postavi njene elemente v vrsto (strogo linearno urejenost), ki nima padajočih verig. Končno množico lahko dobro uredimo na več načinov, na primer elemente $\{0, 1, 2, \ldots, n-1\}$ lahko postavimo v vrsto na $n!$ načinov. Množico vseh naravnih števil lahko postavimo v vrsto brez padajočih verig vsaj na tri načine,

$$0, 1, 2, 3, 4, 5, \ldots, n, n+1, \ldots$$

in

$$1, 0, 3, 2, 5, 4, \ldots, 2n+1, 2n, \ldots$$

in

$$0, 2, 4, 6, 8, \ldots, 1, 3, 4, 5, \ldots$$

Zdi se, da sta prvi in drugi način »isti tip« urejenosti in se razlikujeta od tretjega. Res, v tretji vrsti ima 1 neskončno predhodnikov, v prvi in drugi pa takega elementa ni. Govorimo o naslednjem pojmu.

Definicija 13.16 Dobri ureditvi $(P, \leq_P)$ in $(Q, \leq_Q)$ **izomorfni**, če obstajata monotoni preslikavi $f : P \to Q$ in $Q \to P$, da velja $f \circ g = \mathrm{id}_Q$ in $g \circ f = \mathrm{id}_P$.

Seveda je izomorfnost ekvivalenčna relacija, ki je definirana na pravem razredu vseh dobrih urejenosti. Koristno bi bilo imeti kak izbor predstavnikov zanjo, saj bi lahko z njimi merili »dolžino« dobre urejenosti. Takim predstavnikom pravimo **ordinalna števila**. A kako bi jih dobili? Pri 19. letih je John von Neumann predlagal:

»Ordinalno število je množica svojih predhodnikov, urejeno z relacijo $\in$.«

Poglejmo, kako deluje njegova ideja:

- Končna ordinalna števila sovpadajo z naravnimi števili:

$$\begin{aligned} 0 &:= \emptyset \\ 1 &:= \{0\} = \{\emptyset\} \\ 2 &:= \{0, 1\} = \{\emptyset, \{\emptyset\}\} \\ 3 &:= \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\ &\vdots \end{aligned}$$

- Množica vseh končnih ordinalnih števil je prvo neskončno ordinalno število

$$\omega = \{0, 1, 2, 3, \ldots\}.$$

- Številu ω sledijo

$$\begin{aligned} \omega + 1 &:= \{0, 1, 2, \ldots, \omega\} \\ \omega + 2 &:= \{0, 1, 2, \ldots, \omega, \omega + 1\} \\ \omega + 3 &:= \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2\} \\ &\vdots \\ \omega + \omega &:= \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots\} \\ \omega + \omega + 1 &:= \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots, \omega + \omega\} \\ &\vdots \end{aligned}$$

Naloga 13.17 Kako bi si predstavljali naslednje ordinale: $\omega + \omega + \omega$, $\omega \cdot \omega$, ω^3, ω^ω?

Von Neumann je imel pravo idejo, a pušča kanček dvoma, ker je definicija ordinalnega števila *rekurzivna* (se nanaša sama nase). Če se malce potrudimo, lahko von Neumannove ordinale opredelimo neposredno.

Definicija 13.18 Množica z je **tranzitivna**, če iz $x \in y$ in $y \in z$ sledi $x \in z$.

Poimenovanje je smiselno, saj je pogoj v definiciji ravno tranzitivnost relacije $\in$. Ekvivalentno lahko pogoj izrazimo takole: množica z je tranzitivna, če iz $y \in z$ sledi $y \subseteq z$.

Primer 13.19 Množica $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$ je tranzitivna, niso pa vsi njeni elementi tranzitivne množice, saj $\{\{\emptyset\}\}$ ni tranzitivna, ker $\emptyset \in \{\emptyset\} \in \{\{\emptyset\}\}$ vendar $\emptyset \notin \{\{\emptyset\}\}$.

Naloga 13.20 Dokažite, da so ekvivalentni pogoji:
1. A je tranzitivna množica,
2. $\bigcup A \subseteq A$,
3. $A \subseteq \mathcal{P}(A)$.

Sedaj lahko zapišemo definicijo von Neumannovih ordinalov, ki ni rekurzivna.

Definicija 13.21 (Von Neumannov) ordinal je tranzitivna množica, ki je z relacijo $\in$ dobro urejena.

Razred vseh von Neumannovih ordinalov označimo z On (v angleščini »ordinal number«). To je pravi razred, česar ne bomo dokazali. Kogar zanima dokaz, naj poišče »Burali-Fortijev paradoks«, ki je celo starejši od Russellovega paradoksa.

Naloga 13.22 Poiščite množico, ki *ni* tranzitivna in je dobro urejena z relacijo $\in$.

Ali definicija 13.21 res sovpada z idejo, da je ordinal množica svojih prednikov? To potrjuje naslednja izjava.

Izjava 13.23 *Če je α ordinal in $\beta \in \alpha$, potem je β ordinal.*

Dokaz. Ker je α tranzitivna množica, je $\beta \subseteq \alpha$, zato je β z relacijo $\in$ dobro urejen. Dokazati moramo še, da je β tranzitivna množica. Denimo, da je $\delta \in \gamma \in \beta$, in pokažimo, da velja $\delta \in \beta$. Ker je α tranzitivna in velja $\gamma \in \alpha$, velja tudi $\delta \in \alpha$. Ker je α linearno urejena, velja bodisi $\delta \in \beta$ bodisi $\delta = \beta$ bodisi $\beta \in \delta$. Druga in tretja možnost bi nam dali cikel v α, kar ni mogoče, torej velja prva možnost. ∎

Naloga 13.24 V zgornjem dokazu smo uporabili naslednje dejstvo: če je $(P, <)$ dobra ureditev in $Q \subseteq P$, tedaj je Q z relacijo $<$ zoženo na Q tudi dobra ureditev. Zapišite dokaz.

Brez dokaza navedimo, da so von Neumannovi ordinali izbor predstavnikov za dobre urejenosti.

Izrek 13.25 *Vsaka dobra ureditev je izomorfna natanko enemu von Neumannovemu ordinalu.*

Poglavje 14

Moč množic

V tej lekciji bomo govorili o velikosti množic, končnih množicah in neskončnih množicah.

14.1 Aksiom odvisne izbire

Kasneje bom potrebovali inačico aksioma izbire, ki se glasi:

Aksiom 14.1 (Odvisna izbira) *Naj bo A neprazna množica in $R \subseteq A \times A$ celovita relacija, se pravi $\forall x \in A \,.\, \exists y \in A \,.\, x \,R\, y$. Tedaj obstaja tako zaporedje $a : \mathbb{N} \to A$, da za vse $n \in N$ velja $a_n \,R\, a_{n+1}$.*

Aksiom odvisne izbire sledi iz aksioma izbire, česar tu ne bomo dokazali.

Aksiom odvisne izbire se v praksi uporabi, kadar želimo konstruirati zaporedje $a : \mathbb{N} \to A$, pri čemer sta izpolnjena dva pogoja:

1. za vsak člen zaporedja a_n imamo na voljo eno ali več izbir,
2. izbire za člen a_{n+1} so odvisne od tega, kaj smo izbrali za a_n.

Primer uporabe bomo videli v nadaljevanju.

14.2 Končne množice

Kako bi definirali pojem »končna množica«?

Definicija 14.2 Za vsako naravno število $n \in \mathbb{N}$, naj bo **standardna končna množica** $[n] = \{k \in \mathbb{N} \mid k < n\}$.

Torej velja

$$\begin{aligned} [0] &= \{\} \\ [1] &= \{0\} \\ [2] &= \{0, 1\} \\ [3] &= \{0, 1, 2\} \\ &\vdots \end{aligned}$$

Definicija 14.3 Množica je **končna**, če je izomorfna kaki standardni končni množici.

Velja naslednje (ne bomo dokazali): če je $A \cong [m]$ in $A \cong [n]$, potem je $m = n$. Torej za končno množico A obstaja natanko en $n \in N$, da velja $A \cong [n]$. Temu n pravimo **moč** množice A, saj nam pove, koliko elementov ima A. Moč končne množice A označimo z $|A|$.

Za moči končnih množic velja

$$\begin{aligned} |[n]| &= n, \\ |A \times B| &= |A| \times |B|, \\ |A + B| &= |A| + |B|, \\ |B^A| &= |B|^{|A|}. \end{aligned}$$

Zgornje enačbe je treba razumeti pravilno: na levi nastopajo $\times$, $+$ in potenciranje kot operacije na množicah, na desni pa kot operacije na naravnih številih.

Za unijo velja **pravilo vključitve in izključitve**:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Pravilo se tako imenuje, ker smo pri štetju elementov $A \cup B$ *vključili* elemente A in B, nato pa *izključili* elemente preseka $A \cap B$, da jih ne bi šteli dvakrat. Pravilo vključitve in izključitve za tri množice se glasi

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|.$$

Naloga 14.4 Zapišite pravilo vključitve in izključitve za unijo $A_1 \cup A_2 \cup \cdots \cup A_n$.

14.3 Neskončne množice

Definicija 14.5 Množica je **neskončna**, če ni končna.

Izrek 14.6 *Množica A je neskončna natanko tedaj, ko obstaja injektivna preslikava $\mathbb{N} \to A$.*

Dokaz.

($\Rightarrow$) Denimo, da A ni končna. Injektivno preslikavo $e : \mathbb{N} \to A$ definiramo s pomočjo aksioma odvisne izbire. Ker A ni izomorfna $[0]$, ni prazna, torej obstaja $e(0) \in A$. Denimo, da smo že definirali e kot injektivno preslikavo $[n] \to A$. Tedaj jo lahko razširimo na injektivno preslikavo $e : [n+1] \to A$ takole: ker e ni surjektivna (če bi bila, bi veljalo $A \cong [n]$ in A bi bila končna), obstaja $x \in A$, ki ni v sliki e. Sedaj *izberemo* $e(n) \in A$, ki ni v sliki. Tako dobimo $e : \mathbb{N} \to A$, ki je injektivna.

($\Leftarrow$) Denimo, da obstaja injektivna preslikava $e : \mathbb{N} \to A$. Če bi za neki n veljalo $A \cong [n]$, bi imeli izomorfizem $f : A \to [n]$. Tedaj bi bil kompozitum $f \circ e : \mathbb{N} \to [n]$ injektivna preslikava, ta pa ne obstaja (dokaz opustimo). ∎

14.3.1 Moč množic

Tudi neskončnim množicam želimo prirediti moč, se pravi, neko mero velikosti. Preden pa nam bo to uspelo, se najprej naučimo primerjati velikost množic, ne da bi pri tem govorili o »številu elementov«.

Definicija 14.7 Množici A in B imata enako moč, sta **ekvipolentni**, kadar sta izomorfni.

Ekvipolentnost in izomorfnost sta torej sinonima, ki pa se uporabljata v različnih situacijah. O ekvipolentnosti govorimo, ko imamo v mislih velikost množic ali število elementov. Izomorfnost je širši pojem, ki se uporablja tudi v algebri, topologiji in povsod, kjer imamo opravka z matematičnimi strukturami, in pomeni »enakovredna struktura«.

Spomnimo se, da je izomorfnost in torej tudi ekvipolentnost ekvivalenčna relacija. Torej lahko tvorimo ekvivalenčne razrede glede na ekvipolentnost: vsaki množici A priredimo razred vseh množic, ki so ji ekvipolentne:

- $[\emptyset]_{\cong} = \{\emptyset\}$,
- $[\{()\}]_{\cong}$ je *pravi razred* vseh enojcev,
- $[\{0,1\}]_{\cong}$ je *pravi razred* vseh množic z dvema elementoma,
- itd.

Dejstvo, da so razredi glede na izomorfnost pravi razredi in ne množice, je precej nerodna reč, saj z njimi ne moremo udobno delati (potrebovali bi »super razrede«, katerih elementi so razredi). Izognemo se jim tako, da namesto z razredi delamo z izborom predstavnikov.

Pravzaprav smo ta trik že uporabili, ko smo govorili o moči končnih množic, ko smo za predstavnike ekvipolenčnih razredov končnih množic izbrali standardne končne množice. Le-te nam lahko služijo kot »števila«, s katerimi opišemo moči končnih množic, saj med standardno končno množico $[n]$ in številom n ni bistvene razlike. (Še več, kasneje bomo videli, da lahko naravna števila obravnavamo tako, da dejansko so standardne končne množice!)

Kako bi torej izbrali predstavnike razredov za ekvipolentnost za vse množice? Če bi nam to uspelo, bi take predstavnike lahko uporabili kot števila, imenujejo se **kardinalna števila**, s katerimi bi merili moč množic.

Definicija 14.8 **Kardinalno število** je tako ordinalno število κ, za katerega velja $|\alpha| < |\kappa|$ za vse $\alpha \in \kappa$.

Primer 14.9 Tu ne bomo dokazali, da je vsaka množica ekvipolentna natanko enemu kardinalnemu številu. Raje si poskušajmo predstavljati kardinalna števila:

- Končni ordinali, ki so seveda kar naravna števila, so kardinalna števila, saj je naravno število strogo večje od svojih predhodnikov.
- Ordinal $\omega = \mathbb{N} = \{0, 1, 2, \ldots\}$, ki vsebuje vse končne ordinale, je kardinalno število. Označujemo ga tudi z $\aleph_0$.
- Ordinal $\omega + 1 = \{0, 1, 2, \ldots, \omega\}$ *ni* kardinalno število, saj je ekvipolenten ω. Prav tako so ordinali

  $$\omega + 2, \omega + 3, \ldots, \omega + \omega, \ldots, \omega + \omega + \omega, \ldots, \omega^2, \omega^3$$

  vsi ekvipolentni ω, zato niso kardinali. Pravzaprav si je precej težko predstavljati ordinal, katerega moč je strogo večja od ω.

Vsaki množici A torej priredimo nekega predstavnika razreda $[A]_{\cong}$, ki ga označimo $|A|$ in ga imenujemo **moč** množice A. Za končne množice so to kar naravna števila, za splošne množice pa so to kardinalna števila.

Moči množic lahko primerjamo med seboj, čeprav ne vemo, kaj točno naravna števila so!

Definicija 14.10 Naj bosta A in B poljubni množici. Pravimo:

1. A ima enako moč kot B, pišemo $|A| = |B|$, ko obstaja bijektivna preslikava $A \to B$.
2. A ima moč manjšo ali enako B, pišemo $|A| \leq |B|$, ko obstaja injektivna preslikava $A \to B$.
3. A ima moč manjšo kot B, pišemo $|A| < |B|$, če velja $|A| \leq |B|$ in $|A| \neq |B|$.

Izrek 14.11 *$|A| \leq |B|$ natanko tedaj, ko je $A = \emptyset$ ali obstaja surjekcija $B \to A$.*

Dokaz. Denimo, da je $f : A \to B$ injektivna in $A \neq \emptyset$. Torej obstaja neki $a \in A$. Definiramo preslikavo $g : B \to A$ takole:

$$g(y) = x \quad :\Longleftrightarrow \quad f(x) = y \vee (y \notin f_*(A) \wedge x = a).$$

Povedano malo drugače:

$$g(y) = \begin{cases} f^{-1}(y) & \text{če } y \in f_*(A), \\ a & \text{če } y \notin f_*(A). \end{cases}$$

Ker velja $g \circ f = \mathrm{id}_A$, je g retrakcija in zato surjektivna.

Obratno, denimo, da je A prazna ali obstaja surjekcija $f : B \to A$. Če je A prazna, je edina preslikava $\emptyset \to B$ injektivna. Če je $f : B \to A$ surjektivna, ima prerez (zakaj?), ki je injektivna preslikava. ∎

14.3.2 Cantorjev izrek

Izrek 14.12 (Cantor) $|A| < |\mathcal{P}(A)|$.

Dokaz. Najprej dokažimo $|A| \leq |\mathcal{P}(A)|$. Iščemo injektivno preslikava $f : A \to \mathcal{P}(A)$. Vzemimo $f(x) = \{x\}$. Zlahka preverimo, da je f res injektivna.

Sedaj dokazujemo, da ne obstaja bijekcija $A \to \mathcal{P}(A)$. Dokazali bomo, da ne obstaja surjekcija $A \to \mathcal{P}(A)$, kar zadostuje. Denimo, da je $g : A \to \mathcal{P}(A)$ poljubna preslikava. Trdimo, da g ni surjekcija. Res, podmnožica

$$S = \{x \in A \mid x \notin g(x)\}$$

ni v sliki g. Če bi bila, bi za neki $y \in A$ veljalo $g(y) = S$, a to bi vodilo v protislovje:

- velja $y \notin S$: če $y \in S$ potem $y \notin g(y) = S$ po definiciji S,
- velja $\neg(y \notin S)$: če $y \notin S$ potem $y \notin g(y) = S$.

∎

14.3.3 Števne in neštevne množice

Kot smo že povedali, moč množice $\mathbb{N}$ označimo z $\aleph_0$.

Definicija 14.13 Množica A je **števna**, če velja velja $|A| \leq \aleph_0$.

Definicija 14.14 Množica A je **neštevna**, če ni števna.

Izrek 14.15 *Za vsako množico A so ekvivalentne naslednje izjave:*

1. *A je števna,*
2. *obstaja injektivna preslikava $A \to \mathbb{N}$,*
3. *A je prazna ali obstaja surjektivna preslikava $\mathbb{N} \to A$,*
4. *obstaja surjektivna preslikava $\mathbb{N} \to \mathbb{1} + A$,*
5. *A je končna ali izomorfna $\mathbb{N}$.*

Dokaz. $(1 \Rightarrow 2)$ Če je A števna, velja $|A| \leq \aleph_0 = |\mathbb{N}|$, torej obstaja injektivna $A \to \mathbb{N}$ po definiciji relacije $\leq$.

$(2 \Rightarrow 3)$ To sledi neposredno iz Izreka 14.11.

$(3 \Rightarrow 4)$ Denimo, da je A prazna ali obstaja surjektivna preslikava $\mathbb{N} \to A$:

1. Če je $A = \emptyset$, potem seveda obstaja surjektivna preslikava $\mathbb{N} \to \mathbb{1} + A$, in sicer $n \mapsto \mathsf{in}_1()$.
2. Če obstaja surjektivna preslikava $f : \mathbb{N} \to A$, potem lahko definiramo surjektivno preslikavo $g : \mathbb{N} \to \mathbb{1} + A$ s predpisom

$$g(n) = \begin{cases} \mathsf{in}_1() & \text{če } n = 0, \\ \mathsf{in}_2(f(n-1)) & \text{če } n > 0. \end{cases}$$

$(4 \Rightarrow 5)$ Denimo, da obstaja surjektivna preslikava $r : \mathbb{N} \to \mathbb{1} + A$. Dokazali bomo, da je A izomorfna $\mathbb{N}$, če ni končna. Predpostavimo torej, da A ni končna. Preslikava r ima prerez $s : \mathbb{1} + A \to \mathbb{N}$, ki je seveda injektivna preslikava. Preslikav $s \circ \mathsf{in}_2 : A \to \mathbb{N}$ je kompozitum injektivnih preslikav, zato je injektivna. Ker A ni končna, obstaja tudi injektivna preslikava $\mathbb{N} \to A$. Po izreku Cantor-Schröder-Bernstein, ki ga bomo dokazali spodaj, je torej A izomorfna $\mathbb{N}$.

$(5 \Rightarrow 1)$ Če je A končna, je števna, ker očitno velja $A = |[n]| \leq |\mathbb{N}| = \aleph_0$. Če je A izomorfna $\mathbb{N}$, potem velja $|A| = |\mathbb{N}| \leq |\mathbb{N}| = \aleph_0$. ∎

Izrek 14.16 $\mathbb{N} \times \mathbb{N} \cong \mathbb{N}$.

Dokaz. Za vajo, poiščite dokaz v zapiskih iz analize ali na internetu. ∎

Števna družina je družina $A : I \to \mathsf{Set}$, katere indeksna množica I je števna.

Izrek 14.17 *Unija števne družine števnih množic je števna.*

Dokaz. Izrek bomo dokazali le za primer, ko je indeksna množica $\mathbb{N}$. Najprej obravnavajmo unijo družine $A : \mathbb{N} \to \mathsf{Set}$, kjer je A_n števna za vse $n \in \mathbb{N}$. Za vsak $n \in \mathbb{N}$ obstaja surjektivna preslikava $\mathbb{N} \to A_n + \mathbb{1}$. Po aksiomu izbire obstaja funkcija izbire

$$e \in \prod_{n \in \mathbb{N}} \{f : \mathbb{N} \to A_n + \mathbb{1} \mid f \text{ surjekcija}\}.$$

Definiramo $e' : \mathbb{N} \times \mathbb{N} \to \mathbb{1} + \bigcup_{n \in \mathbb{N}} A_n$ s predpisom

$$e'(n, k) = e(n)(k).$$

Trdimo, da je e' surjekcija iz $\mathbb{N} \times \mathbb{N}$ na $\mathbb{1} + \bigcup_{n \in \mathbb{N}} A_n$. ∎

14.3.4 Cantor-Schröder-Bernsteinov izrek in zakon trihotomije

Izrek 14.18 (Cantor-Schröder-Bernstein) *Če obstajata injektivni preslikava $A \to B$ in $B \to A$, potem obstaja bijektivna preslikava $A \to B$.*

Dokaz. Definirajmo družino $C : \mathbb{N} \to \mathsf{Set}$ takole:

$$C_0 = A \setminus g_*(B),$$
$$C_{n+1} = g_*(f_*(C_n).$$

Naj bo $D = \bigcup_{n \in \mathbb{N}} C_n$. Očitno je $C_n \subseteq A$ za vse $n \in \mathbb{N}$, zato velja tudi $D \subseteq A$.

Ker je g injektivna, je bijekcija kot preslikava $g : B \to g_*(B)$, zato obstaja inverz $g^{-1} : g_*(B) \to B$. Trdimo, da velja $A \setminus D \subseteq g_*(B)$. Res, če velja $x \in A \setminus D$, tedaj $x \notin D$ in zato $x \notin C_0 = A \setminus g_*(B)$, od koder sledi $x \in g_*(B)$. Od tod sledi, da lahko g^{-1} uporabimo na $x \in A \setminus D$.

Definirajmo $h : A \to B$ s predpisom

$$h(x) = \begin{cases} f(x), & \text{če } x \in D, \\ g^{-1}(x) & \text{če } x \in A \setminus D. \end{cases}$$

Dokažimo, da je h injektivna preslikava. Denimo, da za $x, y \in A$ velja $h(x) = h(y)$. Obravnavamo štiri primere:

1. Če je $x \in D$ in $y \in D$, potem je $f(x) = h(x) = h(y) = f(y)$ in zato $x = y$, saj je f injektivna.
2. Če je $x \in A \setminus D$ in $y \in A \setminus D$, potem je $g^{-1}(x) = h(x) = h(y) = g^{-1}(y)$ in zato $x = y$, saj je g^{-1} injektivna.
3. Če je $x \in D$ in $y \in A \setminus D$, potem je $f(x) = h(x) = h(y) = g^{-1}(y)$, zato je $y = g(g^{-1}(y)) = g(f(x))$. Obstaja $n \in \mathbb{N}$, da je $x \in C_n$, od tod pa sledi $y = g(f(x)) \in C_{n+1} \subseteq D$, kar je v protislovju z $y \in A \setminus D$. Torej se ta primer sploh ne more zgoditi.
4. Če je $x \in A \setminus D$ in $y \in D$, je razmislek kot v prejšnjem primeru, le da zamenjamo vlogi x in y.

Preveriti moramo še, da je h surjektivna preslikava. Naj bo $z \in B$. Poiskati moramo tak $x \in A$, da velja $h(x) = z$. Obravnavamo dva primera:

1. Če $z \in f_*(D)$, potem obstaja $x \in D$, da je $f(x) = y$, s tem pa velja tudi $h(x) = f(x) = z$.

2. Če velja $z \notin f_*(D)$, potem vzamemo $x = g(z)$. Preverimo, da velja $h(x) = z$.
   Najprej dokažimo $x \notin D$. Če bi namreč veljalo $x \in D$, potem bi obstajal $n \in \mathbb{N}$, da je $x \in C_n$. Poleg tega $x = g(z) \notin A \setminus g_*(B) = C_0$, zato velja $n > 0$. Se pravi, da obstaja $y \in C_{n-1}$, da je $g(z) = x = g(f(y))$. Ker je g injektivna, sledi $z = f(y)$, kar je v nasprotju z predpostavko $z \notin f_*(D)$. Torej res velja $x \notin D$.
   Ker $x \notin D$, velja $h(x) = g^{-1}(x) = g^{-1}(g(z)) = z$, kar smo želeli dokazati.

∎

Posledica 14.19 *Če $|A| \leq |B|$ in $|B| \leq |A|$, potem $|A| = |B|$.*

Dokaz. To sledi neposredno iz izreka CSB in definicije $\leq$. ∎

Brez dokaza omenimo še, da velja **zakon trihotomije**: za vsaki množici A in B velja

$$|A| < |B| \vee |A| = |B| \vee |B| < |A|.$$

Relacija $\leq$ torej uredi moči množic linearno.

14.3.5 Moč kontinuuma in Cantorjeva hipoteza

Na vajah boste spoznali, da ima množica realnih števil $\mathbb{R}$ enako moč kot potenčna množica $\mathcal{P}(\mathbb{N})$. Moči $\mathbb{R}$ in $\mathcal{P}(\mathbb{N})$ pravimo **moč kontinuuma** (ker je »kontinuum« tudi staro ime za $\mathbb{R}$). Že Georg Cantor, utemeljitelj teorije množic, je postavil naslednji domnevo:

> ***Cantorjeva hipoteza*** *Vsaka neštevna podmnožica realnih števil je izomorfna $\mathbb{R}$.*

Povedano, z drugimi besedami, po moči ni nobene množice strogo med $\mathbb{N}$ in $\mathbb{R}$. Cantorjeva hipoteza je ostala odprta dlje časa. Dokončno je Cohen pred dobrega pol stoletja dokazal naslednje:

Izrek 14.20 (Cohen) *Iz Zermelo-Fraenkelovih aksiomov teorije množic Cantorjeve hipoteze ne moremo niti dokazati niti ovreči.*

Pravimo, da je Cantorjeva hipoteza *neodvisna* od aksiomov teorije množic. Poznamo še posplošeno Cantorjevo hipotezo, ki se glasi:

> **Posplošena Cantorjeva hipoteza:** Če je $|A| \leq |B| \leq |\mathcal{P}(A)|$, potem je $|B| = |A|$ ali $|B| = |\mathcal{P}(A)|$.

Tudi posplošena Cantorjeva hipoteza je neodvisna od aksiomov teorije množic. Danes vemo zelo veliko o tej hipotezi in poznamo še mnoge druge izjave o množicah, ki so neodvisne od Zermelo-Fraenkelovih aksiomov teorije množic. Ti veljajo za nekakšno uradno različico teorije množic in jih bomo obravnavali na naslednjih predavanjih.

Poglavje 15

Aksiomatska teorija množic

15.1 Kodiranje matematičnih objektov z množicami

Z množicami smo izrazili številne matematične objekte, na primer:

- ordinalna števila smo predstavili kot množice svojih predhodnikov,
- preslikavo $f : A \to B$ lahko izrazimo kot funkcijsko relacijo med A in B, torej kot podmnožico $A \times B$,
- kvocientna množica A/R je množica ekvivalenčnih razredov, ekvivalenčni razredi so spet množice,

Ali je možno vse matematične objekte predstaviti z množicami? Da!

15.1.1 Urejeni pari

Par (x, y) lahko predstavimo z množico $\{\{x\}, \{x, y\}\}$. Tako dobimo

$$A \times B := \{\{\{x\}, \{x, y\}\} \mid x \in A \wedge y \in B\}.$$

15.1.2 Vsota

Elemente vsote $A + B$ kodiramo takole:

$$\begin{aligned} \mathsf{in}_1(x) &:= (x, 0) = \{\{x\}, \{x, \emptyset\}\}, \\ \mathsf{in}_2(x) &:= (x, 1) = \{\{x\}, \{x, \{\emptyset\}\}\}. \end{aligned}$$

15.1.3 Naravna števila

Kot smo že videli, lahko ordinalna števila kodiramo kot množice svojih predhodnikov, poseben primer pa so naravna števila, ki so končni ordinali.

Kako pa kodiramo operacijo naslednik? Definirajmo preslikavo **naslednik** $^+ : \mathsf{Set} \to \mathsf{Set}$,

$$x^+ := x \cup \{x\}.$$

Če si predstavljamo, da je x število, tedaj so elementi x^+ predhodniki x in še x, kar je

ravno naslednik x. Naravna števila res dobimo tako, da na $\emptyset$ uporabljamo naslednik $^+$:

$$\begin{aligned}
0 &= \emptyset \\
1 &= 0^+ = \{0\} = \{\emptyset\} \\
2 &= 1^+ = \{0,1\} = \{\emptyset, \{\emptyset\}\} \\
3 &= 2^+ = \{0,1,2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\
4 &= 3^+ = \{0,1,2,3\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} \\
&\vdots
\end{aligned}$$

15.1.4 Cela števila

Cela števila so kvocient $\mathbb{N} \times \mathbb{N}$:

$$\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/\sim,$$

kjer je

$$(a,b) \sim (c,d) \quad :\Longleftrightarrow \quad a + d = c + b.$$

Urejeni par (a,b) predstavlja razliko števil a in b.

15.1.5 Racionalna števila

Racionalna števila so kvocient:

$$\mathbb{Q} = (\mathbb{Z} \times \{n \in \mathbb{N} \mid n > 0\})/\approx,$$

kjer je

$$(a,m) \approx (b,n) \quad :\Longleftrightarrow \quad an = bm.$$

Urejeni par (a,n) predstavlja kvocient števil a in n.

15.1.6 Realna števila

Realno število je Dedekindov rez, torej podmnožica $\mathbb{Q}$. Reze ste obravnavali pri Analizi, tako da jih na tem mestu ne bomo obnavljali.

In tako naprej. Ne pravimo, da je kodiranje vseh matematičnih objektov z množicami vedno dobra ideja, vendar pa je dejstvo, da je to možno, pomembno spoznanje osnov matematike. Iz njega na primer sledi tole: če je teorija množic neprotislovna, potem je neprotislovna tudi vsa matematika, ki jo lahko kodiramo z množicami (torej več ali manj vsa običajna matematika).

15.2 Zermelo-Fraenkelovi aksiomi

Aksiomi opredeljujejo množice brez urelementov (»*Vse* je množica«). Za aksiomatizacijo razredov bi morali zapisati drugačne aksiome, kot so na primer von Neumann-Bernays-Gödelovi aksiomi.

Ekstenzionalnost: množici A in B, ki imata iste elemente, sta enaki.

Neurejeni par : za vsak x in y je $\{x, y\}$ množica, ki vsebuje natanko x in y:

$$\forall xyz \,.\, z \in \{x, y\} \Leftrightarrow z = x \vee z = y$$

Okrajšava: $\{x\} = \{x, x\}$.

Unija: za vsako množico A je $\bigcup A$ množica, ki vsebuje natanko vse elemente množic iz A:

$$\forall Ax \,.\, x \in \bigcup A \Leftrightarrow \exists B \in A \,.\, x \in B.$$

Prazna množica: množica $\emptyset$ nima elementa:

$$\forall x \,.\, x \notin \emptyset.$$

Neskončna množica obstaja množica, ki vsebuje $\emptyset$ in je zaprta za operacijo naslednik ($x^+ = x \cup \{x\}$):

$$\exists A \,.\, \emptyset \in A \wedge \forall x \in A \,.\, x^+ \in A.$$

Podmnožica: za vsako množico A in formulo ϕ je $\{x \in A \mid |\phi(x)\}$ množica, ki vsebuje natanko vse element iz A, ki zadoščajo ϕ:

$$\forall y \,.\, y \in \{x \in A | \phi(x)\} \Leftrightarrow \phi(y).$$

Potenčna množica: za vsako množico A je $\mathcal{P}(A)$ množica, ki vsebuje natanko vse njene podmnožice:

$$\forall S \,.\, S \in \mathcal{P}(A) \Leftrightarrow S \subseteq A.$$

Zamenjava če je A množica in $f : A \to \mathsf{Set}$ preslikava, je $f_*(A) = \{y \mid \exists x \in A \,.\, y = f(x)\}$ množica.

Dobra osnovanost: relacija $\in \subseteq \mathsf{Set} \times \mathsf{Set}$ je dobro osnovana.

Aksiom izbire: vsaka družina nepraznih množic ima funkcijo izbire.

15.3 Kumulativna hierarhija

Če lahko vse matematične objekte kodiramo z množicami, potem lahko na razred vseh množic Set gledamo kot na celotni matematični svet. Razred Set ima zanimivo strukturo, ki ji pravimo **kumulativna hierarhija**. Namreč, s pomočjo Zermelo-Fraenkelovih aksiomov lahko tvorimo vse množice iz $\emptyset$ z operacijama potenčna množica in unija. Postopek

je **transfiniten** (neskončen), ima pa toliko korakov, kot je ordinalnih števil:

$$\begin{aligned}
V_0 &= \emptyset \\
V_1 &= \mathcal{P}(V_0) = \{\emptyset\} \\
V_2 &= \mathcal{P}(V_1) = \{\emptyset, \{\emptyset\}\} \\
V_3 &= \mathcal{P}(V_2) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\} \\
&\vdots \\
V_\omega &= \textstyle\bigcup_{k<\omega} V_k \\
V_{\omega+1} &= \mathcal{P}(V_\omega) \\
V_{\omega+2} &= \mathcal{P}(V_{\omega+1}) \\
&\vdots \\
V_{\omega+\omega} &= \textstyle\bigcup_{\alpha<\omega+\omega} V_\alpha \\
&\vdots
\end{aligned}$$

Splošna formula se glasi $V_\alpha = \bigcup_{\beta<\alpha} \mathcal{P}(V_\beta)$.

Naloga 15.1 Koliko elementov ima V_5?

Bistvo kumulativne hierarhije je, da zaobjame vse množice.

Izrek 15.2 (Kumulativna hierarhija) $\mathsf{Set} = \bigcup_{\alpha\in\mathsf{On}} V_\alpha$.

Dokaz. Dokaz opustimo, povejmo le, da je za izrek bistven aksiom o dobro osnovanosti. Le ta nam zagotavlja, da se vsaka padajoča $\in$-veriga konča z $\emptyset$. ∎

15.4 Aksiom izbire

Za konec povejmo še nekaj več o aksiomu izbire in Zornovi lemi, ki mu je ekvivalentna. Le-ta se uporablja v algebri.

Lema 15.3 (Zornova lema) *Če ima v delni urejenosti $(P, \leq)$ vsaka veriga zgornjo mejo, potem ima P maksimalni element.*

Dokaz. Dokaz se naslanja na aksiom izbire in Bourbaki-Wittov izrek o negibnih točkah (glej spodaj). Naj bo C množica vseh verig v P. Uredimo jo z $\subseteq$. Na njej definiramo preslikavo $f : C \to C$, ki razširi verigo, če ni maksimalna, sicer je ne spremeni (tu uporabimo izbiro):

- Če je $V \in C$ maksimalna veriga v P (glede na $\subseteq$), definiramo $f(V) := V$.
- Če $V \in C$ ni maksimalna veriga v P, potem obstaja tak $x \in P \setminus V$, da je $V \cup \{x\}$ spet veriga. V tem primeru *izberemo* tak x in definiramo $f(V) := V \cup \{x\}$.

Po izreku Bourbaki-Witt ima f negibno vrednost $V \in C$. Ta V je maksimalna veriga V, saj bi sicer veljalo, da je $V = f(V) = V \cup \{x\}$ za neki $x \notin V$, kar ni možno. Naj bo m zgornja meja za verigo V. Trdimo, da je m maksimalni element v P: denimo, da velja $m \leq y$ za $m \in P$. Ker je $V \cup \{y\}$ veriga, ki vsebuje maksimalno verigo V, sledi $V = V \cup \{y\}$, od tod pa $y \in V$ ter $y \leq m$. Torej je $m = y$ in m je res maksimalni element. ∎

Definicija 15.4 Naj bo $(P, \leq)$ delna ureditev. Preslikava $f : P \to P$ je **progresivna**, ko velja $x \leq f(x)$ za vsak $x \in P$.

Opomba 15.5 Progresivna preslikava ni nujno monotona – poiščite primer!

Izrek 15.6 (Bourbaki-Witt) *Naj bo $(P, \leq)$ neprazna delna ureditev, v kateri ima vsaka veriga zgornjo mejo in $f : P \to P$ progresivna preslikava. Tedaj ima f negibno točko: to je tak $x \in P$, da velja $f(x) = x$.*

Dokaz. Dokaz opustimo. ∎

Izrek 15.7 *V teoriji množic* brez *aksioma izbire so naslednje izjave ekvivalentne:*

1. *Aksiom izbire*
2. *Zornova lema*
3. *Princip dobre urejenosti: vsaka množica ima dobro ureditev.*

Dokaz. (1 ⇒ 2) Glej Zornovo lemo.

(2 ⇒ 3) Skica dokaza: naj bo A poljubna množica, ki jo želimo dobro urediti. Definirajmo *delne* dobre ureditev množice A: to so pari (B, R), kjer je $B \subseteq A$ in $R \subseteq B \times B$ dobra ureditev na B. Za delni dobri ureditvi (B, R) in (C, Q) pravimo, da je (C, Q) *razširitev* (B, R), kadar velja $B \subseteq C$, $R \subseteq Q$ in še, da je B začetni segment v C, kar pomeni

$$\forall xy \in C \,.\, x \; Q \; y \wedge y \in B \Rightarrow x \in B.$$

Kadar je (C, Q) razširitev (B, R), pišemo $(B, R) \preceq (C, Q)$. Naj bo P množica vseh delnih dobrih ureditev množice A,

$$P := \{(B, R) \mid B \subseteq A \text{ in } R \subseteq B \times B \text{ in } R \text{ je dobra ureditev } B\},$$

urejena z relacijo $\preceq$. Očitno je $\preceq$ delna ureditev. Trdimo, da imajo verige v P zgornje meje glede na $\preceq$: če je $V \subseteq P$ veriga dobro urejenih podmnožic A, je njena zgornja meja (D, S) kar unija po komponentah:

$$D := \bigcup \{B \mid (B, R) \in V\}$$
$$S = \bigcup \{R \mid (B, R) \in V\}.$$

Preverimo, da velja $(D, S) \in P$. Očitno je (D, S) stroga linearna ureditev (vaja). Denimo, da bi v (D, S) imeli neskončno padajočo verigo

$$\cdots \; S \; x_3 \; S \; x_2 \; S \; x_1 \; S \; x_0.$$

Obstaja $(B, R) \in V$, da je $x_0 \in B$. Potem bi bila $x_0, x_1, x_2, x_3, \ldots$ padajoča veriga v (B, R), kar ni možno, saj je (B, R) dobro urejena. Res, ker je $x_i \in V$, obstaja (C, Q), da je $x_i \in C$. Če velja $(B, R) \preceq (C, Q)$, potem $x_i \in B$ po definiciji $\preceq$. Če velja $(C, Q) \preceq (B, R)$, potem $x_i \in B$, ker velja $C \subseteq B$. Torej je (D, S) res delna ureditev P.

Preverimo še, da velja $(B, R) \preceq (D, S)$ za vsak $(B, R) \in V$. Denimo, da je $y \in D$, $x \in B$ in $y \; S \; x$. Obstaja $(C, Q) \in V$, da je $y \in C$. Če velja $(C, Q) \preceq (B, R)$, potem $y \in C \subseteq B$. Če pa velja $(B, R) \preceq (C, Q)$, potem je $y \in B$ po definiciji $\preceq$.

Po Zornovi lemi obstaja maksimalni element (B, R) v P. Trdimo, da je $B = A$. Če bi namreč obstajal $x \in B \setminus A$, bi lahko razširili (B, R) na večjo dobro ureditev tako, da bi dodali x na konec B:

$$\begin{aligned} &(B \cup \{x\}, R') \\ &y \; R' \; z \quad :\Longleftrightarrow \quad z = x \wedge y \; R \; z. \end{aligned}$$

To ni možno, ker je (B, R) maksimalna delna ureditev. Torej je res $A = B$ in našli so dobro ureditev A.

$(3 \Rightarrow 1)$ Naj bo $A : I \to \mathsf{Set}$ družina nepraznih množic. Naj bo $\prec$ dobra ureditev na uniji $\bigcup A$. Ker so vse množice A_i neprazne, ima vsaka od njih prvi element glede na $\prec$. Torej lahko definiramo funkcijo izbire f s predpisom $f(i) :=$ »prvi element A_i«. ∎

Izrek 15.8 *Vsak vektorski prostor ima bazo.*

Dokaz. Naj bo L vektorski prostor. Definiramo množico

$$P := \{B \subseteq L \mid B \text{ je linearno neodvisna}\}.$$

Množico P delno uredimo z relacijo $\subseteq$. Trdimo, da imajo verige v P zgornje meje: zgornja meja verige $V \subseteq P$, je kar njena unija $\bigcup_{B \in V} B$. Seveda je treba preveriti, da je unija verige linearno neodvisnih množic spet linearno neodvisna (vaja). Po Zornovi lemi obstaja maksimalni element v P, torej maksimalna linearno neodvisna množica B v L. To pa je seveda vektorska baza za L. ∎

Literatura

[Pri92] Niko Prijatelj. *Osnove matematične logike, 1. del.* DMFA Založništvo, 1992.

[verzija 13. november 2022]