

# Logika in Množice

Vid Drobnič

# Kazalo

<b>1</b>	<b>Množice</b>	<b>4</b>
<b>2</b>	<b>Preslikava ali Funkcija</b>	<b>4</b>
<b>3</b>	<b>Aritmetika Množic</b>	<b>7</b>
3.1	Kartezični produkt ali zmnožek . . . . .	7
3.2	Eksponentna množica . . . . .	8
3.3	Vsota množic . . . . .	8
3.4	Izomorfni množici . . . . .	8
3.5	Kompozitum . . . . .	9
<b>4</b>	<b>Simbolni zapis</b>	<b>11</b>
4.1	Izjavni račun: . . . . .	11
4.2	Predikatni račun: . . . . .	11
4.3	Prednosti veznikov: . . . . .	12
<b>5</b>	<b>Dokazovanje</b>	<b>12</b>
5.1	Oblika dokaza . . . . .	12
5.2	Pravila sklepanja . . . . .	12
5.2.1	Pravila upeljave . . . . .	12
5.2.2	Pravila uporabe . . . . .	13
<b>6</b>	<b>Boolova algebra</b>	<b>14</b>
6.1	Zakoni Boolove algebre . . . . .	14
6.2	Polni nabori . . . . .	16

6.3	Računska pravila . . . . .	16
6.4	Pravila za kvantifikatorje . . . . .	17
<b>7</b>	<b>Definicije in enoličen opis</b>	<b>18</b>
<b>8</b>	<b>Podmnožice</b>	<b>19</b>
<b>9</b>	<b>Potenčne množice</b>	<b>19</b>
9.1	Boolova algebra na $\mathcal{P}(A)$ . . . . .	20
<b>10</b>	<b>Razredi</b>	<b>20</b>
<b>11</b>	<b>Družine množic</b>	<b>22</b>
11.1	Konstrukcija z družinami množic . . . . .	23
11.1.1	Kartezični produkt . . . . .	24
11.1.2	Unija in presek . . . . .	24
11.1.3	Vsota ali koprodukt družine množic . . . . .	25
<b>12</b>	<b>Lastnosti Preslikav, Praslike &amp; Slike</b>	<b>26</b>
12.1	Računska pravila . . . . .	27
<b>13</b>	<b>Relacije</b>	<b>32</b>
13.1	Osnovne lastnosti . . . . .	33
13.2	Operacije na relacijah . . . . .	33
13.3	Graf preslikave . . . . .	34
13.4	Ekvivalenčne relacije in kvocientne množice . . . . .	36
13.4.1	Ekvivalenčni razredi . . . . .	36
13.4.2	Univerzalne lastnosti kvocientnih množic . . . . .	37

13.5 Delne ureditve . . . . .	39
<b>14 Kanonični razcep preslikave</b>	<b>40</b>
14.1 Različica . . . . .	41
<b>15 Indukcija</b>	<b>41</b>
15.1 Peanovi aksiomi: . . . . .	41
15.2 Indukcija na dvojiških drevesih . . . . .	42
15.3 Različica indukcije za $\mathbb{N}$ . . . . .	42

# 1 Množice

$A$  - množica

$x \in A$  -  $x$  je element  $A$

**Načelo ekstenzionalnosti:**

Če imata množici iste elemente, sta enaki.

Končna množica:  $\{a, b, c, \dots, z\}$ , primer:

$$A = \{1, 2, 5\}$$

$$B = \{2, 1, 1, 5\}$$

$$A = B$$

Prazna množica:  $\{\}$  oznaka  $\emptyset$

Enojec:  $\{a\}$

Dvojec ali neurejeni par:  $\{a, b\}$  za katerikoli  $a$  in  $b \Rightarrow$  lahko sta enaka  $\Rightarrow$  enojec je poseben primer dvojca.

$$\{c, c\} = \{c\}$$

Standardni enojec:  $1 = \{\{\}\}$

## 2 Preslikava ali Funkcija

(1) **domena:** množica  $A$

(2) **kodomena:** množica  $B$

(3) **prirejanje:** pove kako elementom iz  $A$  priredimo elemente iz  $B$

- **Celovitost:** vsakemu elementu iz  $A$  priredi vsaj 1 element iz  $B$
- **Enoličnost:** če sta elementu  $x$  prirejena  $y_1$  in  $y_2$ , potem velja  $y_1 = y_2$

$A \rightarrow B$  (brezimna) preslikava iz  $A$  v  $B$

$A$  - domena

$B$  - kodomena

$f : A \rightarrow B$  funkcija (preslikava) poimenovana  $f$

$A \xrightarrow{f} B$

## Funkcijski predpis

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

$x$  se slika v  $1 + x^2$

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

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

Opomba: funkciji manjka še domena in kodomena.

$$\{1, 2, 5\} \rightarrow \{1, 2, 3, 4, \dots, 10\}$$

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

$g(2)$ :  $g$  uporabimo ali apliciramo na argumentu 2

$g : \mathbb{R} \rightarrow \mathbb{R}$ : predpis

$g$ : preslikava

$g(3)$ : število

$g(x)$ : število

(1)  $x \mapsto ax + b$  ( $x$  je vezana spremenljivka,  $a$  in  $b$  sta parametra)

(2)  $a \mapsto ax + b$

(3)  $y \mapsto ay + b$

(1) in (2) sta isti preslikavi.

$$g : \mathbb{R} \rightarrow \mathbb{R}$$

$$g(x) = 1 + x^3$$

$$g(7) = 1 + 7^3$$

Opomba: ni treba izračunati.

$$\mathbb{R} \rightarrow \mathbb{R}$$

$$x \mapsto 1 + x^3$$

$$(x \mapsto 1 + x^3)(7) = 1 + 7^3$$

$$(x \mapsto ax + b)(7) = 7x + b$$

Uporaba funkcije - **aplikacija**.

Preslikave  $\emptyset \rightarrow A$ ?

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

Prيرهjanje “vsi elementi domene se preslikajo v 1”.

$$x \mapsto 1$$

$$x \mapsto 2$$

Preslikavi sta enaki.

Sklep: iz  $\emptyset \rightarrow A$  imamo natanko eno preslikavo.

Opomba: Za vse elemente prazne množice velja karkoli.

$$\mathbb{R} \rightarrow \mathbb{R}$$

$$x \mapsto x \cdot x$$

$$x \mapsto x \cdot x + x - x$$

Preslikavi sta enaki.

**Načelo ekstenzionalnosti preslikav:**

Če imata preslikavi enaki domeni in enaki kodomeni, ter prirejata elementom domene enake vrednosti, potem sta enaki.

$$f : A \rightarrow B$$

$$g : C \rightarrow D$$

Če  $A = C$  in  $B = D$  in za vsak  $x \in A$  velja  $f(x) = g(x)$ , potem  $f = g$ .

Drugače povedano (se izpelje):

Če  $A = C$  in  $B = D$  in za vsak  $x_1, x_2 \in A$  velja, da iz  $x_1 = x_2$  sledi:  $f(x_1) = g(x_2)$ , potem  $f = g$ .

## 3 Aritmetika Množic

### 3.1 Kartezični produkt ali zmnožek

$A$  in  $B$  množici

$A \times B$  zmnožek

Elementi  $A \times B$  so urejeni pari  $(a, b)$ , kjer sta  $a \in A$  in  $b \in B$ .

Projekciji:

$$\pi_1 : A \times B \rightarrow A$$

$$\pi_2 : A \times B \rightarrow B$$

Enačbe:

Za vse  $a \in A$  in  $b \in B$  velja:

$$\pi_1(a, b) = a$$

$$\pi_2(a, b) = b$$

**Ekstenzionalnost za zmnožke:**

Za vse  $p, q \in A \times B$ , če  $\pi_1(p) = \pi_1(q)$  in  $\pi_2(p) = \pi_2(q)$ , potem  $p = q$

$$f : A \times B \rightarrow C$$

$$f : p \mapsto \dots$$

$$f : (x, y) \mapsto \dots x \dots y \dots$$

$$g : A \rightarrow B \times C$$



$$g : a \mapsto (...a..., ...a...)$$

Kaj je  $\emptyset \times A$ ?  $\emptyset \times A = \emptyset$

### 3.2 Eksponentna množica

Če sta  $A$  in  $B$  množici, je  $B^A$  množica vseh preslikav z domeno  $A$  in kodomeno  $B$ .

### 3.3 Vsota množic

Če sta  $A$  in  $B$  množici je vsota  $A + B$  množica.

Za vsak  $a \in A$  je  $\iota_1(a) \in A + B$

Za vsak  $b \in B$  je  $\iota_2(b) \in A + B$

Elementa  $u$  in  $v$  iz  $A + B$  sta enaka, če bodisi obstaja  $a \in A$  da je  $u = \iota_1(a)$  in  $v = \iota_1(a)$ , bodisi obstaja  $b \in B$  da je  $u = \iota_2(b)$  in  $v = \iota_2(b)$ .

$$\{1, 2\} + \{1, 2\} = \{\iota_1(1), \iota_1(2), \iota_2(1), \iota_2(2)\}$$

### 3.4 Izomorfni množici

Def.: Izomorfizem je preslikava  $f : A \rightarrow B$ , za katero obstaja preslikava  $g : B \rightarrow A$ , da je:

- za vsak  $x \in A$  je  $g(f(x)) = x$  in
- za vsak  $y \in B$  je  $f(g(y)) = y$

Pravimo da je  $g$  inverz  $f$ .

Če obstaja izomorfizem  $X \rightarrow Y$ , pravimo, da sta  $X$  in  $Y$  **izomorfni**, pišemo  $X \cong Y$

### 3.5 Kompozitum

$B^A$  je množica preslikav iz  $A$  v  $B$ .

Kompozicija preslikav  $g \circ f$ .

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

$$\circ : C^B \times B^A \rightarrow C^A$$

$$\circ : (g, f) \mapsto (x \mapsto g(f(x))) \text{ (ugnezden funkcijski prepis)}$$

Pišemo  $g \circ f$

Zakaj ne raje  $f \bullet g$ ?

Npr., da imamo:

$$\bullet : B^A \times C^B \rightarrow C^A$$

$$\bullet : (f, g) \mapsto (x \mapsto g(f(x)))$$

Računsko pravilo za  $\circ$ :

$(g \circ f)(a) = g(f(a))$  ✓ izberemo, ker se ohrani vrstni red.

$$(f \bullet g)(a) = g(f(a))$$

Imamo dve preslikavi:

$$\mathbb{R} \rightarrow \mathbb{R}$$

$$x \mapsto 4 - x^2$$

$$\mathbb{R} \rightarrow \mathbb{R}$$

$$x \mapsto 2 - x$$

$$(x \mapsto 4 - x^2) \circ (x \mapsto 2 - x) = (x \mapsto (x \mapsto 4 - x^2)((x \mapsto 2 - x)x))$$

Zaradi dvoumnosti preimenujemo vezane spremenljivke:

$$x \mapsto 4 - x^2 \Rightarrow y \mapsto 4 - y^2$$

$$x \mapsto 2 - x \Rightarrow z \mapsto 2 - z$$

$$(y \mapsto 4 - y^2) \circ (z \mapsto 2 - z) = (x \mapsto (y \mapsto 4 - y^2)((z \mapsto 2 - z)x))$$

**Identiteta** na množici  $A$  je preslikava:

$$id_A : A \rightarrow A$$

$$id_A : x \mapsto x$$

Def:  $f : A \rightarrow B, g : B \rightarrow A$  rečemo, da je  $g$  **inverz**  $f$ , ko velja:

$$f \circ g = id_B \wedge g \circ f = id_A$$

Če ime  $f$  inverz, pravimo, da je *izomorfizem*.

Če obstaja izomorfizem  $A \rightarrow B$ , pravimo, da sta  $A$  in  $B$  **izomorfni** množici.

Pišemo  $A \cong B$

Primeri:

(a)  $A \times \emptyset \cong \emptyset$

$$f : A \times \emptyset \rightarrow \emptyset$$

Predpis ni potreben, ker ni nobenih elementov.

$$g : \emptyset \rightarrow A \times \emptyset$$

Iz prazne množice obstaja ena sama preslikava.

(b)  $1 = \{()\}$

$$A \times 1 \cong A$$

$$f : A \times 1 \rightarrow A$$

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

$$g : A \rightarrow A \times 1$$

$$x \mapsto (x, ())$$

$$A \times 1 \rightarrow A \rightarrow A \times 1$$

$$(x, y) \xrightarrow{f} x \xrightarrow{g} (x, ())$$

(c)  $A^{B \times C} \cong (A^B)^C$

$$\theta : A^{B \times C} \rightarrow (A^B)^C$$

$$\theta : \star \mapsto (c \mapsto (b \mapsto \star(b, c)))$$

$$\phi : (A^B)^C \rightarrow A^{B \times C}$$

$$\phi : \mathcal{C} \mapsto ((\beta, \gamma) \mapsto (\mathcal{C}(\gamma))(\beta))$$

## 4 Simbolni zapis

### 4.1 Izjavni račun:

- konstanti

–  $\perp$  - neresnica

–  $\top$  - resnica

- logični vezniki:

–  $p \wedge q$  -  $p$  in  $q$  ( $p, q$  sta izjavi)

–  $p \vee q$  -  $p$  ali  $q$

–  $p \Rightarrow q$

če  $p$  potem  $q$

iz  $p$  sledi  $q$

$p$  je zadosten (pogoj) za  $q$

$q$  je potreben (pogoj) za  $p$

–  $p \Leftrightarrow q$

$p$  če in samo če  $q$

$p$  čee  $q$

$p$  iff  $q$  (if and only if)  $p$  in  $q$  sta enakovredna ali ekvivalentna

–  $\neg p$  - ne  $p$

### 4.2 Predikatni račun:

Izjavni + **kvantifikatorja**

- univerzalni kvantifikator:

$\forall x \in B. p$

$(\forall x \in B)p$

$\forall x \in B : p$

$\forall x \in B(p)$

“za vsak  $x$  iz  $B$  velja  $p$ ”

“vsi  $x$ -i iz  $B$  zadoščajo  $p$ ”

- eksistenčni kvalifikator

$\exists x \in B.p$

“obstaja  $x$  iz  $B$ , da velja  $p$ ”

“obstaja  $x$  iz  $B$ , za katerega  $p$ ”

“za neki  $x$  iz  $B$  velja  $p$ ”

### 4.3 Prednosti veznikov:

Vezniki si po prednosti sledijo od tistega z največjo, do tistega z najmanjšo v naslednjem vrstnem redu:

$\neg, \wedge, \vee, (\Rightarrow, \Leftrightarrow), (\forall, \exists)$

## 5 Dokazovanje

Dokaz ima drevesno strukturo in more biti končen.

Vedeti moramo:

1. Kaj trenutno dokazujemo
2. Katere *spremenljivke* in *predpostavke* imamo na voljo (kontekst).

### 5.1 Oblika dokaza

Za obliko glej zvezek. Žal se mi ne da prepisovati vseh različnih dokazov in skic kako naj izgledajo.

### 5.2 Pravila sklepanja

#### 5.2.1 Pravila upeljave

1. *Resnica*  $\top$ : je res
2. *Neresnica*  $\perp$ : ni pravila
3. *Konjunkcija*: da dokažemo  $p \wedge q$  moramo dokazati  $p$ , nato pa še  $q$ .

4. *Disjunkcija*: da dokažemo  $p \vee q$  lahko dokažemo  $p$ , ali pa  $q$ .
5. *Implikacija*: da dokažemo  $p \Rightarrow q$ , predpostavimo  $p$  in nato dokažemo  $q$ .
6. *Ekvivalenca*: ker je  $p \Leftrightarrow q$  okrajšava za  $(p \Rightarrow q) \wedge (q \Rightarrow p)$ , to dokažemo tako, da po pravilu 5. najprej dokažemo  $p \Rightarrow q$ , nato pa še  $q \Rightarrow p$ .
7. *Negacija*: za dokaz  $\neg p$  predpostavimo  $p$  in nato dokažemo  $\perp$ . Drugače povedano: “iščemo protislovje”.
8. *Zakon o izključeni tretji možnosti*:<sup>1</sup> vemo da je  $q$  ali pa  $\neg q$ . Ne more biti oboje.
9. *Univerzalni kvalifikator*: za dokaz  $\forall x \in A : p(x)$ , najprej izberemo poljubni  $x$  s trditvijo: “Naj bo  $x \in A$ ”<sup>2</sup>, nato pa dokažemo  $p(x)$ .
10. *Eksistenčni kvalifikator*: da dokažemo  $\exists x \in A : p(x)$ , si izberemo  $x$  s trditvijo: “Vzemimo  $x := a$ ”. Nato najprej dokažemo  $a \in A$  in potem še  $p(a)$ .

### 5.2.2 Pravila uporabe

1. *Resnica*  $\top$ : ni uporabno.
2. *Neresnica*  $\perp$ : če vemo neresnico, lahko dokažemo katerokoli izjavo tako, da uporabimo neresnico.
3. *Konjunkcija*: če vemo  $p \wedge q$ , lahko rečemo da vemo  $p$ , ali pa da vemo  $q$ .
4. *Disjunkcija*: če vemo  $p \vee q$ , lahko dokažemo izjavo tako da “Obravnavamo primera  $p, q$  zaradi  $p \vee q$ ”. Nato imamo dva primera. V enem predpostavimo  $p$ , v drugem pa  $q$ .
5. *Implikacija*: če vemo  $p \Rightarrow q$  in vemo  $p$ , potem vemo  $q$ .
6. *Ekvivalenca*: če vemo  $p \Leftarrow q$  vemo  $p \Rightarrow q$  in  $q \Rightarrow p$ . Prav tako imamo tudi *pravilo zamenjave*, ki pravi, da lahko  $p$  nadomestimo s  $q$  in obratno.
7. *Negacija*: če vemo  $q$  in vemo  $\neg q$ , velja  $\perp$ .

---

<sup>1</sup>posebno, osnovno pravilo

<sup>2</sup> $x$  mora bit “svež”, t.j: trenutno še ne uporabljen.

8. *Univerzalni kvantifikator*: če vemo  $\forall a \in A : p(a)$  in vemo  $a \in A$ , potem vemo  $p(a)$ .
9. *Eksistenčni kvantifikator*: če vemo  $\exists x \in A : p(x)$ , lahko rečemo da imamo  $x \in A$ . Potem vemo  $p(x)$ .

## 6 Boolova algebra

Izjava  $p$  ima *pomen* in *resničnostno vrednost* ( $\perp$  ali  $\top$ ).

V izjavi  $\neg p \vee q$  sta  $p$  in  $q$  *izjavna simbola*.

Množica  $2 = \{\perp, \top\}$  je *množica resničnostnih vrednosti*.

$n$ -člena Boolova preslikava je

$$\underbrace{2 \times 2 \times \cdots \times 2}_n \rightarrow 2$$

Primer:

$$\begin{aligned} 2 \times 2 &\rightarrow 2 \\ (p, q) &\mapsto \neg p \vee q \end{aligned}$$

*Tautologija* je izjava, ki je resnična ne glede na vrednosti parametrov.

### Zakon o zamenjavi ekvivalentnih izjav

Če  $p \iff q$  potem lahko  $p$  nadomestimo s  $q$ , če gledamo le na resničnostno vrednost izjav.

### 6.1 Zakoni Boolove algebre

Operacije:

- Konstanti:  $\top, \perp$
- Negacija:  $\neg$

- Konjunkcija:  $\wedge$
- Disjunkcija:  $\vee$

Konjunkcija:

- $p \wedge q = q \wedge p$
- $p \wedge (q \wedge r) = (p \wedge q) \wedge r$
- $p \wedge \top = p$
- $p \wedge p = p$

Disjunkcija:

- $p \vee q = q \vee p$
- $p \vee (q \vee r) = (p \vee q) \vee r$
- $p \vee \perp = p$
- $p \vee p = p$

Distributivnost:

- $(p \wedge q) \vee r = (p \vee r) \wedge (q \vee r)$
- $(p \vee q) \wedge r = (p \wedge r) \vee (q \wedge r)$

Absorpcija:

- $(q \wedge p) \vee p = p$
- $(q \vee q) \wedge p = p$

Negacija:

- $p \wedge \neg p = \perp$
- $p \vee \neg p = \top$



*Izrek:* (za izjavo  $p$  v kateri nastopajo samo izjavni simboli  $q_1 \dots q_n$ )

1. Če ima izjava dokaz je tautologija.
2. Če je izjava tautologija ima dokaz.

Izrek ne velja za izjave, ki vsebujejo parametre iz množic.

## 6.2 Polni nabori

Nabor operacij je *poln*, če lahko z njim dobimo poljubno resničnostno tabelo.

Primeri:

- $\top, \perp, \wedge, \vee, \neg$  je poln
- $\top, \neg, \wedge$  je poln
- $\perp, \uparrow$  (nand) je poln

## 6.3 Računska pravila

Pravila za  $\top$ :

- $p \vee \top = \top$
- $p \wedge \top = p$
- $\neg \top = \perp$

Pravila za  $\perp$ :

- $p \vee \perp = p$
- $p \wedge \perp = \perp$
- $\neg \perp = \top$

Pravila za negacijo:

- $\neg\neg p = p$
- de Morganova pravila:
  - $\neg(p \wedge q) = \neg p \vee \neg q$
  - $\neg(p \vee q) = \neg p \wedge \neg q$

Ostalo (*kontrapozitivna oblika*):

- $(p \Rightarrow q) = (\neg q \Rightarrow \neg p)$
- $(p \vee q) = (\neg p \Rightarrow q)$
- $(p \Rightarrow q) = (\neg p \vee q)$

Izjava ima lahko dve obliki:

- *konjunktivna* oblika:  $(\neg p \vee q) \wedge r \wedge (r \vee \neg p)$
- *disjunktivna* oblika:  $(u \wedge \neg v) \vee (u \wedge w \wedge \neg u)$

## 6.4 Pravila za kvantifikatorje

- $(\neg\exists x \in A.p(x)) \iff (\forall x \in A.\neg p(x))$
- $(\neg\forall x \in A.p(x)) \iff (\exists x \in A.\neg p(x))$
- $(\forall x \in \emptyset.p(x)) \iff \top$
- $(\exists x \in \emptyset.p(x)) \iff \perp$
- $(p \Rightarrow \forall x \in A.q(x)) \iff (\forall x \in A.p \Rightarrow q(x))$
- $(\forall u \in A \times B.p(u)) \iff (\forall x \in A \forall y \in B.p(x, y))$
- $(\exists u \in A \times B.p(u)) \iff (\exists x \in A \exists y \in B.p(x, y))$
- $(\forall u \in A + B.p(u)) \iff (\forall x \in A.p(\iota_1(x))) \wedge (\forall y \in B.p(\iota_2(y)))$
- $(\forall u \in A \cup B.p(u)) \iff (\forall a \in A.p(a)) \wedge (\forall b \in B.p(b))$
- $(\forall x \in \{a\}.p(x)) \iff p(a)$

- $(\exists x \in \{a\}.p(x)) \iff p(a)$

Dokaza za

$$(\exists x \in \emptyset.p(x)) \iff \perp$$

in

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

se nahajta v zvezku. Sta tudi dokaj samoumevna, zato ju ne bom prepisoval.

## 7 Definicije in enoličen opis

1) Okrajšava, uvedemo nov simbol

$$c := \dots$$

$$c \triangleq \dots$$

$$c \stackrel{\text{def}}{=} \dots$$

$$c = \dots$$

$$f(x) := \dots$$

2) Enoličen opis

$$\exists! x \in A.p(x)$$

$$\exists^1 x \in A.p(x)$$

“obstaja natanko en  $x \in A$ , da velja  $p(x)$ ”

To je okrajšva za:

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

Če dokažemo

$$\exists! x \in A.p(x)$$

potem lahko uvedemo novo oznako  $c$  in pravilo

$$c \in a \text{ in } p(c)$$

Lahko pišemo tudi:

$$\iota x \in A.p(x)$$

kar pomeni “tisti  $x \in A$ , za katerega velja  $p(x)$ ”, podobno kot anonimna funkcija. Primer uporabe:

$$(\iota y \in \mathbb{R}.y^3 = 2)^6 + 7 = 11$$

## 8 Podmnožice

*Definicija:* Za množici  $A$  in  $B$ :

$$\begin{aligned} A \subseteq B &:= \forall x \in A. x \in B \\ \subseteq &:= (A, B) \mapsto \forall x \in A. x \in B \end{aligned}$$

Namesto  $\subseteq (A, B)$  pišemo  $A \subseteq B$ .

Konstrukcija podmnožice:

- množica  $A$
- izjava  $p(x)$ , kjer  $x \in A$

Tvorimo množico:

$$\{x \in A | p(x)\}$$

Elementi te množice so natanko tisti  $a \in A$ , za katere velja  $p(a)$ .

Ostali zapisi so:

$$\begin{aligned} \{x \in A : p(x)\} \\ \{x \in A; p(x)\} \end{aligned}$$

Računski pravili:

- 1)  $(\forall x \in \{y \in A | p(y)\}. q(x)) \iff (\forall z \in A. p(z) \Rightarrow q(z))$
- 2)  $(\exists x \in \{y \in A | p(y)\}. q(x)) \iff (\exists z \in A. p(z) \wedge q(z))$

## 9 Potenčne množice

$\mathcal{P}(A)$  je potenčna množica  $A$ . Njeni elementi so natanko vse podmnožice  $A$ .

Primeri:

$$\begin{aligned} \mathcal{P}(\{1, 7\}) &= \{\emptyset, \{1\}, \{7\}, \{1, 7\}\} \\ \mathcal{P}(\emptyset) &= \{\emptyset\} \end{aligned}$$

Spomnimo:  $2 = \{\perp, \top\}$

Podmnožice  $A$  so preslikave  $A \rightarrow 2$ .

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

$$\mathcal{P}(A) \rightarrow 2^A$$
$$\chi : S \mapsto \left( x \mapsto \begin{cases} \perp & x \notin S \\ \top & x \in S \end{cases} \right)$$

$$2^A \rightarrow \mathcal{P}(A)$$
$$f \mapsto \{x \in A \mid f(x)\}$$

Nato te funkcije se preverimo, kot smo delali že mnogokrat na vajah.

## 9.1 Boolova algebra na $\mathcal{P}(A)$

Imamo operacije  $\cup, \cap$ , komplement

$$S \cap T := \{x \in A \mid x \in S \wedge x \in T\}$$
$$S \cup T := \{x \in A \mid x \in S \vee x \in T\}$$
$$\emptyset := \{x \in A \mid \perp\}$$
$$A := \{x \in A \mid \top\}$$
$$S^C := \{x \in A \mid \neg(x \in S)\}$$

## 10 Razredi

Vzemimo množico vseh množic

$$V = \{x \mid x \text{ je množica}\}$$

Definirajmo podmnožico:

$$R = \{x \in V \mid x \notin x\}$$

Dokazali bomo  $R \notin R$  in  $R \in R$ :

1)  $R \notin R$

Predpostavimo  $R \in R$  in iščemo protislovje. Po predpostavki vemo  $R \in R$ . To pomeni, da po definiciji  $R$  velja  $R \notin R$ , s čimer smo prišli do protislovja, torej velja  $R \notin R$ .

2)  $R \in R$

To bomo dokazali s protislovjem (pozor: prejšni dokaz je bil dokaz negacije!). Predpostavimo  $R \notin R$  in iščemo protislovje. Po predpostavki vemo, da  $R \notin R$ , kar pomeni da po definiciji  $R$  velja  $R \in R$ . Prišli smo do protislovja, kar pomeni da velja  $R \in R$ .

Dokazali smo  $\perp$ , torej velja vse. Tudi takšne nesmiselnosti kot  $0 = 1$ .

Da se znebimo tega problema uvedemo razred, ki ga tvorimo<sup>3</sup>:

$$\{x|p(x)\}$$

Velja:

$$a \in \{x|p(x)\} \iff p(a)$$

Pri tem je  $a$  bodisi osnovni matematični objekt (število, urejeni par) ali množica, ne sme pa biti razred. Drugače povedano: razredi niso elementi.

Razred  $C$  je množica, če lahko tvorimo množico, ki ima iste elemente kot  $C$

$$a \in C \iff a \in S$$

kjer je  $S$  množica.

Vsaka množica  $S$  je razred:

$$\{x|x \in S\}$$

Razred, ki ni množica se imenuje *pravi razred*.

Primeri pravih razredov:

- Razred vseh množic:

$$V = \{x|x \text{ je množica}\} = \{x|\top\}$$

oznaka za tak razred je Set.

---

<sup>3</sup>Tvorba je različna od tvorbe množic. Za množice imamo točno določene načine tvorbe (kartezični produkt, podmnožica, presek, unija, ...)

- $R = \{x | x \notin x\}$
- $\{A | \exists! x \in A : \top\}$  razred vseh enojcev
- $\{X | X \text{ je vektorski prostor}\}$   
 $\{X | X \text{ je grupa}\}$

## 11 Družine množic

Imamo naslednje množice:

$$A_0 = \dots$$

$$A_1 = \dots$$

$$A_2 = \dots$$

Družina množic je preslikava:

$$A : I \rightarrow \text{Set}$$

kjer  $I$  je indeksna množica in  $i \in I$  so indeksi.

Namesto  $A(i)$  pišemo  $A_i$ .

PRIMERI:

- 1) Če imamo množice  $A, B, C, D, E$ , lahko tvorimo družino:

$$I = \{1, 2, 3, 4, 5\}$$

$$Q : I \rightarrow \text{Set}$$

$$Q_1 = A, Q_2 = B, Q_3 = C, Q_4 = D, Q_5 = E$$

- 2) Družina vseh zaprtih intervalov:

$$K = \{(a, b) \in \mathbb{R} \times \mathbb{R} | a \leq b\}$$

$$I : K \rightarrow \text{Set}$$

$$I(a, b) := [a, b] = \{x \in \mathbb{R} | a \leq x \leq b\}$$

- 3) Nekateri elementi družine so lahko enaki:

$$I = \{1, 2, 3, 4, 5\}$$

$$A : I \rightarrow \text{Set}$$

lahko velja  $A_1 = A_3$ .

4) Konstanta družina  $A : I \rightarrow \text{Set}$ .

$$\forall i, j \in I : A_i = A_j$$

5) Prazna družina  $\emptyset \rightarrow \text{Set}$

6) Družina praznih množic

$$\begin{aligned} A : I &\rightarrow \text{Set} \\ \forall i \in I : A_i &= \emptyset \end{aligned}$$

7) Neprazna družina

$$\begin{aligned} A : I &\rightarrow \text{Set} \\ I &\neq \emptyset \end{aligned}$$

8) Družina nepraznih

$$\begin{aligned} A : I &\rightarrow \text{Set} \\ \forall i \in I : A_i &\neq \emptyset \end{aligned}$$

## 11.1 Konstrukcija z družinami množic

Naj bo  $A : I \rightarrow \text{Set}$  družina.

*Funkcija izbire*  $f$  za dano družino  $A$  je prirejanje, ki vsakemu  $i \in I$  priredi natanko en element  $f(i) \in A_i$ .

PRIMER: družina vseh zaprtih intervalov

$$\begin{aligned} I &= \{(a, b) \in \mathbb{R} \times \mathbb{R} \mid a \leq b\} \\ K(a, b) &= [a, b] \\ f(a, b) &= \frac{a+b}{2} \\ g(a, b) &= b \end{aligned}$$

$f$  in  $g$  sta primera funkcije izbire.

Če imamo  $A : I \rightarrow \text{Set}$  in  $A_j = \emptyset$  za neki  $j \in I$ , potem za  $A$  ni nobene funkcije izbire.



### 11.1.1 Kartezični produkt

$$\prod_{i \in I} A_i$$

Elementi so funkcije izbire za  $A$ .

Za vsak  $i \in I$  imamo  $i$ -to projekcijo:

$$\begin{aligned} \pi_i : \prod_{j \in I} A_j &\rightarrow A_i \\ f &\mapsto f(i) \end{aligned}$$

$B \times C$  je poseben primer:

$$B \times C \cong \prod_{i \in I} A_i$$

kjer  $I = \{1, 2\}$  in  $A_1 = B, A_2 = C$ .

Tudi  $C^B$  je poseben primer

$$C^B \cong \prod_{j \in J} D_j$$

kjer  $J = B$  in  $D_j = C$ .

### 11.1.2 Unija in presek

$$\begin{aligned} \bigcup_{i \in I} A_i &= \{x; \exists i \in I : x \in A_i\} \\ \bigcap_{i \in I} A_i &= \{x; \forall i \in I : x \in A_i\} \end{aligned}$$

Presek prazne družine:

$$\bigcap_{i \in \emptyset} A_i \{x; \forall i \in \emptyset : x \in A_i\} = \{x; \top\} = V$$

je pravi razred.

Presek neprazne družine je množica, če imamo  $j \in I$

$$\bigcap_{i \in I} A_i = \{x; \forall i \in I : x \in A_i\} = \{x \in A_j; \forall i \in I : x \in A_i\}$$

AKSIOM O UNIJI: Unija družine množic je množica.

PRIMER:

$$\begin{aligned} A &: \mathbb{N} \rightarrow \text{Set} \\ A_0 &= \mathbb{N} \\ A_1 &= P(\mathbb{N}) \\ A_2 &= P(P(\mathbb{N})) \\ A_{n+1} &= P(A_n) \end{aligned}$$

$\bigcup_{n \in \mathbb{N}} A_n$  je unija po aksiomu.

Računska pravila z  $\in$ :

- $x \in \emptyset \iff \emptyset$
- $x \in A \times B \iff \pi_1(x) \in A \wedge \pi_2(x) \in B$
- $x \in \{y \in A | P(y)\} \iff x \in A \wedge P(x)$
- $x \in A \cup B \iff x \in A \vee x \in B$
- $x \in \bigcup_{i \in I} A_i \iff \exists i \in I : x \in A_i$
- $x \in \bigcap_{i \in I} A_i \iff \forall i \in I : x \in A_i$

### 11.1.3 Vsota ali koproduct družine množic

Družina  $A : I \rightarrow \text{Set}$

$\coprod_{i \in I} A_i$  je koproduct družine  $A$ . Elementi takega koprodukta so  $\iota_k(x)$ , kjer je  $k \in I$  in  $x \in A_k$ .

$$\coprod_{i \in I} A_i = \{\iota_k(x) | k \in I \wedge x \in A_k\}$$

**Opomba:** Na tak način ponavadi zapišemo razred, ki pa v tem primeru ni pravi razred in ga zato lahko obravnavamo kot množico.

$\sum_{i \in I} A_i$  je vsota družine  $A$ . Elementi so tako kot pri koproduktu  $\iota_k(x)$  za  $k \in I$  in  $x \in A_k$ . Elemente lahko zapišemo tudi kot *odvisne pare*  $(k, x)$  za  $k \in I$  in  $x \in A_k$ , kar je samo drug zapis za  $\iota_k(x)$ .

VELJA:

$$B + C \cong \sum_{i \in \{1,2\}} A_i \quad A : \{1,2\} \rightarrow \text{Set}$$

$$A_1 = B$$

$$A_2 = C$$

$$B \times C \cong \sum_{b \in B} A_b \quad A : B \rightarrow \text{Set}$$

$$A_b = C$$

## 12 Lastnosti Preslikav, Praslike & Slike

Naj bodo:

$$f : A \rightarrow B$$

$$S \subseteq A$$

$$T \subseteq B$$

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

$$B \in \mathcal{P}(B)$$

DEFINICIJE:

- *Slika* je množica:

$$f_*(S) = \{y \in B \mid \exists x \in S : f(x) = y\}$$

- *Praslika* je množica:

$$f^*(T) = \{x \in A \mid f(x) \in T\}$$

Poznamo tudi ostale zapise, ki pa so slabši:

- $f_*(S)$  se piše tudi kot  $f(S)$  ali  $f[S]$ .

- $f^*(S)$  se piše tudi kot  $f^{-1}(S)$  ali  $f^{-1}[S]$ .

$$\begin{aligned} f &: A \rightarrow B \\ f_* &: \mathcal{P}(A) \rightarrow \mathcal{P}(B) \\ f^* &: \mathcal{P}(B) \rightarrow \mathcal{P}(A) \end{aligned}$$

Pravimo, da je  $f_*$  *kovariantna* (ne obrne smeri  $f$ ) in da je  $f^*$  *kontravariantna* (obrne smer  $f$ ).

VELJA:

$$\begin{array}{ll} f^*(\emptyset) = \emptyset & f_*(\emptyset) = \emptyset \\ f^*(B) = A & \underbrace{f_*(A)}_{Z_f} \subseteq B \end{array}$$

## 12.1 Računska pravila

$$f : A \rightarrow B \qquad S : I \rightarrow \mathcal{P}(A)$$

$$\begin{aligned} f^*\left(\bigcup_{i \in I} S_i\right) &= \bigcup_{i \in I} f^*(S_i) \\ f^*\left(\bigcap_{i \in I} S_i\right) &= \bigcap_{i \in I} f^*(S_i) \\ f^*(S_1 \cup S_2) &= f^*(S_1) \cup f^*(S_2) \\ f^*(S_1 \cap S_2) &= f^*(S_1) \cap f^*(S_2) \\ f_*\left(\bigcup_{i \in I} S_i\right) &= \bigcup_{i \in I} f_*(S_i) \\ f_*\left(\bigcap_{i \in I} S_i\right) &\subseteq \bigcap_{i \in I} f_*(S_i) \\ f^*(S^{\complement}) &= (f^*(S))^{\complement} \end{aligned}$$

DEFINICIJE injektivne, surjektivne, bijektivne, epi in mono

Naj bo  $f : A \rightarrow B$  preslikava

- $f$  je *injektivna* če velja:

$$\forall x, y \in A : f(x) = f(y) \Rightarrow x = y$$

včasih uporabimo tudi:

$$\forall x, y \in A : x \neq y \Rightarrow f(x) \neq f(y)$$

- $f$  je *surjektivna*, če velja:

$$\forall y \in B \exists x \in A : f(x) = y$$

lahko rečemo tudi, da je zaloga vrednosti za  $f$  celoten  $B$ , kar zapišemo s pomočjo slike:

$$f_*(A) = B$$

- $f$  je *bijektivna* kadar je surjektivna in injektivna. Simbolno to zapišemo kot:

$$\forall y \in B \exists! x \in A : f(x) = y$$

- $f$  je *monomorfizem* (pravimo, da je  $f$  *mono*).

Če za preslikavi  $g, h : C \rightarrow A$  velja:

$$f \circ g = f \circ h \Rightarrow g = h$$

pravimo, da lahko  $f$  *krajsamo* na levi.

DEFINICIJA:  $f : A \rightarrow B$  je *mono*, kadar za vse preslikave  $g, h : C \rightarrow A$  velja:

$$f \circ g = f \circ h \Rightarrow g = h$$

- $f$  je *epimorfizem* (pravimo, da je  $f$  *epi*), kadar velja:

$$\forall C \in \text{Set} \forall g, h : B \rightarrow C : g \circ f = h \circ f \Rightarrow g = h$$

Dokažimo nekatere izjave, ki so na voljo na <https://github.com/andrejbauer/ucbenik-logika-in-mnozice/blob/master/predavanja-2017/07-funkcije.md>.

- 1)  $f$  mono in  $g$  mono  $\Rightarrow g \circ f$  mono.

Naj bo  $f : A \rightarrow B$  in  $g : B \rightarrow C$  in  $k, l : D \rightarrow A$ . Dokazujemo:

$$(g \circ f) \circ k = (g \circ f) \circ l \Rightarrow k = l$$

Predpostavimo

$$(g \circ f) \circ k = (g \circ f) \circ l$$

po definiciji je kompozitum asociativen, torej lahko zapišemo:

$$g \circ (f \circ k) = g \circ (f \circ l)$$

Ker je  $g$  mono, lahko krajšamo  $g$ :

$$f \circ k = f \circ l$$

Ker je  $f$  mono, lahko krajšamo  $f$ :

$$k = l$$

□

3)  $g \circ f$  mono  $\Rightarrow f$  mono

Dokazujemo:

$$f \circ k = f \circ l \Rightarrow k = l$$

Predpostavimo:

$$f \circ k = f \circ l$$

Na vsaki strani lahko enačbo “razširimo” z  $g$ :

$$g \circ f \circ k = g \circ f \circ l$$

Ker je kompozitum asociativen velja:

$$(g \circ f) \circ k = (g \circ f) \circ l$$

Lahko krajšamo  $g \circ f$  po predpostavki:

$$k = l$$

□

Naj bo  $f : A \rightarrow B$

1)  $f$  je mono  $\iff f$  je injektivna

( $\Rightarrow$ ) Prepostavimo:  $f$  je mono in dokazujemo:

$$\forall x, y \in A : f(x) = f(y) \Rightarrow x = y$$

Naj bosta  $x, y \in A$ . Predpostavimo  $f(x) = f(y)$  in dokazujemo  $x = y$ .

Definirajmo:

$$\begin{array}{ll} k : 1 \rightarrow A & l : 1 \rightarrow A \\ * \mapsto x & * \mapsto y \end{array}$$

Spomnimo se:  $1$  je enojec,  $1 = \{*\}$

Trdimo:  $f \circ k = f \circ l$  ker:

$$\begin{aligned} (f \circ k)(*) &= f(k(*)) = f(x) \\ (f \circ l)(*) &= f(l(*)) = f(y) \end{aligned}$$

Po predpostavki  $f(x) = f(y)$  zgornja trditev velja.

Ker je  $f \circ k = f \circ l$  sledi,  $k = l$ , ker je  $f$  mono.

Funkcij  $k$  in  $l$  slikata iz enojca, torej lahko zapišemo:

$$k(*) = l(*)$$

Torej po definiciji  $k$  in  $l$  velja:

$$x = y$$

( $\Leftarrow$ ) Predpostavimo, da je  $f$  injektivna in dokazujemo, da je mono.

Naj bosta  $g, h : C \rightarrow A$ . Predpostavimo  $f \circ g = f \circ h$ . Dokazujemo:

$$g = h \iff \forall c \in C : g(c) = h(c)$$

Naj bo  $c \in C$ . Dokazujemo  $g(c) = h(c)$ . Vemo  $f \circ g = f \circ h$ . Sledi:

$$\Rightarrow (f \circ g)(c) = (f \circ h)(c) \iff f(g(c)) = f(h(c))$$

Ker je  $f$  injektivna sledi:

$$g(c) = h(c)$$

TRDITVI:

- $f$  je *epi*  $\iff f$  surjektivna

- $f$  je izomorfizem  $\iff f$  bijekcija

Dokažimo drugo trditev:

( $\Rightarrow$ ) Dokazujemo  $f$  izo  $\Rightarrow f$  bijekcija. Predpostavimo, da je  $f$  izomorfizem in dokazujemo, da je bijekcija. Po definiciji bijekcije to pomeni, da je injektivna in surjektivna. Po prejšnjih trditvah velja, da mora biti  $f$  mono in epi.

1.  $f$  je mono

Vemo  $id_A = f^{-1} \circ f$  in  $id_A$  je mono. Torej je  $f^{-1} \circ f$  mono. Spomnimo se trditve od zadnjič:

$$g \circ h \text{ mono} \Rightarrow h \text{ mono}$$

Torej je  $f$  mono.

2.  $f$  je epi: podoben dokaz kot za 1. točko.

Vemo  $id_B = f \circ f^{-1}$  in  $id_B$  je epi. Torej je  $f \circ f^{-1}$  epi. Ponovno se spomnimo trditve od zadnjič:

$$g \circ h \text{ epi} \Rightarrow g \text{ epi}$$

Sledi  $f$  je epi.

( $\Leftarrow$ )  $f$  je bijekcija  $\Rightarrow f$  je izomorfizem.

Predpostavimo, da je  $f$  bijekcija in dokazujemo, da je izomorfizem. Po definiciji izomorfizma:

$$\exists g : B \rightarrow A : f \circ g = id_B \wedge g \circ f = id_A$$

Definirajmo  $g : B \rightarrow A$  s predpisom:

$$g(y) = \text{“tisti } x \in A \text{ za katerega je } f(x) = y\text{”}$$

Utemeliti moramo:

$$\forall y \in B \exists! x \in A : f(x) = y$$

Z drugimi besedami:

1.  $g$  je celovit predpis:

$$\forall y \in B \exists x \in A : f(x) = y$$

Opazimo, da je to definicija surjektivnosti in velja, ker je  $f$  bijektivna.



2.  $g$  je enoličen predpis:

$$\forall y \in B \forall x_{1,2} \in A : f(x_1) = y \wedge f(x_2) = y \Rightarrow x_1 = x_2$$

Vemo injektivnost  $f$ :

$$\forall z_1, z_2 \in A : f(z_1) = f(z_2) \Rightarrow z_1 = z_2$$

Če velja  $f(x_1) = y$  in  $f(x_2) = y$ , potem velja  $f(x_1) = f(x_2)$ , torej tudi  $x_1 = x_2$  ker  $f$  injektivna.

Sedaj vemo, da je  $g$  dobro definirana funkcija. Preverimo:

1.  $f \circ g = id_B$

Naj bo  $y \in B$  Preverimo  $f(g(y)) = y$ . Velja po definiciji  $g$ .

2.  $g \circ f = id_A$

Naj bo  $x \in A$  Preverimo  $g(f(x)) = x$ . Po definiciji  $g$  je to tisti element, ki ga  $f$  slika v  $f(x)$ . Torej velja.

□

## 13 Relacije

DEFINICIJA: Relacija na množicah  $A_1, A_2, \dots, A_n$  je podmnožica  $A_1 \times A_2 \times \dots \times A_n$ .

PRIMERI:

- “točka  $A$  je med točkama  $B$  in  $C$ ”. (trojiška relacija)
- $R \subseteq A_1 \times A_2$  dvojiška relacija na  $A_1, A_2$
- $R \subseteq A \times A$  relacija na  $A$ .

PRIMERI:

- $\leq$  je relacija na  $\mathbb{R}$  in lahko zapišemo:

$$\leq \subseteq \mathbb{R} \times \mathbb{R}$$

- $R \subseteq A \times B, a \in A, b \in B$   $(a, b) \in R$  preberemo kot: “ $a$  in  $b$  sta v relaciji  $R$ ”. Zapišemo tudi

$$aRb$$

PRIMER:  $a \leq b$  lahko zapišemo kot  $(a, b) \in \leq$

## 13.1 Osnovne lastnosti

Naj bo  $R \subseteq A \times A$ .

- **refleksivnost**  $\forall x \in A : xRx$   $=, \leq$
- **irefleksivnost**  $\forall x \in A : \neg(xRx)$   $<, \perp$
- **simetričnost**  $\forall x, y \in A : xRy \Rightarrow yRx$   $\perp, \parallel, =$
- **asimetričnost**  $\forall x, y \in A : xRy \Rightarrow \neg(yRx)$   $<$
- **antisimetričnost**  $\forall x, y \in A : xRy \wedge yRx \Rightarrow x = y$   $\leq$
- **tranzitivnost**  $\forall x, y, z \in A : xRy \wedge yRz \Rightarrow xRz$   $<, \leq, \parallel$
- **sovisnost**  $\forall x, y \in A : x \neq y \Rightarrow xRy \vee yRx$   $<, \leq$
- **stroga sovisnost**  $\forall x, y \in A : xRy \vee yRx$   $\leq$

DEFINICIJE:

- *Prazna relacija* na  $A$  je  $\emptyset$ .
- *Polna relacija* na  $A$  je  $A \times A$ .
- *Enakost* na  $A$  je relacija  $\{(x, y) \in A \times A \mid x = y\} \subseteq A \times A$ .

Relacije lahko predstavimo kot grafe (tiste iz teorije grafov, ne kot grafe funkcij).

## 13.2 Operacije na relacijah

### Transponirana relacija

Naj bo  $R \subseteq A \times B$ .

$$R^T \subseteq B \times A$$

Definiramo kot

$$R^T := \{(b, a) \in B \times A \mid (a, b) \in R\}$$

PRIMERA:  $\leq^T = \geq$  in  $\subseteq^T = \supseteq$

Velja:

$$(R^\top)^\top = R$$

Relacijo in njeno transpozicijo lahko predstavimo kot tabelo:

Tabela 1: Relacija  $R$

$R$	1	2	3
$a$	$\perp$	$\top$	$\top$
$b$	$\perp$	$\perp$	$\top$

Tabela 2: Transponirana relacija  $R$

$R^\top$	$a$	$b$
1	$\perp$	$\perp$
2	$\top$	$\perp$
3	$\top$	$\top$

## Kompozicija relacij

Naj bosta  $R \subseteq A \times B$  in  $S \subseteq B \times C$  relaciji.

Kompozicijo  $S \circ R \subseteq A \times C$  definiramo kot<sup>4</sup>:

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

TRDITEV: Kompozicija relacij je asociativna:

$$(S \circ R) \circ T = S \circ (R \circ T)$$

DEFINIRAMO:

$$\underbrace{R \circ R \circ R \circ \dots \circ R}_n =: R^n$$

## 13.3 Graf preslikave

Naj bo  $f : A \rightarrow B$ . Graf je  $\Gamma_f \subseteq A \times B$  definiran z:

$$\Gamma_f := \{(x, y) \mid f(x) = y\}$$

$\Gamma_f$  ima lastnost:

---

<sup>4</sup>Vrstni red je nekoliko zmeden in je potrebno biti nanj pozoren. Jaz si zapomnim na sledeč način: gremo iz  $A$  v  $C$ , torej gremo najprej čez relacijo  $R$ , in nato čez relacijo  $S$ . Tako kot kompozitum funkcij, pa se ta zapiše iz desne proti levi. Torej  $S \circ R$  preberemo: "gremo čez  $R$  in nato čez  $S$ ." Čedalje bolj verjamem, da si je kompozitum izmislil fizik, ker gre vse v rikverc in je zmedeno.

1. Celovita relacija
2. Enolična relacija

DEFINICIJA:  $R \subseteq A \times B$  je:

1. *celovita*, če velja:

$$\forall x \in A \exists y \in B : xRy$$

2. *enolična*, če velja:

$$\forall x \in A \forall y, z \in B : xRy \wedge xRz \Rightarrow y = z$$

$R$  je *funkcijska relacija*, če je celovita in enolična.

TRDITEV:

1. Za vsako  $f : A \rightarrow B$  je  $\Gamma_f$  funkcijska relacija.
2. Vsaka funkcijska relacija je graf neke funkcije.

DOKAZ:

1. Opazimo, da je  $R$  funkcijska  $\iff \forall x \in A \exists! y \in B : xRy$ . Ali je  $\Gamma_f$  funkcijska?

$$\forall x \in A \exists! y \in B : (x, y) \in \Gamma_f \iff \forall x \in A \exists! y \in B : f(x) = y$$

Veja, ker je  $f$  preslikava.

2. Denimo, da je  $R \subseteq A \times B$  funkcijska. Dokazujemo:

$$\exists f : A \rightarrow B : R = \Gamma_f$$

Vzemimo  $f : A \rightarrow B$  s predpisom:

$$f(x) = \text{tisti } y \in B, \text{ da velja } xRy = \iota y \in B : xRy$$

Preverimo  $R = \Gamma_f$

**Poanta**<sup>5</sup>

$$B^A \cong \{R \subseteq A \times B \mid R \text{ funkcijska}\}$$

Torej lahko funkcije definiramo kot funkcijske relacije.

---

<sup>5</sup>za ljubitelje slovenščine: izraz je uporabil profesor, jaz pa se ne morem spomniti boljšega

## 13.4 Ekvivalenčne relacije in kvocientne množice

DEFINICIJA:  $R \subseteq A \times A$  je *ekvivalenčna*, ko je refleksivna, simetrična in tranzitivna. Uporabljamo simbole  $= \equiv \cong \approx$ .

PRIMERI: enakost  $=$ , polna relacija na  $A$ .

Naj bo  $f : A \rightarrow B$  in definiramo  $R \subseteq A \times A$  s

$$xRy \iff f(x) = f(y)$$

Tedaj je  $R$  ekvivalenčna. Pravimo, da je  $R$  *inducirana* s  $f$ .

### 13.4.1 Ekvivalenčni razredi

Naj bo  $R \subseteq A \times A$  ekvivalenčna. Za  $x \in A$  definiramo ekvivalenčni razred  $x$

$$[x]_R := \{y \in A \mid xRy\}$$

Za  $x, y$  velja:

$$\begin{aligned} xRy &\iff [x]_R = [y]_R \\ &\iff x \in [y]_R \\ &\iff y \in [x]_R \end{aligned}$$

PRIMER: Relacija  $\sim$  na  $\mathbb{Z}$ .

$$\begin{aligned} m \sim n &\iff m \mid n \wedge n \mid m \\ [12]_{\sim} &= \{12, -12\} \\ [-2]_{\sim} &= \{2, -2\} \\ [0]_{\sim} &= \{0\} \end{aligned}$$

Če je  $R \subseteq A \times A$  ekvivalenčna, velja:

- ekvivalenčni razredi so neprazni:  $x \in [x]_R$  (Če  $A = \emptyset \Rightarrow$  ni ekvivalenčnih razredov)
- $[x]_R \cap [y]_R \neq \emptyset \Rightarrow [x]_R = [y]_R$

Pravimo, da ekvivalenčni razredi tvorijo *particijo* ali *razdelitev*  $A$ .

Ekvivalenčno relacijo lahko podamo z ekvivalenčnimi razredi tako, da podamo družino  $\{E_i\}, i \in I$ , da velja:

- $E_i \neq \emptyset \forall i \in I$  neprazni
- paroma diskunktni
- $\bigcup E_i = A$  tvorijo pokritje  $A$

Pripadajoča  $R \subseteq A \times A$  je:

$$xRy \iff \exists i \in I : x \in E_i \wedge y \in E_i$$

### 13.4.2 Univerzalne lastnosti kvocientnih množic

DEFINICIJA: Naj bo  $R \subseteq A \times A$ . Kvocientna množica je:

$$\begin{aligned} A/R &:= \{[x]_R : x \in A\} \\ &:= \{S : \exists x \in A : S = [x]_R\} \\ &:= \{S \in \mathcal{P}(A) : \exists x \in A : S = [x]_R\} \\ &:= \{S \in \mathcal{P}(A) : \exists x \in A \forall y \in A : y \in S \iff xRy\} \end{aligned}$$

#### Kvocientna preslikava

$$\begin{aligned} q_R : A &\rightarrow A/R \\ x &\mapsto [x]_R \end{aligned}$$

$q_R$  je surjektivna:  $\forall \xi \in A/R \exists x \in A : q_R(x) = \xi$

Naj bo  $\xi \in A/R$ . Tedaj obstaja  $y \in A$ , da je  $\xi = [y]_R$ . Vzamemo  $x := y$ . Preverimo  $q_R(x) = \xi$ .

$$q_R(x) = q_R(y) = [y]_R = \xi$$

IZREK: Naj bo  $R \subseteq A \times A$  ekvivalenčna relacija in  $f : A \rightarrow B$  preslikava, ki je *skladna* z  $R$ , kar pomeni:

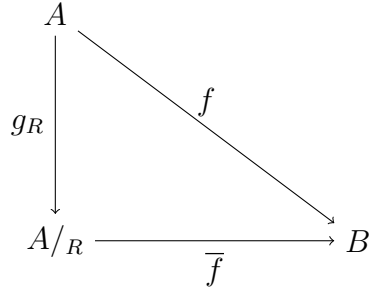
$$xRy \Rightarrow f(x) = f(y)$$

Pravimo tudi, da je  $f$  *kongluenca* za  $R$ .

Tedaj obstaja natanko ena preslikava  $\bar{f} : A/R \rightarrow B$ , da velja

$$f = \bar{f} \circ q_R$$

DOKAZ: Pokazati moramo, enoličnost in obstoj  $\bar{f}$ .



**Enoličnost:** denimo, da imamo  $\overline{f_1}, \overline{f_2} : A/R \rightarrow B$  in

$$f = \overline{f_1} \circ g_R \quad \text{in} \quad f = \overline{f_2} \circ g_R$$

Dokazujemo  $\overline{f_1} = \overline{f_2}$ . Vemo

$$\overline{f_1} \circ g_R = f = \overline{f_2} \circ g_R$$

Ker je  $g_R$  surjektivna, je epi

$$\overline{f_1} = \overline{f_2}$$

**Obstoj:** Vzemimo  $\overline{f} : A/R \rightarrow B$  definirano z:

$$\overline{f}(S) := \iota b \in B \exists x \in A : b = f(x) \wedge [x]_R = S$$

Preverimo, da je  $\overline{f}$  dobro definirana:

1. **Celovitost:** naj bo  $S \in A/R$ . Ker je  $S \in A/R$ , obstaja  $x \in A$ , da je  $[x]_R = S$ . Za  $b$  vzemimo  $b := f(x)$ . Teda j velja  $b = f(x)$ .
2. **Enoličnost:** Če imamo:

$$b_1 \in B \exists x_1 \in A : b_1 = f(x_1) \wedge [x_1] = S$$

$$b_2 \in B \exists x_2 \in A : b_2 = f(x_2) \wedge [x_2] = S$$

Dokazujemo  $b_1 = b_2$ . Ker  $[x_1] = S = [x_2]$ , velja  $x_1 R x_2$ . Ker je  $f$  skladna z  $R$ , velja  $f(x_1) = f(x_2)$ , torej:

$$b_1 = f(x_1) = f(x_2) = b_2$$

□

## 13.5 Delne ureditve

DEFINICIJA: Relacija  $R \subseteq A \times A$  je *šibka ureditev*, če je refleksivna in tranzitivna.  $R$  je *delna ureditev*, če je refleksivna, tranzitivna in antisimetrična. Za delno ureditev uporabljamo simbole  $\leq \sqsubseteq \preceq \subseteq$ .

PRIMERI:

- običajna relacija „manjši ali enak” na  $\mathbb{R}$
- tudi „večji ali enak”
- „deli” na  $\mathbb{N}$
- $=$  na  $A$

PROTIPRIMERI:

- $<$  na  $\mathbb{R}$
- „deli” na  $\mathbb{Z}$  ( $2 \mid -2 \wedge -2 \mid 2$  ampak  $2 \nmid -2$ )

DEFINICIJA:  $R \subseteq A \times A$  delna ureditev, je *linear*, če velja

$$\forall x, y \in A : xRy \vee yRx$$

PRIMERI:

- $\leq$  na  $\mathbb{Q}$  linear
- $=$  na  $\mathbb{Q}$  ni linear
- $\subset$  na  $\mathcal{P}(\mathbb{N})$  ni linear

Narišemo lahko *Hassejev diagram* (glej zvezek kako izgleda).

DEFINICIJA: Naj bo  $(A, \leq)$  delna ureditev in naj bo  $S \subseteq A$ .

- $x \in A$  je *spodnja meja* za  $S$ , če velja  $\forall y \in S : x \leq y$
- $x \in A$  je *zgornja meja* za  $S$ , če velja  $\forall y \in S : x \geq y$



- $x \in A$  je *natančna zgornja meja* za  $S$ , če velja
  1.  $x$  je zgornja meja
  2.  $\forall y \in A : y \text{ zgornja meja za } S \Rightarrow x \leq y$

Pravimo, da je  $x$  *supremum*  $S$ .

- *infimum* ali *natančna spodnja meja* podobno.

## 14 Kanonični razcep preslikave

Naj bo preslikava  $f : A \rightarrow B$ . Definiramo:

$$\begin{aligned}\sim &: x \sim y \Rightarrow f(x) = f(y) \\ q(x) &:= [x]_{\sim} \\ b([x]_{\sim}) &:= f(x) \\ i(y) &:= y\end{aligned}$$

- $q$  epi:  $q$  je surjektivna, ker so ekvivalenčni razredi neprazni
- $i$  je mono:  $i$  je injektivna  $i(y) = i(z) \Rightarrow y = z$
- $b$  je izo:

$$\begin{aligned}c &: f_*(A) \rightarrow A/\sim \\ f_*(A) &= \{y \in B : \exists x \in A : f(x) = y\} \\ c(y) &= [x]_{\sim} \text{ če velja } f(x) = y \\ &:= f^*(\{y\}) = \{x \in A : f(x) = y\}\end{aligned}$$

Trdimo, da je  $\{x \in A : f(x) = y\}$  ekvivalenčni razred za  $y$ :

- je neprazna, ker je  $y \in f_*(A)$ , torej obstaja  $x_0 \in A$ , da je  $f(x_0) = y$
- $x', x'' \in f^*(\{y\}) \Rightarrow f(x') = y = f(x'') \Rightarrow x' \sim x''$
- če  $x' \sim x_0$  potem je  $x' \in f^*(\{y\})$

$$x' \sim x_0 \Rightarrow f(x') = f(x_0) = y \Rightarrow x' \in f^*(\{y\})$$

Preveriti je treba:

- $b(c(y)) = y \quad \forall y \in f_*(A)$
- $c(b([x]_{\sim})) = [x]_{\sim} \quad \forall x \in A$

Preostane še  $f = i \circ b \circ q$

$$i(b(q(x))) = i(b([x]_{\sim})) = i(f(x)) = f(x)$$

## 14.1 Različica

Vsak  $f$  lahko razcepimo na  $f = m \circ e$ . Vzamemo  $e = b \circ q$  in  $m = i$  v zgornjem razcepu

IZREK: Kanonični razcep preslikave je enoličen do izomorfizma natančno.

## 15 Indukcija

### 15.1 Peanovi aksiomi:

1.  $\forall n \in \mathbb{N} : n^+ \neq 0$
2.  $\forall n, m \in \mathbb{N} : n^+ = m^+ \Rightarrow n = m$
3.  $\forall n \in \mathbb{N} : n + 0 = n$
4.  $\forall n, m \in \mathbb{N} : n + m^+ = (n + m)^+$
5.  $\forall n \in \mathbb{N} : n \cdot 0 = 0$
6.  $\forall n, m \in \mathbb{N} : n \cdot m^+ = n + n \cdot m$
7. *Princip indukcije:* Za vsako izjavo  $\varphi(n)$ , kjer  $n \in \mathbb{N}$  velja:

$$\begin{aligned} & \varphi(0) \wedge (\forall k \in \mathbb{N} : (\varphi(k) \Rightarrow \varphi(k^+))) \Rightarrow \forall n \in \mathbb{N} : \varphi(n) \\ & \forall S \subseteq \mathbb{N} : 0 \in S \wedge (\forall k \in \mathbb{N} : k \in S \Rightarrow k^+ \in S) \Rightarrow S = \mathbb{N} \end{aligned}$$

UPORABA INDUKCIJE: Za vsak  $n \in \mathbb{N}$  dokaži  $\varphi(n)$ .

Dokaz z indukcijo:

- baza (osnova) indukcije: preverimo  $\varphi(0)$
- indukcijski korak: predpostavimo  $\varphi(k)$  in dokazujemo  $\varphi(k^+)$

IZREK:  $\forall n \in \mathbb{N} : 0 + n = n$

DOKAZ: z indukcijo

- baza:  $0 + 0 = 0$  zaradi (3)
- korak: predpostavimo  $0 + n = n$  (IH)  
Dokazujemo  $0 + n^+ = n^+$

$$0 + n^+ = (0 + n)^+ = n^+$$

## 15.2 Indukcija na dvojiških drevesih

Imamo prazno drevo in sestavljeno drevo.

**Aksiomi za drevesa:**  $(\mathbb{D}, \text{Empty}, \text{Tree})$

- $\text{Empty} \in \mathbb{D}$
- $\text{Tree}(\text{Empty}, \text{Empty})$
- $\text{Tree}(\text{Empty}, \text{Tree}(\text{Empty}, \text{Tree}(\text{Empty}, \text{Empty})))$

## 15.3 Različica indukcije za $\mathbb{N}$

$$\forall S \subseteq \mathbb{N} : (\forall m \in \mathbb{N} : (\forall k \in \mathbb{N} : k < m \Rightarrow k \in S) \Rightarrow m \in S) \Rightarrow S = \mathbb{N}$$

Z besedami: Denimo, da ima  $S$  lastnost:

Če so vsi predhodniki  $m$  v  $S$  je tudi  $M \in S$ .

Potem je  $S = \mathbb{N}$ .

Iz tega sledi, da je  $0 \in S$  na prazno izpolnjen.

DEFINICIJA: *Stroga* delna ureditev je  $R \subseteq A \times A$ , ki je

1. irefleksivna

2. tranzitivna

Stroga delna ureditev je *linearna*, če je

3. sovisna  $\forall x, y \in A : x \neq y \Rightarrow xRy \vee yRx$

Za stroge ureditve uporabljamo:  $<, \sqsubset, \subset, \prec$

DEFINICIJA: Relacija  $R \subseteq A \times A$  je *dobro osnovana*, če

$$\forall S \subseteq A : (\forall y \in A : (\forall x \in A : xRy \Rightarrow x \in S) \Rightarrow y \in S) \Rightarrow S = A$$

$R$  je *dobra ureditev*, če je strogo linearna in je dobro osnovana.

IZREK: Naj bo  $\sqsubset$  stroga linearna ureditev na  $A$ . Ekvivalentne so izjave:

1.  $\sqsubset$  je dobra ureditev
2. vsaka neprazna  $S \subseteq A$  ima prvi element

$$\exists x \in S \forall y \in S : x \neq y \Rightarrow x \sqsubset y$$

3.  $A$  nima padajoče verige:

Padajoča veriga je zaporedje  $a : \mathbb{N} \rightarrow A$ , da velja  $a_{n+1} \sqsubset a_n$  za vse  $n \in \mathbb{N}$ . To je:

$$\cdots \sqsubset a_3 \sqsubset a_2 \sqsubset a_1 \sqsubset a_0$$

PRIMERI

1. Relacija  $<$  na  $\mathbb{R}$ : (2) ne velja za  $(0, 1) \Rightarrow <$  na  $\mathbb{R}$  ni dobra ureditev
2.  $A = \mathbb{N} \cup \{\omega\}$  uredimo:

$$0 < 1 < 2 < \cdots < \omega$$

$$x < y \iff (y = \omega \wedge x \in \mathbb{N}) \vee (y, x \in \mathbb{N} \wedge x < y \text{ običajno za } \mathbb{N})$$

Velja (3): ni neskončnih padajočih verig  $\Rightarrow$  je dobra ureditev

3.

$$0 < 1 \cdots < \omega < \omega + 1 < \cdots < \omega + \omega < \omega + \omega + 1 \cdots < \omega + \omega + \omega$$