Logika in Množice

Vid Drobnič

Kazalo

1 Množice

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

Načelo ekstenzionalnosti:

Če imata množici iste elemte, sta enaki.

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

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

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

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

Enojec: $\{a\}$

Dvojec ali neurejeni par: $\{a, b\}$ za katerikoli a in $b \Rightarrow$ lahko sta enaka $\Rightarrow$ enojec je posebni 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 elemnte 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 $y_1 = y_2$

$A \to B$ (brezimna) preslikava iz A v B
A - domena
B - kodomena

$f : A \to B$ 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.

$$\{1, 2, 5\} \to \{1, 2, 3, 4, ...10\}$$
$$x \mapsto 1 + x^2$$

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

$g : \mathbb{R} \to \mathbb{R}$: 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.

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

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

Opomba: ni treba izračunati.

$$\mathbb{R} \to \mathbb{R}$$
$$x \mapsto 1 + x^3$$
$$(x \mapsto 1 + x^3)(7) = 1 + 7^3$$
$$(x \mapsto ax + b)(7) = 7x + b$$

Uporaba funkcije - **aplikacija.**

Preslikave $\varnothing \to A$?

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

Prirejanje "vsi elementi domene se preslikajo v 1".

$$x \mapsto 1$$
$$x \mapsto 2$$

Preslikavi sta enaki.

Sklep: iz $\varnothing \to A$ imamo natanko eno preslikavo.

Opomba: Za vse elemente prazne množice velja karkoli.

$$\mathbb{R} \to \mathbb{R}$$
$$x \mapsto x \cdot x$$
$$x \mapsto x \cdot x + x - x$$

Preslikavi sta enaki.

Načelo ekstenzionalnosti preslikav:

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

$$f : A \to B$$
$$g : C \to D$$

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:

$$\pi_1 : A \times B \to A$$
$$\pi_2 : A \times B \to B$$

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 $p = q$

$$f : A \times B \to C$$
$$f : p \mapsto ...$$
$$f : (x, y) \mapsto ...x...y...$$

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

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

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

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 $f : A \to B$, za katero obstaja preslikava $g : B \to A$, 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 $X \to Y$, 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 $g \circ f$.

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

$$\circ : C^B \times B^A \to C^A$$
$$\circ : (g, f) \mapsto (x \mapsto g(f(x))) \text{ (ugnezden funkcijski prepis)}$$

Pišemo $g \circ f$

Zakaj ne raje $f \bullet g$?

Npr., da imamo:

$$\bullet : B^A \times C^B \to C^A$$
$$\bullet : (f, g) \mapsto (x \mapsto g(f(x)))$$

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:

$$\begin{array}{cc} \mathbb{R} \to \mathbb{R} & \mathbb{R} \to \mathbb{R} \\ x \mapsto 4 - x^2 & x \mapsto 2 - x \end{array}$$

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

Zaradi dvoumnosti preimenujemo vezane spremenljivke:

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

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

Identiteta na množici A je preslikava:

$$id_A : A \to A$$
$$id_A : x \mapsto x$$

Def: $f : A \to B, g : B \to A$ 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 $A \to B$, pravimo, da sta A in B **izomorfni** množici. Pišemo $A \cong B$

Primeri:

(a) $A \times \varnothing \cong \varnothing$
$f : A \times \varnothing \to \varnothing$
Predpis ni potreben, ker ni nobenih elementov.
$g : \varnothing \to A \times \varnothing$
Iz prazne množice obstaja ena sama preslikava.

(b) $1 = \{()\}$
$A \times 1 \cong A$

$$f : A \times 1 \to A \qquad g : A \to A \times 1$$
$$(x, y) \mapsto x \qquad x \mapsto (x, ())$$

$$A \times 1 \to A \to A \times 1$$
$$(x, y) \overset{f}{\mapsto} x \overset{g}{\mapsto} (x, ())$$

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

$$\theta : A^{B \times C} \to (A^B)^C$$
$$\theta : ☼ \mapsto (c \mapsto (b \mapsto ☼(b, c)))$$

$$\phi : (A^B)^C \to A^{B \times C}$$
$$\phi : ☾ \mapsto ((\beta, \gamma) \mapsto (☾(\gamma))(\beta))$$

4 Simbolni zapis

4.1 Izjavni račun:

- konstanti
  - $\bot$ - 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:

  $\forall x \in B.p$ — "za vsak x iz B velja p"
  $(\forall x \in B)p$
  $\forall x \in B : p$ — "vsi x-i iz B zadoščajo p"
  $\forall x \in B(p)$

- 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* $\bot$*:* 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 $\bot$. Drugače povedano: "iščemo protislovje".

8. *Zakon o izključeni tretji možnosti:*[1] 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 $x \in A$"[2], 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* $\bot$*:* če vemo neresnico, lahko dokažemo katerokli 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 $\bot$.

[1] posebno, osnovno pravilo

[2] 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* ($\bot$ ali $\top$).

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

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

n-člena Boolova preslikava je

$$\underbrace{2 \times 2 \times \cdots \times 2}_{n} \to 2$$

Primer:

$$2 \times 2 \to 2$$
$$(p, q) \mapsto \neg p \vee q$$

Tavtologija 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: $\top, \bot$
- 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:

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

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:

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

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

1. Če ima izjava dokaz je tavtologija.
2. Če je izjava tavtologija 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:

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

6.3 Računska pravila

Pravila za $\top$:

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

Pravila za $\bot$:

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

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

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

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

Dokaza za

$$(\exists x \in \varnothing.p(x)) \iff \bot$$

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

$$c := \cdots$$
$$c \stackrel{\triangle}{=} \cdots$$
$$c \stackrel{\text{def}}{=} \cdots$$
$$c = \cdots$$
$$f(x) := \cdots$$

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:

$$A \subseteq B := \forall x \in A.x \in B$$
$$\subseteq := (A, B) \mapsto \forall x \in A.x \in B$$

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

Ostali zapsi so:

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

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:

$$\mathcal{P}(\{1, 7\}) = \{\varnothing, \{1\}, \{7\}, \{1, 7\}\}$$
$$\mathcal{P}(\varnothing) = \{\varnothing\}$$

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

Podmnožice A so preslikave $A \to 2$.

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

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

$$\begin{aligned} 2^A &\to \mathcal{P}(A) \\ f &\mapsto \{x \in A | f(x)\} \end{aligned}$$

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

$$\begin{aligned} S \cap T &:= \{x \in A | x \in S \wedge x \in T\} \\ S \cup T &:= \{x \in A | x \in S \vee x \in T\} \\ \varnothing &:= \{x \in A | \bot\} \\ A &:= \{x \in A | \top\} \\ S^C &:= \{x \in A | \neg(x \in S)\} \end{aligned}$$

10 Razredi

Vzemimo množico vseh množic

$$V = \{x | x \text{ je množica}\}$$

Definirajmo podmnožico:

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

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 protilsovja, torej velja $R \notin R$.

2) $R \in R$

   To bomo dokazali s protislovjem (pozor: prejšen 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[3]:

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

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.

[3]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
- $\{X | X$ je vektorski prostor$\}$
  $\{X | X$ je grupa$\}$

11 Družine množic

Imamo naslednje množice:

$$A_0 = \cdots$$
$$A_1 = \cdots$$
$$A_2 = \cdots$$

Družina množic je preslikava:

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

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:

$$I = \{1, 2, 3, 4, 5\}$$
$$Q : I \to \text{Set}$$
$$Q_1 = A, Q_2 = B, Q_3 = C, Q_4 = D, Q_5 = E$$

2) Družina vseh zaprtih intervalov:

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

3) Nekateri elementi družine so lahko enaki:

$$I = \{1, 2, 3, 4, 5\}$$
$$A : I \to \text{Set}$$

lahko velja $A_1 = A_3$.

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

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

5) *Prazna družina* $\varnothing \to \text{Set}$

6) *Družina praznih množic*

$$A : I \to \text{Set}$$
$$\forall i \in I : A_i = \varnothing$$

7) *Neprazna družina*

$$A : I \to \text{Set}$$
$$I \neq \varnothing$$

8) *Družina nepraznih*

$$A : I \to \text{Set}$$
$$\forall i \in I : A_i \neq \varnothing$$

11.1 Konstrukcija z družinami množic

Naj bo $A : I \to \text{Set}$ 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

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

f in g sta primera funkcije izbire.

Če imamo $A : I \to \text{Set}$ in $A_j = \varnothing$ 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:

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

$B \times C$ 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:

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

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:

$$A : \mathbb{N} \to \text{Set}$$
$$A_0 = \mathbb{N}$$
$$A_1 = P(\mathbb{N})$$
$$A_2 = P(P(\mathbb{N}))$$
$$A_{n+1} = P(A_n)$$

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

Računska pravila z $\in$:

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

11.1.3 Vsota ali koprodukt družine množic

Družina $A : I \to \text{Set}$

$\coprod_{i \in I} A_i$ je koprodukt 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:

$$B + C \cong \sum_{i \in \{1,2\}} A_i \qquad A : \{1,2\} \to \text{Set}$$
$$A_1 = B$$
$$A_2 = C$$
$$B \times C \cong \sum_{b \in B} A_b \qquad A : B \to \text{Set}$$
$$A_b = C$$

12 Lastnosti Preslikav, Praslike & Slike

Naj bodo:

$$f : A \to B$$
$$S \subseteq A \qquad S \in \mathcal{P}(A)$$
$$T \subseteq B \qquad B \in \mathcal{P}(B)$$

Definicije:

- *Slika* je množica:

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

- *Praslika* je množica:

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

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 $f^{-1}[S]$.

$$f : A \to B$$
$$f_* : \mathcal{P}(A) \to \mathcal{P}(B)$$
$$f^* : \mathcal{P}(B) \to \mathcal{P}(A)$$

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

Velja:

$$f^*(\varnothing) = \varnothing \qquad\qquad f_*(\varnothing) = \varnothing$$
$$f^*(B) = A \qquad\qquad \underbrace{f_*(A)}_{Z_f} \subseteq B$$

12.1 Računska pravila

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

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

Definicije injektivne, surjektivne, bijektivne, epi in mono

Naj bo $f : A \to B$ preslikava

- f je *injektivna* če velja:

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

  včasi 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 $g, h : C \to A$ velja:

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

  pravimo, da lahko f *krajšamo* na levi.

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

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

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

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

Dokažimo nekatere izjeve, 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 $f : A \to B$ in $g : B \to C$ in $k, l : D \to A$. 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 $f : A \to B$

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:

$$\begin{aligned} k : 1 &\to A & \qquad l : 1 &\to A \\ * &\mapsto x & * &\mapsto y \end{aligned}$$

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 $g, h : C \to A$. 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 izomofizem.

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

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

Definirajmo $g : B \to A$ 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 $A_1, A_2, \ldots, A_n$ je podmnožica $A_1 \times A_2 \times \ldots \times A_n$.

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:

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

- $R \subseteq A \times B, a \in A, b \in B$ $(a, b) \in \mathbb{R}$ 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** $\forall x \in A : xRx$ $\quad =, \leq$
- **irefleksivnost** $\forall x \in A : \neg(xRx)$ $\quad <, \perp$
- **simetričnost** $\forall x, y \in A : xRy \Rightarrow yRx$ $\quad \perp, \parallel, =$
- **asimetričnost** $\forall x, y \in A : xRy \Rightarrow \neg(yRx)$ $\quad <$
- **antisimetričnost** $\forall x, y \in A : xRy \wedge yRa \Rightarrow x = y$ $\quad \leq$
- **tranzitivnost** $\forall x, y, z \in A : xRy \wedge yRz \Rightarrow xRz$ $\quad <, \leq, \parallel$
- **sovisnost** $\forall x, y \in A : x \neq y \Rightarrow xRy \vee yRx$ $\quad <, \leq$
- **stroga sovisnost** $\forall x, y \in A : xRy \vee yRx$ $\quad \leq$

Definicije:

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

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

13.2 Operacije na relacijah

Transponirana relacija

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

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

Definiramo kot

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

Primera: $\leq^\intercal = \geq$ in $\subseteq^\intercal = \supseteq$

Velja:

$$(R^\intercal)^\intercal = R$$

Relacijo in njeno transpozicijo lahko predstavimo kot tabelo:

Tabela 1: Relacija R

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

Tabela 2: Transponirana relacija R

$R^\intercal$	a	b
1	$\bot$	$\bot$
2	$\top$	$\bot$
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[4]:

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

Trditev: Kompozicija relacij je asociativna:

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

Definiramo:

$$\underbrace{R \circ R \circ R \circ \ldots \circ R}_{n} =: R^n$$

13.3 Graf preslikave

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

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

Γ_f ima lastnost:

[4]Vrstni red je nekoliko zmeden in je potebno 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 $f : A \to B$ je Γ_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 Γ_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:
$$\exists f : A \to B : R = \Gamma_f$$
Vzemimo $f : A \to B$ s predpisom:
$$f(x) = \text{ tisti } y \in B, \text{ da velja } xRy = \iota y \in B : xRy$$
Preverimo $R = \Gamma_f$

Poanta[5]
$$B^A \cong \{R \subseteq A \times B | R \text{ funkcijska}\}$$
Torej lahko funkcije definiramo kot funkcijske relacije.

[5]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 $= \equiv \equiv \sim \approx \cong$.

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

Naj bo $f : A \to B$ 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

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

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 $\mathbb{Z}$.

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

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

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

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:

- $E_i \neq \varnothing \forall i \in I$ 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

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

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 $f : A \to B$ preslikava, ki je *skladna* z R, kar pomeni:

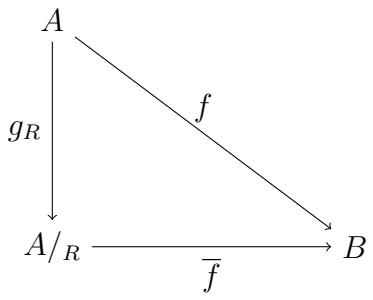
$$xRy \Rightarrow f(x) = f(y)$$

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

Tedaj obstaja natanko ena preslikava $\overline{f} : A/_R \to B$, da velja

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

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



Enoličnost: denimo, da imamo $\overline{f_1}, \overline{f_2} : A/_R \to B$ 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 $\overline{f} : A/_R \to B$ definirano z:

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

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 $b := f(x)$. Tedaj 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 $\leq \sqsubseteq \preccurlyeq \subseteq$.

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 $\mathbb{Z}$ ($2| - 2 \wedge -2|2$ ampak $2 \neq -2$)

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

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

PRIMERI:

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

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. $\forall y \in A : y$ 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 $f : A \to B$. 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:

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

  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 $f = i \circ b \circ q$

$$i(b(q(x))) = i(b([x])) = i(f(x)) = f(x)$$

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:

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

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: ($\mathbb{D}$, Empty, Tree)

- Empty $\in \mathbb{D}$
- Tree(Empty, Empty)
- Tree(Empty, Tree(Empty, Tree(Empty, 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 $S \subseteq A$ ime 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 $a : \mathbb{N} \to A$, 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.

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

Denimo, da je $<$ stroga urejenost na A. Pravimo, da je $S \subseteq A$ *progresivna* (glede na $<$), ko velja

$$\forall x \in A : (\forall y \in A : y < x \Rightarrow y \in S) \Rightarrow x \in S$$

Relacija $<$ je *dobro osnovona*, če velja

$$\forall S \subseteq A : S \text{ progresivna} \Rightarrow S = A$$

Relacija $<$ je *dobro urejena*, če je linearna in dobro osnovana.

Lema: Naj bo $<$ stroga urejenost na $A, A \neq \varnothing$. Če A nima $\leq$-minimalnega elementa, potem v A obstaja padajoča veriga. Ponovimo: A ima $\leq$-minimalni element:

$$\exists x \in A \forall y \in A : y \leq x \Rightarrow y = x$$

A nima minimalnega elementa:

$$\forall x \in a \exists y \in A : y \leq x \wedge y \neq x \iff \forall x \in A \exists y \in A : y < x$$

Dokaz: Dokazujemo, da v A obstaja $a : \mathbb{N} \to A$, da velja $a(n+1) < a(n)$ za vse $n \in \mathbb{N}$. Ker $A \neq \varnothing$, obstaja $a(0) \in A$.

Denimo, da smo že skonstruirali $a(n) < a(n-1) < \cdots < a(2) < a(1) < a(0)$. Ker $a(n)$ ni minimalni, obstaja $y \in A$, da je $y < a(n)$. Za $a(n+1)$ *izberemo* enega od $y < a(n)$.

Postopek nadaljujemo in dobimo $a(n+2), a(n+3), \ldots$

□

Izrek: Naj bo $\sqsubset$ stroga urejenost na A. Ekvivalentne so izjave:

1. $\sqsubset$ je dobro osnovana
2. Vsaka neprazna $S \subseteq A$ ima $\sqsubseteq$-minimalni element
3. A nima padajoče $\sqsubset$-verige

Dokaz

$1 \Rightarrow 2$ Denimo, da je $\sqsubset$ dobro osnovana.

Nj bo $S \subseteq A$ neprazna in naj bo

$$M := \{x \in S : x \text{ je minimalni v } S\}$$

Dokazujemo $M \neq \varnothing$. V ta namen definiramo:

$$T := \{x \in A : (\exists y \in S : y \sqsubset x) \Rightarrow \exists m \in M : m \sqsubset x\}$$

Trdimo, da je T progresivna.

Naj bo $v \in A$ in denimo, da velja

$$\forall u \in A : u \sqsubset v \Rightarrow u \in T \qquad (\divideontimes)$$

Dokazujemo $v \in T$.

Predpostavimo, da obstaja $y \in S$, da je $y \sqsubset v$. Dokazujemo

$$\exists m \in M : m \sqsubset v$$

Iz $(\divideontimes)$ sledi, $y \in T$. Obravnavamo dva primera:

(a) Če $\exists z \in S : z \sqsubset y$:
Ker $y \in T$, obstaja $m' \in M$, da je $m' \sqsubset y$.
Imamo $m' \sqsubset y \sqsubset v$
Torej $\exists m \in M : m \sqsubset v$, namreč $m := m'$

(b) Če $\neg\exists z \in S : z \sqsubset y$
Tedaj je $y \in M$.
Torej $\exists m \in M : m \sqsubset v$, namreč $m := y$.

Ker je T progresivna in velja 1, sledi $T = A$.

Ker je S neprazna, obstaja $t \in S$. Dva primera:

(a) Če $\exists z \in S : z \sqsubset t$
Velja $t \in T$. Po definicija T, torej $\exists m \in M : m \sqsubset t$.
Torej $M \neq \varnothing$.

(b) Če $\neg\exists z \in S : z \sqsubset t$:
Potem je $t \in M$. Torej $M \neq \varnothing$.

$2 \Rightarrow 3$ Predpostavimo: vsaka neprazna $S \subseteq A$ ima minimalni element.

Dokazujemo: A nima padajoče verige.

$$\neg\exists a : \mathbb{N} \to A : a \text{ padajoča veriga}$$

Predpostavimo, da je $a : \mathbb{N} \to A$ padajoča veriga. Iščemo protislovje.

Množica $C = \{a(n) : n \in \mathbb{N}\} \subseteq A$ je neprazna ($a(0)$ vsebuje).

Po predpostavki ima minimalni element $a(j)$, vendar C nima minimalnega elementa, ker za $\forall i \in \mathbb{N} : a(i+1) \sqsubset a(i)$

$\rightarrow\leftarrow$

$3 \Rightarrow 1$ Predpostavimo A nima padajoče verige.

Dokazujemo: $\sqsubset$ je dobro osnovana.

Naj bo $S \subseteq A$ progresivna. Dokazujemo $S = A$. Trdimo, da $C := A \setminus S$ nima minimalnega elementa. Če bi bil $c \in S$ minimalni, bi to pomenilo:

$$\forall x \in A : x \sqsubset c \Rightarrow x \notin C \iff$$
$$\forall x \in A : x \sqsubset c \Rightarrow x \in S \text{ ker je } A \setminus C = S$$

Ker je S progresivna, sledi $c \in S$, kar je v nasprotju z $c \in A \setminus S$.

Torej C nima minimalnega elementa.

Dokažimo $S = A$ s protislovjem.

Denimo $S \neq A$. Potem obstaja element v $A \setminus S$. Torej $C = S \setminus A$ ni prazna in nima minimalnega elementa. Po lemi v C obstaja padajoča veriga, ki je tudi padajoča veriga v A. Protislovje s predpostavko (3). $\rightarrow\leftarrow$

□

15.4 Aksiom Izbire

V lemi smo uporabili **aksiom odvisne izbire:**

Naj bo A neprazna in $R \subseteq A \times S$ celovita: $\forall x \in A \exists y \in A : xRy$. Tedaj obstaja $f : \mathbb{N} \to A$, da velja $\forall n \in \mathbb{N} : f(n)Rf(n+1)$.

V lemi: R je bila relacija $xRy \iff y < x$ in f je bila padjoča veriga.

Bolj splošen je **aksiom izbire:**

Vsaka družina nepraznih množic ima funkcijo izbire.

Če je $A : I \to \text{Set}$ družina množic in $\forall i \in I : A_i \neq \varnothing$, potem

$$\exists f \in \prod_{i \in I} A_i : \top$$

To pomeni $f : I \to \bigcup_{i \in I} A_i$ in velja

$$\forall i \in I : f(i) \in A_i$$

Posledica aksioma izbire: Vsaka surjekcija ima prerez. To pomeni $f : A \to B$ surjektivna, prerez f je $g : B \to A$, da vleja $f \circ g = id_B$

Uporabimo izbiro na družini $D : I \to \text{Set}$

$$I := B$$
$$D_y := f^*(\{y\}) = \{x \in A : f(x) = y\}$$

$D_y \neq \varnothing$, ker je f surjektivna.

Torej obstaja funkcija izbire $g : B \to \bigcup_{y \in B} D_y = A$, da je

$$\forall y \in B : g(y) \in D_y$$
$$\forall y \in B : f(g(y)) = y$$
$$f \circ g = id_B$$

Premislek: Če ima vsaka surjekcija prere, potem velja aksiom izbire.

16 Moč množic

Za vsako $n \in \mathbb{N}$ definiramo *standardno množico* z n elementi:

$$n := \{k \in \mathbb{N} : k < n\} = \{0, 1, \ldots, n-1\}$$

Primer:

$$[0] = \{\}$$
$$[1] = \{0\}$$
$$[4] = \{0, 1, 2, 3\}$$

Definicija: Množica je *končna*, če je izomorfn kaki standardni množici

$$A \text{ končna} \iff \exists n \in \mathbb{N} : A \cong [n]$$

Izrek: $A \cong [m] \wedge A \cong [n] \Rightarrow m = n$

Dokaz: Opustimo, ker je očitno.

Definicija: *Moč končne množice* A je tisti $n \in \mathbb{N}$, za katerega velja

$$A \cong [n]$$

Moč A označimo z $|A|$

16.1 Računanje moči

$$
\begin{aligned}
|A \times B| &= |A| \cdot |B| \\
|A + B| &= |A| + |B| \\
\left|B^A\right| &= |B|^{|A|} \\
|A \cup B| &= |A| + |B| - |A \cap B|
\end{aligned}
$$

Princip vključitve in izključitve

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

DEFINICIJA: A je *neskončna*, če ni končna.

IZREK: A je neksončna $\iff$ obstaja injektivna $\mathbb{N} \to A$.

DOKAZ:

($\Rightarrow$) Denimo, da je A neskončna. Ideja dokaza: injektivno $e : \mathbb{N} \to A$ definiramo po korakih.

Zaporedje $e(0), e(1), e(2), \ldots$ definiramo rekurzivno: če smo že definirali $e(0), \ldots, e(n-1)$, potem lahko dodamo še $e(n)$.

Definiramo $e(0)$: ker $A \neq [0], A \neq \varnothing$, torej lahko izberemo $e(0) \in A$.

Denimo, da že imamo $e(0), \ldots, e(n-1)$ in da so $e(0), \ldots, e(n-1)$ paroma različni (e je injektivna). Iščemo element $A \setminus \{e(0), \ldots, e(n-1)\}$. Če bi veljajo $A \setminus \{e(0), \ldots, e(n-1)\} = \varnothing$, bi imeli $A \cong [n]$, kar ni res. Torej lahko izberemo $e(n) \in A \setminus \{e(0), \ldots, e(n-1)\}$.

($\Leftarrow$) Denimo $e : \mathbb{N} \to A$ injektivna. Dokazujemo, da je A neskončna, t.j.: $\neq \exists n \in \mathbb{N} : A \cong [n]$.

Predpostavimo, da je $n \in \mathbb{N}$ in $A \cong [n]$, ter iščemo protislovje.

Potem bi imeli $\mathbb{N} \xrightarrow{e} A \overset{\text{bijekcija}}{\longrightarrow} [n]$ injekcijo, kar ni možno. Na predavanjih nismo dokazali, vendar v smo dobili za premislek: $\mathbb{N}$ je neskončna, t.j.: $\neq \exists m \in \mathbb{N} : \mathbb{N} \cong [m]$).

Če je A končna, je moč $|A|$ naravno število. V splošnem je moč $|A|$ *kardinalno število*.

DEFINICIJA: Naj bosta A in B množici.

1. A ima enako moč kot B (A in B sta *ekvipolentni*), ko velja $A \cong B$. Pišemo $|A| = |B|$.

2. A ima manjšo ali enako moč kot B, ko obstaja injektivna preslikava $A \to B$. Pišemo $|A| \leq |B|$.

3. A ima manjšo moč kot B, ko velja

$$|A| \leq |B| \wedge |A| \neq |B|$$

   Pišemo $|A| < |B|$.

PRIMER:

$$S = \{n \in \mathbb{N} : n \text{ je sodo}\}$$
$$|S| \leq |\mathbb{N}| \text{ ker } n \mapsto n \text{ injektivna } S \to |NN$$
$$|S| = |NN| \text{ ker } n \mapsto 2n \text{ bijektivna } \mathbb{N} \to S$$

IZREK: $|A| \leq |B| \iff A \neq \varnothing$ ali obstaja surjektivna $B \to A$.

DOKAZ:

($\Rightarrow$) Denimo $f : A \to B$ injektivna in $A \neq \varnothing$. Potem obstaja $x_0 \in A$. Surjekcijo $g : B \to A$ definiramo s predpisom

$$g(y) = \begin{cases} x, & f(x) = y \\ x_0, & \forall z \in A : f(z) \neq y \end{cases}$$

($\Leftarrow$) Denimo A prazna ali obstaja surjektivna $f : B \to A$.

Če $A = \varnothing$, je $\varnothing \to B$ injektivna.

Če $f : B \to A$ surjektivna, potem ima prerez $g : A \to B$. $f \circ g = id_A$, torej je g injektivna.

□

IZREK: (Cantor) $|A| < |\mathcal{P}(A)|$.

DOKAZ: Najprej dokažimo $|A| \leq |\mathcal{P}(A)|$.

Iščemo injektivno preslikavo $f : A \to \mathcal{P}(A)$.

$$f(x) = \{x\}$$

Ta je injektivna, ker iz $\{x\} = \{y\}$ sledi $x \in \{y\}$ sledi $x = y$.

Dokažimo $|A| \neq |\mathcal{P}(A)|$. Dokazujemo

$$\begin{aligned} \neg\exists g : A \to \mathcal{P}(A) : g \text{ bijekcija} \\ \forall g : A \to \mathcal{P}(A) : g \text{ ni bijekcija} \end{aligned}$$

Naj bo $g : A \to \mathcal{P}(A)$. Dokazujemo, da g ni surjektivna ali g ni injektivna. Dokažimo, da g ni surjektivna.

Trdimo, da množica

$$S := \{x \in A : x \notin g(x)\} \in \mathcal{P}(A)$$

ni v sliki g (in torej g ni surjektivna).

$$\begin{aligned} \neg\exists y \in A : g(y) = S \\ \forall y \in A : g(y) \neq S \end{aligned}$$

Naj bo $y \in A$. Dokazujemo $g(y) \neq S$. Predpostavimo $g(y) = S$ in iščemo protislovje

1. velja $y \notin S$
   Če $y \in S$, bi sledilo $y \notin g(y) = S$. $\to\leftarrow$
2. velja $\neg(y \notin S)$
   Če $y \notin S$, bi sledilo $y \notin g(y) = S$. Po definiciji S sledi, $y \in S$. $\to\leftarrow$

Torej (1) $\to\leftarrow$ (2)

16.2 Števne in neštevne množice

Moc množice $\mathbb{N}$ označimo z $\aleph_0$.

$$|\mathbb{N}| = \aleph_0$$

Definiicija: Množica je *števna*, če je njea moč $\leq \aleph_0$. Množica je *neštevna* če ni števna.

Izrek: Za množico A je ekvivalentno:

1. A je števna
2. obstaja injektivna $A \to \mathbb{N}$
3. A je prazna ali obstaja surjektvina $\mathbb{N} \to A$
4. obstaja preslikava $\mathbb{N} \to 1 + A$, katere slika vsebuje A
5. A je končna ali izomorfna $\mathbb{N}$

DOKAZ: (1) in (2) sta ekvivalentni po definiciji. (2) in (3) sta ekvivalentni po izreku. (1) in (5) sta ekvivalentni po definiciji.

IZJAVA: $\mathbb{N} \cong \mathbb{N} \times \mathbb{N}$

DOKAZ: Da je $\mathbb{N} \times \mathbb{N}$ števna lahko dokažemo na podoben način, kot dokazujemo, da je $\mathbb{Q}$ števna. Urejene pare $(x, y), x, y \in \mathbb{N}$ uredimo v kvadrat, in jih navedemo po diagonalah. Bolj korekten dokaz smo pokazali na vajah.

IZREK: Števna unija števnih množic je števna.

DOKAZ: Imamo I števna, $A : I \to \text{Set}$ in A_i je števna za vsak $i \in I$. Dokazujemo, da je $\bigcup_{i \in I} A_i$ števna. Iz dokaza za posebene primer lahko izpeljemo splošen dokaz, zato smo na vajah dokazali samo za poseben primer.

Poseben primer: $I = \mathbb{N}$ in A_i števna neprazna.

Imamo $A : \mathbb{N} \to Set$, $A_n \neq \varnothing$ števna.

Vemo $\forall n \in \mathbb{N} : A_n \neq \varnothing$ števna. Po točki (3) v prejšnjem izreku, velja

$$\forall n \in \mathbb{N} \exists e : \mathbb{N} \to A_n \text{ surjektivna}$$

Po aksiomu izbire obstaja f preslikava

$$f \in \prod_{n \in \mathbb{N}} \{g : \mathbb{N} \to A_n : g \text{ surjekcija}\}$$

Se pravi: za $\forall n \in \mathbb{N}$ smo izbrali surjekcijo

$$f_n : \mathbb{N} \to A_n$$

Definiramo $h : \mathbb{N} \times \mathbb{N} \to \bigcup_{n \in \mathbb{N}} A_n, \quad h(i, j) = f_i(j)$

Trdimo, da je h surjekcija.

Naj bo $x \in \bigcup_{n\in\mathbb{N}} A_n$. Torej obstaja $m \in \mathbb{N}$, da je $x \in A_m$.

Ker je $f_m : \mathbb{N} \to A_m$ surjektivna, obstaja $l \in \mathbb{N}$, da je $f_m(l) = x$, torej

$$h(m, l) = f_m(l) = x$$

Imamo Surjekcijo $\mathbb{N} \overset{\text{bijektivna}}{\longrightarrow} \mathbb{N} \times \mathbb{N} \xrightarrow{h} \bigcup_{n\in\mathbb{N}} A_n$

□

Izrek: (Cantor-Schröder-Bernstein) Če obstaja injektivni preslikavi $A \to B$ in $B \to A$, potem obstaja bijektivna preslikava $A \to B$.

$$|A| \leq |B| \wedge |B| \leq |A| \Rightarrow |A| = |B|$$

Dokaz: Denimo, da sta $f : A\ toB$ in $g : B \to A$ injektivni. Dokazujemo, da obstaja bijekcija $A \to B$.

Orbita za $x \in A$ je zaporedje

$$\ldots, f^{-1}\left(g^{-1}(x)\right), x, f(x), g(f(x)), f(g(f(x))), \ldots$$

Na levi se orbita konča, če dobimo element, ki ni v sliki f oziroma ni v sliki g (ker potem ne moremo uporabiti f^{-1} oziroma g^{-1}).

Na desni se orbita ne konča.

Imamo tri možnosti:

1. Orbita se na levi ne konča
2. Na levi se orbita konča z elementom iz A
3. Na levi se orbita konča z elementom iz B

Trdimo, da orbite tvorijo razbitje A in B:

- element orbite že določa celotno orbito
- če je element v dveh orbitah sta enaki
- vsak element je v natanko eni orbiti

1. Če se orbita ne konča na levi:

   Vsak $x \in A$ se preslika s f v svojega soseda ne desni (za skico glej zvezek).

2. Če se orbita konča na levi z A:

   $x \in A$ v tej orbiti preslikamo z f v sosede na desni (za skico ponovno glej zvezek).

3. Če se orbita konča z B:

   $\forall x \in A$ v orbiti slikamo z g^{-1} v levega soseda (v tretje gre rado: skica je v zvezku).

□

17 Kumulativna Hierarhija

17.1 Kodiranje matematičnih objektov z množicami

- Preslikavo $A \to B$ lahko predstavimo kot funkcijsko relacijo, t.j. $\subseteq A \times B$.
- Kvocientna množica $A/_R$ je množica ekvivalenčnih razredov in vsak ekvivalenčni razred je tudi množica.

Kodiranje:

- urejeni par $(x, y) = \{\{x\}, \{x, y\}\}$

$$\{\{2, 3\}, \{2\}\} = (2, 3)$$
$$\{\{7\}, \{7\}\} = (7, 7)$$

- vsota $A + B$:

$$\iota_1 := (x, \varnothing)$$
$$\iota_2 := (y, \{\varnothing\})$$

- naravna števila:

$$0 := \varnothing$$
$$x^+ := x \cup \{x\}$$

  Primer:

$$1 = 0^+ = \varnothing \cup \{\varnothing\} = \{\varnothing\} = \{0\}$$
$$2 = 1^+ = \{0\} \cup \{\{0\}\} = \{0, \{0\}\} = \{0, 1\}$$
$$3 = \cdots = \{0, 1, 2\}$$

- $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/_\sim$, kjer je

$$\underbrace{(a, b)}_{a-b} \sim (c, d) \iff a + d = c + b$$

- $\mathbb{Q} = \mathbb{Z} \times \{n \in \mathbb{N} : n > 0\}/_\simeq$, kjer je

$$(k, a) \simeq (l, b) \iff kb = al$$

- $\mathbb{R} \subseteq \mathcal{P}(\mathbb{Q})$, kjer je $x \in \mathbb{R}$ Dedekindov rez, torej $\subseteq \mathbb{Q}$.

Razred vseh množic V je sestavljen:

- $V_0 = \varnothing$
- $V_1 = \mathcal{P}(V_0) = \{\varnothing\}$
- $V_2 = \mathcal{P}(V_1)$
- $\vdots$
- $V_\omega = \bigcup_{k<\omega} V_k$
- $V_{\omega+1} = \mathcal{P}(V_\omega)$
- $V_{\omega+\omega}$ *ordinalna števila*

Temu pravimo *transfinitna konstrukcija.*

DEFINICIJA:(von Neumann) Množica A je *ordinalno število*, če je tranzitivna in vsak njen element je tranzitivne.

Množica A je *tranzitivna*, če $\forall x \in A : x \subseteq A$.

Ideja: Ordinalno število je množica svojih prednikov

- $0 = \varnothing$
- $1 = \{0\}$
- $2 = \{0, 1\}$
- $\omega = \{0, 1, 2, 3, \ldots\} = \mathbb{N}$
- $\omega + 1 = \omega \cup \{\omega\}$
- $\omega + 2 = \{0, 1, 2, \ldots, \omega, \omega + 1\}$

17.2 Zermelo-Fraenkelovi aksiomi teorije množic

1. *Ekstenzionalnost:* množici sta enaki, če imata iste elemente.
2. *Neurejeni par:* za vsak x in y (množici) je $\{x, y\}$ množica, ki vsebuje natanko x in y.
3. *Unije:* Za vsako družino $A : I \to \text{Set}$ je $\bigcup_{i \in I} A_i$ množica, ki vsebuje natanko tiste x, ki so v nekem A_i.
4. *Prazna množica:* $\varnothing$ nima elementa.
5. *Potenčna množica:* Za vsak A je $\mathcal{P}(A)$ množica, ki ima za elemente natanko podmnožice A.
6. *Neskončna množica:* Obstaja množica, ki vsebuje $\varnothing$ in je zaprta za operacijo naslednik.

   $$\exists A : \varnothing \in A \wedge \forall x \in A : x \cup \{x\} \in A$$

   (sledi, da imamo ω)
7. *Podmnožica:* Če je A množica in φ lastnost, je $\{x \in A : \varphi(x)\}$ množica tistih $x \in A$, za katere velja $\varphi(x)$.
8. *Dobra osnovanost:* Relacija $\in$ je dobro osnovana (se pravi, da nima padajoče verige: $\cdots \in x_3 \in x_2 \in x_1 \in x_0$ ne gre)
9. *Zamenjava:* Slika preslikave $f : A \to \text{Set}$, kjer je A množica je množica.

   Po domače: „Slika množice je množica (ni pravi razred)".
10. *Aksiom izbire:* Družina nepraznih ima funkcijo izbire.

17.3 Aksiom izbire

DEFINICIJA: *Veriga* v delni urejenosti $(P, \leq)$ je $C \subseteq P$, ki je linearno urejena s $\leq$.

$$\forall x, y \in C : x \leq y \vee y \leq x$$

PRIMER: neštevna veriga v $(\mathcal{P}(\mathbb{Q}), \subseteq)$ - Dedekindov razred.

17.3.1 Zornova lema

Če ima v delni ureditvi $(P, \leq)$ vsaka veriga zgornjo mejo, ima P maksimalni element.

DOKAZ: glej profesorjeve zpiske na GitHubu.

IZREK: V teoriji množic brez aksioma izbire so ekvivalentne izjave:

1. aksiom izbire
2. zornova lema
3. Princip dobre ureditve (vsaka množica ima dobro ureditev)
4. Vsak vektorski prostor ima bazo

DOKAZ: Del dokaza smo naredili na vajah.