PONOVITEV LOGIKA

$\boxed{\text{logika 1}}$

- V stoletjih se je pri matematiki razvil neke vrste „stenografski" zapis, ki poudarja kaj je v nekem stavku pomembnega in ~~kaj~~ izpusti obrobne stvari.

Npr. Če je število, imenovano a, negativno, potem ne obstaja nobeno realno število, katerega kvadrat je enak a.

Zelo dolgo poved skrajšamo na bistvo (boljše razumevanje!):

$$a < 0 \Rightarrow \nexists x \left(x \in \mathbb{R} \wedge x^2 = a \right)$$

- Osnove za ta krajši zapis so logični simboli:
  - konjunkcija $\wedge$
  - disjunkcija $\vee$
  - implikacija $\Rightarrow$
  - ekvivalenca $\Leftrightarrow$
  - negacija $\sim$ ali pa $\neg$

- V matematiki stvari DOKAZUJEMO,
  imamo neko trditev $\overset{= \text{IZJAVO}}{}$, ki je bodisi resnična ali pa napačna,
  in poskušamo preveriti pravilnost te trditve. (= IZJAVE)

Npr. Ali boš šel na sprehod? ... NI IZJAVA, saj nima smisla govoriti o pravilnosti

- Včeraj sem bil ~~a~~ na tekmi ... pa je IZJAVA ... (bodisi pravilna, bodisi napačna)

- Iz ~~izjav tvorimo nove izjave;~~

Npr. Naj bo A izjava: „Včeraj sem bil na tekmi"

B ... „Včeraj je bilo vreme lepo".

$A \vee B$
$A \wedge B$
$A \Rightarrow B$
$A \Leftrightarrow B$
$\neg A$

SO ZOPET IZJAVE (sestavljene izjave)

Kdaj so sestavljene izjave pravilne?

Pravilnostna tabela

- Poseben primer izjave je
  - TAVTOLOGIJA .. $A \vee \neg A$ vedno pravilna
  - PROTISLOVJE ... $A \wedge \neg A$

Zgled. $((A \Rightarrow B) \wedge A) \Rightarrow B$ je tavtologija; Nepravilna bi bila edino v primeru $1 \Rightarrow 0$ ... tj $B = 0$, $(A \Rightarrow B) \wedge A = 1$

SKLEPANJE

~~IZ~~ Če imamo nekaj izjav, lahko sklepamo na novo izjavo.

npr. • Če je tlak 1 ATM in Temp $\geq 100°$ potem voda vre

• Barometer je pokazal, da je Tlak = 1 ATM

• Temp. vode je $100°$

SKLEP: Voda vre!

Sklepanje je pravilno, če je $H_1 \wedge H_2 \wedge .. \wedge H_n \Rightarrow$ Sklep TAVTOLOGIJA

• Izjava A je <u>ekvivalentna</u> izjavi B, če ~~imata~~ v tabeli identično vrednosti,
pravzaprav

Oz. ~~...~~ če A velja mora veljati tudi B in obratno: če B velja mora veljati tudi A

Oz: A je ekviv. B natanko tedaj ko je $A \Leftrightarrow B$ tavtologija.

Zgled. $$\sim(A \Rightarrow B) \equiv A \wedge \sim B$$

$$\sim(A \wedge B) \equiv (\sim A) \vee (\sim B) \equiv A \Rightarrow \sim B.$$

glej (b za I. del)

A	B	$(A \Rightarrow B)$	$\sim(A \Rightarrow B)$	$A \wedge \sim B$
0	0	1	0	0
1	0	0	1	1
0	1	1	0	0
1	1	1	0	0

• ~~Logični~~ V sestavljeni izjavi lahko podizjavo A nadomestimo z njej ekvivalentno izjavo B

<u>Npr</u> $$A \vee (\sim(A \Rightarrow B)) \equiv A \vee (A \wedge \sim B) \equiv (A \vee A) \wedge (A \wedge \sim B) \equiv$$
$$\equiv A \wedge (A \wedge \sim B) \equiv A \wedge \sim B \equiv \sim(A \Rightarrow B)$$

• Izjavni račun pa ne zadostuje za vse primere: <u>Rabimo predikatni račun</u> →

- ZA VSAK individuum x velja da ima lastnost L : $\forall x \; L(x)$

EKSISTIRA -||- ki ima lastnost L : $\exists x \; L(x)$

NPR: vsak ~~zajec~~ zajec prehiti vsako želvo:

$$\forall x \, \forall y \, (\text{Zajec}(x) \text{ in } \text{Želva}(y) \Rightarrow \text{Hitrejši}(x, y))$$

$$\sim[\forall x \; L(x)] \equiv \exists x \sim L(x)$$

$$\sim[\exists x \; L(x)] \equiv \forall x \sim L(x)$$

Zgled Funkcija je zvezna v x_0, če velja sledeče:
$$\forall \varepsilon \, (\varepsilon > 0 \Rightarrow \exists \delta \, (\delta > 0 \text{ in } (\forall x \, (|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \varepsilon))))$$

Npr.: H_1: Vsi ljudje so umrljivi

H_2: Sokrat je človek

→ Sokrat je umrljiv

Ta sklep ne moremo preveriti samo z logičnimi izjavami, saj bi dobili $H_1 \wedge H_2 \Rightarrow$ Sokrat ~~umrljiv~~ ni tavtologija!

- Skupna točka H_1 in H_2 je „BITI ČLOVEK". To je še bolj očitno, če prvo predpostavko napišemo v drugačni obliki: Če je NEKDO človek, potem je ta NEKDO umrljiv.

Pišimo NEKDO → x in ohranjamo x JE ČLOVEK → $Č(x)$

Temu rečemo PREDIKATI x JE UMRLJIV → $U(x)$

$(*)$: $Č(x) \Rightarrow U(x)$

$Č(\text{Sokrat})$

ERGO: $U(\text{Sokrat})$

f NI ZVEZNA V $x_0 \in \mathbb{R}$

$\sim \forall \varepsilon (\ldots) \equiv \exists \varepsilon \sim (\ldots) \equiv$

$\equiv \exists \varepsilon (\varepsilon>0 \text{ in } \sim \exists \delta (\ldots)) \equiv$

$\boxed{\sim(A \Rightarrow B) \equiv A \wedge \sim B}$

$\equiv \exists\varepsilon(\varepsilon>0 \text{ in } \forall\delta \sim(\ldots)) \equiv$

$\equiv \exists\varepsilon(\varepsilon>0 \text{ in } \forall\delta(\delta>0 \Rightarrow \sim\forall x(\ldots\Rightarrow\ldots)))$

$\boxed{\sim(A\wedge B) \equiv A \Rightarrow \sim B}$

$\equiv \exists\varepsilon(\varepsilon>0 \text{ in } \forall\delta(\delta>0 \Rightarrow [\exists x \sim(\ldots)] \equiv$

$\equiv \exists\varepsilon(\varepsilon>0 \text{ in } \forall\delta(\delta>0 \Rightarrow \exists x(|x-x_0|<\delta \text{ in } \ldots$

$$= \exists\varepsilon\Big(\varepsilon>0 \text{ in } \forall\delta\big[\delta>0 \Rightarrow \exists x\,[\,|x-x_0|<\delta \text{ in } |f(x)-f(x_0)|\geq\varepsilon\,]\big]\Big)$$

$$\boxed{\sim(A \Rightarrow B) \equiv A \wedge \sim B}$$

MNOŽICE

• Osnovni koncept v sodobni matematiki je pojem <u>množice</u>, ki jo sestavljajo <u>elementi</u>. Govorimo npr. o:

- množici vseh študentov
- množici vseh črk slovenske abecede, ITD.

{Začetnik tega koncepta je Georg Cantor 189? }

• V matematiki smo navajeni NATANČNO DEFINIRATI reči, t.j. pojme, s katerimi nato operiramo.
Izjema pri tem pa je ravno osnovni pojem, tj. pojem MNOŽICA, ki je <u>nedefiniran pojem</u>, določen s svojimi aksiomi, ki opisujejo njegove lastnosti.

• Množice ~~običajno~~ ko označujemo s črkami $A, B, C, \ldots$, Poljubne množice pa z X, Y, Z
(Pri tem npr. črka A NI MNOŽICA, temveč le ime za neko množico)
in zapišemo tako, da v zavitem oklepaju naštejemo vse njene elte.
Npr. množico prvih 5 črk slovenske abecede zapišemo kot: $A := \{a, b, c, č, d\}$.
$= \{c, d, č, b, a\}$ — Vrstni red ni pomemben

- to deluje, če ni preveč elementov.

Drugače pa množico zapišemo tako da povemo tisto lastnost, ki množico ~~točno~~ točno določa.

Npr: množica vseh praštevil: $P := \{x;\ x \text{ je praštevilo}\}$

Množica vseh individuumov x, ki imajo lastnost da so praštevila

• Včasih vidimo tudi zapis $\{x \mid x \text{ je praštevilo}\}$

$\{x :\ x \text{ je praštevilo}\}$

• Zapis $a \in A$ preberemo: reč, ki jo označimo z a je element (je vsebovana v) množici, ki smo jo označili s črko A. Obratno, če katera reč NE SODI v množico to zapišemo z: $b \notin A$ ... kratko: b ni elt množice A.

(2)

- Sprva so mislili, da velja tudi obratno, tj. da vsaka smiselna lastnost določa neko množico ... npr. $A = \{X;\ X \in A\}$

Toda 1902 je Russel pokazal, da to ne more biti res (in s tem uničil delo Frege)

Njegov razmislek, znan kot RUSSELOVA ANTINOMIJA je sledeč

Naj bo $R := \{X;\ X \notin X\}$ .... množica vseh takih množic, ki niso same sebi elt.

Ta lastnost je definitivno smiselna. Če bi določala neko množico (oz. če bi R res bila množica), bi se lahko vprašala, če ima tudi R to lastnost?

tj. ali je $R \in R$ ali ne?

- $R \in R \Rightarrow R \notin R$ ... po definiciji množice R
- $R \notin R \Rightarrow R \in R$ -11-

$R \in R \Leftrightarrow R \notin R$

PROTISLOVJE.

- Pri definicijah množice moramo biti previdnejši!

Zato so vpeljali aksiome teorije množic. V von-Neumann-Barnaysovem pristopu ~~...~~ se vpelje se (nedefiniran) pojem RAZREDA, in: množica je po definiciji tak razred, ki je element nekega drugega razreda.

(v tem primeru se Russelova antinomija glasi: Razred R ne more biti množica)

Drug možen pristop ~~...~~ (Zermelo - Fraenkelov) ostanemo pri množicah, smiselno lastno pa omejimo na že znane množice - na tiste, za katere vemo, da obstajajo.

Mi bomo gradili na tem drugem pristopu.

Naštejmo nekaj najpomembnejših ~~lastnost~~ aksiomov:

- Aksiom o podmnožicah: Naj bo X dana množica eltov, ~~...~~ in L neka smiselna lastnost. Tedaj obstaja množica

$$Y := \{x;\ x \in X \text{ in } L(x)\}$$

tudi krajše: $Y := \{x \in X;\ L(x)\}$

• Ta množica sestoji kvečjemu iz eltov neke znane množice X; pravimo, da je Y podmnožica X in označimo kot $Y \subseteq X$.

Stroga definicija: $A \subseteq B$ če $\forall x \, (x \in A \Rightarrow x \in B)$

• Množici A in B sta enaki $(A = B)$, kadar imata natanko iste reči za svoje elte; tj.

$$(A = B) \overset{DEF}{\Leftrightarrow} \forall x \, (x \in A \Leftrightarrow x \in B),$$

• Če je $A \subseteq B$, vendar $A \neq B$ to ~~napišemo~~ poudarjeno zapišemo kot: $A \subset B$

ali: $A \subsetneq B$

in preberemo: A je PRAVA PODMNOŽICA B.

<u>Trditev</u> $A = B \Leftrightarrow A \subseteq B$ in $B \subseteq A$

<u>dokaz</u> Če $A = B$ in $x \in A$, mora tudi $x \in B$, saj imata A in B iste elte. Torej $A \subseteq B$. Podobno tudi $B \subseteq A$.

Obratno, če $A \subseteq B$ in $B \subseteq A$, ~~in tako~~ tedaj očitno A in B vsebujeta iste elte $\boxtimes$

<u>Axiom o prazni množici</u> Obstaja ena sama množica, ki ne vsebuje nobenega elta.

Oznaka: $\emptyset = \{\} :\overset{DEF}{=} \{x ; \forall x (x \notin \emptyset)\}$

Torej: $\emptyset \subseteq X$ za $\forall$ množico X.

<u>Axiom o potenčni množici</u> Naj bo X neka množica. VEC O POTENCNI MNOZICI-> DS1

Tedaj $\exists$ množica $\mathcal{P}(X) := \{Y ; Y \subseteq X\}$

Npr.: $\mathcal{P}(\emptyset) = \{\emptyset\}$.

PAZI: $\{\emptyset\} \neq \emptyset$, saj $\{\emptyset\}$ vsebuje en elt

• Če ima X n eltov, ima $\mathcal{P}(X)$ 2^n eltov ... važno

Operacije med množicami

- Osnovne operacije med množicami so UNIJA, PRESEK, RAZLIKA in KARTEZ. PRODUKT.

- imejmo dve množici X, Y

  - unija: $X \cup Y := \{x;\ \overset{x\in X \,\vee\, x\in Y}{x \in X \text{ ali } x \in Y}\}$ ... obstaja po aksiomu o paru

    - npr. $A = \{0,1,\pi\}$, $B = \{-1,1\}$ $\Rightarrow$ $A \cup B = \{-1,1,0,1,\pi\} =$
      $= \{-1,0,1,\pi\}$

  - presek $X \cap Y := \{x;\ \overset{x\in X \,\wedge\, x\in Y}{x \in X \text{ in } x \in Y}\}$ ... obstaja po aksiomu o podmnožicah

    - npr $A \cap B = \{1\}$

  - razlika $X \setminus Y := \{x;\ x \in X \wedge x \notin Y\}$ .... obstaja po aksiomu o podmnožicah.

    - npr $A \setminus B = \{0,\pi\}$, $B \setminus A = \{-1\}$

- Pri uporabah teorije množic nas običajno zanima neka izbrana, t.i. „UNIVERZALNA" množica U in njeni elti ter podmnožice. Glede na U lahko vpeljemo pojem komplementa kot: $X \subseteq U$, potem $X^c := U \setminus X = \{x;\ x \in U \text{ in } x \notin X\}$

Lastnosti

$X \cup X = X$	$X \cap X = X$	... idempotentnost
$\emptyset \cup X = X$	$\emptyset \cap X = \emptyset$	
$X \cup Y = Y \cup X$	$X \cap Y = Y \cap X$	..... komutativnost
$(X \cup Y) \cup Z = X \cup (Y \cup Z)$	$(X \cap Y) \cap Z = X \cap (Y \cap Z)$	.... asociativnost
$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$	$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$	.... distributivnost
$X \cup (X \cap Y) = X$	$X \cap (X \cup Y) = X$	..... absorbcija

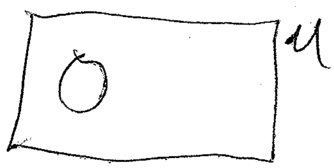
Lastnosti razlike
$$X \setminus X = \emptyset$$
$$X \setminus \emptyset = X$$
$$\emptyset \setminus X = \emptyset$$

Lastnosti komplementa $X \cup X^c = \mathcal{U}$ $\qquad X \cap X^c = \emptyset$
$$(X^c)^c = X$$
$$\emptyset^c = \mathcal{U}$$
$$\mathcal{U}^c = \emptyset$$
$$(X \cup Y)^c = X^c \cap Y^c \qquad (X \cap Y)^c = X^c \cup Y^c$$
... de Morganova zakona.

<u>dokaz</u> le za $(X \cup Y)^c = X^c \cap Y^c$:

$x \in (X \cup Y)^c \iff x \notin X \cup Y \iff x \notin X$ in $x \notin Y \iff x \in X^c$ in $x \in Y^c \iff$
$x \in X^c \cap Y^c$ ■

Množice si lahko nazorno predstavimo z Vennovimi diagrami



Kartezični produkti ... zadnja elementarna operacija

$$X \times Y = \{(x,y);\ x \in X \wedge y \in Y\}$$

kjer je (x,y) t.i. urejeni par, tj. objekt s karakteristično lastnostjo
$$(x,y) = (u,v) \iff x = u \text{ in } y = v$$

BTW: Po von Neumannu ima takšno lastnost tudi množica
$(x,y) := \{\{x\}, \{x,y\}\}$, torej lahko urejeni par smatramo za množico z dvema eltoma.

Velja: $(x,y) = \{\{x\},\{x,y\}\} \in \mathcal{P}(\mathcal{P}(X \cup Y))$

in s tem $X \times Y = \{(x,y) \in \mathcal{P}(\mathcal{P}(X\cup Y))\ ;\ x \in X \text{ in } y \in Y\} \subseteq$

$\subseteq \mathcal{P}(\mathcal{P}(X \cup Y))$.

Lastnosti

- $X \times Y = \emptyset \iff (X = \emptyset) \vee (Y = \emptyset)$
- $X \times Y \neq Y \times X$; enačaj velja natanko tedaj, ko je $X = Y$, ali ko je $X = \emptyset$ ali $Y = \emptyset$
- $X \times (Y \cup Z) = (X \times Y) \cup (X \times Z)$
- $X \times (Y \cap Z) = (X \times Y) \cap (X \times Z)$
- $X \times (Y \setminus Z) = (X \times Y) \setminus (X \times Z)$

- Kartezični produkt lahko posplošimo na več faktorjev:

$$X \times Y \times Z := (X \times Y) \times Z = \{((x,y),z)\ ;\ (x,y) \in X \times Y \text{ in } z \in Z\}$$

$$= \{(x,y,z)\ ;\ x \in X,\ y \in Y,\ z \in Z\}$$

urejene trojke s podobno lastnostjo kot urejeni pari.

definiramo jih lahko tudi kot: $(x,y,z) := ((x,y),z)$

⋮

induktivno:

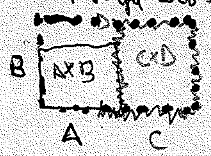
$\dots \times X_{n-1}) \times X_n = \{(x_1,\dots,x_n)\ ;\ x_i \in X_i \text{ za } i=1,\dots,n\}$

① $A = \{1,2,3\}$ $B = \{2,4,8,9\}$ — $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$, $A \times B$

1.3 $\mathcal{P}(A) = ?$

1.4 V kartezičnem koord. sistemu predstavi $A = \{(x,y);\ y < x\}$

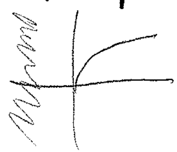
- Ali velja $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$? DA
- Ali velja celo enačaj? NE vedno!



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

Funkcije

• Imejmo 2 množici A, B (lahko tudi enaki)
Funkcija je predpis f, ki $\forall$ eltu množice A priredi natanko določen elt iz množice B. Zgled



NI FJA

opomba Funkcijam iz $\mathbb{R}^n$ v $\mathbb{R}^m$ rečemo včasih tudi preslikave, ???

Običajen zapis za fjo je $f: A \to B$ ali $A \xrightarrow{f} B$;
predpis sam pa zapišemo kot $f: x \mapsto f(x)$

Pozor! Razlikuj med f ... fjo in f(x) ... vrednost fje v točki $x \in A$.

Množico A imenujemo **domena**, B pa **kodomena**, množico
$G_f = \{(x, f(x)) ; x \in A\} \subseteq A \times B$ pa **graf** fje f

• Obratno, podmnožica $G \subseteq A \times B$ je graf NEKE FJE natanko tedaj ko sta izpolnjena pogoja: (1) $\forall x \in A \ \exists y \in B: (x,y) \in G$

(2) $(x,y_1),(x,y_2) \in G \Rightarrow y_1 = y_2$ .... y iz točke (1) je EN SAM!

Parcialna fja je podmnozica AxB, za katero velja pogoj (2), ne pa nujno pogoj (1).
Naravno definicijsko obmocje je mnozica tistih x \in A, za katere velja tudi pogoj (1).

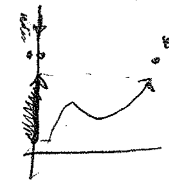
• S tem pogledom lahko smatramo fjo za podmnožico $A \times B$, ki ustreza pogojema (1) in (2). Tako je npr.
v primeru $A = \emptyset$ obstaja natanko ena fja $f: A \to B$
$\emptyset \to B$. To je kar $f = \emptyset \subseteq A \times B$
prazna fja.

• Seveda pa $\nexists$ fja $f: A \to B = \emptyset$,
razen, če tudi $A = \emptyset$

BTW: Za nekatere pogosto uporabljane fje uporabljamo posebne oznake,
npr: $sgn: \mathbb{R} \to \{-1,0,1\}$ je fja, definirana R

$$x \mapsto \begin{cases} -1; & x<0 \\ 0; & x=0 \\ 1; & x>0 \end{cases}$$

Množico $Z_f := \{ y \in B \,;\, \exists\, x \in A : f(x) = y \}$



imenujemo zaloga vrednosti fje f. To je torej množica vseh slik eltov iz domene.

(npr. pri konstantni fji, ki $f: x \mapsto a$ je $Z_f = \{a\}$)

- Če je $Z_f = B$ je f SURJEKTIVNA FJA, ali surjekcija

Zgled sgn: $\mathbb{R} \to \{-1, 0, 1\}$ je surjekcija, saj
$\operatorname{sgn}(-1) = -1$
$\operatorname{sgn}(0) = 0$
$\operatorname{sgn}(2) = 1$

- Če za $\forall\, x, x' \in A$ velja sklep: $f(x) = f(x') \Rightarrow x = x'$

je f INJEKTIVNA fja ali injekcija.

To je torej preslikava za katero velja, da ima poljuben par različnih originalov tudi različni sliki, ali, drugače povedano: $\forall$ elt v kodomeni B je slika NAJVEČ ENEGA elta iz domene A

- Če je $f: A \to B$ injektivna in surjektivna, jo imenujemo tudi BIJEKCIJA.

To je taka fja, da je $\forall\, y \in B$ slika NATANKO ENEGA elta $x \in A$.

Zgled 1 sgn: $\mathbb{R} \to \{-1, 0, 1\}$ je surjekcija, vendar ni injektivna, saj
$\operatorname{sgn}(-2) = \operatorname{sgn}(-1)$.
Torej tudi ni bijekcija.

2) $f: \mathbb{N} \to \mathbb{N}$
$x \mapsto 2x$
je injektivna, a ni surjekcija saj $1 \notin Z_f$.

KOMPOZICIJA FJIJ

Naj bo $f : X \to Y$ in $g : Y \to Z$

Tedaj je $(g \circ f)$ funkcija, ki : $(g \circ f) : X \to Z$

$\equiv g$ KOMPOZITUM f

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

To je torej fja z domeno X in kodomeno Z.

Na kratko si jo lahko predstavljamo z naslednjim komutativnim

dgm:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, dashed, "g \circ f"'] & Y \arrow[d, "g"] \\ & Z \end{tikzcd}$$

.... pravimo, da dgm KOMUTIRA

Pazi! Če kodomena za f $\neq$ domeni za g, ne moremo narediti $g \circ f$.

Zgled $g, f : \mathbb{R} \to \mathbb{R}$ $\quad f(x) = x^2$

$g(x) = x + 3$

Lastnosti $\quad g \circ f \neq f \circ g$, v splošnem.

$f \circ g : x \mapsto (x+3)^2$

$g \circ f : x \mapsto x^2 + 3$

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

Dokaz asociativnosti: Imamo torej $X \xrightarrow{f} Y$, $Y \xrightarrow{g} Z$, $Z \xrightarrow{h} U$

leva ... $\circ f) : X \to U$

desna ... $\circ f : X \to U$

Tlm Če sta $f : X \to Y$ in

$g : Y \to Z$ surjektivni (injekt)

je tudi $(g \circ f)$ surjektivna (injekt)

– torej s dokaz

... ni strani.

– ... $= h(g(f(x))) = (h \circ g)(f(x))$ ☒

$k \in Z$. Ker je g surjekcija je $k \in Z_g$

oz: $g(y) = k$. Ker je f surjekc.

je $y \in Z_f$ oz: $f(x) = y$. Tedaj $(g \circ f)(x) = k$

$\Rightarrow k \in Z_{g \circ f}$ $\Rightarrow Z_{g \circ f} = Z$ ☒

injekt: Če $g(f(x_1)) = g(f(x_2)) \Rightarrow f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

Zgled (1) Naj bo $f: X \to Y$ poljubna fja in $Id_Y : Y \to Y$ identiteta na Y, tj. fja, ki $y \mapsto y$. (obnaša se kot 1 za množenje)
Tedaj $f \circ Id_Y = f$.

(2) Če je $Id_X : X \to X$ identiteta na X, je $Id_X \circ f = f$.

Trditev Naj bosta $f: X \to Y$ in $g: Y \to X$ dve fje.

a) Če je $g \circ f = Id_X$ je f injektivna, g pa surjektivna

b) Če je $g \circ f = Id_X$ in $f \circ g = Id_Y$ sta f in g bijekciji.

Dokaz ad a) • Najprej injektivnost f: Če $x, x' \in X$ in $f(x) = f(x')$ ⇒

$$\Rightarrow g(f(x)) = g(f(x')) \quad \text{oz:} \quad (g \circ f)(x) = (g \circ f)(x')$$
$$Id_X(x) = Id_X(x')$$
$$x = x'$$

$\boxed{\text{injekt } f}$

• Surjektivnost g: Let $x \in X$; iščemo $y \in Y$, da je $g(y) = x$.
Toda tak y je kar $y := f(x)$, saj $g(y) = g(f(x)) = (g \circ f)(x) = x$

ad b) Očitno

QED.

def Če $f: X \to Y$, $g: Y \to X$ in je $g \circ f = Id_X$, $f \circ g = Id_Y$, pravimo, da je g INVERZ OD f in označimo $g = f^{-1}$.

BTW: seveda je tudi f inverz od g in $f = g^{-1}$.

KOMPOZICIJA FJIJ

Naj bo $f: X \to Y$ in $g: Y \to Z$

Tedaj je $(g \circ f)$ funkcija, ki: $(g \circ f): X \to Z$

= g kompozitum f

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

To je torej fja z domeno X in kodomeno Z.

Na kratko si jo lahko predstavljamo z naslednjim komutativnim dgm:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, dashed, "g\circ f"'] & Y \arrow[d, "g"] \\ & Z \end{tikzcd}$$

... pravimo, da dgm KOMUTIRA

Pazi! Če kodomena za f $\neq$ domeni za g, ne moremo narediti $g \circ f$.

Zgled: $g, f: \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, $g(x) = x+3$

Lastnosti: $g \circ f \neq f \circ g$, v splošnem.

$f \circ g: x \mapsto (x+3)^2$

$g \circ f: x \mapsto x^2+3$

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

Dokaz asociativnosti: Imejmo torej $X \xrightarrow{f} Y$, $Y \xrightarrow{g} Z$, $Z \xrightarrow{h} U$

leva stran: $(g \circ f): X \to Z \Rightarrow h \circ (g \circ f): X \to U$

desna stran: $(h \circ g): Y \to U \Rightarrow (h \circ g) \circ f: X \to U$

- torej se ujema domeni in kodomeni na levi oz. desni strani.

- še predpis: $h \circ (g \circ f): x \mapsto h\big((g \circ f)(x)\big) = h\big(g(f(x))\big) = (h \circ g)(f(x))$

__Thm.__ Če sta $f: X \to Y$ in $g: Y \to Z$ surjektivni (injekt.) je tudi $(g \circ f)$ surjektivna (injekt.)

__Dokaz__

$z \in Z$. Ker je g surjekcija je $z \in Z_g$ tz: $g(y) = z$. Ker je f surjekc. je $y \in Z_f$ tz: $f(x) = y$. Tedaj $(g \circ f)(x) = z$ $\Rightarrow$ $z \in Z_{g \circ f}$ $\Rightarrow Z_{g \circ f} = Z$ $\boxed{\circ}$

injekt: Če $g(f(x_1)) = g(f(x_2)) \Rightarrow f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

• Inverz f^{-1} je taka fja, da $(f^{-1} \circ f) = Id_X$ in $(f \circ f^{-1}) = Id_Y$, obstaja LE, ČE JE f BIJEKCIJA.

• Poleg tega, če $y = f(x)$, je $f^{-1}(y) = f^{-1}(f(x)) = x$.

Torej je inverz fja dana s predpisom:

Za $\forall\, y \in Y$ vrne tisti, edini $x \in X$ za katerega je $f(x) = y$.

Zgled Denimo, da je $f : A \to B$ injekcija. Če kodomeno B utesnimo na zalogo vrednosti, dobimo novo fjo $\tilde{f} : A \to Z_f$, z istim predpisom kot f (i.e.: $f(x) = \tilde{f}(x)$), ki PA JE BIJEKTIVNA.

Torej ima drugačne lastnosti kot fja f; med drugim npr. za $\tilde{f}$ velja, da ima inverz, $\tilde{f}^{-1}$, medtem ko ga fja f nima, če ni surjekcija!

Torej sta 2 fji enaki (tj. imata iste lastnosti)

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

če, če:
- $A = C$
- $B = D$
- $f(x) \equiv g(x)$

Zgled 2 Naj bo $f : X \to Y$ in $G \subseteq Y$.

Tedaj je
$$g : G \to Y$$
$$x \mapsto f(x)$$

spet fja, ki ji rečemo zožitev f na množico G in označimo

$$g = f|_G$$

konkreten zgled
$$f|_{[-\frac{\pi}{2}, \frac{\pi}{2}]} : [-\tfrac{\pi}{2}, \tfrac{\pi}{2}] \to [-1, 1]$$
$$x \mapsto \sin x$$
pa se izkaže, da je bijekcija.

Njen inverz imenujemo arcsin. Torej $\arcsin = \left(\sin|_{[-\frac{\pi}{2}, \frac{\pi}{2}]}\right)^{-1}$

Opomba: Funkcijam, pri katerih domena in kodomena sta podmnožici realnih števil rečemo tudi realne fje. Npr. $f : x \mapsto \frac{1}{x}$.
Pri njih običajno niti ne navajamo domene in kodomene; ~~...~~ V takem primeru za domeno vzamemo vsa tista števila, za katera je predpis dobro definiran, oz. je $f(x)$ realno število. Množici vseh teh števil rečemo tudi (NARAVNO) DEFINICIJSKO OBMOČJE, D_f.

Zgled: D_f za $f(x) = \frac{1}{x}$ je množica $D_f = \mathbb{R} \setminus \{0\}$.

Naj bosta

$$\begin{tikzcd} X \arrow[r, "f"] & Y \arrow[d, "g"] \\ & Z \end{tikzcd}$$

f in g bijekciji. Tedaj je bijekcija tudi $(g \circ f)$, zato $\exists (g \circ f)^{-1}$

Trditev: Če sta g in f bijekciji je $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

Dokaz:

$$\left.\begin{array}{l} g \circ f : X \to Z \\ f^{-1} : Y \to X \\ g^{-1} : Z \to Y \end{array}\right\} \Rightarrow f^{-1} \circ g^{-1} : Z \to X$$

Dalje,

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ Id_Y \circ g^{-1} = g \circ g^{-1} = Id_Z$$

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ g^{-1} \circ g \circ f = f^{-1} \circ Id_Y \circ f = f^{-1} \circ f = Id_X$$

QED

RELACIJE

Posplošitev pojma f-ja je relacija. Kot smo že omenili, je f-ja natanko določena s svojim GRAFOM. Graf lahko smatramo, da je podmnožica: $\mathcal{G} \subseteq X \times Y$ z določenimi lastnostmi

def **Relacija** pa je poljubna podmnožica $X \times Y$.

Zgled ① $R = \{(x,y);\ x > y\} \subseteq \mathbb{R} \times \mathbb{R}$ je relacija „strogo večje od".

Torej $xRy \Leftrightarrow x > y$

② $\{(x,y);\ x \text{ deli } y\} \subseteq \mathbb{N} \times \mathbb{N}$ je relacija deljivosti števil, ki jo označujemo tudi kot x/y.

Nekaj lastnosti relacij

Relacija $R \subseteq X \times X$ je

- simetrična, če $xRy \Rightarrow yRx$ $\forall x,y$
- refleksivna, če xRx $\forall x$
- tranzitivna, če $xRy \wedge yRz \Rightarrow xRz$ $\forall x,y,z$
- asimetrična, če $xRy \Rightarrow y \not{R} x$ $\forall x,y$
- antisimetrična, če $xRy \wedge yRx \Rightarrow y = x$ $\forall x,y$
- sovisna, če $x \neq y \Rightarrow xRy$ ali yRx $\forall x,y$
- strogo sovisna, če xRy ali yRx, $\forall x,y$
- ekvivalenca, če je refleksivna, simetrična, tranzitivna
- delna urejenost, če je refleksivna, antisimetrična, tranzitivna
- linearna urejenost: STROGO SOVISNA, ANTISIMETRIČNA, TRANZITIVNA [npr. $(\mathbb{R}, \leq)$]

Zgled 1 Na množici $\mathbb{Z} \times \mathbb{N}$, uvedemo relacijo takole:

$$(a,b) \, R \, (c,d) \iff ad = bc$$

To je ekvivalenčna relacija, kar hitro vidimo, če (a,b) zapišemo bolj običajno kot ulomek: $\frac{a}{b}$

Med sabo ekvivalentni ulomki določajo isto racionalno število.

Zgled 2 Na $\mathcal{P}(X)$ uvedimo relacijo: $A \, R \, B \overset{\text{DEF}}{\iff} A \subseteq B$

"je podmnožica od". To je relacija delne urejenosti.

UNIJE in PRESEKI DRUŽIN MNOŽIC.

Naj bo $\mathcal{J}$ poljubna (indeksna) množica in $\lambda \in \mathcal{J}$.
$\forall \lambda \in \mathcal{J}$ priredimo množico X_λ. Tako dobimo družino množic $(X_\lambda)_{\lambda \in \mathcal{J}}$

__def__ $$\bigcup_{\lambda \in \mathcal{J}} X_\lambda := \{x;\ \exists \lambda \in \mathcal{J} \text{ da je } x \in X_\lambda\}$$

$$\bigcup_{\lambda \in \emptyset} X_\lambda := \emptyset$$

$$\bigcap_{\lambda \in \mathcal{J}} X_\lambda := \{x;\ x \in X_\lambda \text{ za } \forall \lambda \in \mathcal{J}\} \ldots$$

pazi: $\bigcap_{\lambda \in \emptyset} X_\lambda$ bi bila množica vseh reči. taka množica NE OBSTAJA! Pri preseku torej $\mathcal{J} \neq \emptyset$!

__Zgled__ 1 $\mathcal{J} = \{1,2\}$; $X_1 = A$, $X_2 = B$.

Tedaj $$\bigcup_{\lambda \in \mathcal{J}} X_\lambda = \{x;\ \exists \lambda \in \{1,2\} \text{ da je } x \in X_\lambda\} =$$
$$= \{x;\ x \in X_1 \vee x \in X_2\} = A \cup B$$

$$\bigcap_{\lambda \in \mathcal{J}} X_\lambda = \{x;\ x \in X_1 \wedge x \in X_2\} = A \cap B.$$

__Zgled__ 2 Če je $\mathcal{J} = \{1,2,\ldots,n\}$, je $$\bigcup_{\lambda \in \mathcal{J}} X_\lambda = X_1 \cup X_2 \cup \ldots \cup X_n$$
$$\bigcap_{\lambda \in \mathcal{J}} X_\lambda = X_1 \cap X_2 \cap \ldots \cap X_n$$

$\bigcup_{\lambda\in\mathbb{N}} X_\lambda$ pišemo tudi kot $\bigcup_{\lambda=1}^{\infty} X_\lambda$

$\bigcap_{\lambda\in\mathbb{N}} X_\lambda$ -||- $\bigcap_{\lambda=1}^{\infty} X_\lambda$

---

preseke in unije povezujeta naslednja de Morganova zakona:

$$\left(\bigcup_{\lambda\in J} X_\lambda\right)^c = \bigcap_{\lambda\in J} X_\lambda^c$$

velja za $J \neq \emptyset$!

$$\left(\bigcap_{\lambda\in J} X_\lambda\right)^c = \bigcup_{\lambda\in J} X_\lambda^c$$

SLIKE IN PRASLIKE --> DS1

SLIKE IN PRASLIKE MNOŽIC

Naj bo $f: X \to Y$ fja. Za $U \subseteq X$ lahko gledamo množico vseh slik $\{f(x);\ x\in U\} \subseteq Y$

$$\{f(x);\ x\in U\} = \{y;\ \exists x\in X \text{ da je } y=f(x)\} \subseteq Y$$

To množico imenujemo SLIKA množice U pri preslikavi f in običajno označimo z $f(U)$.

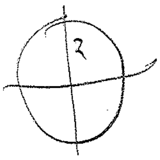
Zgled: $f(\emptyset)=\emptyset$, saj v $\emptyset \subseteq X$ ni $\exists$ noben x, ki bi se kam slikal

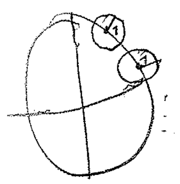
$f(X) = Z_f$

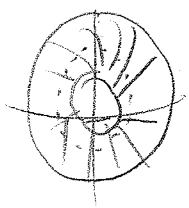
Zgled 3

$$J := \{(\alpha,\beta)\in\mathbb{R}^2 \,;\, \alpha^2+\beta^2=4\}$$

$$X_{(\alpha,\beta)} := \{(x,y) \,;\, (x-\alpha)^2+(y-\beta)^2=1\}$$

$J =$ 

$\bigcup_{(\alpha,\beta)\in J} X_{(\alpha,\beta)} =$ 

$=$  kolobar med $[1,3]$

$$\bigcap_{(\alpha,\beta)\in J} X_{(\alpha,\beta)} = \emptyset$$

Podobno za $V \subseteq Y$ množico vseh elementov iz X, ki se slikajo v V imenujemo **PRASLIKA** ~~Oznaka~~: množice V. Oznaka:

$$f^{-1}(V) := \{x \in X \,;\, f(x) \in V\} \subseteq X$$

$f^{-1}(\emptyset) = \emptyset$

$f^{-1}(Y) = X$

Nekaj lastnosti:

- $U \subseteq U' \subseteq X \Rightarrow f(U) \subseteq f(U')$
- $V \subseteq V' \subseteq Y \Rightarrow f^{-1}(V) \subseteq f^{-1}(V')$

$$f^{-1}(V_1) \setminus f^{-1}(V_2) = f^{-1}(V_1 \setminus V_2)$$

$$f^{-1}\Big(\bigcup_{\lambda \in J} V_\lambda\Big) = \bigcup_{\lambda \in J} f^{-1}(V_\lambda)$$

$$f^{-1}\Big(\bigcap_{\lambda \in J} V_\lambda\Big) = \bigcap_{\lambda \in J} f^{-1}(V_\lambda)$$

Če $y \in f(A) \setminus f(B) \Rightarrow \exists\, a \in A$: $f(a) = y$. Seveda $a \notin B$ drugače bi $y \in f(B)$. Torej $a \in A \setminus B \Rightarrow y = f(a) \in f(A \setminus B)$

TODA:

$$f\Big(\bigcup_{\lambda \in J} U_\lambda\Big) = \bigcup_{\lambda \in J} f(U_\lambda)$$

$$f(U_1) \setminus f(U_2) \subseteq f(U_1 \setminus U_2)$$

$$f\Big(\bigcap_{\lambda \in J} U_\lambda\Big) \subseteq \bigcap_{\lambda \in J} f(U_\lambda)$$ .... če f ni injektivna v splošnem nimamo enačaja

$$f^{-1}(f(U)) \supseteq U$$ .... enakost velja, če je f injektivna

$$f(f^{-1}(V)) \subseteq V$$ .... enakost velja, če je f surjekcija

Moč množic

- Radi bi primerjali dve množici med seboj. V primeru končnih množic pač preštejemo njene (različne!) elte, in pravimo, da ima množica A isto moč kot B, če imata enako število eltov.

- Proces si lahko predstavljamo tudi takole: Iz A vzamemo nek elt in ga združimo z nekim drugim eltom iz B.
  To ponavljamo dokler ne izčrpamo vseh eltov v A, ali pa, dokler ne zmanjka „parov" iz množice B.
  A in B sta enako močni, če na koncu ne ostane noben elt niti v A, niti v B.
  Prestikavi, ki elte iz A pari z elti iz B pa je fja, in sicer bijekcija.

- Na tak način lahko primerjamo tudi ∞ množice po moči:

Def Množici A in B imata isto moč, če obstaja neka bijekcija $f: A \to B$. $(A \sim B)$

Lastnosti:

$A \sim A$

$A \sim B \Rightarrow B \sim A$ ... bijekcija je ~~ima~~ f^{-1}

$A \sim B$ in $B \sim C \Rightarrow A \sim C$ ... tranzitivnost

} ekvivalenčna relacija na RAZREDU vseh množic.

Zgled $f: \{0,1,2,3,\ldots\} \to \{0,2,4,6,\ldots\}$

$\mathbb{N} \to 2\mathbb{N}$

$x \longmapsto 2x$

je bijekcija med $\mathbb{N}$ in $2\mathbb{N}$. Torej sta $\mathbb{N}$ in $2\mathbb{N}$ enakomočni

Zgled $f : \mathbb{Z} \to \mathbb{N}$

$$x \mapsto \begin{cases} 2x; & x > 0 \\ -2x-1; & x < 0 \\ 0; & x = 0 \end{cases}$$ je bijekcija med $\mathbb{Z}$ in $\mathbb{N}$

~~Npr.~~ Tj. cela števila uredimo v naslednje zaporedje:

$\mathbb{Z} = \; 0, -1, 1, -2, 2, -3, 3, -4, 4, \ldots$

$\mathbb{N} = \; 0, 1, 2, 3, 4, 5, 6, 7, 8, \ldots$

- Kaj če takšne bijekcije ni?

Temeljni izrek teorije množic pravi:

Naj bosta A, B dani množici. Tedaj velja vsaj ena od obeh možnosti:

(a) $\exists A_0 \subseteq A$, da je $A_0 \sim B$

(b) $\exists B_0 \subseteq B$, da je $A \sim B_0$

- Če veljata (a) in (b), je $A \sim B$ (Schröder – Bernsteinov izrek)
- Če velja (a) in ne (b), ~~je~~ ima A večjo moč kot B oz.: $A \succ B$
- Če -||- (b) in ne (a) pa ima B večjo moč kot A oz.: $A \prec B$.

Izrek o TRIHOTOMIJI: Za poljubni množici A, B je bodisi

- $A \prec B$
- $B \prec A$
- $A \sim B$

VELJA NATANKO ENA OD TEH 3. MOŽNOSTI

- V prej. dveh zgledih smo videli primere množic ($\mathbb{Z}$ in $\mathbb{N}$) ki ima isto moč kot njena prava podmnožica. ~~Take so~~ Za take nam intuicija pravi, da ne morejo imeti končno elementov.

def Množica A je neskončna, če ima isto moč kot kakšna njena prava podmnožica

- V pogl. Uvod zgledih smo videli, da je $\mathbb{N}$ neskončna množica.
- Ali so vse neskončne množice iste moči kot $\mathbb{N}$? ~~[illegible]~~

def Če ima množica isto moč kot $\mathbb{N}$ pravimo, da je 'števno neskončna'.

Zgled Če je A poljubna množica, ima $\mathcal{P}(A)$ večjo moč kot A.
Torej obstajajo množice, ki niso števno neskončne
neskončne

dokaz • Za $A=\emptyset$ je očitno.

- $A \neq \emptyset$. Pa predpostavimo da obstaja bijekcija $f: A \to \mathcal{P}(A)$.

(*) Tedaj obstaja nek $a \in A$, da je $f(a)=\emptyset \Longrightarrow a \notin f(a)$

(**) -||- $b \in A$ -||- $f(b)=A \Rightarrow b \in f(b)$

Naj bo A_1 množica tistih eltov $x \in A$, da je $x \notin f(x)$

- očitno $A_1 \neq \emptyset$ po (*), pa tudi $A_1 \neq A$ po (**) (saj vemo da $b \in f(b)$)

- Ker smo predpostavili, da je f surjekcija, moramo najti nek $x_1 \in A_1$, da je $f(x_1)=A_1$.

- Sedaj se vprašajmo ali $x_1 \in f(x_1)=A_1$ ali ne?

  - Če $x_1 \in A_1$, je po def. množice A_1 tudi $x_1 \notin f(x_1)=A_1$ $\rightarrow\leftarrow$
  - Če $x_1 \notin A_1$ -||- $x_1 \in f(x_1)=A_1$ $\rightarrow\leftarrow$

Torej NE OBSTAJA BIJEKCIJA.

Obstaja pa bijekcija med A in PODMNOŽICO $\mathcal{P}(A)$, tj množico $\{\{a\};\ a \in A\}$, $a \mapsto \{a\}$

QED

AKSIOMATIKA REALNIH ŠTEVIL.

• Realna števila so množica $\mathbb{R}$, na kateri imamo definirani dve operaciji: seštevanje in množenje, ter relacijo strogo lin. urejenosti. Te operacije niso čisto nepovezane, temveč ustrezajo z $\boxed{XVI}$ aksiomi.

– Gremo po vrsti: Operacijo seštevanja imamo lahko tudi za neko f-jo $\mathbb{R}\times\mathbb{R} \to \mathbb{R}$

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

Podobno je z operacijo množenja.

4 aksiomi (pravila seštevanja)

I $(x+y)+z = x+(y+z)$

II $x+y = y+x$

III $\exists$ število $0\in\mathbb{R}$: $x+0 = x \ \forall x\in\mathbb{R}$

IV $\forall x\in\mathbb{R}$ $\exists (-x)\in\mathbb{R}$: $x+(-x)=0$

NASPROTNI ELT

4 aksiomi (pravila množenja)

V $(x\cdot y)\cdot z = x\cdot(y\cdot z)$ ... ASOCIATIVNOST

VI $x\cdot y = y\cdot x$ ... KOMUTATIVNOST

VII $\exists$ število $1\in\mathbb{R}$: $x\cdot 1 = x \ \forall x\in\mathbb{R}$

VIII $1 \neq 0$

IX $\forall x\neq 0$ iz množice $\mathbb{R}$ $\exists$ število $(x^{-1})\in\mathbb{R}$: $x\cdot(x^{-1}) = 1$

INVERZNI

X $(x+y)\cdot z = x\cdot z + y\cdot z$ DISTRIBUTIVNOST MNOŽENJA

~~Zato~~

Množici, kjer veljajo le I–IV pravimo ABELOVA GRUPA.
Če veljajo dodatno še V–X pa KOMUTATIVEN OBSEG ALI KRATKO: POLJE.

Zgled: Množica $\mathbb{R} := \{0,1\}$ za operaciji

$$\left.\begin{array}{ll} 0+x := x & x = 0 \text{ ali } 1 \\ 1+0 := 1 & \\ 1+1 := 0 & \\ & \\ 0\cdot x := 0 & \\ 1\cdot x := x & \end{array}\right\}$$

seštejemo ali množimo, in si nato ogledamo rezultat modulo 2

ustreza vsem X aksiomom, pa seveda ni množica realnih števil.

Pred nadaljevanjem še tele trditve

Trditev Aksiomi I - IV imajo za posledico naslednje trditve

i) $a + x = b + x \Rightarrow a = b$ ... PRAVILO KRAJŠANJA

ii) $x + \tilde{0} = x \Rightarrow \tilde{0} = 0$ .... OBSTAJA EN SAM NEVTRALNI ELT ZA SEŠTEVANJE

iii) $x + \hat{x} = 0 \Rightarrow \hat{x} = (-x)$ -11- NASPROTNI ELT

iv) Če ima enačba $a + x = b$ rešitev, je $x = b + (-a) \equiv b - a$

dokaz

ad i) $a \overset{III}{=} a + 0 \overset{IV}{=} a + [x + (-x)] \overset{I}{=} [a + x] + (-x) = [b + x] + (-x) \overset{IV}{=} b + [x + (-x)] = b + 0 \overset{III}{=} b$

ad ii) V i) vstaviš $a := 0$ in $b := \tilde{0}$. Tedaj $0 + x = x = x + \tilde{0} \overset{II}{=} \tilde{0} + x$
Po pravilu krajšanja je $0 = \tilde{0}$.

ad iii) V i) vstaviš $a := \hat{x}$ in $b := (-x)$
Tedaj $\hat{x} + x \overset{II}{=} x + \hat{x} = 0 = x + (-x) \overset{II}{=} (-x) + x \Rightarrow \hat{x} = (-x)$

ad (iv). $a + x = b$. Na obeh straneh prištejmo $(-a)$

$(a + x) + (-a) = b + (-a) = b - a$
$(x + a) + (-a) = b - a$
$x + [a + (-a)] = b - a$
$x + 0 = b - a$
$x = b - a$

Trditev Aksiomi V - X imajo za posledico:

(i') Če $x \neq 0$, in je $ax = bx \Rightarrow a = b$

(ii') Če $x \neq 0$ in je $x \cdot \tilde{1} = x \Rightarrow \tilde{1} = 1$

(iii') Če $x \neq 0$ in je $x \cdot \hat{x} = 1 \Rightarrow \hat{x} = x^{-1}$

(iv') Če $x \neq 0$ in ima enačba $ax = b$ rešitev, je $x = b \cdot a^{-1} \equiv \frac{b}{a}$.

22

Trditev: Aksiomi I – X imajo za posledico:

(i') $0\cdot x = 0 \quad \forall x \in M$

(ii') $(-x)y = -(xy) = x(-y)$

Trditev (ii) na strani 21

Dokaz (ad i') $0\cdot x + 0\cdot x \underset{X}{=} (0+0)\cdot x \underset{III}{=} 0\cdot x \Rightarrow 0\cdot x = 0$

ad (ii') $(-x)\cdot y + xy \underset{X}{=} [(-x)+x]\cdot y = 0\cdot y = 0 \Rightarrow (-x)y \underset{(ii)}{=} -(xy)$

(ii) ... dokazuje za sam nasprotni el.

Realna števila so urejena po velikosti: V množici M imamo definirano 2 mestno relacijo $<$, ki ustreza naslednjim aksiomom:

XI $x < y$ in $y < z \Rightarrow x < z$ ... tranzitivnost

XII $x < y \Rightarrow y \not< x$ ... asimetričnost

XIII $x \neq y \Rightarrow x < y$ ali $y < x$ ... sovisnost

RELACIJA STROGE LINEARNE UREJENOSTI

Na kratko: $<$ je tranzitivna in za $\forall x, y \in M$ velja NATANKO ENA od možnosti:

ali $x < y$ ali $x = y$ ali $y < x$ ...

ČE NAMREČ $x = y$ IN ČE BI NPR $x < y$, BI BILO PO XII $y \not< x$ TODA $x = y$ OZ: $x < x \underset{XII}{\Rightarrow} x \not< x$ →←

Opomba: Če $y < x$ pišemo tudi $x > y$.

Opomba: $y \not< x$ pišemo tudi kot $y \geq x$ ali pa $x \leq y$

definicijsko in pomeni: $x = y$ ali pa je $x < y$.

XIV $\quad x < y \Rightarrow x + z < y + z$

XV $\quad 0 < x$ in $0 < z \Rightarrow 0 < x \cdot z$

} usklajenost z binarnima operacijama seštevanja in množenja;

(≡ množica z aksiomi I - X), ki je urejena z relacijo $<$ (tj. ki ustreza aksiomom XI - XIII) in ki je usklajena z $+, \cdot$ preko XIV - XV imenujemo ~~linearno~~ strogo linearno urejen komut. obseg.

Elte $x \in \Pi$, za katere je

$0 < x$ imenujemo pozitivne,

$x < 0$ NEGATIVNE

$0 \leq x$ NENEGATIVNE

$x \leq 0$ NEPOZITIVNE

Trditev V ∀ strogo linearno urejenem komutat. obsegu velja

(i''') $\quad x > 0 \Rightarrow -x < 0$

(ii''') $\quad x < y$ in $0 < z \Rightarrow x \cdot z < y \cdot z$

(iii''') $\quad x < y$ in $z < 0 \Rightarrow x \cdot z > y \cdot z$ ... množenje z negat. številom obrne neenakost.

(iv''') $\quad x \neq 0 \Rightarrow x^2 > 0$. Torej je $1 = 1^2 > 0$

IV
$x < 0 \Rightarrow -x > 0$
$x < 0 \Rightarrow \underbrace{x + (-x)}_{0} < 0 + (-x) = -x$

dokaz

ad (i''') $\quad 0 < x \xRightarrow{\text{v XIV}} 0 + (-x) < x + (-x) = 0$

ad (ii''') $\quad x < y \xRightarrow{\text{XIV}} x + (-x) < y + (-x)$, $\; 0 < y + (-x)$ $\xRightarrow{\text{XV}} 0 < [y + (-x)] z = y z + (-x) \cdot z$

$0 \leq y \cdot z + (-(xz)) \xRightarrow{\text{XIV}} xz < yz$

ad (iii''') $\quad$ Po (i''') je $-z > 0 \xRightarrow{(ii''')} -zx < -zy \xRightarrow{\text{XIV}} -zx + zy < 0 \Rightarrow zy < zx$

ad (iv''') • Če je $0 < x$, je $0 < x \cdot x = x^2$, po $\underline{XV}$

Če je $x < 0$, je $x \cdot x > \cancel{x} \cdot 0 = 0$, po (iii''')... neenačbo $x < 0$ pomnožimo z negat. številom

Zgled $\Pi = \{0, 1\}$ ne more biti ~~...~~ strogo lin. urejen obseg, saj

$$\left.\begin{array}{l} 0 < 1 \Rightarrow 0+1 < 1+1 \\ 1 < 1+1 \end{array}\right\} \underset{\text{TRANZITIVNOST}}{\Rightarrow} 0 < 1+1$$

Def Naj bo $\Omega \subseteq \Pi$. • Če obstaja tak $\beta \in \Pi$, da $x \leq \beta \ \forall x \in \Omega$, je Ω navzgor omejena in β je zgornja meja

- Če obstaja tak $\alpha \in \Pi$, da je $x \geq \alpha \ \forall \alpha \in \Omega$, je Ω navzdol omejena
- Če je Ω navzgor in navzdol omejena, je OMEJENA
- Če je Ω navzgor omejena, in če $\beta_0 \in \Pi$ je tak da:
  - β_0 je zgornja meja Ω
  - Če je β' neka druga zgornja meja Ω, je $\beta' \geq \beta_0$

Potem β_0 imenujemo najmanjša zgornja meja ali $\beta_0 = \sup \Omega$ (supremum)

- Če je Ω navzdol omejena, pa največjo spodnjo mejo imenujemo infimum Ω: $\inf \Omega$

Lastnosti supremuma:
1) β_0 je zg. meja Ω
2) $\forall \varepsilon > 0 \ \exists x \in \Omega : \beta_0 - \varepsilon < x \leq \beta_0$

Zgled $\Omega = \emptyset$ je navzgor in navzdol omejena. Katerokoli število je zgornja meja. Ne obstaja pa najmanjša zgornja meja Ω: ~~sup~~ $\sup \Omega$ ne obstaja

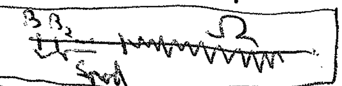
podobno: $\inf \Omega$ — $\shortparallel$ —

Zgled $\Omega = \{\frac{1}{n}; n \in \mathbb{N} \setminus \{0\}\}$ je omejena, $\sup \Omega = 1$, $\inf \Omega = 0$ $(\inf \Omega \notin \Omega)$

XVI (Dedekindova lastnost) V M ima vsaka neprazna, navzgor omejena množica natančno zgornjo mejo
NVZGOR MNŽCA

Množico M z lastnostmi I – XVII imenujemo obseg realnih števil in označimo z M. $M = \mathbb{R}$. (taka množica $\exists$ in je do izomorfizma enolično določena
glej RUDIN)

Posledica: V $\mathbb{R}$ ima $\forall$ neprazna, NVZD. omejena mnžca infimum.

SLIKA: 

Dokaz: Bodi $\Omega \subseteq \mathbb{R}$ neprazna. Naj bo Spod $:= \{B \in \mathbb{R};\ B$ je spod. meja $\Omega\}$.

- Spod $\neq \emptyset$.
- Mnžca Spod je NAVZGOR OMEJENA (nobena spodnja meja Ω ne more biti večja od nekega elta iz Ω)
- Torej $\exists$ $s := \sup(\text{Spod})$ … najmanjša zgornja meja Spod.

– Ta s je tudi $\inf \Omega$:

$\forall$ elti iz Spod bi bili kvečjemu manjši od x.

– Če $x \in \Omega$ je manjši od s, potem Spod $\leq x < s$ in s ne bi bila najmanjša zgornja meja od mnžce Spod.

– Torej je s spod meja od Ω oz: $s \in$ Spod

– Če s ne bi bila največja spodnja meja, bi $\exists$ $y \in$ Spod, $s < y$ … Tedaj tudi $s \neq \sup$ Spod $\rightarrow\leftarrow$

Ergo: s je največja spod. meja Ω oz: $s = \inf \Omega$

INTERVALI

Bodi $a \leq b$; $a, b \in \mathbb{R}$.

Množico — imenujemo

$(a,b) := \{x \in \mathbb{R};\ a < x < b\}$ — odprt interval

$(a,b] := \{x \in \mathbb{R};\ a < x \leq b\}$ — na LEVO polodprt ali polzaprt

$[a,b) := \{x \in \mathbb{R};\ a \leq x < b\}$ — na desno polodprt

$[a,b] := \{x \in \mathbb{R};\ a \leq x \leq b\}$ — zaprt interval

Zgled: Če je $a = b$ je $(a,a) = \emptyset = (a,a] = [a,a)$
$[a,a] = \{a\}$

Če $a < b$ je $\inf = a$ in $\sup = b$ za vsakega od teh intervalov.

RAZŠIRJENA REALNA ŠTEVILA

- Dodajmo $\mathbb{R}$ še dva elta, ki ju v $\mathbb{R}$ ni, označimo ju s $+\infty$ in $-\infty$

Dobimo $\mathbb{R}^* := \mathbb{R} \cup \{-\infty, +\infty\}$ ... razširjena realna števila.

Relacijo urejenosti razširimo še na $\mathbb{R}^*$, če definiramo

(1) $-\infty < +\infty$

(2) $-\infty < x \quad \forall x \in \mathbb{R}$

(3) $x < +\infty \quad \forall x \in \mathbb{R}$

Na tak način je $+\infty$ zgornja meja $\forall$ neprazne množice v $\mathbb{R}$, in ima torej $\forall$ neprazna množica supremum (lahko $= +\infty$)

Podobno ima $\forall$ neprazna množica infimum

- v $\mathbb{R}^*$ imamo še ~~dva~~ 4 intervale, ~~ki jih ni v $\mathbb{R}$~~:

$$(-\infty, a) := \{x \in \mathbb{R};\ x < a\}$$
$$(-\infty, a] := \{x \in \mathbb{R};\ x \leq a\}$$
$$(b, \infty) := \{x \in \mathbb{R};\ x > b\}$$
$$[b, \infty) := \{x \in \mathbb{R};\ x \geq b\}$$

- $\mathbb{R}^*$ ni več komutat. obseg, saj ne znamo definirati $-\infty + \infty$

Kljub temu včasih prav pride:

$$(-\infty) + (-\infty) = -\infty$$
$$-\infty + x = -\infty \quad \forall x \in \mathbb{R}$$
$$(-\infty) \cdot (-\infty) = (+\infty) \cdot (+\infty) = +\infty$$
$$(-\infty) \cdot x = x \cdot (-\infty) = -\infty \quad \text{za } x > 0$$

Izrek (o vloženih zaprtih intervalih)

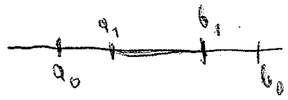
Imejmo zaporedje zaprtih intervalov $[a_0, b_0] \supseteq [a_1, b_1] \supseteq \dots \supseteq [a_n, b_n] \supseteq \dots$

$a_i \leq b_i$ za $i = 0, 1, 2, \dots$

Tedaj

$$\bigcap_{n=0}^{\infty} [a_n, b_n] \neq \emptyset$$

~~Šema~~ SLIKA:



Dokaz Bodi $A := \{a_n ; n \in \mathbb{N}\}$ ... leva krajišča

$B := \{b_n ; n \in \mathbb{N}\}$ ... desna krajišča.

Tedaj sta A, B neprazni, A je navzgor omejena z b_0, pa tudi $b_1, b_2, \dots, b_n \dots$

(kajti $a_k \leq a_{k+n} \leq b_{k+n} \leq b_{k+n-1} \leq \dots \leq b_n$)

Torej $\exists\ a := \sup A \leq b_n$ za $\forall$ index n.

Očitno pa je $a_0 \leq a_1 \leq \dots \leq a$

Torej $a \in [a_n, b_n]$ za $\forall$ index $n \Rightarrow a \in \bigcap_{n=0}^{\infty} [a_n, b_n]$.

D.N.

$$\bigcap_{n=0}^{\infty} [a_n, b_n] = [\sup A, \inf B]$$