Увод у теорију скупова

Појам скупа је интуитивно врло јасан:
скуп је колекција неких елемената

$A = \{1, 2, 3, 4\}$

$B = \{1, 2, 3, \dots\}$

$C = \{x \in \mathbb{N} \mid x \text{ је парно}\} = \{0, 2, 4, 6, \dots\}$

Парадокс берберина:
У неком селу постоји берберин који брије све људе који не бријају сами себе. Да ли берберин брије сам себе?
Берберин брије сам себе тако и само ако берберин не брије сам себе

Није једноставно описати нешто што је скуп!

Расеров парадокс: $S = \{x \mid x \notin x\}$

- ако $S \in S$ онда $S \notin S$
- ако $S \notin S$ онда $S \in S$

Основна релација између скупова је релација припадности
Скуп A припада скупу B записујемо са $A \in B$

Скупови се дефинишу (заснивају) аксиомама
(Зермело – Франкелова теорија скупова)

У наставку наводимо неке од аксиома:

<u>Аксиома екстензиционалности</u>
Два скупа су једнака ако имају исте елементе.

$A = \{2, 3\}$
$B = \{x \in \mathbb{R} \mid x^2 - 5x + 6 = 0\}$ $\Rightarrow A = B$

Аксиома празног скупа

Постоји скуп који нема ниједан елемент. Означавамо га са $\emptyset$.

приметимо да је празан скуп јединствен

def: Скуп A је подскуп скупа B, у ознаци $A \subseteq B$, ако за све $x \in A$ важи да $x \in B$.

A – произвољан скуп

$\emptyset \subseteq A$, $A \subseteq A$

$A = B$ ако $A \subseteq B$ и $B \subseteq A$.

Аксиома партитивног скупа

За сваки скуп X постоји скуп $P = \mathcal{P}(X)$ који се састоји од свих подскупова скупа X.

$\{a,b\}$

подскупови: $\emptyset$, $\{a\}$, $\{b\}$, $\{a,b\}$

$\mathcal{P}(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$

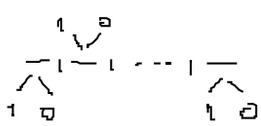
X – произвољан скуп

$\mathcal{P}(X) = \{Y \mid Y \subseteq X\}$

$\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$

$\mathcal{P}(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$

Генерално, ако X има n елемената, онда ће $\mathcal{P}(X)$ имати 2^n елемената.



Аксиома издвајања подскупа (сепарације)

Ако је A скуп и $P(x)$ нека формула, онда постоји скуп $\{x \in A \mid P(x)\}$.

- унија скупова A и B је скуп $A \cup B$

$$A \cup B = \{x \mid x \in A \text{ или } x \in B\}$$

- пресек скупова A и B је скуп $A \cap B$

$$A \cap B = \{x \mid x \in A \text{ и } x \in B\}$$

- разлика скупова A и B је скуп $A \setminus B$

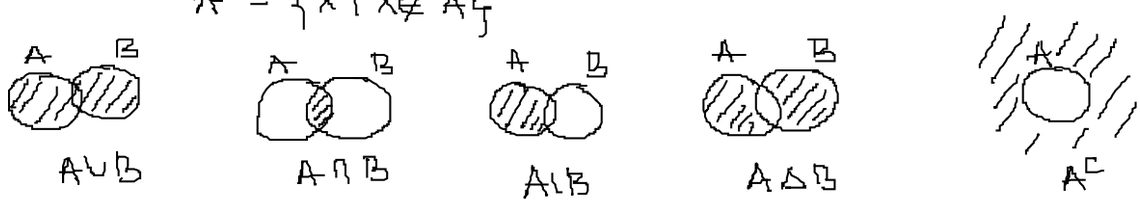
$$A \setminus B = \{x \mid x \in A \text{ и } x \notin B\}$$

- симетрична разлика скупова A и B је скуп $A \triangle B$

$$A \triangle B = \{x \mid x \in A \setminus B \text{ или } x \in B \setminus A\}$$

- комплемент скупа A је скуп A^c

$$A^c = \{x \mid x \notin A\}$$



<u>Аксиома уније</u>

За сваки скуп X постоји скуп Z тако да $u \in Z$ ако и само ако $u \in Y$ за неко $Y \in X$. Скуп Z представља унију елемената скупа X, и означавамо га са $\bigcup X$.

$$\bigcup \{A, B\} = A \cup B$$

Основни скуповни идентитети:

- комутативност $\cup, \cap, \triangle$

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$
$$A \triangle B = B \triangle A$$

али, $A \setminus B \neq B \setminus A$

- асоцијативност $\cup, \cap, \triangle$

$(A \cup B) \cup C = A \cup (B \cup C) = A \cup B \cup C$ (можемо да изоставимо заграде)

$(A \cap B) \cap C = A \cap (B \cap C) = A \cap B \cap C$

$(A \triangle B) \triangle C = A \triangle (B \triangle C) = A \triangle B \triangle C$

али, $(A \setminus B) \setminus C \neq A \setminus (B \setminus C)$

- дистрибутивност пресека у односу на унију и обрнуто

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

$x \in A \cap (B \cup C)$ако $x \in A$ и $x \in B \cup C$

ако $x \in A$ и ($x \in B$ или $x \in C$)

ако ($x \in A$ и $x \in B$) или ($x \in A$ и $x \in C$)

ако $x \in A \cap B$ или $x \in A \cap C$

ако $x \in (A \cap B) \cup (A \cap C)$

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

- идемпотентност $\cup$ и $\cap$

$A \cup A = A$

$A \cap A = A$

- закон апсорпције за $\cup$ и $\cap$

$A \cup (A \cap B) = A$

$A \cap (A \cup B) = A$

- де Морганови закони

$(A \cap B)^c = A^c \cup B^c$

$(A \cup B)^c = A^c \cap B^c$

$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

$x \in A \setminus (B \cup C)$ ако $x \in A$ и $x \notin B \cup C$

ако $\underline{x \in A}$ и $\underline{x \notin B}$ и $x \notin C$

ако $x \in A \setminus B$ и $x \in A \setminus C$

ако $x \in (A \setminus B) \cap (A \setminus C)$

$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

$A \triangle B = \emptyset$ ако $A = B$

$A \setminus B = \emptyset$ ако $A \subseteq B$

def: Индексирана фамилија је фамилија скупова F која је облика $F = \{A_i \mid i \in I\}$

$\downarrow$

индексни скуп

$$\bigcup F := \bigcup_{i \in I} A_i$$

$$\bigcap F := \bigcap_{i \in I} A_i$$

закони:

$$A \cap \bigcup_{i \in I} B_i = \bigcup_{i \in I} (A \cap B_i)$$

$x \in A \cap \bigcup_{i \in I} B_i$ акко $x \in A$ и $x \in \bigcup_{i \in I} B_i$

акко $x \in A$ и постоји $i_0 \in I$ тад. $x \in B_{i_0}$

акко постоји $i_0 \in I$ тад. $x \in A$ и $x \in B_{i_0}$

акко постоји $i_0 \in I$ тад. $x \in A \cap B_{i_0}$

акко $x \in \bigcup_{i \in I} (A \cap B_i)$

$$A \cup \bigcap_{i \in I} B_i = \bigcap_{i \in I} (A \cup B_i)$$

$$\bigcup_{i \in I} A_i \cap \bigcup_{j \in J} B_j := \bigcup_{\substack{i \in I \\ j \in J}} (A_i \cap B_j) \quad \left(= \bigcup_{i \in I} \bigcup_{j \in J} (A_i \cap B_j)\right)$$

$$\bigcap_{i \in I} A_i \cup \bigcap_{j \in J} B_j := \bigcap_{\substack{i \in I \\ j \in I}} (A_i \cup B_j)$$

Уређени пар

дефиниција: Уређени пар елемената a и b је објекат (a,b) који задовољава особину

$$(a,b)=(c,d) \text{ ако } a=c \text{ и } b=d.$$

Уређени пар можемо дефинисати

$$(a,b):=\{\{a\},\{a,b\}\}$$

ако је $a=c$ и $b=d$

$$\underbrace{\{\{a\},\{a,b\}\}}_{=(a,b)}=\underbrace{\{\{c\},\{c,d\}\}}_{=(c,d)} \Rightarrow (a,b)=(c,d)$$

ако $(a,b)=(c,d)$ тј. $\{\{a\},\{a,b\}\}=\{\{c\},\{c,d\}\}$

постоје две могућности:

1° $\{a\}=\{c\}$ и $\{a,b\}=\{c,d\}$

$a=c$ $\qquad$ $b=d$

2° $\{a\}=\{c,d\}$ и $\{a,b\}=\{c\}$

$a=\underline{c=d}$ $\qquad$ $\underline{c}=a=\underline{b}$

$a=c$ и $b=d$

дефиниција: Декартов производ скупова A и B је скуп

$$A\times B=\{(a,b)\mid a\in A \text{ и } b\in B\}.$$

$A=\{1,2,3\}$

$B=\{x,y\}$

$A\times B=\{(1,x),(1,y),(2,x),(2,y),(3,x),(3,y)\}$

$B\times A=\{(x,1),(x,2),(x,3),(y,1),(y,2),(y,3)\}$

особине:

$A \times B = \emptyset$ ако $A = \emptyset$ или $B = \emptyset$

$A \times (B \cap C) = (A \times B) \cap (A \times C)$

$(x,y) \in A \times (B \cap C)$ ако $x \in A$ и $y \in B \cap C$

ако $x \in A$ и $y \in B$ и $y \in C$

ако $(x,y) \in A \times B$ и $(x,y) \in A \times C$

ако $(x,y) \in (A \times B) \cap (A \times C)$

$A \times (B \cup C) = (A \times B) \cup (A \times C)$

<u>деф</u>: Уређена n-торка елемената $a_1, a_2, \ldots, a_n$ је објекат $(a_1, a_2, \ldots, a_n)$ такав да важи:

$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ ако $a_1 = b_1, a_2 = b_2, \ldots, a_n = b_n$.

$(a_1, a_2, \ldots, a_n) := (a_1, (a_2, (\ldots, (a_{n-1}, a_n) \ldots)))$

(a_1, a_2)

$(a_1, a_2, a_3) := (a_1, (a_2, a_3))$

$(a_1, a_2, a_3, a_4) := (a_1, (a_2, (a_3, a_4)))$

<u>деф</u>: Декартов производ скупова $A_1, A_2, \ldots, A_n$ је скуп

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}$$

$A_1 \times A_2 \times A_3 := A_1 \times (A_2 \times A_3)$

<u>деф</u>: Декартов степен скупа A је скуп

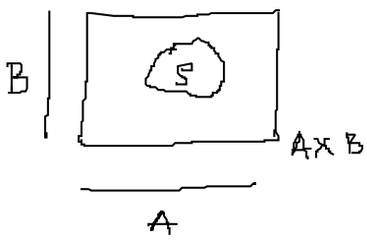
$$A^n := \underbrace{A \times A \times \ldots \times A}_{n \text{ пута}}, \quad n \geq 1.$$

сасуђајно, $A^0 := \{\emptyset\}$.

Релације

def: Бинарна релација између скупова A и B је било који подскуп $\rho \subseteq A \times B$.

Ако је $A = B$, тј. ако је $\rho \subseteq A^2$, кажемо да је ρ бинарна релација на скупу A.



def: n-арна релација између скупова $A_1, \dots, A_n$ је било који подскуп $\rho \subseteq A_1 \times A_2 \times \dots \times A_n$.

Ако је $A_1 = A_2 = \dots = A_n = A$, тј. ако је $\rho \subseteq A^n$, кажемо да је ρ n-арна релација на скупу A.

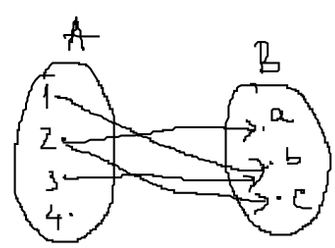
За $n=1$, $\rho \subseteq A$ је унарна релација на скупу A

Пример:

$A = \{1, 2, 3, 4\}$

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

$\rho = \{(1,b), (2,a), (2,c), (3,b)\} \subseteq A \times B$



$(a,b) \in \leq$ ако $a \leq b$

уместо $(a,b) \in \rho$ пишемо $a \rho b$

$\rho \subseteq A \times B$

$Dom(\rho) = \{a \in A \mid a \rho b$, за неко $b \in B\} \subseteq A$

$Im(\rho) = \{b \in B \mid a \rho b$, за неко $a \in A\} \subseteq B$

Инверзна релација

ако $\rho \subseteq A \times B$

$\rho^{-1} = \{(b,a) \mid (a,b) \in \rho\} \subseteq B \times A$

$(b,a) \in \rho^{-1}$ ако $(a,b) \in \rho$

$b \rho^{-1} a$ ако $a \rho b$

$\rho = \{(1,b), (2,a), (2,c), (3,b)\}$

тада је $\rho^{-1} = \{(b,1), (a,2), (c,2), (b,3)\}$

$\leq^{-1}$ је $\geq$

$b \geq a$ акко $a \leq b$

$\overset{\shortparallel}{\leq^{-1}}$

особине:

1° $(\rho^{-1})^{-1} = \rho$

2° $Dom(\rho^{-1}) = Im(\rho)$

$Im(\rho^{-1}) = Dom(\rho)$

Композиција релација

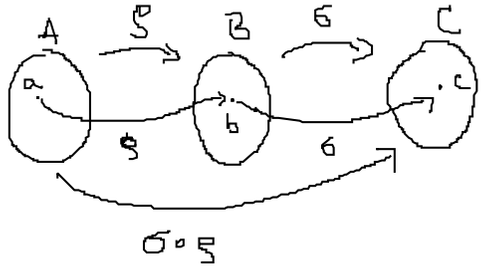
$\rho \subseteq A \times B$, $\sigma \subseteq B \times C$

$\sigma \circ \rho \subseteq A \times C$

$\downarrow$

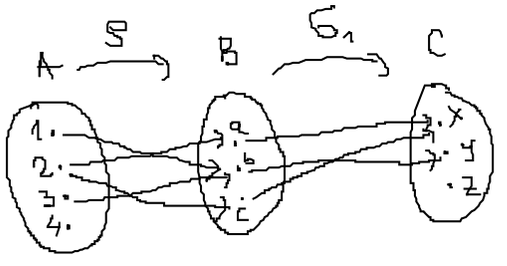
композиција релација ρ и σ

$\sigma \circ \rho = \{(a,c) \in A \times C \mid (a,b) \in \rho$ и $(b,c) \in \sigma$, за неко $b \in B\}$



$a \, (\sigma \circ \rho) \, c$ акко постоји $b \in B$ тај. $a \, \rho \, b$ и $b \, \sigma \, c$

пример:



$A = \{1,2,3,4\}$

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

$C = \{x,y,z\}$

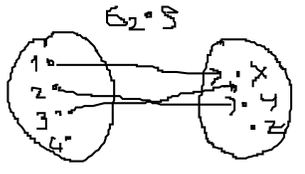
$\rho = \{(1,b), (2,a), (2,c), (3,b)\}$

$\sigma_1 = \{(a,x), (b,y), (c,x)\}$

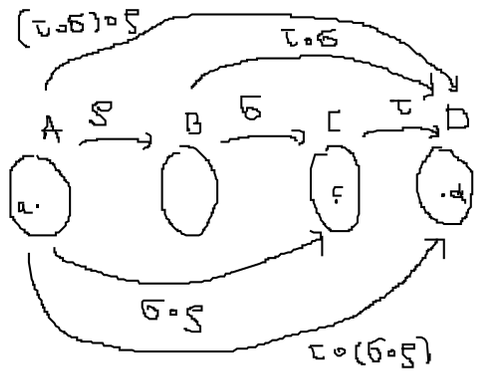
$\sigma_1 \circ \rho = \{(1,y), (2,x), (3,y)\}$

$\sigma_2 = \{(a,y), (b,x)\}$

$\sigma_2 \circ \rho = \{(1,x), (2,y), (3,x)\}$



особине композиције:



1° $\rho \subseteq A\times B$, $\sigma \subseteq B\times C$, $\tau \subseteq C\times D$

$$\underbrace{\underbrace{\tau\circ(\sigma\circ\rho)}_{\substack{\subseteq\\ A\times C}}}_{\substack{\subseteq\\ A\times D}} = \underbrace{\underbrace{(\tau\circ\sigma)\circ\rho}_{\subseteq B\times D}}_{\substack{\subseteq\\ A\times D}}$$

$(a,d)\in \tau\circ(\sigma\circ\rho)$ акко $(a,c)\in\sigma\circ\rho$ и $(c,d)\in\tau$, за неко $c\in C$

акко $(a,b)\in\rho$ и $\underbrace{(b,c)\in\sigma \text{ и } (c,d)\in\tau}_{(b,d)\in\tau\circ\sigma}$, за неке $b\in B, c\in C$

акко $(a,b)\in\rho$ и $(b,d)\in\tau\circ\sigma$, за неко $b\in B$

акко $(a,d)\in(\tau\circ\sigma)\circ\rho$

пишемо $\tau\circ\sigma\circ\rho$

2° $\rho\subseteq A\times B$, $\sigma\subseteq B\times C$

$(\sigma\circ\rho)^{-1} = \rho^{-1}\circ\sigma^{-1}$

$\sigma\circ\rho \subseteq A\times C$

$(\sigma\circ\rho)^{-1}\subseteq C\times A$

$(c,a)\in(\sigma\circ\rho)^{-1}$ акко $(a,c)\in\sigma\circ\rho$

акко $(a,b)\in\rho$ и $(b,c)\in\sigma$, за неко $b\in B$

акко $(b,a)\in\rho^{-1}$ и $(c,b)\in\sigma^{-1}$, за неко $b\in B$

акко $(c,a)\in\rho^{-1}\circ\sigma^{-1}$

<u>Пресек</u> <u>релација</u>:

$\rho_1,\rho_2\subseteq A\times B$

$(a,b)\in\rho_1\cap\rho_2$ акко $(a,b)\in\rho_1$ и $(a,b)\in\rho_2$

тј. $a\,\rho_1\,b$ и $a\,\rho_2\,b$

<u>Унија</u> <u>релација</u>:

$\rho_1,\rho_2\subseteq A\times B$

$(a,b)\in\rho_1\cup\rho_2$ акко $(a,b)\in\rho_1$ или $(a,b)\in\rho_2$

тј. $a\,\rho_1\,b$ или $a\,\rho_2\,b$

Особине пресека и унија:

1° $(\rho_1 \cap \rho_2)^{-1} = \rho_1^{-1} \cap \rho_2^{-1}$

2° $(\rho_1 \cup \rho_2)^{-1} = \rho_1^{-1} \cup \rho_2^{-1}$

} за домаћи

3° $\sigma \circ (\rho_1 \cup \rho_2) = (\sigma \circ \rho_1) \cup (\sigma \circ \rho_2)$ $\qquad \rho_1, \rho_2 \subseteq A \times B$

$\subseteq$ ✓

$\supseteq$ ✓ $\qquad \sigma \subseteq B \times C$

$\boxed{\subseteq}$ $(a,c) \in \sigma \circ (\rho_1 \cup \rho_2)$

тада $(a,b) \in \rho_1 \cup \rho_2$ и $(b,c) \in \sigma$, за неко $b \in B$

$(a,b) \in \rho_1$ или $(a,b) \in \rho_2$

посматрамо два случаја

1° ако $(a,b) \in \rho_1$ и $(b,c) \in \sigma$, за неко $b \in B$

онда $(a,c) \in \sigma \circ \rho_1$

па $(a,c) \in (\sigma \circ \rho_1) \cup (\sigma \circ \rho_2)$

2° ако $(a,b) \in \rho_2$ и $(b,c) \in \sigma$, за неко $b \in B$

онда $(a,c) \in \sigma \circ \rho_2$

па $(a,c) \in (\sigma \circ \rho_1) \cup (\sigma \circ \rho_2)$

$\boxed{\supseteq}$ нека $(a,b) \in (\sigma \circ \rho_1) \cup (\sigma \circ \rho_2)$

$(a,b) \in \sigma \circ \rho_1$ или $(a,b) \in \sigma \circ \rho_2$

1° $(a,c) \in \sigma \circ \rho_1$

тада $\underbrace{(a,b) \in \rho_1}_{(a,b) \in \rho_1 \cup \rho_2}$ и $(b,c) \in \sigma$, за неко $b \in B$

па $(a,b) \in \rho_1 \cup \rho_2$ и $(b,c) \in \sigma$, за неко $b \in B$

$(a,c) \in \sigma \circ (\rho_1 \cup \rho_2)$

2° $(a,c) \in \sigma \circ \rho_2$

тада $\underbrace{(a,b) \in \rho_2}_{(a,b) \in \rho_1 \cup \rho_2}$ и $(b,c) \in \sigma$, за неко $b \in B$

па $(a,b) \in \rho_1 \cup \rho_2$ и $(b,c) \in \sigma$, за неко $b \in B$

$(a,c) \in \sigma \circ (\rho_1 \cup \rho_2)$

4° $\sigma \circ (\rho_1 \cap \rho_2) \subseteq (\sigma \circ \rho_1) \cap (\sigma \circ \rho_2)$

$(a,c) \in \sigma \circ (\rho_1 \cap \rho_2)$

тада $(a,b) \in \rho_1 \cap \rho_2$ и $(b,c) \in \sigma$, за неко $b \in B$

$\underbrace{(a,b) \in \rho_1}_{①}$ и $\underbrace{(a,b) \in \rho_2}_{②}$ и $\underbrace{(b,c) \in \sigma}_{①\,②}$, за неко $b \in B$

из ① $(a,c) \in \sigma \circ \rho_1$

из ② $(a,c) \in \sigma \circ \rho_2$

па $(a,c) \in (\sigma \circ \rho_1) \cap (\sigma \circ \rho_2)$

Обратна инклузија у општем случају не важи:

$A = \{a\}$

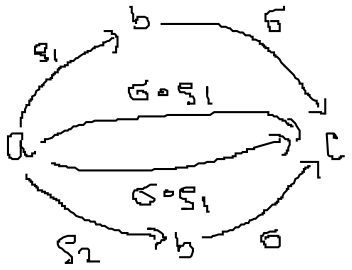
$B = \{b_1, b_2\}$

$C = \{c\}$

$\rho_1 = \{(a,b_1)\}$

$\rho_2 = \{(a,b_2)\}$

$\sigma = \{(b_1,c), (b_2,c)\}$



$\sigma \circ \rho_1 = \{(a,c)\}$
$\sigma \circ \rho_2 = \{(a,c)\}$ $\Rightarrow$ $(\sigma \circ \rho_1) \cap (\sigma \circ \rho_2) = \{(a,c)\}$

$\rho_1 \cap \rho_2 = \emptyset \Rightarrow \sigma \circ (\rho_1 \cap \rho_2) = \emptyset$

Релације на скупу A

$\rho \subseteq A \times A$

Кажемо да је ρ:

* рефлексивна ако за све $a \in A$ важи $a \rho a$ (тј. $(a,a) \in \rho$)
* антирефлексивна ако за све $a \in A$ не важи $a \rho a$
* симетрична ако за све $a,b \in A$ из $a \rho b$ следи $b \rho a$
* антисиметрична ако за све $a,b \in A$ из $a \rho b$ и $b \rho a$ следи $a = b$
* асиметрична ако за све $a,b \in A$ из $a \rho b$ следи да не важи $b \rho a$
* транзитивна ако за све $a,b,c \in A$ из $a \rho b$ и $b \rho c$ следи $a \rho c$

примери:

1° $\leq$ на $\mathbb{R}$

(P) за свако $x \in \mathbb{R}$ важи $x \leq x$ (T)

(AP) за свако $x \in \mathbb{R}$ важи $x \nleq x$ (⊥)

(C) за све $x, y \in \mathbb{R}$ ако $x \leq y$ онда $y \leq x$ (⊥)

$1 \leq 2$ или $2 \nleq 1$

(АНТИС) за све $x, y \in \mathbb{R}$ ако $x \leq y$ и $y \leq x$ следи $x = y$ (T)

(AC) за све $x, y \in \mathbb{R}$ ако $x \leq y$ онда $y \nleq x$ (⊥)

$1 \leq 1$ и $1 \leq 1$

(T) за све $x, y, z \in \mathbb{R}$ ако $x \leq y$ и $y \leq z$ онда $x \leq z$ (T)

2° паралелност правих на скупу правих у простору

(P) $a \parallel a$ (T)

(AP) $a \nparallel a$ (⊥)

(C) $a \parallel b \overset{?}{\Rightarrow} b \parallel a$ (T)

(АНТИС) $a \parallel b$ и $b \parallel a \overset{?}{\Rightarrow} a = b$ (⊥)

(AC) $a \parallel b \overset{?}{\Rightarrow} b \nparallel a$ (⊥)

(T) $a \parallel b$ и $b \parallel c \overset{?}{\Rightarrow} a \parallel c$ (T)

3° нормалност правих на скупу правих у простору

(P) $a \perp a$ (⊥)

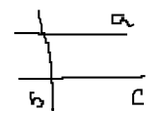
(AP) $a \not\perp a$ (T)

(C) $a \perp b \overset{?}{\Rightarrow} b \perp a$ (T)

(АНТИС) $a \perp b$ и $b \perp a \overset{?}{\Rightarrow} a = b$ (⊥)

(AC) $a \perp b \overset{?}{\Rightarrow} b \not\perp a$ (⊥)

(T) $a \perp b$ и $b \perp c \overset{?}{\Rightarrow} a \perp c$ (⊥)



$\Delta_A \subseteq A \times A$

$\Delta_A = \{(a,a) \mid a \in A\}$ – дијагонала

$(x,y) \in \Delta_A$ ако $x = y$

$\rho \subseteq A^2$

* ρ рефлексивна ако $\Delta_A \subseteq \rho$
* ρ антирефлексивна ако $\rho \cap \Delta_A = \emptyset$
* ρ симетрична ако $\rho \subseteq \rho^{-1}$

  ако $x \rho y$ онда $x \rho^{-1} y$ (јер $\rho \subseteq \rho^{-1}$)

  ако $x \rho^{-1} y$ онда $y \rho x$

* ρ асиметрична ако $\rho \cap \rho^{-1} = \emptyset$
* ρ антисиметрична ако ако $\rho \cap \rho^{-1} \subseteq \Delta_A$
* ρ транзитивна ако $\rho \circ \rho \subseteq \rho$

  $(a,c) \in \rho \circ \rho$ онда постоји $b \in A$ тј. $(a,b) \in \rho$ и $(b,c) \in \rho$ $\overset{T}{\Rightarrow}$ $(a,b) \in \rho$

  обрнуто, $a \rho b$ и $b \rho c$ онда $(a,c) \in \rho \circ \rho$ па ако је $\rho \circ \rho \subseteq \rho$ следи $(a,c) \in \rho$ тј. $a \rho c$

Пример:

1° $A = \{a, b, c\}$ $\Delta_A = \{(a,a), (b,b), (c,c)\}$

$\rho = \{(a,a), (b,b), (a,b), (b,a)\}$

$\rho^{-1} = \{(a,a), (b,b), (b,a), (a,b)\}$

$\rho \circ \rho = \{(a,a), (a,b), (b,b), (b,a)\}$

(Р)	(АР)	(С)	(АНТИС)	(АС)	(Т)
$\Delta_A \subseteq \rho$	$\Delta_A \cap \rho = \emptyset$	$\rho \subseteq \rho^{-1}$	$\rho \cap \rho^{-1} \subseteq \Delta_A$	$\rho \cap \rho^{-1} = \emptyset$	$\rho \circ \rho \subseteq \rho$
⊥	⊥	T	⊥	⊥	T

$\rho \subseteq \rho^{-1}$

$\rho \subseteq \rho^{-1} \overset{?}{\Rightarrow} \rho^{-1} \subseteq \rho$

$(x,y) \in \rho^{-1} \Rightarrow (y,x) \in \rho$ in ρ^{-1}

$\Rightarrow (y,x) \in \rho^{-1}$

$\Rightarrow (x,y) \in \rho$

$\rho \subseteq \rho^{-1}$

$\Downarrow$

$\rho^{-1} \subseteq \rho$ $\qquad \rho^{-1} = \rho$

пример:

$A = \{a,b,c\}$ $\qquad \Delta_A = \{(a,a), (b,b), (c,c)\}$

$\rho \subseteq A^2$

$\rho = \{(a,c), (b,a)\}$

$\rho^{-1} = \{(c,a), (a,b)\}$

$\rho \circ \rho = \{(b,c)\}$

(P)	(AP)	(C)	(AC)	(АНТИС)	(T)
$\Delta_A \subseteq \rho$	$\Delta_A \cap \rho = \emptyset$	$\rho \subseteq \rho^{-1}$	$\rho \cap \rho^{-1} = \emptyset$	$\underbrace{\rho \cap \rho^{-1}}_{\emptyset} \subseteq \Delta_A$	$\rho \circ \rho \subseteq \rho$
⊥	⊤	⊥	⊤	⊤	⊥

Релација еквиваленције

дф: Релација $\rho \subseteq A^2$ је еквиваленција ако је рефлексивна, симетрична и транзитивна.

примери:

1° $=$ је релација еквиваленције

$\downarrow$

Δ_A

2° нека је $m \geq 2$, на $\mathbb{Z}$ дефинишемо релацију $\equiv_m$ (једнакост по модулу) на следећи начин:

$$x \equiv_m y \quad \text{акко} \quad m \mid x-y$$

(P) $x \equiv_m x$?

$m \mid x-x$, тј. $m \mid 0$ ⊤

(C) $x \equiv_m y \overset{?}{\Rightarrow} y \equiv_m x$

$m \mid x-y \overset{?}{\Rightarrow} m \mid y-x$

$x-y = k \cdot m \Rightarrow y-x = (-k) \cdot m \Rightarrow m \mid y-x$ ⊤

$k \in \mathbb{Z}$

(T) $\left.\begin{array}{l} x \equiv_m y \\ y \equiv_m z \end{array}\right\} \overset{?}{\Rightarrow} x \equiv_m z$

$\left.\begin{array}{l} m \mid x-y \\ m \mid y-z \end{array}\right\} \overset{?}{\Rightarrow} m \mid x-z$

$\begin{array}{l} x-y = k_1 \cdot m \\ y-z = k_2 \cdot m \\ k_1, k_2 \in \mathbb{Z} \end{array} \Rightarrow (x-y)+(y-z) = k_1 m + k_2 m$

$x-z = (k_1+k_2)\cdot m$

тј. $m \mid x-z \Rightarrow x \equiv_m z$ (T)

Def: Нека је $\varrho \subseteq A^2$ еквиваленција. Класа еквиваленције елемента $a \in A$ је скуп

$$C_a = a/_\varrho = [a]_\varrho = \{x \in A \mid a \varrho x\}.$$

a-представник класе

$C_a \subseteq A$

због симетричности важи $C_a = \{x \in A \mid x \varrho a\}$

Дакле, $x \in C_a$ акко $a \varrho x$

акко $x \varrho a$

Особине класа:

1° $a \in C_a$ јер је ϱ рефлексивна, тј. $a \varrho a$

па је $C_a \neq \emptyset$

2° $a \varrho b$ акко $C_a = C_b$

$\Leftarrow$: Нека је $C_a = C_b$

$a \in C_a$, $C_a \subseteq C_b$, односно $a \in C_b$, а тада је $a \varrho b$

$\Rightarrow$: Нека је $a \varrho b$

$\underline{C_a \subseteq C_b}$:

$x \in C_a \Rightarrow x \varrho a$

$x \varrho a$ и $a \varrho b \overset{(T)}{\Rightarrow} x \varrho b$

тј. $x \in C_b$

$\underline{C_b \subseteq C_a}$:

$x \in C_b \Rightarrow b \varrho x$

$a \varrho b$ и $b \varrho x \overset{(T)}{\Rightarrow} a \varrho x$

тј. $x \in C_a$

3° $a \not\varrho b$ акко $C_a \cap C_b = \emptyset$

$\Leftarrow$: Нека $C_a \cap C_b = \emptyset$

како су $C_a, C_b \neq \emptyset$ (према 1°) следи да је $C_a \neq C_b$ па $a \not\varrho b$ (према 2°)

$\Rightarrow$: $a \not\varrho b$

претпостављамо супротно: $C_a \cap C_b \neq \emptyset$

тада постоји $x \in C_a \cap C_b$

$$\left.\begin{array}{l} x \in C_a \Rightarrow a \varrho x \\ x \in C_b \Rightarrow b \varrho x \text{ па и } x \varrho b \end{array}\right\} \overset{(T)}{\Rightarrow} a \varrho b$$

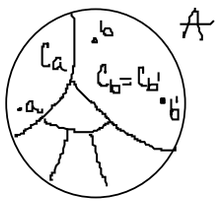
тј. $C_a = C_b$

(на основу 2°) ↯

def: Нека је $\varrho \subseteq A^2$ релација еквиваленције. Количнички скуп еквиваленције ϱ је скуп

$$A/_\varrho = \{C_a \mid a \in A\}.$$

Јасно је да је $A/_\varrho \subseteq \mathcal{P}(A)$ јер су $C_a \subseteq A$.



Особине количничког скупа:

1° Ако $X, Y \in A/_\varrho$ и $X \neq Y$, тада $X \cap Y = \emptyset$

Нека $X, Y \in A/_\varrho$ и $X \neq Y$

тада је $X = C_a$ и $Y = C_b$, за неке $a, b \in A$

Како је $C_a \neq C_b$ следи $C_a \cap C_b = \emptyset$

тј. $X \cap Y = \emptyset$

2° $\bigcup A/_\varrho = \bigcup_{X \in A/_\varrho} X = A$

$\subseteq$: Нека $x \in \bigcup A/_\varrho$

тада $x \in X$, за неко $X \in A/_\varrho$

Знамо да је $X = C_a$, за неко $a \in A$ па $x \in C_a \subseteq A$

Дакле, $x \in A$.

$\supseteq$: $x \in A$

Тада $x \in C_x$, а $C_x \in A/_\varrho$ па $x \in \bigcup A/_\varrho$.

def: Партиција скупа A је сваки подскуп $P \subseteq \mathcal{P}(A)$ који задовољава следеће услове:

1) Ако $X, Y \in P$ и $X \neq Y$, важи $X \cap Y = \emptyset$

2) $\bigcup P = A$

3) За свако $X \in P$ важи $X \neq \emptyset$.

На основу особина A/ϱ закључујемо да је A/ϱ партиција скупа A.

Пример: Одредити све партиције скупа $A=\{1,2,3\}$.

$P_1=\{\{1,2,3\}\}$ $P_2=\{\{1\},\{2,3\}\}$ $P_3=\{\{1,2\},\{3\}\}$ $P_4=\{\{1,3\},\{2\}\}$ $P_5=\{\{1\},\{2\},\{3\}\}$

Дакле, на скупу A постоји 5 партиција.

Тврђење: Нека је P партиција на скупу A. Дефинишимо бинарну релацију ϱ на скупу A на следећи начин:

$$a\varrho b \text{ ако } a,b\in X, \text{ за неко } X\in P.$$

Тада:

1° ϱ је еквиваленција на A

2° $A/\varrho = P$.

доказ:

1° (Р) $a\varrho a$ за свако $a\in A$?

$a\in A$, тада $a\in \underbrace{\cup P}_{=A}$, тј. $a\in X$, за неко $X\in P$

$a,a\in X \Rightarrow a\varrho a$ (Т)

(С) $a\varrho b \overset{?}{\Rightarrow} b\varrho a$

$a\varrho b$ тада $a,b\in X$, где $X\in P$, па $b\varrho a$

(Т) $\left.\begin{array}{l} a\varrho b \\ b\varrho c \end{array}\right\} \overset{?}{\Rightarrow} a\varrho c$

$a\varrho b \Rightarrow a,b\in X$, где $X\in P$

$b\varrho c \Rightarrow b,c\in Y$, где $Y\in P$

Дакле, $b\in X\cap Y$ па $X\cap Y\neq\emptyset$, односно по дефиницији партиције $X=Y$

$a,c\in X$ и $X\in P$ па закључујемо $a\varrho c$. (Т)

$\Rightarrow$ ϱ јесте релација еквиваленције

2° $A/\varrho = P$

$\subseteq$: Нека $X\in A/\varrho$

тада $X=C_a$, за неко $a\in A$

како је $a\in A=\cup P$, то $a\in X'$, где $X'\in P$

Доказујемо $C_a = X'$:

$\subseteq$: Нека $x \in C_a$, тј. $x \xi a$

$x, a \in Y$, где $Y \in P$

Како $a \in Y \cap X'$, то $X' = Y$ па $x \in X'$

$\supseteq$: Нека $x \in X'$

тада $a, x \in X'$ и $X \in P$ па $a \xi x$, тј. $x \in C_a$

Дакле, $X = C_a = X' \in P$.

$\supseteq$: Нека је $X \in P$

Тада је $X \neq \emptyset$, па изаберемо $a \in X$

Доказујемо да је $X = C_a$:

$\subseteq$: Нека $x \in X$

како $a, x \in X$ следи да је $a \xi x$ па $x \in C_a$

$\supseteq$: Нека $x \in C_a$, тј. $x \xi a$

како је $x \xi a$, следи $x, a \in Z$, где $Z \in P$

$a \in X \cap Z$, а $X, Z \in P$ па $X = Z$

Дакле, $x \in Z = X$

Закључујемо, $X = C_a \in A/\xi$.

Примери:

1° $A = \mathbb{Z}$, $m \geq 2$

$x \equiv_m y$ акко $m \mid x - y$

Класа еквиваленције a?

$x \in C_a$ акко $x \equiv_m a$ акко $m \mid x - a$

$m \mid x - a$ акко постоји $k \in \mathbb{Z}$ тј. $x - a = k \cdot m$

акко постоји $k \in \mathbb{Z}$ тј. $x = a + k \cdot m$

акко $x \in a + m\mathbb{Z} := \{a + mk \mid k \in \mathbb{Z}\}$

Дакле, $C_a = a + m\mathbb{Z}$

$C_0 = m\mathbb{Z}$ ← скуп свих целих бројева који су дељиви са m

$C_1 = 1 + m\mathbb{Z}$ ← скуп свих целих бројева који при дељењу са m дају остатак 1

$\vdots$

$C_{m-1} = (m-1) + m\mathbb{Z}$ ← скуп свих целих бројева који при дељењу са m дају остатак $m-1$

постоји укупно m различитих класа

на пример, $C_0 = C_m = C_{-m} = C_{5m} \dots$

$C_1 = C_{m+1} = C_{12m+1} \dots$

$\mathbb{Z}/\equiv_m = \{m\mathbb{Z}, 1+m\mathbb{Z}, \dots, (m-1)+m\mathbb{Z}\}$

2° $A = \mathbb{R}^2$

$\rho \subseteq A^2 = \mathbb{R}^2 \times \mathbb{R}^2$

$(x_1, y_1) \rho (x_2, y_2)$ акко $x_1^2 + y_1^2 = x_2^2 + y_2^2$

ρ је еквиваленција:

(Р) $(x,y) \rho (x,y)$?

$x^2 + y^2 = x^2 + y^2$ Т

(С) $(x_1,y_1) \rho (x_2,y_2) \overset{?}{\Rightarrow} (x_2,y_2) \rho (x_1,y_1)$

$x_1^2 + y_1^2 = x_2^2 + y_2^2 \overset{?}{\Rightarrow} x_2^2 + y_2^2 = x_1^2 + y_1^2$ Т

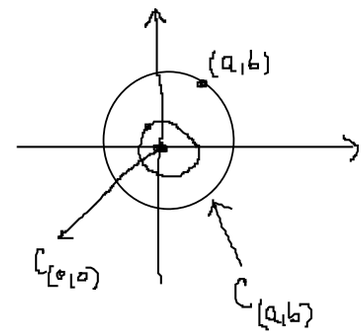
(Т) $\left.\begin{array}{l}(x_1,y_1) \rho (x_2,y_2)\\ (x_2,y_2) \rho (x_3,y_3)\end{array}\right\} \Rightarrow (x_1,y_1) \rho (x_3,y_3)$

$\left.\begin{array}{l}x_1^2 + y_1^2 = x_2^2 + y_2^2\\ x_2^2 + y_2^2 = x_3^2 + y_3^2\end{array}\right\} \Rightarrow x_1^2 + y_1^2 = x_3^2 + y_3^2$ Т

Класа елемента $(a,b) \in \mathbb{R}^2$?

$(x,y) \in C_{(a,b)}$ акко $(x,y) \rho (a,b)$

акко $x^2 + y^2 = \underbrace{a^2 + b^2}_{\text{фиксирано}}$



$r^2 := a^2 + b^2$

$(x,y) \in C_{(a,b)}$ акко $x^2 + y^2 = r^2$

Дакле, $C_{(a,b)} = \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = r^2\}$ ← кружница са центром $(0,0)$ и полупречником $r = \sqrt{a^2+b^2}$

$(x,y) \in C_{(0,0)}$ акко $(x,y) \rho (0,0)$

акко $x^2 + y^2 = 0^2 + 0^2 = 0$

акко $x = 0$ и $y = 0$

$C_{(0,0)} = \{(0,0)\}$

$(x,y) \in C_{(3,4)}$ акко $(x,y) \rho (3,4)$

акко $x^2 + y^2 = 3^2 + 4^2 = 25 = 5^2$

$C_{(3,4)} = K((0,0), 5)$ ← кружница са центром у тачки $(0,0)$ и полупречником 5.

A/ρ - скуп свих кружница са центром у $(0,0)$ и полупречником $r \geq 0$

3° $A = \{0,1,2\}$

$B = A \times A = A^2$

$\rho \subseteq B^2$

$(x_1, y_1) \rho (x_2, y_2)$ ако $x_1 y_1 = x_2 y_2$

ρ је еквиваленција:

(Р) $(x,y) \rho (x,y)$

$xy = xy$ Т

(С) $(x_1,y_1) \rho (x_2,y_2) \overset{?}{\Rightarrow} (x_2,y_2) \rho (x_1,y_1)$

$x_1 y_1 = x_2 y_2 \overset{?}{\Rightarrow} x_2 y_2 = x_1 y_1$ Т

(Т) $\left.\begin{array}{l}(x_1,y_1) \rho (x_2,y_2) \\ (x_2,y_2) \rho (x_3,y_3)\end{array}\right\} \overset{?}{\Rightarrow} (x_1,y_1) \rho (x_3,y_3)$

$\left.\begin{array}{l}x_1 y_1 = x_2 y_2 \\ x_2 y_2 = x_3 y_3\end{array}\right\} \Rightarrow x_1 y_1 = x_3 y_3$ Т

Класа елемента $(a,b) \in B$?

$(x,y) \in C_{(a,b)}$ ако $(x,y) \rho (a,b)$

ако $x \cdot y = \underbrace{ab}_{\text{фиксирано}}$

$C_{(0,0)} = \{(x,y) \in B \mid xy = 0\}$

$= \{(0,0), (0,1), (0,2), (1,0), (2,0)\} = C_{(0,1)} = C_{(0,2)} = C_{(1,0)} = C_{(2,0)}$

$C_{(1,1)} = \{(x,y) \in B \mid xy = 1\} = \{(1,1)\}$

$C_{(1,2)} = \{(x,y) \in B \mid xy = 2\} = \{(1,2), (2,1)\} = C_{(2,1)}$

$C_{(2,2)} = \{(x,y) \in B \mid xy = 4\} = \{(2,2)\}$

$B/\rho = \{\{(0,0), (0,1), (0,2), (1,0), (2,0)\}, \{(1,1)\}, \{(1,2), (2,1)\}, \{(2,2)\}\}$

Релације поретка

деф: Релација $\rho \subseteq A^2$ је поредак (уређење) ако је ρ рефлексивна, антисиметрична и транзитивна.

примери:

1° $\leq$ је поредак на $\mathbb{R}$

2° $\subseteq$ је поредак на $\mathcal{P}(X)$, X - произвољан скуп

(Р) $Y \in \mathcal{P}(X)$

$Y \subseteq Y$ (Т)

(АНТИС) $Y_1 \subseteq Y_2$ и $Y_2 \subseteq Y_1 \Rightarrow Y_1 = Y_2$ (Т)

(Т) $Y_1 \subseteq Y_2$, $Y_2 \subseteq Y_3 \Rightarrow Y_1 \subseteq Y_3$

3° $m \mid n$ ако $(\exists k \in \mathbb{Z})$ $n = m \cdot k$

$\mid$ је поредак на $\mathbb{N}$

(Р) $m \mid m$!

$m = 0$ тада је $0 = 0 \cdot k$, $k \in \mathbb{N}$ $\Rightarrow$ важи и за $m = 0$ (Т)

(АНТИС) $m \mid n$ и $n \mid m \underset{!}{\Rightarrow} m = n$

$n = k \cdot m$
$m = k' \cdot n$ $\quad k, k' \in \mathbb{N}$

$n = k \cdot k' \cdot n \Rightarrow n(1 - kk') = 0$

$n = 0$ или $1 - kk' = 0$

ако је $n = 0 \Rightarrow m = k' \cdot 0 = 0 \Rightarrow m = n$

ако је $\left.\begin{array}{l} kk' = 1 \\ k, k' \in \mathbb{N} \end{array}\right\} \Rightarrow k = k' = 1 \Rightarrow m = n$ (Т)

(Т) $m \mid n$ и $n \mid l \underset{!}{\Rightarrow} m \mid l$

$\left.\begin{array}{l} n = k \cdot m \\ l = k' \cdot n \\ k, k' \in \mathbb{N} \end{array}\right\} \Rightarrow l = k'km$ тј. $m \mid l$ (Т)

деф: Нека је $\rho \subseteq A^2$ поредак. Елементи a и b су упоредиви ако важи $a \rho b$ или $b \rho a$. У супротном, a и b су неупоредиви.

Поредак је потпуан (тотални) ако су сваки два елемента упоредиви. Уколико сваки два елемента нису упоредиви, онда је тај поредак парцијалан.

Примери:

1° $\leq$ је линеарни поредак на $\mathbb{R}$

за све $a, b \in \mathbb{R}$ важи $a \leq b$ или $b \leq a$

2° $\subseteq$ није линеарни поредак на $\mathcal{P}(X)$

нпр. $X = \{1,2\}$

тада $\{1\}, \{2\} \in \mathcal{P}(X)$

$\{1\} \not\subseteq \{2\}$ и $\{2\} \not\subseteq \{1\}$

$\{1\}$ и $\{2\}$ су неупоредиви елементи

3° $\mid$ није линеарни поредак на $\mathbb{N}$

нпр. $2 \nmid 3$ и $3 \nmid 2$

2 и 3 нису упоредиви

$a \varrho b$ читамо: a је ϱ-мање од b

b је ϱ-веће од a

дефиниција: Нека је ϱ уређење на скупу A и нека је $B \subseteq A$.

- b је најмањи елемент (минимум) скупа B ако:

  $b \in B$ и за све $x \in B$ важи $b \varrho x$

- b је највећи елемент (максимум) скупа B ако:

  $b \in B$ и за све $x \in B$ важи $x \varrho b$

- b је минималан елемент скупа B ако $b \in B$ и важи:

  ако $x \varrho b$, онда је $x = b$, за све $x \in B$

  (тј. не постоји ништа ϱ-мање од b)

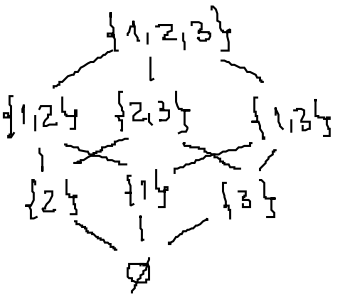
- b је максималан елемент скупа B ако $b \in B$ и важи:

  ако $b \varrho x$, онда је $x = b$, за све $x \in B$

  (тј. не постоји ништа ϱ-веће од b)

Примери:

1° $A = \mathcal{P}(\{1,2,3\})$, $\subseteq$



A има најмањи елемент: $\emptyset$

(то је и минимални ел.)

A има највећи елемент: $\{1,2,3\}$

(то је и максимални ел.)

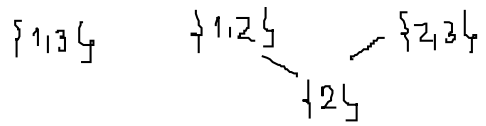
$B = A \setminus \{\emptyset\}$

B нема најмањи елемент

B има минималне елементе: $\{1\}, \{2\}, \{3\}$

B има највећи елемент: $\{1,2,3\}$
(то је уједно и максималан елемент)

$C = \{\{2\}, \{1,2\}, \{1,3\}, \{2,3\}\}$



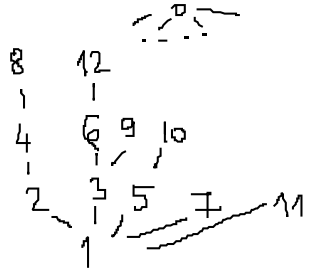
C нема најмањи елемент

C има минималне елементе: $\{1,3\}, \{2\}$

C нема највећи елемент

C има максималне елементе: $\{1,3\}, \{1,2\}, \{2,3\}$

2° | на $\mathbb{N}$



$n \in \mathbb{N}$

$0 = n \cdot 0 \Rightarrow n \mid 0$

$\mathbb{N}$ има најмањи елемент: 1 јер за све $n \in \mathbb{N}$ $1 \mid n$

$\mathbb{N}$ има највећи елемент: 0 јер за све $n \in \mathbb{N}$ $n \mid 0$

$S = \mathbb{N} \setminus \{1\} = \{0, 2, 3, 4, 5, \dots\}$

S нема најмањи елемент:

нека $a \in S$ $(a \neq 1)$

ако је $a = 0$ онда $0 \nmid 2 \Rightarrow 2$ није најмањи ел.

ако је $a \neq 0$ онда $a \nmid a+1 \Rightarrow a$ није најмањи ел.

S има минималне елементе: прости бројеви

нека је $p \in S$ прости број

ако $x \mid p$ за неко $x \in S$ тада $\underset{x \in S}{\cancel{x \mid 1}}$ или $x = p$

ако $a \in S$ није прости број тада постоји прости број $p \in S$ т.д. $p \mid a$ па a није минималан елемент.

Тврђење: Ако постоји најмањи елемент скупа B, онда је он и једини најмањи елемент и једини минимални елемент скупа B.

Доказ:

Нека је b најмањи елемент скупа B

Најмањи елемент је јединствен:

пос. нека је b' такође најмањи елемент скупа B и $b \neq b'$

$b \leq b'$, јер је b најмањи
$b' \leq b$, јер је b' најмањи $\Big\} \overset{(АНТИС)}{\Longrightarrow} b = b'$ ↯

b јесте минималан елемент у B:

нека $x \leq b$ за неко $x \in B$
како је $b \leq x$ јер је b најмањи $\overset{(АНТИС)}{\Longrightarrow} x = b$

$\Rightarrow b$ је минималан ел.

b је једини минималан елемент у B:

пос. нека је b' минималан у B и $b \neq b'$
важи $b \leq b'$, јер је b најмањи у B
b' је минималан $\Rightarrow b = b'$ ↯

Последице:

1° Ако немамо минималне елементе, немамо ни најмањи елемент

2° Ако имамо бар два минимална елемента, немамо најмањи елемент.

Приметимо следеће:

Ако B има један минималан елемент, он не мора бити најмањи елемент (тј. најмањи елемент не мора постојати)

Аналогно важи и за највећи елемент:

он је јединствен ако постоји и једини је максималан елемент

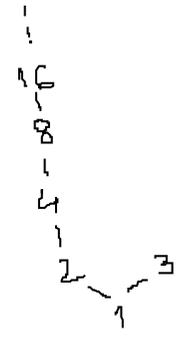
Ознаке:

$\max(B)$ – највећи елемент скупа B
$\min(B)$ – најмањи елемент скупа B

пример:

$B = \{2^n \mid n \geq 0\} \cup \{3\} = \{1, 2, 3, 4, 8, 16, 32, \dots\}$

1 на B



3 је максималан елемент (једини)
али 3 није највећи елемент, нпр. $4 \not\leq 3$

немамо највећи елемент

def: Нека је $\rho \subseteq A^2$ поредак, $B \subseteq A$ и $a \in A$.

- елемент a је доње ограничење скупа B ако:

  $a \rho x$ за све $x \in B$

- елемент a је горње ограничење скупа B ако:

  $x \rho a$ за све $x \in B$

- ако постоји највеће доње ограничење од B, зовемо га инфимум и означавамо га са $\inf(B)$.
- ако постоји најмање горње ограничење од B, зовемо га супремум од B и означавамо га са $\sup(B)$.

Тврђење:

1° Ако постоји минимум од B, онда је он $\inf(B)$.

2° Ако постоји максимум од B, онда је он $\sup(B)$

доказ:

1° Нека је $b = \min(B) \Rightarrow b$ јесте доње ограничење скупа B

(за све $x \in B$ важи $b \rho x$)

Потребно је доказати да је b највеће доње ограничење од B:

нека је b' неко доње ограничење, тада је b' ρ-мање од свих елемената из B, специјално $b' \rho b$

$\Rightarrow b$ јесте највеће доње ограничење

2° слично као под 1°

примери:

1° $\mathbb{R}, \leq$

$B = (0,1) \subset \mathbb{R}$

B нема минимум/максимум

скуп доњих ограничења од B: $(-\infty, 0]$

скуп горњих ограничења од B: $[1, +\infty)$

0 највећи у $[-\infty, 0] \Rightarrow \inf(B) = 0$

1 најмањи у $[1, +\infty) \Rightarrow \sup(B) = 1$

2° $A = \mathbb{R} \times \mathbb{R}$, $\leq$

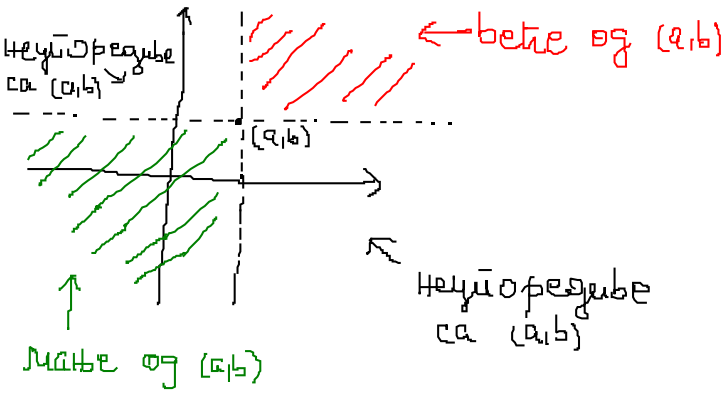
$(a,b) \leq (u,v)$ ако $a \leq u$, $b \leq v$

$\leq$ је уређење на $\mathbb{R} \times \mathbb{R}$ (показати за домаћи)

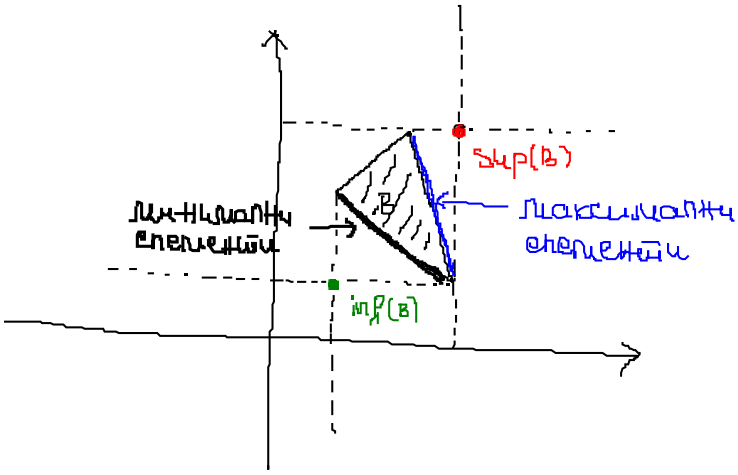
Није тотално (линеарно) уређење:

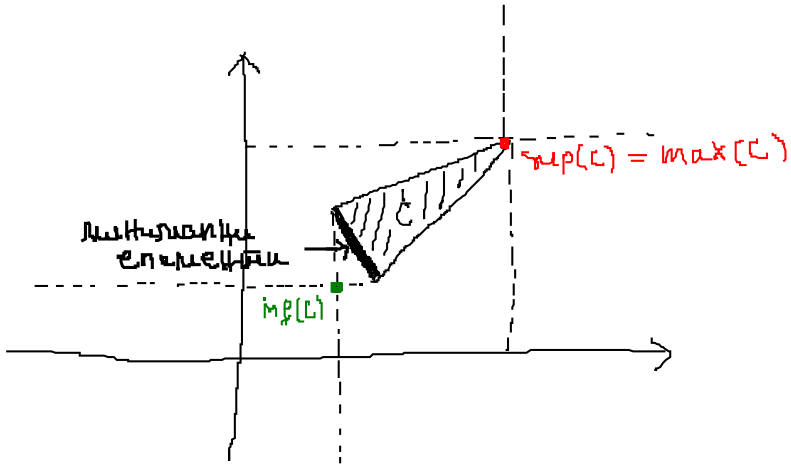
нпр. $(1,2) \not\leq (2,1)$ и $(2,1) \not\leq (1,2)$

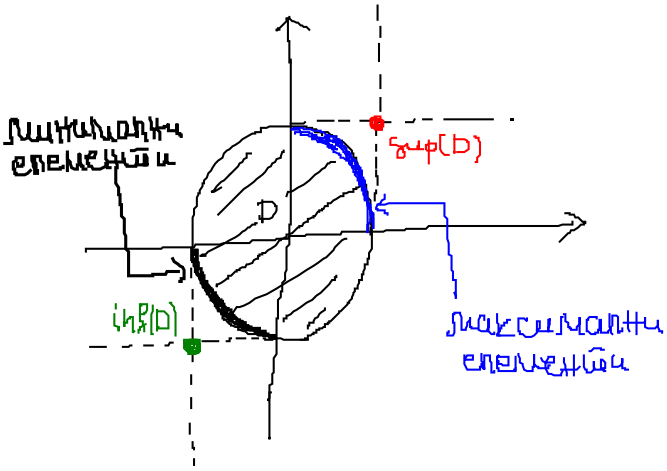
тј. $(1,2)$ и $(2,1)$ су неупоредиве



$B \subseteq \mathbb{R}^2$





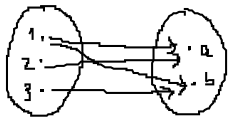


Функције

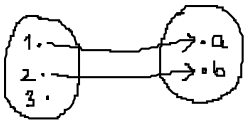
def: Релација $f \subseteq A \times B$ је функција ако:
за сваки елемент $a \in A$ постоји тачно један елемент $b \in B$ тако да је $a f b$ (тј. $(a,b) \in f$).

У том случају елемент b зовемо слика елемента a при пресликавању f и означавамо са $b = f(a)$

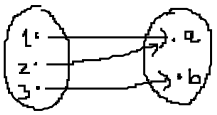
Пишемо $f: A \to B$ и читамо f је функција из A у B.



није функција
(1 у релацији
са два елемента)



није функција
(3 није у релацији
ни са једним
елементом)



јесте
функција

пример:

Релација $f \subseteq \mathbb{R} \times \mathbb{R}$ дефинисана са $f = \{(x, x^2) \mid x \in \mathbb{R}\}$ је функција.

$f(x) = x^2$

Релација $g \subseteq \mathbb{R} \times \mathbb{R}$ дефинисана са $g = \{(x^2, x) \mid x \in \mathbb{R}\}$ није функција.

$-1 \in \mathbb{R}$
за -1 не постоји b тд. $(-1, b) \in g$ јер $-1 \neq x^2$ за све $x \in \mathbb{R}$

$4 \in \mathbb{R}$
за 4 важе $(4, 2) \in g$ и $(4, -2) \in g$

Нека $f: A \to B$. Тада:

- A је домен функције f, ознака $A = Dom(f)$
- B је кодомен функције f
- слика функције f је скуп $Im(f) = \{f(a) \mid a \in A\} \subseteq B$

пример:

Ако $f: \mathbb{R} \to \mathbb{R}$ задата са $f(x) = x^2$, тада је

$Dom(f) = \mathbb{R}$

кодомен је $\mathbb{R}$

$Im(f) = \{f(x) \mid x \in \mathbb{R}\} = \{x^2 \mid x \in \mathbb{R}\} = [0, +\infty)$

Шта је f^{-1} ако је f функција?

f^{-1} јесте релација

f^{-1} не мора бити функција!

Релација $f^{-1} \subseteq B \times A$ је функција ако за свако $b \in Im(f)$ постоји тачно један $a \in A$ тј. $(b,a) \in f^{-1}$, односно ако за свако $b \in Im(f)$ постоји тачно један a такво да је $(a,b) \in f$.

деф: Нека је $f: A \to B$

- f је "1-1" или инјекција ако за све $a_1, a_2 \in A$ важи:
  ако је $f(a_1) = f(a_2)$ тада је $a_1 = a_2$
- f је "на" или сурјекција ако за све $b \in B$ постоји $a \in A$ тј. $b = f(a)$
  (односно, $Im(f) = B$)
- f је бијекција ако је "1-1" и "на".

примери:

$f: \mathbb{R} \to \mathbb{R}$ задата са $f(x) = x^2$

није "1-1": $f(2) = f(-2)$ а $2 \neq -2$

није "на": не постоји $x \in \mathbb{R}$ такво да је $f(x) = -2$

$g: \mathbb{N} \to \mathbb{N}$ задата са $g(n) = 2n$

јесте "1-1": $g(n_1) = g(n_2) \Rightarrow 2n_1 = 2n_2 \Rightarrow n_1 = n_2$

није "на": не постоји $n \in \mathbb{N}$ такво да је $g(n) = 3$

$h: \mathbb{R} \to \mathbb{R}$ задата са $h(x) = x+1$

јесте "1-1": $h(x_1) = h(x_2) \Rightarrow x_1 + 1 = x_2 + 1 \Rightarrow x_1 = x_2$

јесте "на": за све $x \in \mathbb{R}$ важи $h(x-1) = x$

h је бијекција

Тврђење: Релација f^{-1} је функција ако f је "1-1".

доказ:

$b \in Im(f) \iff$ постоји $a \in A$ тј. $f(a) = b$

и тачно једно a се слика у b ако је f "1-1"

па је $f^{-1}: Im(f) \to A$ функција

али $f^{-1}: B \to A$ не мора бити функција!

Тврђење: Нека је $f: A \to B$. Тада:

$f^{-1}: B \to A$ акко f је бијекција.

$\Rightarrow$ ✓

$\Leftarrow$ ✓

Доказ:

$\Rightarrow$: Нека $f^{-1}: B \to A$

f је "1-1":

$f(a_1) = f(a_2) \overset{?}{\Longrightarrow} a_1 = a_2$

$b = f(a_1) = f(a_2)$

$(a_1, b), (a_2, b) \in f \Rightarrow (b, a_1), (b, a_2) \in f^{-1}$

f^{-1} је функција па $a_1 = a_2$

f је "на":

Нека $b \in B$

f^{-1} је функција која B слика у A па постоји $a \in A$ тај.

$f^{-1}(b) = a$, тј. $(b, a) \in f^{-1}$

$\Rightarrow (a, b) \in f$, тј. $b = f(a)$

f је бијекција

$\Leftarrow$: Нека је $f: A \to B$ бијекција

$b \in B$

f је "на" $\Rightarrow$ постоји $a \in A$ тај. $f(a) = b$, односно $(a, b) \in f$

тј. $(b, a) \in f^{-1}$

да ли је a јединствено?

пос. $(b, a), (b, a') \in f^{-1}$ и $a \neq a'$

$\Rightarrow (a, b)$ и $(a', b) \in f$

$f(a) = b = f(a')$ и $a \neq a'$ ↯ јер је f "1-1"

$f \subseteq A \times B$, $g \subseteq B \times C$

$g \circ f \subseteq A \times C$

$(a, c) \in g \circ f$ акко постоји $b \in B$ тај. $(a, b) \in f$ и $(b, c) \in g$

Тврђење: Ако су $f \subseteq A \times B$ и $g \subseteq B \times C$ функције, онда је и $g \circ f \subseteq A \times C$ функција и важи $(g \circ f)(a) = g(f(a))$.

Доказ:

$g \circ f \subseteq A \times C$ је функција:

Нека $(a, c_1), (a, c_2) \in g \circ f$ тада постоје $b_1, b_2 \in B$ тај.

$(a, b_1) \in f$ и $(b_1, c_1) \in g$

$(a, b_2) \in f$ и $(b_2, c_2) \in g$

Како $(a, b_1), (a, b_2) \in f$, а f је функција $\Rightarrow b_1 = b_2$

Означимо $b = b_1 = b_2$

g је функција и $(b, c_1), (b, c_2) \in g \Rightarrow c_1 = c_2$

Дакле, $g \circ f$ јесте функција.

$(g \circ f)(a) = ?$

$a \in Dom(g \circ f)$ тада $(a, c) \in g \circ f$ тј. постоји $b \in B$ тај. $(a, b) \in f$ и $(b, c) \in g$

$(a, b) \in f \Rightarrow b = f(a)$

$(b, c) \in g \Rightarrow c = g(b)$

$c = g(b) = g(f(a)) = (g \circ f)(a)$

Тврђење: Ако је $f: A \to B$ и $g: B \to C$, тада $g \circ f: A \to C$ и важи $(g \circ f)(a) = g(f(a))$, за све $a \in A$.

Доказ:

$Dom(g \circ f) = A$?

Увек важи $Dom(g \circ f) \subseteq A$

$\supseteq$: за свако $a \in A$ постоји $f(a) \in B$ (јер $f: A \to B$)

даље, постоји $\underbrace{g(\underbrace{f(a)}_{B})}_{(g \circ f)(a)} \in C$ (јер $g: B \to C$)

дакле, $a \in Dom(g \circ f)$

$id_A: A \to A$ дефинисана са $id_A(a) = a$ за све $a \in A$

$\downarrow$

идентитет на скупу A

Тврђење: Нека $f: A \to B$. Тада важи:

f је бијекција акко постоји функција $g: B \to A$ тј.

$$g \circ f = id_A \quad \text{и} \quad f \circ g = id_B$$

(у том случају је $f^{-1} = g$)

доказ:

$\Rightarrow$: ако је f бијекција, онда је $f^{-1}: B \to A$ функција па је $g = f^{-1}$

Нека је $f(a) = b \Rightarrow f^{-1}(b) = a$

$$(f^{-1} \circ f)(a) = f^{-1}(\underbrace{f(a)}_{=b}) = f^{-1}(b) = a \quad \Rightarrow \quad f^{-1} \circ f = id_A$$

$$(f \circ f^{-1})(b) = f(\underbrace{f^{-1}(b)}_{a}) = f(a) = b \quad \Rightarrow \quad f \circ f^{-1} = id_B$$

$\Leftarrow$: f је "1-1":

$$f(a_1) = f(a_2) \overset{?}{\Rightarrow} a_1 = a_2$$

$$f(a_1) = f(a_2) \in B \quad / g$$

$$\underbrace{g(f(a_1))}_{\substack{id_A(a_1) \\ \| \\ a_1}} = \underbrace{g(f(a_2))}_{\substack{id_A(a_2) \\ \| \\ a_2}} \quad \Rightarrow \quad a_1 = a_2$$

f је "на":

$b \in B$

Нека је $a = g(b)$

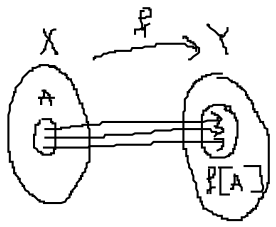
$$\Rightarrow f(a) = f(g(b)) = (f \circ g)(b) = id_B(b) = b$$

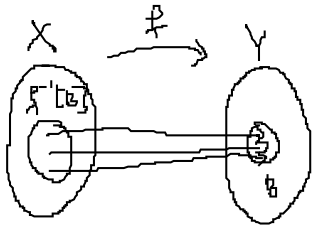
дакле, $b = f(a)$

Директна и инверзна слика скупа

деф: Нека $f: X \to Y$, $A \subseteq X$, $B \subseteq Y$.

- директна слика скупа A при пресликавању f је скуп
$$f[A] = \{ f(x) \mid x \in A \} \subseteq Y$$
- инверзна слика скупа B при пресликавању f је скуп
$$f^{-1}[B] = \{ x \in X \mid f(x) \in B \} \subseteq X.$$





$y \in f[A]$ акко $y = f(x)$ за неко $x \in A$
$\cap$
Y

$x \in f^{-1}[B]$ акко $f(x) \in B$
$\cap$
X

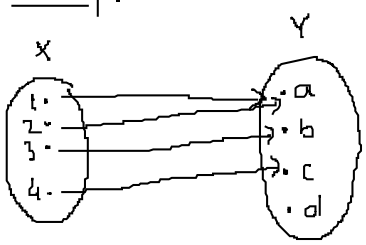
Инверзна слика увек постоји и нема веze са инверзном функцијом!

Суштински важни:

$f[X] = Im(f)$

$f^{-1}[Y] = X$

<u>Пример</u>:



$f[\{1\}] = \{f(1)\} = \{a\}$

$f[\{1,2\}] = \{f(1), f(2)\} = \{a,a\} = \{a\}$

$f[\{1,3\}] = \{f(1), f(3)\} = \{a,b\}$

$f^{-1}[\{a\}] = \{1,2\}$

$f^{-1}[\{a,b\}] = \{1,2,3\}$

$f^{-1}[\{a,b,d\}] = \{1,2,3\}$

$f^{-1}[\{d\}] = \emptyset$

Основне особине директне и инверзне слике:

1° Ако је $A_1 \subseteq A_2$, онда је $f[A_1] \subseteq f[A_2]$.

2° Ако је $B_1 \subseteq B_2$, онда је $f^{-1}[B_1] \subseteq f^{-1}[B_2]$.

3° Важи $f^{-1}[f[A]] \supseteq A$.

ако је f "1-1", онда је $f^{-1}[f[A]] = A$

4° Важи $f[f^{-1}[B]] \subseteq B$.

ако је f "на", онда је $f[f^{-1}[B]] = B$.

<u>доказ</u>:

1° нека је $A_1 \subseteq A_2$

нека $y \in f[A_1] \Rightarrow y = f(x)$ за неко $x \in A_1$

Како $x \in A_1$ и $A_1 \subseteq A_2 \Rightarrow x \in A_2$

$y = f(x)$ и $x \in A_2 \Rightarrow f(x) \in f[A_2]$

тј. $y \in f[A_2]$

2° Нека $B_1 \subseteq B_2$

$$\left.\begin{array}{l} x \in f^{-1}[B_1] \Rightarrow f(x) \in B_1 \\ B_1 \subseteq B_2 \end{array}\right\} \Rightarrow f(x) \in B_2$$

тј. $x \in f^{-1}[B_2]$

3° Нека $x \in A$

тада $f(x) \in f[A]$ па $x \in f^{-1}[f[A]]$

претпостављамо да је f "1-1"

Нека $x \in f^{-1}[f[A]] \Rightarrow f(x) \in f[A]$

Како је f "1-1" $\Rightarrow x \in A$

(у супротности, да f није "1-1", могао би да постоји $x' \notin A$ тај.

$f(x') = f(x) \in f[A]$

у нашем примеру:

$x = 2$

$A = \{1\}$

$f(x) = f(2) = a \in f[A] = f[\{1\}] = \{a\}$

али $2 \notin \{1\}$

тј. $x \notin A$)

4° Нека $y \in f[f^{-1}[B]]$

$\Rightarrow y = f(x)$ за неко $\underbrace{x \in f^{-1}[B]}_{f(x) \in B} \Rightarrow y = f(x) \in B$

претпостављамо да је f "на":

Нека $y \in B$

$$\left.\begin{array}{l} y \in B \subseteq Y \\ f \text{ је "на"} \end{array}\right\} \Rightarrow \text{постоји } x \in X \text{ тај. } f(x) = y$$

$f(x) = y \in B \Rightarrow x \in f^{-1}[B]$

$$\left.\begin{array}{l} x \in f^{-1}[B] \\ y = f(x) \end{array}\right\} \Rightarrow y \in f[f^{-1}[B]]$$

Карактеристичне функције

$\mathbf{2} = \{0,1\}$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$a,b,c \in \mathbf{2}$

$a+b=b+a$

$a+(b+c)=(a+b)+c$

$a+0=a$

$a+a=0$

$a\cdot b=b\cdot a$

$a\cdot(b\cdot c)=(a\cdot b)\cdot c$

$a\cdot 1=a$

$a\cdot a=a$

$a\cdot 0=0$

Нека је U скуп (универзум)

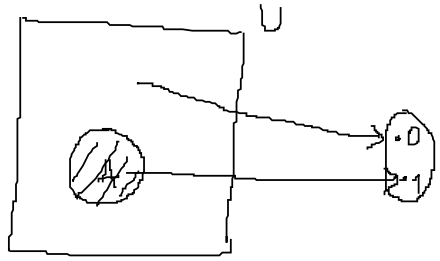
за $A\subseteq U$ дефинишемо функцију:

$$\chi_A : U \to \mathbf{2}$$

на следећи начин:

$$\chi_A(x) = \begin{cases} 0, & x\notin A \\ 1, & x\in A \end{cases}$$

Функцију χ_A називамо карактеристична функција скупа A.



$\chi_A(x)=1$ акко $x\in A$

$\chi_A(x)=0$ акко $x\notin A$

Тврђење: Нека $A,B\in U$. Тада важи:

$$A=B \text{ акко } \chi_A=\chi_B.$$

$\Rightarrow$: очигледна

$\Leftarrow$: $x\in A$ акко $\chi_A(x)=1$

акко $\chi_B(x)=1$

акко $x\in B$

дакле, $A=B$. $\boxtimes$

$2^U = \{ f \mid f : U \to 2 \}$

$f, g \in 2^U$

$f+g,\ f \cdot g : U \to 2$

$(f+g)(x) := f(x) + g(x)$

$(f \cdot g)(x) := f(x) \cdot g(x)$

$0, 1 : U \to 2$

$0(x) = 0$

$1(x) = 1$

$f+g = g+f$

$(f+g)+h = f+(g+h)$

$f+0 = f$

$f+f = 0$

$f \cdot g = g \cdot f$

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

$f \cdot 1 = f$

$f \cdot f = f$

$f \cdot 0 = 0$

$f \cdot (g+h) = f \cdot g + f \cdot h$

за $A \in U \Rightarrow \chi_A \in 2^U$

<u>Тврдење</u>: Важи следеће:

1° $\chi_\emptyset = 0$, $\chi_U = 1$

2° $\chi_{A \cap B} = \chi_A \cdot \chi_B$

3° $\chi_{A \cup B} = \chi_A + \chi_B + \chi_A \cdot \chi_B$

4° $\chi_{A \setminus B} = \chi_A + \chi_A \chi_B$

5° $\chi_{A \triangle B} = \chi_A + \chi_B$

6° $\chi_{A^c} = 1 + \chi_A$

<u>Доказ</u>:

2° $\chi_{A \cap B}(x) = 1$ акко $x \in A \cap B$

акко $x \in A$ и $x \in B$

акко $\chi_A(x) = 1$ и $\chi_B(x) = 1$

акко $\chi_A(x) \cdot \chi_B(x) = 1$

акко $(\chi_A \cdot \chi_B)(x) = 1$

$\Rightarrow \chi_{A \cap B} = \chi_A \cdot \chi_B$

6° $\chi_{A^c}(x) = 1$ акко $x \in A^c$

акко $x \notin A$

акко $\chi_A(x) = 0$

акко $\underset{\underset{1(x)}{\parallel}}{1} + \chi_A(x) = 1$

акко $(1 + \chi_A)(x) = 1$

$\boxtimes$

примјетимо да важи:

$\chi_A + \chi_A = 0$

$\chi_A \cdot \chi_A = \chi_A$

$A^B = \{ f \mid f : B \to A \}$

Тврђење: Постоји бијекција између $\mathcal{P}(X)$ и 2^X, за сваки скуп X.

доказ:

$2^X = \{ f \mid f : X \to \underbrace{\{0,1\}}_{=2} \}$

$F : \mathcal{P}(X) \to 2^X$

$A \in \mathcal{P}(X)$ тј. $A \subseteq X$

$F(A) := \chi_A$

да ли је F бијекција?

F је "1-1":

$F(A) = F(B) \overset{?}{\Rightarrow} A = B$

$F(A) = F(B) \Rightarrow \chi_A = \chi_B \Rightarrow A = B$

F је "на":

нека $f \in 2^X$ тј. $f : X \to 2$

$A = f^{-1}[\{1\}] \Rightarrow f = \chi_A = F(A)$

дакле, $f = F(f^{-1}[\{1\}])$

Кардиналност

деф: Нека су A и B скупови:

1° Кажемо да је скуп A кардиналности мање или једнаке од B, ознака $|A| \leq |B|$, ако постоји $A \xrightarrow{1-1} B$

2° Кажемо да је A једнаке кардиналности са B, $|A| = |B|$, ако постоји $A \xrightarrow[\text{на}]{1-1} B$

3° Кажемо да је кардиналност од A строго мања од B, $|A| < |B|$, ако $|A| \leq |B|$ и $|A| \neq |B|$.

Особине:

1° $|A| = |A|$

$id_A : A \xrightarrow[\text{на}]{1-1} A$

2° Ako je $|A|=|B|$, onda je $|B|=|A|$.

$$f: A \xrightarrow[\text{na}]{1-1} B \quad \Rightarrow \quad f^{-1}: B \xrightarrow[\text{na}]{1-1} A$$

3° Ako je $|A|=|B|$ i $|B|=|C|$, onda je $|A|=|C|$.

$$\left.\begin{array}{l} f: A \xrightarrow[\text{na}]{1-1} B \\ g: B \xrightarrow[\text{na}]{1-1} C \end{array}\right\} \Rightarrow g\circ f: A \xrightarrow[\text{na}]{1-1} C$$

$g\circ f$ je "1-1":

$$g\circ f(x_1) = g\circ f(x_2) \overset{?}{\Rightarrow} x_1 = x_2$$

$$\left.\begin{array}{l} g\circ f(x_1) = g\circ f(x_2) \Rightarrow g(f(x_1)) = g(f(x_2)) \\ \qquad\qquad\qquad\qquad g \text{ je "1-1"} \end{array}\right\} \Rightarrow \left.\begin{array}{l} f(x_1) = f(x_2) \\ f \text{ je "1-1"} \end{array}\right\} \Rightarrow x_1 = x_2$$

$g\circ f$ je "na"

$z \in C$

g je "na" $\Rightarrow$ postoji $y \in B$ tj. $g(y) = z$

f je "na" i $y \in B \Rightarrow$ postoji $x \in A$ tj. $f(x) = y$

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

$$\begin{array}{ccc} x & \xmapsto{g\circ f} & z \\ \cap & & \cap \\ A & & C \end{array}$$

4° Ako je $|A|=|B|$, onda $|A|\le|B|$ i $|B|\le|A|$

$$f: A \xrightarrow[\text{na}]{1-1} B$$

$$f: A \xrightarrow{1-1} B \Rightarrow |A|\le|B|$$

$$f^{-1}: B \xrightarrow{1-1} A \Rightarrow |B|\le|A|$$

f^{-1} je "1-1":

$$f \Big/ \; f^{-1}(y_1) = f^{-1}(y_2) \overset{?}{\Rightarrow} y_1 = y$$

$$f(f^{-1}(y_1)) = f(f^{-1}(y_2))$$

$$\underbrace{f\circ f^{-1}}_{id_B}(y_1) = \underbrace{f\circ f^{-1}}_{id_B}(y_2) \Rightarrow \underbrace{id_B(y_1)}_{=y_1} = \underbrace{id_B(y_2)}_{=y_2} \Rightarrow y_1 = y_2$$

5° Ako je $|A|\le|B|$ i $|B|\le|C|$ onda $|A|\le|C|$

$$\left.\begin{array}{l} f: A \xrightarrow{1-1} B \\ g: B \xrightarrow{1-1} C \end{array}\right\} \Rightarrow g\circ f: A \xrightarrow{1-1} C$$

6° Ако је $|A| \leq |B|$ и $|B| \leq |A|$, онда $|A| = |B|$.

(Кантор – Бернштајнова теорема) доказ касније

7° За свака два скупа A и B важи: $|A| \leq |B|$ или $|B| \leq |A|$

(Бернштајнова теорема) доказ касније

<u>Канторова теорема</u>: За сваки скуп X важи $|X| < |\mathcal{P}(X)|$.

<u>доказ</u>:

Доказујемо $|X| \leq |\mathcal{P}(X)|$ (нађемо инјекцију $X \to \mathcal{P}(X)$)

и $|X| \neq |\mathcal{P}(X)|$ (показаћемо да не постоји сурјекција $X \to \mathcal{P}(X)$, а

пише не бијекција $X \to \mathcal{P}(X)$)

$f: X \to \mathcal{P}(X)$

$a \in X$

$f(a) := \{a\}$

f јесте "1-1": $f(a_1) = f(a_2) \Rightarrow \{a_1\} = \{a_2\} \Rightarrow a_1 = a_2$

доказујемо да не постоји $g: X \xrightarrow{\text{на}} \mathcal{P}(X)$.

пос. постоји $g: X \xrightarrow{\text{на}} \mathcal{P}(X)$

нека је $A = \{x \in X \mid x \notin g(x)\}$

$A \subseteq X$, тј. $A \in \mathcal{P}(X)$

$A \in \mathcal{P}(X)$ и g је "на" $\Rightarrow A = g(a)$, за неко $a \in X$

ако $a \in A \Rightarrow a \notin g(a) = A$ ↯

ако $a \notin A \Rightarrow a \in g(a) = A$ ↯

Дакле, $|X| < |\mathcal{P}(X)|$.

$\boxtimes$

$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$

<u>Пребројиви скупови</u>

<u>деф</u>: Скуп A је пребројив ако је исте кардиналности као скуп природних бројева (тј. $|A| = |\mathbb{N}|$)

def: Скуп A је коначан ако има n елемената, где је n природан број. Ако A није коначан, кажемо да је бесконачан.

A је бесконачан ако постоји прави подскуп $A' \subset A$ такав да су A и A' у бијекцији.

Тврђење: Скуп природних бројева је бесконачан.

доказ:

$\mathbb{N} \setminus \{0\}$ је прави подскуп скупа $\mathbb{N}$

Посматрајмо пресликавање: $f: \mathbb{N} \to \mathbb{N} \setminus \{0\}$

$$f(n) = n+1$$

f је "1-1":

$f(n_1) = f(n_2) \Rightarrow n_1 + 1 = n_2 + 1 \Rightarrow n_1 = n_2$

f је "на":

$n \in \mathbb{N} \setminus \{0\} \Rightarrow f(n-1) = (n-1)+1 = n$

$\Rightarrow \mathbb{N}$ је бесконачан $\boxtimes$

def: Ако је скуп коначан или пребројив, кажемо да је најмање пребројив. Ако скуп није најмање пребројив, онда је непребројив.

X - пребројив

$f: \mathbb{N} \xrightarrow[\text{на}]{1-1} X$

$f(0) = f_0$

$f(1) = f_1$

$\vdots$

$f(n) = f_n$

$\vdots$

$X = \{f_0, f_1, \dots, f_n, \dots\}$ ← елементе скупа X можемо да индексирамо

Примери пребројивих скупова:

1° $\mathbb{Z}$ је пребројив

$f: \mathbb{N} \xrightarrow[\text{на}]{1-1} \mathbb{Z}$

$$\begin{array}{ccccccccc} 0, & 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, \ldots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & -1 & 1 & -2 & 2 & -3 & 3 & -4 & 4 \end{array}$$

$$f(n) = \begin{cases} \frac{n}{2} & , n \text{ je parno} \\ -\frac{n+1}{2} & , n \text{ je neparno} \end{cases}$$

$1 = 2\cdot 1 - 1 \to -1$
$3 = 2\cdot 2 - 1 \to -2$
$5 = 2\cdot 3 - 1 \to -3$
$7 = 2\cdot 4 - 1 \to -4$

2° Ako je $A \subseteq \mathbb{N}$ beskonačan, onda je A prebrojiv.

definišemo niz $(A_n, a_n)_{n\in\mathbb{N}}$:

$A_0 = A$, $a_0 = \min(A_0)$

$A_1 = A_0 \setminus \{a_0\}$, $a_1 = \min(A_1)$

$\vdots$

$A_{n+1} = A_n \setminus \{a_n\}$, $a_{n+1} = \min(A_{n+1})$

Tada je $A = \{a_0, a_1, \ldots, a_n, \ldots\}$

$f : \mathbb{N} \xrightarrow[\text{na}]{1-1} A$

$f(n) = a_n$

$A = 2\mathbb{N} = \{0, 2, 4, 6, 8, \ldots\}$

$A_0 = \{0, 2, 4, 6, 8, \ldots\}$ $\quad a_0 = 0$

$A_1 = \{2, 4, 6, 8, \ldots\}$ $\quad a_1 = 2$

$A_2 = \{4, 6, 8, \ldots\}$ $\quad a_2 = 4$

$A_3 = \{6, 8, \ldots\}$ $\quad a_3 = 6$

$\vdots$

$0 \mapsto 0$
$1 \mapsto 2$
$2 \mapsto 4$
$3 \mapsto 6$
$\vdots$

$f : \mathbb{N} \xrightarrow[\text{na}]{1-1} 2\mathbb{N}$

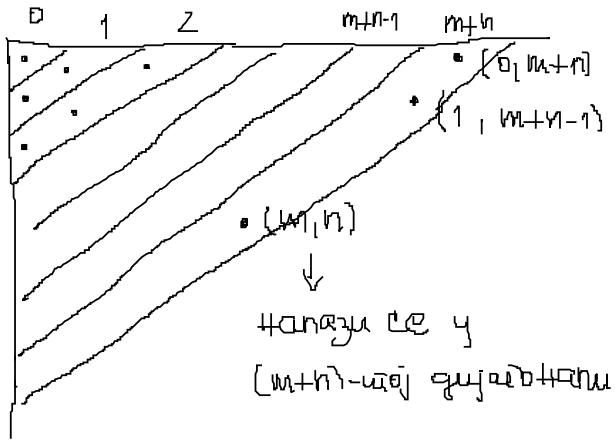
$f(n) = 2n$

3° $\mathbb{N} \times \mathbb{N}_0$ je prebrojiv

$$\begin{array}{cccccc} & 0 & 1 & 2 & 3 & \\ & (0,0)^{0} & (0,1)^{1} & (0,2)^{3} & (0,3)^{6} & \ldots \\ & (1,0)^{2} & (1,1)^{4} & (1,2)^{7} & (1,3) & \ldots \\ & (2,0)^{5} & (2,1)^{8} & (2,2) & (2,3) & \ldots \\ & (3,0)^{9} & (3,1) & (3,2) & (3,3) & \ldots \\ & \vdots & \vdots & \vdots & \vdots & \end{array}$$

$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$f(m, n) = ?$



↓

налази се у (m+n)-ој дијагонали

Број чворова испод (m,n):

$$\underbrace{1}_{\text{бр. el. на 0. дијагонали}} + \underbrace{2}_{\text{бр. el. на 1. дијагонали}} + \dots + \underbrace{(m+n)}_{\text{бр. el. на (m+n-1) дијагонали}} + \underbrace{m}_{\text{у (m+n)-ој дијагонали има m елемената испод (m,n)}}$$

$\Rightarrow$ (m,n) је $1+2+\dots+(m+n)+m+1$ по реду

Ако је неки чвор k-ти по реду, слика се у k-1

(нпр. (1,1) је 5. по реду, а слика су у 4)

Дакле,

$$f(m,n) = 1+2+\dots+(m+n)+m+1-1$$
$$= \frac{1}{2}(m+n)(m+n)+m$$

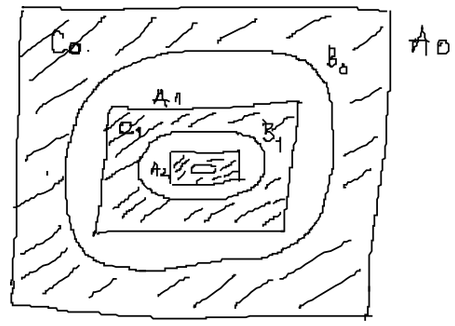
Кантор-Бернштајнова теорема:

Ако постоји $A \xrightarrow{1-1} B$ и $B \xrightarrow{1-1} A$, онда постоји $A \xrightarrow[\text{на}]{1-1} B$.

Најпре доказујемо следећу лему:

<u>лема</u>: Ако је $A_0 \supseteq B_0 \supseteq A_1$ и $|A_0| = |A_1|$, онда је $|A_0| = |B_0|$.

<u>доказ леме</u>:



Нека је $f: A_0 \xrightarrow[\text{на}]{1-1} A_1$

$A_{n+1} := f[A_n]$

$B_{n+1} := f[B_n]$

$A_0 \supseteq B_0 \supseteq A_1 \quad / f[\,]$

$$\underbrace{f[A_0]}_{= A_1} \supseteq \underbrace{f[B_0]}_{= B_1} \supseteq \underbrace{f[A_1]}_{= A_2} \quad \Rightarrow \quad A_1 \supseteq B_1 \supseteq A_2$$

истеранто, $A_n \supseteq B_n \supseteq A_{n+1}$

$C_n := A_n \setminus B_n$

$$f[C_n] = f[A_n \setminus B_n] \overset{(*)}{=} f[A_n] \setminus f[B_n]$$
$$= A_{n+1} \setminus B_{n+1} = C_{n+1}$$

(*): $f: X \to Y$

$A, B \subseteq X$

$f[A] \setminus f[B] \subseteq f[A \setminus B]$ увек важи

$f[A] \setminus f[B] = f[A \setminus B]$ када је f "1-1"

$f[A \cup B] = f[A] \cup f[B]$

$C = \bigcup_{n \geq 0} C_n$ ← све пратирано на слици

$D = A_0 \setminus C$ ← све непратирано

$C' = \bigcup_{n \geq 1} C_n$ ← све пратирано сем C_0

$$f[C] = f\Big[\bigcup_{n \geq 0} C_n\Big] = \bigcup_{n \geq 0} f[C_n] = \bigcup_{n \geq 0} C_{n+1} = \bigcup_{n \geq 1} C_n = C'$$

$A_0 = C \cup D \quad , \quad C \cap D = \emptyset$

$B_0 = C' \cup D \quad , \quad C' \cap D = \emptyset$

$g: A_0 \xrightarrow[\text{на}]{1-1} B_0$

$$g(x) = \begin{cases} f(x), & x \in C \\ x, & x \in D \end{cases}$$

g је "на":

$y \in B_0 \Rightarrow y \in C'$ или $y \in D$

ако $y \in C' \Rightarrow y \in A_1$

f је "на"

$\Rightarrow$ постоји $x \in A_0$ тај. $f(x) = y$

$\Rightarrow g(\underline{x}) = y$

ако $y \in D \Rightarrow g(\underline{y}) = y$

g je "1-1":

$g(x_1) = g(x_2) \in B_0 \Rightarrow g(x_1), g(x_2) \in C'$ $\quad (g(x_1) = f(x_1),\ g(x_2) = f(x_2))$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad f$ je 1-1 $\Rightarrow x_1 = x_2$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \cup\!\cap\!\cup$

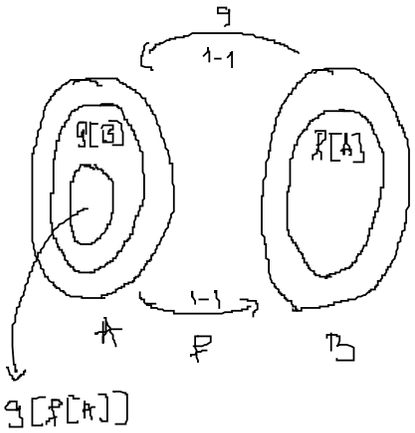
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad g(x_1), g(x_2) \in D$ $\quad (g(x_1) = x_1,\ g(x_2) = x_2 \Rightarrow x_1 = x_2)$

$\boxtimes$

<u>dokaz K.Š.B:</u>

$f: A \xrightarrow{1-1} B$

$g: B \xrightarrow{1-1} A$



$f[A] \subseteq B \quad / g[\ ]$

$g[B] \subseteq A$

$\underbrace{g[f[A]]}_{A_1} \subseteq \underbrace{g[B]}_{B_0} \subseteq \underset{A_0}{\underset{\parallel}{A}}$

$$\begin{tikzcd} A_0 \arrow[r, "1-1", "\text{na}"'] \arrow[rr, bend right, "1-1", "\text{na}"'] & f[A_0] \arrow[r, "1-1", "\text{na}"'] & g[f[A_0]] = A_1 \end{tikzcd}$$

$\Rightarrow |A_0| = |A_1|$

Kako je $A_0 \supseteq B_0 \supseteq A_1$ i $|A_0| = |A_1|$ primenom leme dobijamo:

$|A_0| = |B_0| = |g[B]|$

$B \xrightarrow[\text{na}]{1-1} g[B] \Rightarrow |g[B]| = |B|$

Zaista, $|A| = |g[B]| = |B|$.

$\boxtimes$

Primeri:

1° $\mathcal{P}_{fin}(X) = \{A \subseteq X \mid A$ je konačan$\}$

bazni $|\mathcal{P}_{fin}(\mathbb{N})| = |\mathbb{N}|$

dokazujemo primenom K.Š.B.

$f: \mathbb{N} \xrightarrow{1-1} \mathcal{P}_{fin}(\mathbb{N})$

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

$g: \mathcal{P}_{fin}(\mathbb{N}) \to \mathbb{N}$

$g(\{a_1, a_2, \dots, a_n\}) = 2^{a_1} + 2^{a_2} + \dots + 2^{a_n}$

g je "1-1"

$g(\{a_1, a_2, \dots, a_n\}) = g(\{b_1, b_2, \dots, b_\ell\}) \overset{?}{\Longrightarrow} \{a_1, \dots, a_n\} = \{b_1, \dots, b_\ell\}$

Можемо претпоставити:

$a_1 < a_2 < \dots < a_n$ и $b_1 < b_2 < \dots < b_\ell$

$2^{a_1} + 2^{a_2} + \dots + 2^{a_n} = 2^{b_1} + 2^{b_2} + \dots + 2^{b_\ell}$

Тврдимо $a_n = b_\ell$:

ако $a_n \neq b_\ell$

нпр. $a_n < b_\ell$

$a_n + 1 \leq b_\ell$

$2^{a_n+1} \leq 2^{b_\ell}$ (*)

$$2^{a_1} + 2^{a_2} + \dots + 2^{a_n} \leq 1 + 2 + 2^2 + \dots + 2^{a_{n-1}} + 2^{a_n}$$

$$= \frac{1 \cdot (1 - 2^{a_n+1})}{1-2} = 2^{a_n+1} - 1$$

$$\overset{(*)}{\leq} 2^{b_\ell} - 1$$

$$< 2^{b_\ell}$$

$$\leq 2^{b_1} + 2^{b_2} + \dots + 2^{b_\ell}$$

$$\Rightarrow 2^{a_1} + 2^{a_2} + \dots + 2^{a_n} < 2^{b_1} + 2^{b_2} + \dots + 2^{b_\ell} \quad ↯$$

Дакле, $a_n = b_\ell$

$$2^{a_1} + \dots + 2^{a_{n-1}} + \cancel{2^{a_n}} = 2^{b_1} + \dots + 2^{b_{\ell-1}} + \cancel{2^{b_\ell}}$$

слично закључујемо: $a_{n-1} = b_{\ell-1}$

$\vdots$

$\{a_1, \dots, a_n\} = \{b_1, \dots, b_\ell\}$

$\mathbb{N} \xrightarrow{1-1} \mathcal{P}_{fin}(\mathbb{N})$ и $\mathcal{P}_{fin}(\mathbb{N}) \xrightarrow{1-1} \mathbb{N} \overset{\text{К.Б.Ш}}{\Longrightarrow} \mathbb{N} \underset{\text{на}}{\xrightarrow{1-1}} \mathcal{P}_{fin}(\mathbb{N})$

$\Rightarrow |\mathbb{N}| = |\mathcal{P}_{fin}(\mathbb{N})|$

1° $\mathbb{Q}$ je пребројив

$\mathbb{N} \xrightarrow{1-1} \mathbb{Q}$

$n \longmapsto n$

$|\mathbb{N}| \leq |\mathbb{Q}|$

$\mathbb{Q} \xrightarrow{1-1} \mathbb{Z} \times \mathbb{N}$

$\frac{m}{n} \longmapsto (m, n)$

$m \in \mathbb{Z}$

$n \in \mathbb{N}$

m и n узајамно прости

$|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{N}|$

$\mathbb{Z} \times \mathbb{N} \xrightarrow{1-1} \mathbb{N} \times \mathbb{N}$

$f : \mathbb{Z} \xrightarrow[\text{на}]{1-1} \mathbb{N}$

$$\underset{\mathbb{Z}}{\underset{\cap}{(m}}, \underset{\mathbb{N}}{\underset{\cap}{n)}} \longmapsto (\underset{\mathbb{N}}{\underset{\cap}{f(m)}}, \underset{\mathbb{N}}{\underset{\cap}{\overset{id_{\mathbb{N}}(n)}{\overset{\shortparallel}{n}}}}).$$

$|\mathbb{Z} \times \mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}|$

$$|\mathbb{N}| \leq |\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$$

$$\left.\begin{array}{l} |\mathbb{N}| \leq |\mathbb{Q}| \\ |\mathbb{Q}| \leq |\mathbb{N}| \end{array}\right\} \overset{\text{К.Б.Ш}}{\Longrightarrow} |\mathbb{N}| = |\mathbb{Q}|$$

3° $\mathbb{R}$ није пребројив

довољно је показати да скуп $(0,1)$ није пребројив

пос. $(0,1)$ је пребројив

$(0,1) = \{a_0, a_1, a_2, \dots\}$

$a_n \in (0,1)$

$a_0 = 0,\boxed{a_{00}}a_{01}a_{02}\dots$

$a_1 = 0,a_{10}\boxed{a_{11}}a_{12}\dots$

$a_2 = 0,a_{20}a_{21}\boxed{a_{22}}\dots$

$\vdots$

$a_n = 0,a_{n0}a_{n1}a_{n2}\dots\boxed{a_{nn}}\dots$

$\vdots$

$a = 0,\overline{a_{00}}\,\overline{a_{11}}\,\overline{a_{22}}\dots\overline{a_{nn}}\dots$

$$\overline{a_{ii}} = \begin{cases} 0, & \text{ако је } a_{ii} \neq 0 \\ 1, & \text{ако је } a_{ii} = 0 \end{cases} \quad \text{за све } i \in \mathbb{N}$$

$a \in (0,1) = \{a_0, a_1, \dots\} \Rightarrow$ постоји $k \in \mathbb{N}$ тај. $a = a_k$

$a_k = 0,a_{k0}a_{k1}\dots a_{kk}\dots$

$a = 0,\overline{a_{00}}\,\overline{a_{11}}\dots\overline{a_{kk}}\dots$

$$a_{kk} \neq \overline{a_{kk}} \Rightarrow a \neq a_k \;\lightning$$

Закључак, $(0,1)$ није пребројив па и $\mathbb{R}$ није пребројив.

$|\mathbb{N}| = \aleph_0$ - алеф-нула

$|\mathbb{R}| = \mathfrak{c}$ - континуум

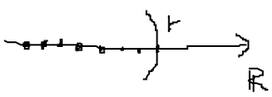
$\aleph_0 < \mathfrak{c}$

basta $|\mathbb{R}| \overset{(1)}{\leq} |\mathcal{P}(\mathbb{Q})| \overset{(2)}{=} |\mathcal{P}(\mathbb{N})| \overset{(3)}{=} |2^{\mathbb{N}}| \overset{(4)}{\leq} |\mathbb{R}|$

(1) $f: \mathbb{R} \xrightarrow{1-1} \mathcal{P}(\mathbb{Q})$

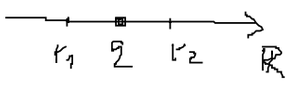
$r \in \mathbb{R}$

$f(r) = \{q \in \mathbb{Q} \mid q < r\} = (-\infty, r) \cap \mathbb{Q}$



f je "1-1":

neka je $r_1 \neq r_2$, $r_1, r_2 \in \mathbb{R}$ u nšp. $r_1 < r_2$



izaberemo $q \in \mathbb{Q}$ tdg. $r_1 < q < r_2$, tada $q \notin f(r_1)$

$q \in f(r_2)$

ta je $f(r_1) \neq f(r_2)$

Zašto postoji racionalan broj između svaka dva realna broja?

$\left.\begin{array}{l} a, b \in \mathbb{R} \\ a < b \end{array}\right\} \overset{?}{\Rightarrow}$ postoji $q \in \mathbb{Q}$ tdg. $a < q < b$

$a = a_0, a_1 a_2 \ldots$ $\quad a_0, b \in \mathbb{Z}_0$

$b = b_0, b_1 b_2 \ldots$

$\left.\begin{array}{l} a_1, a_2 \ldots \\ b_1, b_2 \ldots \end{array}\right\}$ cifre iza zareza

11,6

$a_0 \; a_1 a_2 a_3 a_4$

11, 5347 ...

$q = 11,6$

12, 45198 ...

$b_0 \; b_1 b_2 b_3 b_4 b_5$

ako je $a_0 < b_0$ trivijalno

ako je $a_0 = b_0$

izaberemo n takvo da je $a_i = b_i$ za $i < n$

$a = 11,534\boxed{7}8\ldots$

$b = \underbrace{11,534\boxed{8}}_{q}7\ldots$ $\quad n = 4$

$a = a_0, a_1 a_2 a_3 \ldots a_n$ + nula

$b = \underbrace{b_0, b_1 b_2 b_3 \ldots b_n}_{q}$ + nula

$b_n > a_n$ jer $b > a$

q ima konačno decimala $\Rightarrow q \in \mathbb{Q}$

u $a < q < b$

ako je $b_{n+1} = b_{n+2} = \ldots = 0$

tražimo najmanje $m > n$ tdg. $a_m \neq 9$ (ako su sve 9 iza $a_n \Rightarrow a = b$)

$\overline{a_m} := a_m + 1$

$a < q = a_0, a_1 a_2 \ldots a_n a_{n+1} \ldots a_{m-1} \overline{a_m} < b$ u $q \in \mathbb{Q}$

(2) Ако је $|A| = |B|$, онда $|\mathcal{P}(A)| = |\mathcal{P}(B)|$

$g: \mathcal{P}(A) \xrightarrow[\text{на}]{1-1} \mathcal{P}(B)$

$g(M) = f[M]$ где је $f: A \xrightarrow[\text{на}]{1-1} B$

$\left.\begin{array}{l} M \in \mathcal{P}(A) \\ M \subseteq A \end{array}\right\} \Rightarrow f[M] \subseteq B$

$\Rightarrow f[M] \in \mathcal{P}(B)$

g је "1-1":

$g(M_1) = g(M_2) \overset{?}{\Rightarrow} M_1 = M_2$

$f[M_1] = f[M_2]$

нек. $M_1 \neq M_2 \Rightarrow M_1 \setminus M_2 \neq \emptyset$ или $M_2 \setminus M_1 \neq \emptyset$

хип. $M_1 \setminus M_2 \neq \emptyset$

$a \in M_1$ и $a \notin M_2$

$a \in M_1 \Rightarrow f(a) \in f[M_1] = f[M_2]$

$f(a) \in f[M_2]$

$\Rightarrow$ постоји $b \in M_2$ тад. $f(b) = f(a)$

$\underset{f \text{ је } 1-1}{\Rightarrow} b = a \in M_2$ ↯

$\Rightarrow M_1 = M_2$

g је "на":

$N \in \mathcal{P}(B)$ да ли постоји $? \in \mathcal{P}(A)$ тад. $g(?) = N$

$\left.\begin{array}{l} N \subseteq B \\ f \text{ је "на"} \end{array}\right\} \Rightarrow$ постоји $M \subseteq A$ тд. $f[M] = N$

закључак: $|\mathbb{N}| = |\mathbb{Q}| \Rightarrow |\mathcal{P}(\mathbb{N})| = |\mathcal{P}(\mathbb{Q})|$

(3) Већ доказано на пропедеутици

(4) $F: 2^{\mathbb{N}} \xrightarrow{1-1} \mathbb{R}$

$2^{\mathbb{N}} = \{f \mid f: \mathbb{N} \to \{0,1\}\}$

$g \in 2^{\mathbb{N}} \Rightarrow g: \mathbb{N} \to \{0,1\}$

$F(g) = 0,a_0a_1 \ldots a_n \ldots$

где је $a_i = g(i) \in \{0,1\}$

F je "1-1":

ako je $\left.\begin{array}{l} g_1 \neq g_2 \\ g_1, g_2 \in 2^{\mathbb{N}} \end{array}\right\} \Rightarrow$ $F(g_1)$ и $F(g_2)$ имају различите децимале

$\Rightarrow F(g_1) \neq F(g_2)$

Аксиома избора

Теорема: Нека је A непразан скуп. Постоји $A \xrightarrow{1-1} B$ ако постоји $B \xrightarrow{на} A$.

доказ:

$\Rightarrow$ Нека је $f: A \xrightarrow{1-1} B$

изаберимо $a_0 \in A$ (A је непразан)

дефинишемо $g: B \xrightarrow{на} A$

$$g(y) = \begin{cases} a_0, & y \notin Im f = f[A] \\ x, & y \in f[A] \text{ и } f(x) = y \end{cases}$$

$\downarrow$

f је 1-1 па не могу два различита елемента да се сликају у y

$\Rightarrow$ g је функција

$\Leftarrow$: Нека је $f: B \xrightarrow{на} A$

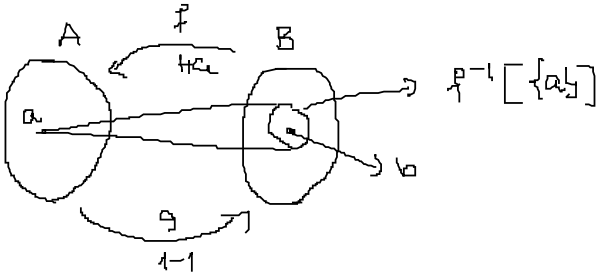
показујемо да постоји $g: A \to B$ такво да је $f \circ g = id_A$ (ако је $f \circ g$ 1-1, онда је g "1-1")

$a \in A$

f је "на" па скуп $f^{-1}[\{a\}]$ није празан

<u>изаберемо</u> $b \in f^{-1}[\{a\}]$ и $g(a) := b$

$f \circ g(a) = f(b) = a \Rightarrow f \circ g = id_A \Rightarrow g$ је "1-1"



$\boxtimes$

Користили смо избор по једном елементима из сваког од међусобно дисјунктних скупова $f^{-1}[\{a\}]$, $a \in A$

Чини се очигледно да то можемо да урадимо, али ниједна од досадашњих аксиома то не гарантује, за то нам је потребна аксиома избора:

Аксиома избора:

Нека је дат скуп F чији су сви елементи непразни скупови и међусобно дисјунктни. Тада постоји скуп C такав да је $C \cap X$ једночлан за све $X \in F$. Тај скуп се назива изборни скуп или трансверзала.

Природни бројеви

Аксиома доброг заснивања или регуларности:

Сваки непразан скуп A садржи елемент a такав да је $A \cap a = \emptyset$.

Последице аксиоме регуларности:

1° Не постоји скуп x такав да је $x \in x$.

2° Не постоје скупови x и y такви да $x \in y$ и $y \in x$.

3° Не постоји низ скупова $x_0, x_1, x_2, \dots$ таквих да $x_0 \ni x_1 \ni x_2 \ni \dots$

доказ:

1° пос. постоји x тд. $x \in x$

посматрајмо скуп $A = \{x\}$

$$\left.\begin{array}{l} x \in x \\ x \in A \end{array}\right\} \Rightarrow A \cap x \neq \emptyset$$

Према аксиоми доброг заснивања постоји $a \in A$ тд. $A \cap a = \emptyset$ ↯

једини елемент скупа A је x и $A \cap x \neq \emptyset$

2° пос. нека $x \in y$ и $y \in x$ за неке скупове x и y

посматрајмо скуп $A = \{x, y\}$

$$\left.\begin{array}{l} y \in x \\ y \in A \end{array}\right\} \Rightarrow A \cap x \neq \emptyset$$

$$\left.\begin{array}{l} x \in y \\ x \in A \end{array}\right\} \Rightarrow A \cap y \neq \emptyset$$

контрадикција са аксиомом доброг заснивања јер су x и y једини елементи у A и њихов пресек са A је непразан

3° Шис. постоји низ $x_0 \ni x_1 \ni x_2 \ni \dots$

Нека је $A = \{x_0, x_1, x_2, \dots\}$

за свако $i \in \{0, 1, 2, \dots\}$

$$\left.\begin{array}{l} x_{i+1} \in x_i \\ x_{i+1} \in A \end{array}\right\} \Rightarrow A \cap x_i \neq \emptyset$$

аксиома доброг заснивања

$\boxtimes$

<u>Тврђење</u>: Ако је $x \cup \{x\} = y \cup \{y\}$, онда је $x = y$. $(*)$

<u>доказ</u>:

шис. $x \neq y$

$x \in x \cup \{x\} = y \cup \{y\} \Rightarrow x \in y$ или $x \in \{y\}$
шј. $x = y$

Како је претпоставка $x \neq y \Rightarrow x \in y$

Слично,

$y \in y \cup \{y\} = x \cup \{x\} \Rightarrow y \in x$ или $y \in \{x\}$ $\Rightarrow$ $y \in x$
шј. $y = x$ $\quad x \neq y$

Закључ. $x \in y$ и $y \in x$. последица 2° аксиоме регуларности

$\boxtimes$

<u>Пеанове аксиоме</u>:

П1: 0 је природан број

П2: Ако је x природан број, онда је и x' природан број.

П3: Ако су x и y природни бројеви и $x' = y'$, онда је $x = y$.

П4: За сваки природан број x важи $x' \neq 0$

П5: Нека је ϕ својство природних бројева за које важи:

1) 0 има својство ϕ

2) Ако природан број x има својство ϕ, тада и x' има својство ϕ.

Тада сваки природан број има својство ϕ.

0 – симбол константе

$'$ – унарни функцијски симбол $\quad x \xmapsto{'} x'$

Пеанове аксиоме описују природне бројеве, али не говоре о којој структури се тачно ради.

Природне бројеве можемо дефинисати на следећи начин:
(фон Нојманов модел заснован на теорији скупова)

$0 := \emptyset$

$n' := n \cup \{n\}$

$1 := 0' = 0 \cup \{0\} = \emptyset \cup \{\emptyset\} = \{\emptyset\} = \{0\}$

$2 := 1' = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0,1\}$

$3 := 2' = 2 \cup \{2\} = \{0,1\} \cup \{2\} = \{0,1,2\}$

$\vdots$

$n+1 := n' = n \cup \{n\} = \{0,1,\dots,n-1\} \cup \{n\} = \{0,1,2,\dots,n\}$

Приметимо следеће:

$m < n$ ако $m \in n$ ако $m \subsetneq n$

За ли фон Нојманов модел задовољава Пеанове аксиоме?

аксиоме П1 и П2 су очигледно задовољене

аксиома П3:

ако је $m' = n' \Rightarrow m \cup \{m\} = n \cup \{n\} \underset{(*)}{\Rightarrow} m = n$

аксиома П4:

$n' = n \cup \{n\} \Rightarrow n \in n' \Rightarrow n' \neq \emptyset \Rightarrow n' \neq 0$

аксиома П5:

Нека је Φ произвољно својство природних бројева и нека важи:

1) $\Phi(0)$ је тачно

2) за све n ако је $\Phi(n)$ тачно, тада је и $\Phi(n')$ тачно

За ли је $\Phi(n)$ за све природне бројеве n? да

пп. постоји $m \in \mathbb{N}$ тачно да $\Phi(m)$ није тачно

$\Rightarrow m \neq 0$

постоји $m_1 \in \mathbb{N}$ тј. $m = m_1' = m_1 \cup \{m_1\}$

Важи да је $\Phi(m) = \Phi(m_1')$ нетачно, па на основу 2) мора важити да је и $\Phi(m_1)$ нетачно

$\Rightarrow m_1 \neq 0$

па постоји $m_2 \in \mathbb{N}$ тј. $m_1 = m_2' = m_2 \cup \{m_2\}$ и није тачно $\Phi(m_2)$

итд. ..

Добијамо низ $m \ni m_1 \ni m_2 \ni m_3 \ni \dots$ ↯ на основу последице 3° аксиоме регуларности

Аксиому 175 називамо аксиомом индукције
услов 1) називамо база индукције
услов 2) називамо индуктивни корак

Принцип потпуне индукције:

Нека је ϕ својство природних бројева и нека важи:

ако је тачно $\phi(0), \phi(1), \dots, \phi(n)$ тачно је и $\phi(n')$

за све $n \in \mathbb{N}$.

Тада $\phi(n)$ важи за све природне бројеве n.

$\phi(0), \phi(1), \dots, \phi(n-1) \Rightarrow \phi(n) \Rightarrow \phi(n+1) \Rightarrow \phi(n+2) \dots$

Принцип најмањег елемента:

Ако је $A \subseteq \mathbb{N}$ и $A \neq \emptyset$ онда A има најмањи елемент.

доказ:

потпуном индукцијом

пп. $A \neq \emptyset$ и A нема најмањи елемент

Дефинишимо својство $\phi(n)$: $n \notin A$

тј. $n \in \mathbb{N} \setminus A$

потпуном индукцијом доказујемо да $\phi(n)$ важи за све $n \in \mathbb{N}$:

пп. да важи $\phi(0), \phi(1), \dots, \phi(n)$ и доказујемо да важи $\phi(n')$

ако $\phi(n')$ не важи онда $n' \in A$, а како $0, 1, \dots, n \notin A$ (јер важи

$\phi(0), \phi(1), \dots, \phi(n)$) онда је n' најмањи елемент у A ↯

Дакле, важи $\phi(n')$

принцип потпуне индукције: $\phi(n)$ важи за све $n \in \mathbb{N}$

тј. $n \in \mathbb{N} \setminus A$ за све $n \in \mathbb{N}$

$\Rightarrow \mathbb{N} \setminus A = \mathbb{N}$ па је $A = \emptyset$ ↯

Сабирање природних бројева:

$m + 0 := m$

$m + n' := (m+n)'$

особине сабирања:

1° $m+0 = 0+m = m$

$m+0 = m$ по дефиницији сабирања

$0+m = m$

$\Phi(m): 0+m = m$

показујемо да $\Phi(m)$ важи за све $m \in \mathbb{N}$ (индукцијом)

$\Phi(0): 0+0=0$ (T) по дефиницији

$\Phi(m) \Rightarrow \Phi(m'):$

нека важи $\Phi(m): 0+m=m$

доказујемо да важи $\Phi(m')$, тј. да $0+m' = m'$

$0+m' = (0+m)' \underset{их}{=} m'$

2° $(m+n)+k = m+(n+k)$

$\Phi(k): (m+n)+k = m+(n+k)$

доказујемо индукцијом да $\Phi(k)$ важи за све $k \in \mathbb{N}$:

$\Phi(0): (m+n)+0 \overset{?}{=} m+(n+0)$ (T)

$(m+n)+0 = m+n$

$m+(n+0) = m+n$

$\Phi(k) \Rightarrow \Phi(k'):$

важи $\Phi(k)$ тј. $(m+n)+k = m+(n+k)$

доказујемо да важи $\Phi(k')$, тј. $(m+n)+k' = m+(n+k')$

$(m+n)+k' = ((m+n)+k)' = (m+(n+k))'$

$= m+(n+k)'$

$= m+(n+k')$

3° $1+m = m+1 \ (= m')$

$m+1 = m+0' = (m+0)' = m'$

индукцијом по m $\Phi(m): 1+m = m+1$

4° $m+n = n+m$

5° $m+n=0 \Rightarrow m=0$ и $n=0$

пос. $m \neq 0$ или $n \neq 0$

онда постоје m_0 или n_0 тј. $m = m_0'$

$n = n_0'$

нека је нпр. $m \neq 0$

$m = m_0'$

$m+n = n+m = n+m_0' = (n+m_0)' \neq 0$ ↯

6° $m+n=m+k \Rightarrow n=k$

индукцијом по m

$\phi(m)$: $m+n=m+k \Rightarrow n=k$ за све $m\in\mathbb{N}$

$\phi(0)$: $\underbrace{0+n}_{=n}=\underbrace{0+k}_{=k} \Rightarrow n=k$

$\phi(m) \Rightarrow \phi(m')$:

доказујемо да важи $\phi(m')$

$m'+n=m'+k$

$n+m'=k+m'$

$(n+m)'=(k+m)' \underset{\text{П3}}{\Longrightarrow} n+m=k+m$

$\Rightarrow m+n=m+k$

$\underset{\text{ИХ}}{\Longrightarrow} n=k$

<u>Множење природних бројева:</u>

$m\cdot 0:=0$

$m\cdot n':=m\cdot n+m$

Особине множења:

1° $m\cdot(n+k)=m\cdot n+m\cdot k$

индукцијом по k

$k=0$: $m\cdot(n+0)\overset{?}{=}m\cdot n+m\cdot 0$

$m\cdot n=m\cdot n+0=m\cdot n$ Ⓣ

$k\to k'$:

важи $m\cdot(n+k)=m\cdot n+m\cdot k$

доказујемо: $m\cdot(n+k')=m\cdot n+m\cdot k'$

$m\cdot(n+k')=m\cdot(n+k)'$

$=m\cdot(n+k)+m$

$\underset{\text{ИХ}}{=}(m\cdot n+m\cdot k)+m$

$=m\cdot n+(m\cdot k+m)$

$=m\cdot n+m\cdot k'$

2° $m\cdot 1=m\cdot 0'=m\cdot 0+m=0+m=m$

3° $m(nk)=(mn)k$

indukcja po k:

$k=0$: $m(n\cdot 0) = m\cdot 0 = 0 = (mn)\cdot 0$ (+)

$k \to k'$:

baza $m(nk) = (mn)k$

dokazujemy: $m(nk') = (mn)k'$

$$
\begin{aligned}
m(nk') &= m(nk+n) \\
&= (m(nk)) + mn \\
&\underset{ix}{=} ((mn)k) + mn \\
&= (mn)k'
\end{aligned}
$$

4° $0\cdot m = 0$

5° $1\cdot m = m$

6° $(m+n)k = mk + nk$

7° $mn = nm$

} udowodnić za domową

Дељивост

у $\mathbb{N}$: $a|b$ ако $b = a\cdot q$, за неко $q\in\mathbb{N}$

видели смо раније да је | релација поретка на $\mathbb{N}$

Особине:

Нека $a,b,c\in\mathbb{N}$. Тада важи:

1° $a|0$

$a\cdot 0 = 0$

2° ако $a|b$ и $a|c$ онда $a|(b+c)$

$b = a\cdot q_1$

$c = a\cdot q_2$

$b+c = aq_1 + aq_2 = a\cdot(q_1+q_2) \Rightarrow a|(b+c)$

3° ако $a|b$ или $a|c$ онда $a|bc$

нап. $a|b$

$b = aq$

$bc = a\cdot cq \Rightarrow a|bc$

4° ако $a|b$ онда $a|b^n$, за све $n\geq 1$

Теорема (о Еуклидској деоби):

Нека $a,b\in\mathbb{N}$ и $b\neq 0$. Тада постоје јединствени $q,r\in\mathbb{N}$ такви да је

$a = bq + r$, где је $0\leq r<b$.

доказ:

Јединственост:

$a = bq + r$ $\quad 0\leq r, r' < b$

$a = b\cdot q' + r'$

нека је нап. $r\leq r'$

$0\leq r'-r<b$

$0 = b(q'-q) + (r'-r)$

$r'-r = b(q-q') \Rightarrow \left.\begin{array}{l} b\,|\,(r'-r) \\ r'-r<b \end{array}\right\} \Rightarrow$ мора бити $r'-r=0$

тј. $r=r'$

$0 = \underset{\neq 0}{b}(q-q') \Rightarrow q-q'=0$

$q=q'$

Егзистенција:

$S = \{ a - xb \mid x \in \mathbb{N},\ a - xb \in \mathbb{N} \}$

$\left.\begin{array}{l} S \subseteq \mathbb{N} \\ S \neq \emptyset \text{ јер } a = a - 0 \cdot b \in S \end{array}\right\} \Rightarrow$ S има најмањи елемент r на основу принципа најмањег елемента

тада је $r = a - qb$, за неко $q \in \mathbb{N}$, тј. $a = q \cdot b + r$

Доказимо да је $r < b$.

пос. $r \geq b$

$r - b = r' \geq 0$

$r - b = a - qb - b$

$\left.\begin{array}{l} r' = a - (q+1) \cdot b \in S \\ \text{међутим, } r' < r \text{ јер } b \neq 0 \end{array}\right\} \Rightarrow \lightning$ r је најмање у S ∎

у $\mathbb{Z}$: $a \mid b$ ако $b = a \cdot q$, за неко $q \in \mathbb{Z}$

видели смо да $\mid$ није поредак на $\mathbb{Z}$ (не важи АНТИС)

(нпр. $2 \mid -2$ и $-2 \mid 2$, али $2 \neq -2$)

<u>Тврђење</u>: Нека су $a, b \in \mathbb{Z}$ и $b \neq 0$. Тада постоје јединствени $q, r \in \mathbb{Z}$ такви да је

$$a = bq + r, \text{ где је } 0 \leq r < |b|.$$

<u>доказ</u>:

1. случај: $a \geq 0$ и $b \geq 0$

претходно тврђење о Еуклидском делењу

2. случај: $a \geq 0$ и $b < 0$

$-b > 0$

постоје $q, r \in \mathbb{N}$ тд. $a = q \cdot (-b) + r$, $0 \leq r < -b$

$a = (-q) \cdot b + r$, $0 \leq r < |b|$

3. случај: $a \leq 0$ и $b > 0$

$-a \geq 0$

постоје $q, r \in \mathbb{N}$ тд. $-a = q \cdot b + r$, $0 \leq r < b$

$a = (-q) \cdot b - r$, $0 \geq -r > -b$

ako je $r=0$ готово

ako je $r\neq 0$ тј. $r>0$

$$a=(-q)\cdot b-r+b-b$$
$$=\underbrace{(-q-1)}_{q'}b+\underbrace{(b-r)}_{r'}$$

$$-b<-r<0 \mid +b$$
$$0<\underbrace{b-r}_{r'}<b \quad\Rightarrow\quad 0\leq r'<|b|$$

4. случај: $a\leq 0$ и $b<0$

$-a>0$ и $-b>0$

постоје $q,r\in\mathbb{N}$ тј. $-a=q\cdot(-b)+r$, $0\leq r<-b$

$a=q\cdot b-r$, $b<-r\leq 0$

ako je $r=0$ готово

ako je $r>0$

$$a=qb-r+b-b$$
$$=\underbrace{(q+1)}_{q'}\cdot b+\underbrace{(-b-r)}_{r'}=q'\cdot b+r'$$

$$b<-r<0 \mid +(-b)$$
$$0<\underbrace{-b-r}_{r'}<\underbrace{-b}_{=|b|} \quad\Rightarrow\quad 0\leq r'<|b|$$

Једнственост се показује исто као у претходном тврђењу.

$\boxtimes$

дефо: Нека $a,b\in\mathbb{Z}$.

1° број $d\geq 0$ је највећи заједнички делилац од a и b, краће НЗД(a,b), ако задовољава следеће услове:

* $d\mid a$ и $d\mid b$
* ако $e\mid a$ и $e\mid b$, онда $e\mid d$.

2° Број $s\geq 0$ је најмањи заједнички садржалац од a и b, краће НЗС(a,b), ако задовољава следеће услове:

* $a\mid s$ и $b\mid s$
* ако $a\mid t$ и $b\mid t$ онда $s\mid t$.

Тврђење: Ако је $a = bq + r$, онда је $НЗД(a,b) = НЗД(b,r)$.

доказ:

S_1 – скуп заједничких делилаца a и b

S_2 – скуп заједничких делилаца b и r

Показујемо да је $S_1 = S_2$

$S_1 \subseteq S_2$:

Нека $d \in S_1$ тј. $\left.\begin{array}{l} d \mid a \text{ и } d \mid b \\ r = \underbrace{a}_{d\mid} - \underbrace{bd}_{d\mid} \end{array}\right\} \Rightarrow d \mid r \Rightarrow d \in S_2$

$S_2 \subseteq S_1$

Нека $d \in S_2$ тј. $\left.\begin{array}{l} d \mid b \text{ и } d \mid r \\ a = \underbrace{bq}_{d\mid} + \underbrace{r}_{d\mid} \end{array}\right\} \Rightarrow d \mid a \Rightarrow d \in S_1$

$НЗД(a,b) = \max S_1 = \max S_2 = НЗД(b,r)$ ∎

Еуклидов алгоритам

(поступак за налажење НЗД-а)

$a, b \in \mathbb{Z}$, $b \neq 0$

$a = b \cdot q_0 + r_0$, $0 \leq r_0 < |b|$

$b = r_0 \cdot q_1 + r_1$, $0 < r_1 < r_0$

$r_0 = r_1 \cdot q_2 + r_2$, $0 < r_2 < r_1$

$\vdots$

$r_{n-2} = r_{n-1} \cdot q_n + \boxed{r_n}$, $0 < r_n < r_{n-1}$

$r_{n-1} = r_n \cdot q_{n+1} + 0$

$r_{n+1} = 0$

Низ $r_0, r_1, r_2, \ldots$ је строго опадајући

$r_0 > r_1 > r_2 > r_3 > \ldots > r_{n-1} > r_n > r_{n+1} > \ldots \geq 0$

па неки остатак мора бити нула (поступак се завршава)

$НЗД(a,b) = НЗД(b, r_0) = НЗД(r_0, r_1) = НЗД(r_1, r_2) = \ldots = НЗД(r_{n-2}, r_{n-1}) =$

$= НЗД(r_{n-1}, r_n) = НЗД(r_n \cdot q_{n+1}, r_n) = r_n$

Тврђење: Ако је НЗД$(a,b)=d$, онда постоје $x,y\in\mathbb{Z}$ тд. $ax+by=d$.

доказ:

$$\begin{aligned}
\text{НЗД}(a,b) = r_n &= r_{n-2} - r_{n-1}\cdot q_n \\
&= r_{n-2} - (r_{n-3} - r_{n-2}\, q_{n-1})\, q_n \\
&= -q_n\cdot r_{n-3} + (1+q_{n-1}q_n)\, r_{n-2} \\
&\ \ \vdots \\
&= ax+by
\end{aligned}$$

$\blacksquare$

Нека $a,b\in\mathbb{Z}$

$$M_0 = \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

M_{n+1} добијамо од M_n на један од следећих начина:

- множењем врсте целим бројем и додавањем другој врсти
- множењем врсте са -1
- заменом места врстама

Тврђење: Нека је $M_n = \begin{bmatrix} x & p & q \\ y & s & t \end{bmatrix}$. Тада је $x=ap+bq$ и $y=as+bt$.

доказ:

индукцијом по n:

$n=0$:

$$M_0 = \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix} \qquad \begin{matrix} x=a & p=1 & q=0 \\ y=b & s=0 & t=1 \end{matrix} \qquad \begin{matrix} a = a\cdot 1 + b\cdot 0 \\ b = a\cdot 0 + b\cdot 1 \end{matrix}$$

$n \to n+1$

$$M_n = \begin{bmatrix} x & p & q \\ y & s & t \end{bmatrix} \longrightarrow M_{n+1} = \begin{bmatrix} x' & p' & q' \\ y' & s' & t' \end{bmatrix}$$

(ИХ) $\begin{matrix} x = ap+bq \\ y = as+bt \end{matrix} \longrightarrow$ доказујемо: $\begin{matrix} x' = ap' + bq' \\ y' = as' + bt' \end{matrix}$

имамо следеће могућности:

1° M_{n+1} смо добили од M_n заменом врста

$$\begin{bmatrix} x' & p' & q' \\ y' & s' & t' \end{bmatrix} = \begin{bmatrix} y & s & t \\ x & p & q \end{bmatrix}$$

(ИХ): $\begin{matrix} x' = ap' + bq' \\ y' = as' + bt' \end{matrix}$

2° M_{n+1} смо добили од M_n тако што смо неку врсту помножили са -1 (нпр. прву)

$$\begin{bmatrix} x' & p' & q' \\ y' & s' & t' \end{bmatrix} = \begin{bmatrix} -x & -p & -q \\ y & s & t \end{bmatrix}$$

$$\begin{aligned} x' &= -x \\ &\underset{(ИХ)}{=} -(ap+bq) \\ &= a(-p)+b(-q) = ap'+bq' \end{aligned}$$

3° M_{n+1} смо добили од M_n тако што смо нпр. првој врсти додали другу помножену са $\alpha \in \mathbb{Z}$

$$\begin{bmatrix} x' & p' & q' \\ y' & s' & t' \end{bmatrix} = \begin{bmatrix} x+\alpha y & p+\alpha s & q+\alpha t \\ y & s & t \end{bmatrix}$$

$$\begin{aligned} x' &= x+\alpha y \\ &\underset{(ИХ)}{=} (ap+bq)+\alpha(as+bt) \\ &= a\underbrace{(p+\alpha s)}_{p'} + b\underbrace{(q+\alpha t)}_{q'} \\ &= ap'+b\cdot q' \end{aligned}$$

$\boxtimes$

<u>Тврђење</u>: Нека је $M_n = \begin{bmatrix} x & p & q \\ y & s & t \end{bmatrix}$. Тада је $НЗД(a,b) = НЗД(x,y)$.

<u>доказ</u>:

индукцијом по n

$n=0$ јасно

$n \to n+1$

$$M_n = \begin{bmatrix} x & p & q \\ y & s & t \end{bmatrix} \rightsquigarrow M_{n+1} = \begin{bmatrix} x' & p' & q' \\ y' & s' & t' \end{bmatrix}$$

(ИХ) $НЗД(x,y) = НЗД(a,b) \longrightarrow$ доказујемо $НЗД(x',y') = НЗД(a,b)$

1° M_{n+1} добијемо од M_n заменом врста

$$НЗД(\underset{y}{\underset{\parallel}{x'}}, \underset{x}{\underset{\parallel}{y'}}) = НЗД(y,x) \underset{ИХ}{=} НЗД(a,b)$$

2° M_{n+1} добијемо од M_n множењем врсте са -1

$$НЗД(x',y') = НЗД(-x,y) = НЗД(x,y) \underset{(ИХ)}{=} НЗД(a,b)$$

3° M_{n+1} добијамо од M_n множењем врсте са $\underset{\in \mathbb{Z}}{d}$ и додавањем другој врсти

$$НЗД(x', y') = НЗД(x + dy, y) = НЗД(x, y) \underset{(ИК)}{=} НЗД(a, b)$$

$\boxtimes$

Дакле, ако је $M_n = \begin{bmatrix} d & p & q \\ 0 & s & t \end{bmatrix}$ и $d \geq 0$, тада је $НЗД(a,b) = НЗД(d, 0) = d$ и $d = a \cdot p + b \cdot q$.

Пример:

$НЗД(1729, 385) = ?$

$$\begin{bmatrix} 1729 & 1 & 0 \\ 385 & 0 & 1 \end{bmatrix} (-4) + \rightsquigarrow \begin{bmatrix} 189 & 1 & -4 \\ 385 & 0 & 1 \end{bmatrix} (-2) +$$

$$\begin{array}{r} 1729 \\ -\ 1540 \\ \hline 189 \end{array} \qquad \begin{array}{r} 385 \\ -\ 378 \\ \hline 7 \end{array}$$

$$\rightsquigarrow \begin{bmatrix} 189 & 1 & -4 \\ 7 & -2 & 9 \end{bmatrix} (-27) + \rightsquigarrow \begin{bmatrix} 0 & 55 & -247 \\ 7 & -2 & 9 \end{bmatrix}$$

$$\rightsquigarrow \begin{bmatrix} \boxed{7} & -2 & 9 \\ 0 & 55 & -247 \end{bmatrix}$$

$НЗД(1729, 385) = 7$

$7 = 1729 \cdot (-2) + 385 \cdot 9$

Деф: Бројеви $a, b \in \mathbb{Z}$ су узајамно прости ако је $НЗД(a,b) = 1$.

Тврђење: Ако $a \mid bc$ и $НЗД(a,b) = 1$, тада $a \mid c$.

Доказ:

постоје $p, q \in \mathbb{Z}$ тј. $ap + bq = 1 = НЗД(a,b) \quad / \cdot c$

$$\left.\begin{array}{l} acp + bcq = c \\ a \mid acp \text{ и } a \mid bcq \end{array}\right\} \Rightarrow a \mid c$$

$\boxtimes$

$6 \mid 9 \cdot 4$

$6 \nmid 9$ и $6 \nmid 4$

$6 \mid 5 \cdot 12$

$НЗД(6,5) = 1$

$\Rightarrow 6 \mid 12$

Тврђење: Нека је $d = НЗД(a,b)$, тада је $НЗС(a,b) = \dfrac{|a \cdot b|}{d}$.

Доказ:

$a = d \cdot a'$

$b = d \cdot b'$

$$S = \frac{|a \cdot b|}{d} = \frac{d^2 \cdot |a'| \cdot |b'|}{d} = d \cdot |a'| \cdot |b'| \in \mathbb{N}$$

$a \mid s$ jer $s = d \cdot |a'| \cdot |b'| = |a| \cdot |b'|$

$b \mid s$ jer $s = d \cdot |b'| \cdot |a'| = |b| \cdot |a'|$

Neka $a, b \mid t$

$$t = a \cdot a'' = b \cdot b''$$

$$t = d \cdot a' \cdot a'' = d \cdot b' \cdot b'' \Rightarrow a'a'' = b'b''$$

$$\left.\begin{array}{l} a' \mid b'b'' \\ \text{НЗД}(a', b') = 1 \end{array}\right\} \overset{\text{уредност. цел.}}{\Longrightarrow} a' \mid b''$$

$$b'' = a' \cdot \ell$$

$$\left.\begin{array}{l} t = d \cdot b' \cdot b'' = d \cdot b' \cdot a' \cdot \ell \\ s = d \cdot |b'| \cdot |a'| \end{array}\right\} \Rightarrow s \mid t$$

Дакле, $s = \text{НЗС}(a, b)$. ∎

Тврђење: Нека је $d = \text{НЗД}(a, b)$, $a = d \cdot a'$ и $b = d \cdot b'$, уз услов да је $\text{НЗД}(a', b') = 1$.

Доказ:

Уз супр. $d' = \text{НЗД}(a', b') \neq 1$

$$a' = d' \cdot q_1$$
$$b' = d' \cdot q_2$$

$$\left.\begin{array}{l} a = d \cdot d' q_1 \\ b = d \cdot d' \cdot q_2 \end{array}\right\} dd' \mid a, b, \quad dd' > d \quad ↯$$

d је највећи заједнички делилац ∎

Диофантове једначине

тражимо целобројна решења једначине

$$ax+by=c, \quad a,b,c\in\mathbb{Z} \quad (*)$$
$$a,b\neq 0$$

(x,y)

Тврђење: Једначина $(*)$ има решење ако $НЗД(a,b)\mid c$.

доказ:

$\Rightarrow$: Нека $(*)$ има решење

(x_0,y_0) - једно решење

$x_0,y_0\in\mathbb{Z}$

Нека је $d=НЗД(a,b)$

$d\mid a,b \quad d\mid ax_0+by_0 \Rightarrow d\mid c$

$\Leftarrow$: Нека је $d=НЗД(a,b)\mid c$

$c=d\cdot c'$

постоје $p,q\in\mathbb{Z}$ тд. $ap+bq=d \,/_{c'}$

$$a\underbrace{(pc')}+b\underbrace{(qc')}=c$$

$\Rightarrow (pc',qc')$ једно решење $(*)$

Како наћи сва решења једначине $(*)$?

$d=НЗД(a,b)\mid c \qquad c=d\cdot c'$

$(\underbrace{pc'}_{x_0},\underbrace{qc'}_{y_0})$ - једно решење

бројеве p и q добијамо из Еуклидовог алгоритма

$a=d\cdot a'$

$b=d\cdot b'$

$НЗД(a',b')=1$

$$\begin{aligned} ax_0+by_0&=c \\ ax+by&=c \end{aligned} \quad -$$

$a(x-x_0)+b(y-y_0)=0$

$a(x-x_0)=-b(y-y_0) \,/:d$

$a'(x-x_0)=-b'(y-y_0)$

$a' \mid b'(y-y_0)$, $НЗД(a', b') = 1 \Rightarrow a' \mid y - y_0$

$b' \mid a'(x-x_0)$, $НЗД(a', b') = 1 \Rightarrow b' \mid x - x_0$

$x - x_0 = b' \cdot t$, $t \in \mathbb{Z}$

$\Rightarrow x = x_0 + b't$

$a'b't = -b'(y-y_0) \quad | : b'$

$a't = -y + y_0$

$\Rightarrow y = y_0 - a't$

Закле, опште решење једначине (*) је:

$$x = p \cdot \frac{c}{d} + \frac{b}{d} \cdot t$$

$$y = q \cdot \frac{c}{d} - \frac{a}{d} \cdot t \quad , \quad t \in \mathbb{Z}$$

где је $d = НЗД(a,b)$ и важи $ap + bq = c$.

Прости бројеви

Број $p > 1$ је прости ако су му једини делиоци 1 и p.
Ако $p > 1$ није прости, онда кажемо да је сложен.

Теорема: Постоји бесконачно много простих бројева.

доказ:

пос. Нека су $p_1, p_2, \dots, p_k$ сви прости бројеви

посматрајмо број $p = p_1 p_2 \cdots p_k + 1$

Приметимо да је $p \neq p_i$ за све $i \in \{1, \dots, k\}$, па је p сложен број.

$\Rightarrow$ постоји прости број q који дели p

тада је $q = p_j$, за неко $j \in \{1, \dots, k\}$, па $p_j \mid p$ ↯

∎

Тврђење: Ако је p прости број и $p \mid ab$ онда $p \mid a$ или $p \mid b$.

доказ:

Нека $p \mid ab$ и претпостављамо да $p \nmid a$, доказимо да $p \mid b$

ако је $НЗД(a,p) > 1$, онда $НЗД(a,p) = p$, јер је p прости број

$\Downarrow$

$p \mid a$ што није тачно

па $НЗД(a,p) = 1$

∎

$$\left.\begin{array}{l} p \mid ab \\ \text{ЗНД}(p,a)=1 \end{array}\right\} \Rightarrow p \mid b$$

Важи и опшшије:

ако $p \mid a_1 a_2 \cdots a_k \Rightarrow p \mid a_1$ или $p \mid a_2$ или $\cdots$ или $p \mid a_k$

<u>Теорема</u>: Сваки природан број $n>1$ је прости или се може представити као производ простих бројева.

<u>доказ</u>:

потпуном индукцијом по n

$\phi(n)$: n је производ простих

(ИХ) претпоставимо да је за сваки природан број мањи од n задовољено својство ϕ

тј. за свако $k<n$, k је производ простих

доказимо да је n производ простих:

- ако је n прости: крај
- ако је n сложен: $n = m \cdot k$, $1<m,k<n$

по (ИХ) m и k су производи простих па је $n = m \cdot k$ производ простих

$\blacksquare$

<u>Основна теорема аритметике</u>:

Сваки природан број $n>1$ се (до на редоследа чинилаца) на јединствен начин записује као производ простих.

<u>доказ</u>:

На основу претходне теореме знамо да је сваки природан број производ простих, показимо да је запис тог производа јединствен (до на редослед чинилаца)

Нека је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$

$\alpha_i, \beta_i \geq 1$

$p_1 < p_2 < \cdots < p_k$, $q_1 < q_2 < \cdots < q_l$

за свако $1 \leq i \leq k$ $p_i \mid n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$

$\Rightarrow$ постоји $j \in \{1, \ldots, l\}$ тд. $p_i \mid q_j$, па $p_i = q_j$

Дакле, $\{p_1, \ldots, p_k\} \subseteq \{q_1, q_2, \ldots, q_l\}$

Аналогно се доказује да је $\{q_1, q_2, \ldots, q_l\} \subseteq \{p_1, p_2, \ldots, p_k\}$

$\Rightarrow \{p_1, \ldots, p_k\} = \{q_1, \ldots, q_l\}$

па је $k=l$

и како је $p_1 < p_2 < \cdots < p_k$ и $q_1 < q_2 < \cdots < q_l$

закључујемо $p_1 = q_1$, $p_2 = q_2$, $\ldots$, $p_k = q_k$

За сада имамо:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} \quad / : p_1^{\alpha_1}$$

ако је нпр. $\alpha_1 < \beta_1$

$$\underbrace{p_2^{\alpha_2} \cdots p_k^{\alpha_k}}_{p_1 \nmid} = \underbrace{p_1^{\overbrace{\beta_1 - \alpha_1}^{\geq 1}} p_2^{\beta_2} \cdots p_k^{\beta_k}}_{p_1 \mid} \quad ↯$$

Дакле, $\alpha_1 = \beta_1$, па важи

$$p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_2^{\beta_2} \cdots p_k^{\beta_k}$$ и настављањем поступка добијамо

$$\alpha_2 = \beta_2$$
$$\vdots$$
$$\alpha_k = \beta_k$$

∎

Конгруенција по модулу

Нека је $m \geq 2$. Дефинишемо бинарну релацију $\equiv_m$ на $\mathbb{Z}$ са:

$$a \equiv_m b \quad \text{акко} \quad m \mid a-b$$

Нпр. за $m=3$

$2 \equiv_3 5$

$13 \equiv_3 10$

Тврђење: $\equiv_m$ је релација еквиваленције.

Доказ:

(Р) $a \equiv_m a$ јер $m \mid a-a=0$

(С) $a \equiv_m b \overset{?}{\Rightarrow} b \equiv_m a$

$$a \equiv_m b \Rightarrow m \mid a-b \Rightarrow m \mid b-a = -(a-b) \Rightarrow b \equiv_m a$$

(Т) $\left.\begin{array}{l} a \equiv_m b \\ b \equiv_m c \end{array}\right\} \overset{?}{\Rightarrow} a \equiv_m c$

$$\left.\begin{array}{l} m \mid a-b \\ m \mid b-c \end{array}\right\} \Rightarrow m \mid a-c = (a-b)+(b-c) \Rightarrow a \equiv_m c$$

∎

$a \in \mathbb{Z}$

$$C_a = [a] = \{x \in \mathbb{Z} \mid x \equiv_m a\}$$
$$= \{x \in \mathbb{Z} \mid m \mid x-a\}$$
$$= \{x \in \mathbb{Z} \mid x-a = m \cdot k, \text{ за неко } k \in \mathbb{Z}\}$$
$$= \{a+mk \mid k \in \mathbb{Z}\}$$

$\equiv_m$ има m класа

$[0], [1], [2], \ldots, [m-1]$

уместо $a \equiv_m b$ често пишемо $a = b \pmod m$

<u>Тврђење</u>! (особине конгруенције): Нека је $a \equiv_m b$ и $c \equiv_m d$. Тада:

1° $a+c \equiv_m b+d$

2° $ac \equiv_m bd$

3° $a^n \equiv_m b^n$, за $n \geq 1$.

<u>доказ</u>:

1° $(a+c)-(b+d) = \underbrace{(a-b)}_{m\mid} + \underbrace{(c-d)}_{m\mid} \Rightarrow m \mid (a+c)-(b+d)$

тј. $a+c \equiv_m b+d$

2° $ac-bd = ac-cb+cb-bd = \underbrace{c(a-b)}_{m\mid} + \underbrace{b(c-d)}_{m\mid} \Rightarrow m \mid ac-bd$

тј. $ac \equiv_m bd$

3° индукцијом по n:

$n=1$ $a^1 = a$, $b^1 = b$

$a \equiv_m b$ (дато) Ⓣ

(ИХ) Нека је $a^n \equiv_m b^n$

$n \to n+1$:

$a^{n+1} = a^n \cdot a$

$$\left.\begin{array}{l} a^n \equiv_m b^n \\ a \equiv_m b \end{array}\right\} \overset{2°}{\Rightarrow} a^n \cdot a \equiv_m b^n \cdot b$$
$$a^{n+1} \equiv_m b^{n+1}$$

$\boxtimes$

Тврђење: Нека $d \mid a, b, m$, и нека је $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ и $m' = \frac{m}{d}$. Тада је $a \equiv_m b$ акко $a' \equiv_{m'} b'$.

доказ:

$\Rightarrow$: Нека је $a \equiv_m b$

$m \mid a-b$

$a-b = m \cdot k$, за неко $k \in \mathbb{Z}$

$da' - d \cdot b' = d \cdot m' \cdot k \quad | : d$

$a' - b' = m' \cdot k$

па $m' \mid a'-b'$ тј. $a' \equiv_{m'} b'$

$\Leftarrow$: Нека $a' \equiv_{m'} b'$

$m' \mid a'-b'$

$a'-b' = m' \cdot l$, за неко $l \in \mathbb{Z}$

$\underbrace{da'}_{a} - \underbrace{db'}_{b} = \underbrace{dm'}_{m} \cdot l$

$a-b = ml$

па $m \mid a-b$ тј. $a \equiv_m b$

$\blacksquare$

Посматрајмо једначину

$$ax \equiv_m b$$

Занима нас: када има решење, шта су решења?

$ax \equiv_m b$ акко $m \mid ax-b$

акко $ax-b = m \cdot (-k)$, за неко $k \in \mathbb{Z}$

акко $ax + mk = b$, за неко $k \in \mathbb{Z}$

$ax \equiv_m b$ има решење акко $ax+mk=b$ има решење

акко $НЗД(a,m) \mid b$

Нека $d = НЗД(a,m) \mid b$. Шта су решења $ax \equiv_m b$?

Према претходном тврђењу, довољно је да решимо

$\frac{a}{d} x \equiv_{\frac{m}{d}} \frac{b}{d}$ тј. $\boxed{a'x \equiv_{m'} b'}$ где је $НЗД(a', m') = 1$

$\frac{a}{d} = a'$, $\frac{b}{d} = b'$, $\frac{m}{d} = m'$

из $НЗД(a', m') = 1 \Rightarrow 1 = a'p + m'q$, за неке $p, q \in \mathbb{Z}$

$\Rightarrow 1 \equiv_{m'} a'p \quad / \cdot b'$

$b' \equiv_{m'} a' \cdot (pb')$

Показаћемо: $a'x \equiv_{m'} b'$ акко $x \equiv_{m'} pb'$.

$\Rightarrow$: $\left.\begin{array}{l} a'x \equiv_{m'} b' \\ p \equiv_{m'} p \end{array}\right\} \overset{2^\circ}{\Rightarrow} \underbrace{a'p}_{\substack{\equiv_{m'} \\ 1}} x \equiv_{m'} pb'$

$x \equiv_{m'} pb'$

$\Leftarrow$: $\left.\begin{array}{l} x \equiv_{m'} pb' \\ a' \equiv_{m'} a' \end{array}\right\} \overset{2^\circ}{\Rightarrow} a'x \equiv_{m'} \underbrace{a'p}_{\substack{\equiv_{m'} \\ 1}} b'$

$a'x \equiv_{m'} b'$

решења једначине $a'x \equiv_{m'} b'$ су $x \equiv_{m'} pb'$

тј. решења су $\{pb' + m't \mid t \in \mathbb{Z}\}$

(само једно решење је ≥ 0 и $< m'$)

$ax \equiv_m b$ где $d = \text{НЗД}(a, m) \mid b$

Колико ова једначина има решења ≥ 0 и $< m$?

има укупно d решења у интервалу $[0, m)$, по једно решење у сваком од следећих интервала:

$[0, m'), [m', 2m'), \ldots, [(d-1)\cdot m', \underbrace{dm'}_{m})$

<u>Вилсонова теорема</u>:

Ако је p прости број, тада је $(p-1)! \equiv -1 \pmod p$.

<u>доказ</u>:

за $p=2$ $\quad (2-1)! = 1! = 1$

$1 \equiv -1 \pmod 2$ јер $2 \mid 1-(-1) = 2$

за $p=3$ $\quad (3-1)! = 2! = 2$

$2 \equiv -1 \pmod 3$ јер $3 \mid 2-(-1) = 3$

Нека је $p \geq 5$

Нека $a \in \{2, 3, 4, \ldots, p-2\}$

посматрајмо једначину $ax \equiv 1 \pmod p$

$\text{НЗД}(a, p) = 1$ па $ax \equiv 1 \pmod p$ има јединствено решење у интервалу $[0, p)$. Нека је то решење x_a.

$x_a \in \{2, 3, 4, \dots, p-2\}$

$0 \leq x_a < p$

ако је $x_a = 0 \Rightarrow a \cdot 0 \equiv_p 1$ ↯

ако је $x_a = 1 \Rightarrow a \cdot 1 \equiv_p 1 \Rightarrow a = 1$ ↯

ако је $x_a = p-1 \Rightarrow a(p-1) \equiv_p 1$

$$ap - a \equiv_p -a \equiv_p 1$$

$$a \equiv_p -1 \equiv_p p-1 \Rightarrow a = p-1 \text{ ↯}$$

$a \neq x_a$:

шта. $a = x_a$

тј. $a^2 \equiv_p 1$

$p \mid a^2 - 1 = (a-1)(a+1)$

$p \mid a-1$ или $p \mid a+1$

$2 \leq a \leq p-2$

$1 \leq a-1 \leq p-3$
$3 \leq a+1 \leq p-1$ } ни $a-1$, ни $a+1$ не могу бити дељиви са p ↯

Поделимо скуп $\{2, 3, \dots, p-2\}$ на парове облика $\{a, x_a\}$:

$\{2, x_2\}, \{3, x_3\}, \dots$

Укупно има $\frac{p-3}{2}$ парова

$a x_a \equiv_p 1$ за сваки пар $\{a, x_a\}$

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-2) \cdot (p-1)$$

$$= 1 \cdot (2 \cdot x_2) \cdot (3 \cdot x_3) \cdots (p-1)$$

$$\equiv_p 1 \cdot \underbrace{1 \cdot 1 \cdots 1}_{\frac{p-3}{2}} \cdot (p-1)$$

$$\equiv_p -1$$

∎

$$x \equiv_{m_1} a_1$$
$$x \equiv_{m_2} a_2$$
$$\vdots$$
$$x \equiv_{m_n} a_n$$

Кинеска теорема о остацима:

Нека су $m_1, m_2, \dots, m_n \geq 2$ узајамно прости у паровима и нека су $a_1, a_2, \dots, a_n \in \mathbb{Z}$. Тада систем конгруенција

$$x \equiv_{m_1} a_1$$
$$x \equiv_{m_2} a_2$$
$$\vdots$$
$$x \equiv_{m_n} a_n$$

има решење. Решење је јединствено у интервалу $[0, m_1 m_2 \cdots m_n)$, а опште решење система је облика

$$x_0 + t \cdot m_1 m_2 \cdots m_n,$$

где $t \in \mathbb{Z}$, а x_0 је решење из интервала $[0, m_1 m_2 \cdots m_n)$.

доказ:

Нека је $m = m_1 m_2 \cdots m_n$.

$$M_1 = \frac{m}{m_1} = m_2 m_3 \cdots m_n$$
$$M_2 = \frac{m}{m_2} = m_1 \cdot m_3 \cdots m_n$$
$$\vdots$$
$$M_n = \frac{m}{m_n} = m_1 \cdot m_2 \cdots m_{n-1}$$

m_i је узајамно просто са $m_1, m_2, \dots, m_{i-1}, m_{i+1}, \dots, m_n$

$\Rightarrow$ НЗД $(m_i, M_i) = 1$ за све $i \in \{1, \dots, n\}$

па је $1 = p_i \cdot m_i + q_i \cdot M_i$, за све $i \in \{1, \dots, n\}$

Приметимо да је

$$q_i M_i \equiv_{m_i} 1, \text{ за све } i \in \{1, \dots, n\}$$

$$q_i M_i \equiv_{m_j} 0, \text{ за све } j \neq i \text{ јер } m_j \mid M_i.$$

Нека је

$$x = a_1 q_1 M_1 + a_2 q_2 M_2 + \dots + a_n q_n M_n$$

$$x \equiv_{m_i} a_1 \underbrace{q_1 M_1}_{0} + a_2 \underbrace{q_2 M_2}_{0} + \dots + a_{i-1} \overset{0}{q_{i-1} M_{i-1}} + a_i \overset{1}{q_i M_i} + a_{i+1} \overset{0}{q_{i+1} M_{i+1}} + \dots + a_n \overset{0}{q_n M_n}$$

$$x \equiv_{m_i} a_i$$

Дакле, x јесте решење система.

Нека је x_0 остатак при дељењу x са m, тј.

$x_0 \equiv_m x$ и $0 \leq x_0 < m$

Тада је $x_0 \equiv_{m_i} x \equiv_{m_i} a_i \Rightarrow x_0 \equiv_{m_i} a_i$ за све $i \in \{1, \dots, n\}$

па је x_0 решење система

Нека је x_1 произвољно решење, тада је $x_1 \equiv_{m_i} a_i \equiv_{m_i} x_0$, па $m_i \mid x_1 - x_0$ за све $i \in \{1, \dots, n\}$.

Како су $m_1, m_2, \dots, m_n$ у паровима узајамно прости $\Rightarrow m \mid x_1 - x_0$

тј. $x_1 \equiv_m x_0$

$x_1 = x_0 + m \cdot t$, $t \in \mathbb{Z}$

$\boxtimes$

<u>Опште</u> <u>тврђење</u>:

Систем конгруенција

$$x \equiv_{m_1} a_1$$
$$x \equiv_{m_2} a_2$$
$$\vdots$$
$$x \equiv_{m_n} a_n$$

има решење акко НЗД$(m_i, m_j) \mid a_i - a_j$ за $1 \leq i < j \leq n$. Решење је јединствено у интервалу $[0, \text{НЗС}(m_1, \dots, m_n))$ и опште решење је облика

$$x_0 + t \cdot \text{НЗС}(m_1, \dots, m_n),$$

где $t \in \mathbb{Z}$ и x_0 је решење из интервала $[0, \text{НЗС}(m_1, \dots, m_n))$.

<u>доказ</u>:

индукцијом по броју конгруенција n

$n = 1$ $\quad x \equiv_{m_1} a_1 \Rightarrow m_1 \mid x - a_1 \quad x - a_1 = mt$, $t \in \mathbb{Z}$

па је опште решење $x = a_1 + m_1 t$

(ИХ) претпоставимо да тврђење важи за n конгруенција

показаћемо да тврђење важи и за $n+1$ конгруенцију

Нека је дат систем конгруенција:

$$x \equiv_{m_1} a_1$$
$$x \equiv_{m_2} a_2$$
$$\vdots$$
$$x \equiv_{m_n} a_n$$
$$x \equiv_{m_{n+1}} a_{n+1}$$

и важи да НЗД$(m_i, m_j) \mid a_i - a_j$ за све $1 \leq i < j \leq n+1$.

Према (ИК) систем који се састоји од првих n конгруенција има решење и опште решење је

$$x = x_0 + t \cdot \text{НЗС}(m_1, \dots, m_n), \text{ где } t \in \mathbb{Z}$$

$\downarrow$

решење из интервала $[0, \text{НЗС}(m_1, \dots, m_n))$

За ли x задовољава и последњу конгруенцију?

$x_0 + t \cdot \text{НЗС}(m_1, \dots, m_n) \equiv_{m_{n+1}} a_{n+1}$ – да ли има решење?

$$t \cdot \text{НЗС}(m_1, \dots, m_n) \equiv_{m_{n+1}} a_{n+1} - x_0 \quad (*) \qquad\qquad ax \equiv_m b$$

једначина има решење ако

$$\text{НЗД}(\text{НЗС}(m_1, \dots, m_n), m_{n+1}) \mid a_{n+1} - x_0$$

$$\text{НЗД}(\text{НЗС}(m_1, \dots, m_n), m_{n+1}) = \text{НЗС}(\text{НЗД}(m_1, m_{n+1}), \text{НЗД}(m_2, m_{n+1}), \dots, \text{НЗД}(m_n, m_{n+1}))$$

Показаћемо да $\text{НЗД}(m_i, m_{n+1}) \mid a_{n+1} - x_0$, за све $i \in \{1, \dots, n\}$

$$a_{n+1} - x_0 = \underbrace{(a_{n+1} - a_i)}_{\text{НЗД}(m_{n+1}, m_i) \mid} + \underbrace{(a_i - x_0)}_{\underbrace{m_i \mid}_{\text{НЗД}(m_{n+1}, m_i) \mid}} \Rightarrow \text{НЗД}(m_{n+1}, m_i) \mid a_{n+1} - x_0$$

Једначина $(*)$ има решење, па и систем има решење.

Нека је $\bar{x}$ неко решење система, тада је

$$\begin{aligned} \bar{x} &\equiv_{m_1} a_1 & x &\equiv_{m_1} a_1 \\ &\vdots & &\vdots \\ \bar{x} &\equiv_{m_{n+1}} a_{n+1} & x &\equiv_{m_{n+1}} a_{n+1} \end{aligned}$$

па је

$$\begin{aligned} \bar{x} &\equiv_{m_1} x \\ \bar{x} &\equiv_{m_2} x \\ &\vdots \\ \bar{x} &\equiv_{m_{n+1}} x. \end{aligned}$$

Што значи да $m_i \mid \bar{x} - x$ за све $i \in \{1, \dots, n+1\}$ па и $\text{НЗС}(m_1, \dots, m_{n+1}) \mid \bar{x} - x$, односно $x = \bar{x} + t \cdot \text{НЗС}(m_1, \dots, m_{n+1})$. ∎

$$\{2 + 6t \mid t \in \mathbb{Z}\}$$
$$\parallel$$
$$\{8 + 6t \mid t \in \mathbb{Z}\}$$

Ојлерова функција

$n \geq 1$

$\Phi(n) = \{a \mid 1 \leq a \leq n,\ \text{НЗД}(a, n) = 1\}$

$\downarrow$

Ојлеров скуп

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

$\Phi(2) = \{1\}$

$\Phi(3) = \{1, 2\}$

$\Phi(4) = \{1, 3\}$

$\Phi(5) = \{1, 2, 3, 4\}$

$\Phi(10) = \{1, 3, 7, 9\}$

$\Phi(12) = \{1, 5, 7, 11\}$

$\varphi(n) = |\Phi(n)|$

$\downarrow$

Ојлерова функција (броји колико има елемената који су узајамно прости са n)

$\varphi(1) = 1$ $\quad$ $\varphi(5) = 4$

$\varphi(2) = 1$ $\quad$ $\varphi(10) = 4$

$\varphi(3) = 2$ $\quad$ $\varphi(12) = 4$

$\varphi(4) = 2$

$\varphi(n) = ?$

p - прости број

* $\varphi(p) = ?$

$\Phi(p) = \{1, 2, 3, \ldots, p-1\} \Rightarrow \varphi(p) = p-1$

* $\varphi(p^2) = ?$

$\text{НЗД}(a, p^2) \in \{1, p, p^2\}$ за све $a \in \mathbb{N}$

$$\left.\begin{array}{lllll}
1-p: & 1 & 2 & 3 \ \ldots & p-1 \\
p+1-2p: & p+1 & p+2 & p+3 \ \ldots & 2p-1 \\
2p+1-3p: & 2p+1 & 2p+2 & 2p+3 \ \ldots & 3p-1 \\
\vdots & & & & \\
(p-1)p+1-p^2: & (p-1)p+1 & (p-1)p+2 & (p-1)p+3 \ \ldots & p^2-1
\end{array}\right\} p \text{ врста}$$

$НЗД(a,p)=1$ акко $НЗД(a,p^2) \notin \{p, p^2\}$

акко $p \nmid a$

$$\varphi(p^2) = p\cdot(p-1) = p^2 - p = p^2\left(1-\frac{1}{p}\right)$$

$*$ $\varphi(p^n)=?$, $n\in\mathbb{N}$

$НЗД(a,p^n) \in \{1, p, p^2, \dots, p^n\}$

$НЗД(a,p^n)=1$ акко $НЗД(a,p^n) \notin \{p, p^2, \dots, p^n\}$

акко $p \nmid a$

$$\left.\begin{array}{ccccc} 1 & 2 & 3 & \dots & p-1 \ \cancel{p} \\ p+1 & p+2 & p+3 & \dots & 2p-1 \ \cancel{2p} \\ 2p+1 & 2p+2 & 2p+3 & \dots & 3p-1 \ \cancel{3p} \\ \vdots & & & & \\ & & & & p^n-1 \ \cancel{p^n} \end{array}\right\} p^{n-1} \text{ бројева}$$

$1-p^n$

$1\ 2 \dots p$

$p+1\ p+2 \dots 2p$

$\vdots$

p^n

$$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1) = p^n\left(1-\frac{1}{p}\right)$$

<u>Теорема</u>: Ојлерова функција је мултипликативна, тј. $\varphi(mn)=\varphi(m)\cdot\varphi(n)$ кад год $НЗД(m,n)=1$.

<u>доказ</u>:

Нека је $НЗД(m,n)=1$.

$s_n(k) :=$ остатак при дељењу k са n , $s_n(k)\in\{0,1,\dots,n-1\}$

Посматрајмо пресликавање:

$$F: \Phi(mn) \to \Phi(m)\times\Phi(n)$$

које је дефинисано са

$$F(a) = (s_m(a), s_n(a))$$

и показаћемо да је бијекција.

1° F је добро дефинисано

за $a\in\Phi(mn)$ треба да показемо да $s_m(a)\in\Phi(m)$ и $s_n(a)\in\Phi(n)$

$НЗД(a,mn)=1 \Rightarrow НЗД(a,m)=1$ и $НЗД(a,n)=1$

$$a = mq + \underset{\substack{\| \\ s_m(a)}}{r} \qquad 0\le r<m$$

$1 = НЗД(a,m) = НЗД(m,r) = НЗД(m, s_m(a)) \Rightarrow s_m(a)\in\Phi(m)$

слично се показује и да $s_n(a)\in\Phi(n)$

2° F je "1-1"

$F(a) = F(b) \overset{?}{\Rightarrow} a = b$

$(\xi_m(a), \xi_n(a)) = (\xi_m(b), \xi_n(b))$

$\xi_m(a) = \xi_m(b) \Rightarrow a \equiv_m b \Rightarrow m \mid a-b$

$\xi_n(a) = \xi_n(b) \Rightarrow a \equiv_n b \Rightarrow n \mid a-b$

Kako je $\text{НЗД}(m,n) = 1 \Rightarrow a \equiv_{mn} b$

$mn \mid a-b$

$0 \le a, b < mn$

$$\left.\begin{array}{l} -mn < a-b < mn \\ mn \mid a-b \end{array}\right\} \Rightarrow \begin{array}{l} a-b = 0 \\ a = b \end{array}$$

3° F je "na"

Neka $(r,s) \in \Phi(m) \times \Phi(n)$

pokažimo da postoji $a \in \Phi(mn)$ tj. $F(a) = (r,s)$

odnosno $(\xi_m(a), \xi_n(a)) = (r,s)$

Postavljamo sistem:

$x \equiv_m r$

$x \equiv_n s$

Kako je $\text{НЗД}(m,n) = 1$, prema Kineskoj teoremi, postoji a tj.

$0 \le a < mn$ i $a \equiv_m r$ i $a \equiv_m s$.

Zašto $a \in \Phi(mn)$?

$$\left.\begin{array}{l} \text{iz } a \equiv_m r,\ \text{НЗД}(r,m) = 1 \Rightarrow \text{НЗД}(a,m) = 1 \\ \qquad\qquad \text{jer } r \in \Phi(m) \\ \text{iz } a \equiv_n s,\ \text{НЗД}(s,n) = 1 \Rightarrow \text{НЗД}(a,n) = 1 \\ \qquad\qquad \text{jer } s \in \Phi(n) \end{array}\right\} \Rightarrow \begin{array}{l} \text{НЗД}(a,mn) = 1 \\ \text{tj. } a \in \Phi(mn) \end{array}$$

$$\underbrace{|\Phi(mn)|}_{=\varphi(mn)} = \underbrace{|\Phi(m)|}_{\varphi(m)} \cdot \underbrace{|\Phi(n)|}_{\varphi(n)}$$

$\blacksquare$

$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$$\begin{aligned} \varphi(n) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) &= \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}) \\ &= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \end{aligned}$$

Примери:

$\varphi(10) = \varphi(2\cdot 5) = \varphi(2)\cdot\varphi(5) = 1\cdot 4 = 4$

$\varphi(12) = \varphi(2^2\cdot 3) = \varphi(2^2)\cdot\varphi(3) = (2^2-2^1)\cdot 2 = 2\cdot 2 = 4$

$\varphi(100) = \varphi(2^2\cdot 5^2) = \varphi(2^2)\cdot\varphi(5^2) = (2^2-2^1)\cdot(5^2-5^1) = 2\cdot 20 = 40$

Ојлерова теорема:

Нека је $НЗД(a,n)=1$, тада је $a^{\varphi(n)} \equiv_n 1$.

доказ:

$k=\varphi(n)$

$\Phi(n) = \{r_1, r_2, \dots, r_k\}$ и $НЗД(r_i, n)=1$ за све $i\in\{1,\dots,k\}$

$$\left.\begin{array}{l} НЗД(r_i,n)=1 \\ НЗД(a,n)=1 \end{array}\right\} \Rightarrow НЗД(ar_i,n)=1$$

па $S_n(ar_i)\in\Phi(n)$ $(*)$

Нека је $s_i = S_n(ar_i)$

Показаћемо да је $\Phi(n)=\{s_1,s_2,\dots,s_k\}$

На основу $(*)$ знамо да $s_i\in\Phi(n)$

Довољно је још показати да је $s_i\neq s_j$ за $i\neq j$

Нека је $s_i=s_j$

$S_n(ar_i) = S_n(ar_j)$

$n \mid ar_i - ar_j$

$$\left.\begin{array}{l} n\mid a(r_i-r_j) \\ НЗД(a,n)=1 \end{array}\right\} \Rightarrow n\mid r_i-r_j$$

$$\left.\begin{array}{l} n\mid r_i-r_j \\ 1\leq r_i,r_j<n \\ -n<r_i-r_j<n \end{array}\right\} \Rightarrow \begin{array}{l} r_i-r_j=0 \\ r_i=r_j \\ i=j \end{array}$$

$$\left.\begin{array}{l} ar_1\equiv_n s_1 \\ ar_2\equiv_n s_2 \\ \vdots \\ ar_k\equiv_n s_k \end{array}\right\} \text{помножимо}$$

$$a^k\cdot\underbrace{r_1r_2\cdots r_k}_{X} \equiv_n \underbrace{s_1s_2\cdots s_k}_{X} \Rightarrow a^k\cdot X\equiv_n X$$

да бисмо могли да "скратимо" x треба показати да је $\text{НЗД}(n,x)=1$

$\text{НЗД}(n,r_i)=1$ за све $i\in\{1,\dots,k\}$ $\Rightarrow$ $\text{НЗД}(n, r_1 r_2 \cdots r_k)=1$

$r_i \in \Phi(n)$ $\qquad$ тј. $\text{НЗД}(n,x)=1$

$$a^k x \equiv_n x \quad \Big| : x$$

$$a^k \equiv_n 1$$

$$a^{\varphi(n)} \equiv_n 1$$

$\boxtimes$

<u>Мала Фермаова теорема:</u>

Ако је p просто број, тада је $a^p \equiv_p a$.

<u>доказ:</u>

ако $p \mid a$ $\Rightarrow$ $a^p \equiv_p 0 \equiv_p a$

ако $p \nmid a$, тада је $\text{НЗД}(p,a)=1 \xRightarrow{\text{тј.}}$ Ојлерова

$$a^{\varphi(p)} \equiv_p 1$$

$$a^{p-1} \equiv_p 1 \quad \Big| \cdot a$$

$$a^p \equiv_p a$$

$\boxtimes$

Булове алгебре

- увео их је Џорџ Бул средином XIX века

деф: Булова алгебра је алгебарска структура $\mathbb{B} = (\underset{\substack{\uparrow \\ \text{домен} \\ \neq \emptyset}}{B}, \vee, \wedge, ', \underset{\substack{\text{н.е.} \\ B}}{0}, \underset{\substack{\text{н.е.} \\ B}}{1})$ која задовољава следеће аксиоме:

1° $x \vee y = y \vee x$
2° $x \wedge y = y \wedge x$ } бинарне операције су комутативне

3° $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$
4° $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ } бинарне операције су дистрибутивне

5° $x \vee 0 = x$
6° $x \wedge 1 = x$ } постоје неутрални елементи

7° $x \vee x' = 1$
8° $x \wedge x' = 0$ } постоји комплемент

9° $0 \neq 1$

за свако $x, y, z \in B$.

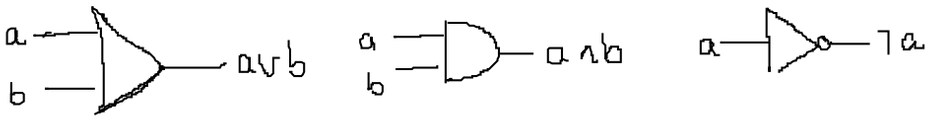
1° Двоелементна Булова алгебра (исказна алгебра)

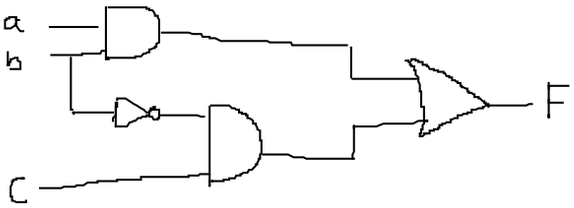
$\mathbf{2} = (\{0,1\}, \vee, \wedge, \neg, 0, 1)$

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

x	$\neg x$
0	1
1	0





← логичка шема

$F = (a \wedge b) \vee (\neg b \wedge c)$ ← одговарајући Булов израз

двоелементна Булова алгебра се још назива и прекидачка алгебра

a	b	c	F
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

$F = (a' \wedge b \wedge c) \vee (a \wedge b' \wedge c) \vee (a \wedge b \wedge c') \vee (a \wedge b \wedge c)$

2° Алгебра скупова

X - произвољан скуп, $X \neq \emptyset$

$B := \mathcal{P}(X)$

$0 := \emptyset$

$1 := X$

$a, b \in \mathcal{P}(X)$

$a \wedge b := a \cap b$

$a \vee b := a \cup b$

$a' := X \setminus a$

$\mathcal{P}(X) = (\mathcal{P}(X), \cup, \cap, ^c, \emptyset, X)$

X може бити коначан и бесконачан

ако је $|X| = n$, $n \in \mathbb{N}$, тада Булова алгебра $\mathcal{P}(X)$ има 2^n елемената

Принцип дуалности

Формуле F_1 и F_2 су дуалне ако се формула F_2 може добити од формуле F_1 тако што се свако појављивање $\wedge$ замени са $\vee$, свако појављивање $\vee$ замени са $\wedge$, свако појављивање 1 замени са 0, и свако појављивање 0 замени са 1.

$x \vee (y \wedge 1)$ ⋮ $x \wedge (y \vee 0)$

$(x' \wedge y) \vee (y' \wedge 0)$ ⋮ $(x' \vee y) \wedge (y' \vee 1)$

$\varphi(\vee, \wedge, ', 0, 1)$ ⋮ $\varphi(\wedge, \vee, ', 1, 0)$ ⇐ дуална формула

↓ исказ — ид. дуални исказ

аксиоме су дуалне и као последица имаћа важи

$\varphi(\vee, \wedge, ', 0, 1)$ је теорема $\Leftrightarrow$ $\varphi(\wedge, \vee, ', 1, 0)$ је теорема

Основни закони Булових алгебри:

1° $x \vee x = x$; $x \wedge x = x$ ⇐ закон идемпотентности

$$x \overset{5°}{=} x \vee 0 \overset{8°}{=} x \vee (x \wedge x') \overset{3°}{=} (x \vee x) \wedge \underbrace{(x \vee x')} \overset{7°}{=} (x \vee x) \wedge 1 \overset{6°}{=} x \vee x$$

$$x \overset{6°}{=} x \wedge 1 \overset{7°}{=} x \wedge (x \vee x') \overset{4°}{=} (x \wedge x) \vee \underbrace{(x \wedge x')}_{0} \overset{8°}{=} (x \wedge x) \vee 0 \overset{5°}{=} x \wedge x$$

2° $x \vee (x \wedge y) = x$; $x \wedge (x \vee y) = x$ ← закон апсорпције

3° ако $x \wedge y = 0$ и $x \vee y = 1 \Rightarrow x = y'$ ← јединственост комплемента

4° $x'' = x$ ← закон инволуције

5° $(x \vee y)' = x' \wedge y'$; $(x \wedge y)' = x' \vee y'$ ← Де Морганови закони

6° $x \vee (y \vee z) = (x \vee y) \vee z$
$x \wedge (y \wedge z) = (x \wedge y) \wedge z$ } закон асоцијативности

Булово уређење

На произвољној Буловој алгебри $B = (B, \vee, \wedge, ', 0, 1)$ можемо увести уређење на следећи начин:

$$x \leq y \iff x \wedge y = x$$

Важи да је $x \wedge y = x$ ако $x \vee y = y$

$\Rightarrow$: нека је $x \wedge y = x$

$$x \vee y = (x \wedge y) \vee y \underset{\substack{\uparrow \\ \text{закон} \\ \text{апсорпције}}}{=} y$$

$\Leftarrow$: нека је $x \vee y = y$

$$x \wedge y = x \wedge (x \vee y) \underset{\substack{\uparrow \\ \text{закон} \\ \text{апсорпције}}}{=} x$$

Према претходном,

$$x \leq y \iff x \wedge y = x \iff x \vee y = y$$

$(B, \leq)$ парцијално уређен скуп!

(Р) $x \leq x$

$x \wedge x = x$ (Т)

$\uparrow$ идемпотенција

(АНТИС) $x \leq y$, $y \leq x \overset{?}{\Rightarrow} x = y$

$\downarrow \qquad \downarrow$

$x \wedge y = x$, $y \wedge x = y$

$x = x \wedge y = y \wedge x = y$

(Т) $x \leq y$, $y \leq z \overset{?}{\Rightarrow} x \leq z$

$x \wedge y = x$
$y \wedge z = y$ } $\Rightarrow x \wedge z = x$

$$x \wedge z = (x \wedge y) \wedge z = x \wedge \underbrace{(y \wedge z)}_{y} = x \wedge y = x$$

$\Rightarrow x \leq z$

У алгебри скупова релација $\leq$ одговара релацији $\subseteq$.

$A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$

Уређење $\leq$ је сагласно са операцијама $\cap, \cup$.

1° ако је $x \leq y$, тада је $x \vee z \leq y \vee z$

$x \wedge y = x$

$(x \vee z) \wedge (y \vee z) = (x \wedge y) \vee z = x \wedge z \Rightarrow x \vee z \leq y \vee z$

2° ако је $x \leq y$, тада је $x \wedge z \leq y \wedge z$

$x \wedge y = x$

$(x \wedge z) \wedge (y \wedge z) = x \wedge y \wedge \underbrace{z \wedge z}_{z} = \underbrace{x \wedge y}_{x} \wedge z = x \wedge z \Rightarrow x \wedge z \leq y \wedge z$

деф: Елемент x Буулове алгебре $B = (B, \vee, \wedge, ', 0, 1)$ је атом уколико $x > 0$ и ако важи: ако постоји $y \leq x$ тада је $y = x$ или $y = 0$.

Нека је $B = (B, \vee, \wedge, ', 0, 1)$ коначна Буулова алгебра, тада важе следеће:

1° Нека је $x \in B$, $x \neq 0$, тада постоји атом $a \in B$ тј. $a \leq x$

ако је x атом $\Rightarrow a = x$

ако x није атом $\Rightarrow$ постоји $x' \in B$ тј. $0 < x' < x$

ако је x' атом $\Rightarrow a = x'$

иначе постоји $x'' \in B$ тј. $0 < x'' < x' < x$

анализирамо x''

настављамо процес

B је коначан скуп па се процес мора завршити у коначно корака

2° Нека је $x \in B$, $x \neq 0$, тада је $x = \bigvee \{a \mid a \in B$ атом и $a \leq x\}$

Нека је $y = \bigvee \{a \mid a \in B$ атом и $a \leq x\}$, показаћемо да је $y = x$

$\{a \mid a \in B$ атом и $a \leq x\} = \{a_1, a_2, \dots, a_k\}$

$y = a_1 \vee a_2 \vee \dots \vee a_k$ и важи $a_i \leq x$ тј. $a_i \wedge x = a_i$ за све $i \in \{1, \dots, k\}$

$y \wedge x = (a_1 \vee a_2 \vee \dots \vee a_k) \wedge x = \underbrace{(a_1 \wedge x)}_{a_1} \vee \underbrace{(a_2 \wedge x)}_{a_2} \vee \dots \vee \underbrace{(a_k \wedge x)}_{a_k} = a_1 \vee a_2 \vee \dots \vee a_k = y$

$\Rightarrow y \leq x$

Тј. $y \neq x$, тј. да је $y < x$

посматрајмо елемент $y' \wedge x$

$y' \wedge x \geq 0$ увек важи

покажимо да је $y' \wedge x > 0$

Ако би било $y' \wedge x = 0$ тада би

$$x \wedge y = (x \wedge y) \vee 0 = (x \wedge y) \vee (x \wedge y') = x \wedge \underbrace{(y \vee y')}_{1} = x \wedge 1 = x \Rightarrow x \leq y \quad ↯$$

Дакле, $y' \wedge x > 0$, па постоји атом $c \in B$ тј. $c \leq y' \wedge x$

$c \leq y' \wedge x \Rightarrow c \wedge y' \wedge x = c$

тада је $c \wedge y' = (c \wedge y' \wedge x) \wedge y' = c \wedge x \wedge \underbrace{y' \wedge y'}_{y'} = c \wedge x \wedge y' = c$

$\Rightarrow c \leq y'$

слично, $c \wedge x = (c \wedge y' \wedge x) \wedge x = c \wedge y' \wedge \underbrace{x \wedge x}_{x} = c \wedge y' \wedge x = c$

$\Rightarrow c \leq x$

Како је $c \leq x$, c је атом $\Rightarrow c = a_i$ за неко $i \in \{1, \dots, k\}$

$$c \wedge y = a_i \wedge (a_1 \vee a_2 \vee \dots \vee a_i \vee \dots \vee a_k) \underset{\text{апсорпција}}{=} a_i = c \Rightarrow c \leq y$$

Закључили смо да је $c \leq y'$ и $c \leq y$.

$c \wedge y' = c$

$c \wedge y = c$

$$c = c \wedge c = (c \wedge y') \wedge (c \wedge y) = c \wedge c \wedge \underbrace{y' \wedge y}_{0} = c \wedge c \wedge 0 = 0 \quad ↯$$

c је атом

Дакле, $x = y$.

Пример:

У алгебри скупова атоми су једночлани скупови (синглетони).

Сваки непразан скуп може се представити као унија синглетона.

Стонова теорема:

За сваку коначну Булову алгебру $B = (B, \vee, \wedge, ', 0, 1)$ постоји скуп X такав да постоји бијекција

$$f: B \to \mathcal{P}(X)$$

За који важи:

за све $x, y \in B$ $\quad f(x \vee y) = f(x) \cup f(y)$

$f(x \wedge y) = f(x) \cap f(y)$

$f(x') = f(x)^c = X \setminus f(x)$.

доказ:

$X := \{a \mid a \in B$ је атом$\}$

$f(x) = \{a \mid a$ је атом и $a \leq x\}$

1° f је хомоморфизам

* $f(x \vee y) = f(x) \cup f(y)$

$a \in f(x \vee y)$ тј. a је атом и $a \leq x \vee y$

$$\left.\begin{array}{l} a \wedge (x \vee y) = a \\ \quad \shortparallel \\ (a \wedge x) \vee (a \wedge y) \end{array}\right\} \Rightarrow (a \wedge x) \vee (a \wedge y) = a$$

$0 \quad a \qquad 0 \quad a$

јер је a атом

па мора важити

$a \wedge x = a$ или $a \wedge y = a$

тј. $a \leq x$ или $a \leq y$

$a \in f(x)$ или $a \in f(y)$

дакле, $a \in f(x) \cup f(y)$

* $f(x \wedge y) = f(x) \cap f(y)$

$a \in f(x \wedge y)$

a је атом и $a \leq x \wedge y \Leftrightarrow a \leq x$ и $a \leq y \Leftrightarrow a \in f(x)$ и $a \in f(y)$

$a \wedge x \wedge y = a$ $\qquad \Leftrightarrow a \in f(x) \cap f(y)$

* $f(x') = X \setminus f(x)$

$a \in f(x')$

a је атом и $a \leq x'$

ако је $a \leq x$ онда је $a = a \wedge a = (a \wedge x') \wedge (a \wedge x) = \underbrace{a \wedge a}_{a} \wedge \underbrace{x' \wedge x}_{0}$

$= a \wedge 0 = 0$ ↯ a је атом

дакле, $a \not\leq x$, па $a \notin f(x)$

$a \in X \setminus f(x)$

2° f је "на"

нека $A \subseteq X$ да ли постоји $x \in B$ тај. $f(x) = A$?

$A \in P(X)$

$x = \bigvee \{a \mid a \in A\}$

$A = \{a_1, \dots, a_k\}$

$x = a_1 \vee a_2 \vee \dots \vee a_k$

$\underline{A \subseteq f(x)}$:

$a \in A \Rightarrow a = a_i$ за неко $i \in \{1, \dots, k\}$

$a_i \wedge x = \underset{=}{a_i} \wedge (a_1 \vee a_2 \vee \dots \vee \underset{=}{a_i} \vee \dots \vee a_k) \underset{\text{антирефлексивност}}{=} a_i$

$\left.\begin{array}{l} a_i \leq x \\ a_i - \text{атом} \\ a_i = a \end{array}\right\} \Rightarrow a \in f(x)$

$\underline{f(x) \subseteq A}$:

нека $b \in f(x)$

b је атом и $b \leq x$

$b \wedge x = b \wedge (a_1 \vee a_2 \vee \dots \vee a_k) = \underset{0 \quad b}{(b \wedge a_1)} \vee \underset{0 \quad b}{(b \wedge a_2)} \vee \dots \vee \underset{0 \quad b}{(b \wedge a_k)} = b$ јер је b атом

па за бар једно $i \in \{1, \dots, k\}$ важи $b \wedge a_i = b \Rightarrow b \leq a_i$

$\left.\begin{array}{l} b \leq a_i \\ b, a_i \text{ атоми} \end{array}\right\} \Rightarrow b = a_i \in A$

3° f је "1-1"

$f(x) = f(y) \overset{?}{\Rightarrow} x = y$

показаћемо да из $f(x) \subseteq f(y) \Rightarrow x \leq y$:

нек, $x \not\leq y$

постоји атом $a \leq x$ и $a \not\leq y$

$\Rightarrow a \in f(x)$ и $a \notin f(y) \Rightarrow f(x) \not\subseteq f(y)$ ↯

Дакле,

$\left.\begin{array}{l} f(x) \subseteq f(y) \Rightarrow x \leq y \\ f(y) \subseteq f(x) \Rightarrow y \leq x \end{array}\right\} \Rightarrow x = y$

$\boxtimes$

Закључујемо:

Коначну Булову алгебру увијек је конструисати само на скупу који има 2^m елемената, $m \in \mathbb{N}$.

<u>Пример</u>:

$\mathbb{B}_1 = (\mathcal{P}(\{a, b\}), \cup, \cap, ^c, \emptyset, \{a, b\})$

$\mathbb{B}_2 = (\underset{\{1,2,3,6\}}{D_6}, \text{НЗС}, \text{НЗД}, \underset{x' = \frac{6}{x}}{\frac{6}{\ }}, 1, 6)$

све уобичајено разлике Булове алгебре које су суштински исте

$\cup$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\{a\}$	$\{a,b\}$	$\{a,b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\{b\}$	$\{a,b\}$
$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$

Нзс	1	2	3	6
1	1	2	3	6
2	2	2	6	6
3	3	6	3	6
6	6	6	6	6

$\emptyset \Leftrightarrow 1$

$\{a\} \Leftrightarrow 2$

$\{b\} \Leftrightarrow 3$

$\{a,b\} \Leftrightarrow 6$

$\cap$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\{a\}$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$
$\{a,b\}$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$

Нзд	1	2	3	6
1	1	1	1	1
2	1	2	1	2
3	1	1	3	3
6	1	2	3	6

A	A^c
$\emptyset$	$\{a,b\}$
$\{a\}$	$\{b\}$
$\{b\}$	$\{a\}$
$\{a,b\}$	$\emptyset$

x	$\frac{6}{x}$
1	6
2	3
3	2
6	1

Исказна логика

Исказна алгебра: $2 = \{0, 1\}$

0 – нетачно

1 – тачно

унарна операција:

	$\neg$
0	1
1	0

бинарне операције

p	q	$\wedge$	$\vee$	$\Rightarrow$	$\Leftrightarrow$	$\uparrow$	$\downarrow$	$\veebar$
1	1	1	1	1	1	0	0	0
1	0	0	1	0	0	1	0	1
0	1	0	1	1	0	1	0	1
0	0	0	0	1	1	1	1	0

$p \veebar q$

$\veebar$ – ексклузивна дисјункција

$p \veebar q$

$\uparrow$ – Шеферова операција

$\downarrow$ – Лукашевичева операција

Језик $\mathcal{L}$ исказне алгебре чине:

* P – пребројив скуп променљивих
* $C = \{\bot, \top\}$ – скуп логичких константи
* логички везници: $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow, \veebar, \uparrow, \downarrow$
* заграде: (,)

формуле језика $\mathcal{L}$:

1° елементи из P и C су формуле

2° ако су A и B формуле, тада су $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \Rightarrow B)$, $(A \Leftrightarrow B)$, $(A \veebar B)$, $(A \uparrow B)$, $(A \downarrow B)$ такође формуле

3° формуле се добијају коначном применом 1° и 2°.

$For\,\mathcal{L}$ – скуп свих формула

$P, C \subseteq For\,\mathcal{L}$

деф: Валуација је пресликавање $v: P \to \{0, 1\}$.

примери:

$P = \{p, q, r\}$

$v_1: \begin{pmatrix} p & q & r \\ 1 & 0 & 1 \end{pmatrix}$ тј. $v_1(p) = 1$, $v_1(q) = 0$, $v_1(r) = 1$

$v_2 : \begin{pmatrix} p & q & r \\ 0 & 0 & 1 \end{pmatrix}$

$p \begin{cases} 0 \\ 1 \end{cases} \quad q \begin{cases} 0 \\ 1 \end{cases} \quad r \begin{cases} 0 \\ 1 \end{cases}$

$2^3 = 8$ различитих валуација

def: Интерпретација или валуацију v је пресликавање $I_v : For\,\mathcal{L} \to \{0,1\}$ тако да је:

1° $I_v(\bot) = 0$, $I_v(\top) = 1$

2° $p \in P$, $I_v(p) = v(p)$

3° $I_v(\neg A) = \neg I_v(A)$

$I_v(A \wedge B) = I_v(A) \wedge I_v(B)$

$I_v(A \vee B) = I_v(A) \vee I_v(B)$

$I_v(A \Rightarrow B) = I_v(A) \Rightarrow I_v(B)$

$I_v(A \Leftrightarrow B) = I_v(A) \Leftrightarrow I_v(B)$

$I_v(A \veebar B) = I_v(A) \veebar I_v(B)$

$I_v(A \uparrow B) = I_v(A) \uparrow I_v(A)$

$I_v(A \downarrow B) = I_v(A) \downarrow I_v(B)$

пример:

$F = (p \wedge q) \Rightarrow (p \wedge r)$

$$I_{v_1}(F) = I_{v_1}(p \wedge q) \Rightarrow I_{v_1}(p \wedge r)$$
$$= (I_{v_1}(p) \wedge I_{v_1}(q)) \Rightarrow (I_{v_1}(p) \wedge I_{v_1}(r))$$
$$= (v_1(p) \wedge v_1(q)) \Rightarrow (v_1(p) \wedge v_1(r))$$
$$= (1 \wedge 0) \Rightarrow (1 \wedge 1) = 0 \Rightarrow 1 = 1$$

$$I_{v_2}(F) = (v_2(p) \wedge v_2(q)) \Rightarrow (v_2(p) \wedge v_2(r))$$
$$= (0 \wedge 0) \Rightarrow (0 \wedge 1) = 0 \Rightarrow 0 = 1$$

def: Нека $F \in For\,\mathcal{L}$. Тада је:

* формула F задовољива ако постоји (бар једна) валуација v у чији $I_v(F) = 1$ (пишемо $v \models F$)
* формула F оборива ако постоји (бар једна) валуација v у чији $I_v(F) = 0$ (пишемо $v \not\models F$)

Ако за све валуације v важи да је $I_v(F) = 1$ кажемо да је F таутологија. (обрнута формула није оборива)

Ако за све валуације v важи да је $I_v(F) = 0$ кажемо да је F контрадикција. (обрнута формула није задовољива)

$\Gamma \subseteq For\mathcal{L}$

скуп Γ је задовољив ако постоји валуација $v: P \to \{0,1\}$ тј. за све $F \in \Gamma$ $I_v(F) = 1$ (пишемо $v \models \Gamma$)

F је логичка (семантичка) последица скупа Γ ($\Gamma \models F$) ако за сваку валуацију v за коју важи $v \models \Gamma$ важи $v \models F$.

<u>деф:</u> формуле A и B су логички (елементарно, семантички) еквивалентне ако $A \models B$ и $B \models A$. (запис $A \equiv B$)

релација $\equiv$ је еквиваленција на скупу $For\mathcal{L}$:

(Р) $A \equiv A$

$A \models A$

(С) $A \equiv B$

$\left.\begin{array}{l} A \models B \\ B \models A \end{array}\right\} \Rightarrow B \equiv A$

(Т) $A \equiv B,\ B \equiv C \overset{?}{\Rightarrow} A \equiv C$

$A \models B,\ B \models C$

нека је v валуација тј. $I_v(A) = 1$

$A \models B$ следи $I_v(B) = 1$

$B \models C$ следи $I_v(C) = 1$ $\Rightarrow A \equiv C$

дакле $A \models C$

слично, како је $B \models A$ и $C \models B$, следи $C \models A$

<u>пример:</u>

$\neg(A \wedge B) \equiv \neg A \vee \neg B$

$For\mathcal{L}/_{\equiv}$ – скуп логички нееквивалентних формула

$[\bot]$ – скуп који садржи све контрадикције (нпр $p \wedge \neg p \in [\bot]$)

$[\top]$ – скуп који садржи све таутологије (нпр $p \vee \neg p \in [\top]$)

$(For\mathcal{L}/_{\equiv}, \wedge, \vee, ', 0, 1)$ је Булова алгебра, тзв. Линденбаум-Тарски алгебра

$[A] \wedge [B] := [A \wedge B]$

$[A] \vee [B] := [A \vee B]$

$[A]' := [\neg A]$

$0 := [\bot]$

$1 := [\top]$

Ако је $|P| = n$, тј. $P = \{p_1, p_2, \dots, p_n\}$ тада постоји 2^n различитих валуација.

$b = 2^n$

	p_1	p_2	...	p_n	F
v_1					0
					1
v_2					0
					1
v_3					0
					1
⋮					
v_b					0
					1

за сваку валуацију бирамо да ли је формула тачна или нетачна за ту валуацију

$$\Rightarrow \left| For\mathcal{L}/_{\equiv} \right| = 2^{2^n}$$

пример:

$P = \{p_1, p_2\}$

	p_1	p_2	F_1	F_2	F_3	...	F_{16}
v_1	1	1	0	1	0		
v_2	1	0	0	0	1		
v_3	0	1	0	0	0		
v_4	0	0	0	0	0		

Конјунктивне и дисјунктивне нормалне форме

Литерал је исказно слово или његова негација.

формула је у КНФ ако је облика

$$A_1 \wedge A_2 \wedge \dots \wedge A_n,$$

где су A_i дисјункције литерала.

пример:

$(p \vee q) \wedge (p \vee \neg q) \wedge (p \vee \neg r) \wedge \neg p$ је у КНФ

формула је у ДНФ ако је облика

$$A_1 \vee A_2 \vee \dots \vee A_n,$$

где су A_i конјункције литерала.

пример:

$(p \wedge \neg q) \vee (q \wedge r) \vee (q \wedge \neg p \wedge \neg r)$ је у ДНФ

Лоше се десити да формула има различите ДНФ, исто важи и за КНФ

$(q \wedge p \wedge r) \vee q \vee r \vee p \equiv p \vee q \vee r$ – различите ДНФ

$F \in For\mathcal{L}$ – произвољна формула

$P(F)$ = скуп свих променљивих које се појављују у формули F

приметимо да је $P(F)$ коначан

Тврдимо:

$$F \equiv \bigvee_{\substack{\vartheta: P(F) \to 2 \\ I_\vartheta(F)=1}} \left(p_1^{\vartheta(p_1)} \wedge p_2^{\vartheta(p_2)} \wedge \dots \wedge p_n^{\vartheta(p_n)} \right)$$ – канонска ДНФ

$$F \equiv \bigwedge_{\substack{\vartheta: P(F) \to 2 \\ I_\vartheta(F)=0}} \left(p_1^{\neg\vartheta(p_1)} \vee p_2^{\neg\vartheta(p_2)} \vee \dots \vee p_n^{\neg\vartheta(p_n)} \right)$$ – канонска КНФ

$p^0 = \neg p$

$p^1 = p$

Нека је $G = \bigvee_{\substack{\vartheta: P(F) \to 2 \\ I_\vartheta(F)=1}} \left(p_1^{\vartheta(p_1)} \wedge p_2^{\vartheta(p_2)} \wedge \dots \wedge p_n^{\vartheta(p_n)} \right)$

желимо да покажемо да је $F \equiv G$.

Примећујемо најпре следеће: $u(p) = \vartheta(p)$ акко $I_u(p^{\vartheta(p)}) = 1$ (*)

$\Rightarrow$: Нека је $u(p) = \vartheta(p)$

ако је $\vartheta(p) = 1$: $I_u(p^{\vartheta(p)}) = I_u(p^1) = I_u(p) = u(p) = \vartheta(p) = 1$

ако је $\vartheta(p) = 0$: $I_u(p^{\vartheta(p)}) = I_u(p^0) = I_u(\neg p) = \neg I_u(p)$

$= \neg u(p) = \neg \vartheta(p) = 1$

$\Leftarrow$: Нека је $I_u(p^{\vartheta(p)}) = 1$

ако је $\vartheta(p) = 1$

$1 = I_u(p) = u(p) \Rightarrow \vartheta(p) = u(p)$

ако је $\vartheta(p) = 0$

$1 = I_u(p^0) = I_u(\neg p) = \neg I_u(p) = \neg u(p) \Rightarrow u(p) = 0 \Rightarrow u(p) = \vartheta(p)$

доказ да је $F \equiv G$:

<u>$G \models F$</u>:

претпостављамо да $\vartheta \models G$, тј. $I_\vartheta(G) = 1$, доказујемо $\vartheta \models F$

$$I_\vartheta(G) = I_\vartheta\left(\bigvee_{I_u(F)=1} \left(p_1^{u(p_1)} \wedge p_2^{u(p_2)} \wedge \dots \wedge p_n^{u(p_n)} \right) \right) = 1$$

$$\bigvee_{I_u(F)=1} I_\vartheta\left(p_1^{u(p_1)} \wedge p_2^{u(p_2)} \wedge \dots \wedge p_n^{u(p_n)} \right) = 1$$

$\Rightarrow$ постоји валуација u тј. $I_u(F) = 1$ и $I_\vartheta\left(p_1^{u(p_1)} \wedge p_2^{u(p_2)} \wedge \dots \wedge p_n^{u(p_n)} \right) = 1$

$I_v(p_1^{u(p_1)}) \wedge I_v(p_2^{u(p_2)}) \wedge \dots \wedge I_v(p_n^{u(p_n)}) = 1$

дакле, за све $1 \leq i \leq n$ $\quad I_v(p_i^{u(p_i)}) = 1$

$\overset{(*)}{\Rightarrow} v(p_i) = u(p_i)$

$\Rightarrow u = v$

$\Rightarrow I_v(F) = I_u(F) = 1$

$\Rightarrow v \models F$

$F \models G$:

нека $v \models F$, тј. $I_v(F) = 1$, доказујемо $v \models G$

за све $1 \leq i \leq n$ $\quad I_v(p_i^{v(p_i)}) = 1$ на основу $(*)$

па је $I_v(p_1^{v(p_1)} \wedge p_2^{v(p_2)} \wedge \dots \wedge p_n^{v(p_n)}) = 1$

$\Downarrow$

због претпоставке за све вредности у којима је формула F тачна

$\Rightarrow I_v(G) = 1 \Rightarrow v \models G$

$\boxtimes$

Пример:

$F = (r \Rightarrow p) \Rightarrow (\neg(q \wedge r) \Rightarrow p)$

КНФ и КДНФ?

	p	q	r	$r \Rightarrow p$ (1°)	$\neg(q \wedge r)$	$\neg(q \wedge r) \Rightarrow p$ (2°)	$F = 1° \Rightarrow 2°$
v_1	1	1	1	1	0	1	1
v_2	1	1	0	1	1	1	1
v_3	1	0	1	1	1	1	1
v_4	1	0	0	1	1	1	1
v_5	0	1	1	0	0	1	1
v_6	0	1	0	1	1	0	$\boxed{0}$
v_7	0	0	1	0	1	0	1
v_8	0	0	0	1	1	0	$\boxed{0}$

КДНФ (узимамо све вредности у којима је формула тачна)

$F \equiv (p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge r)$

ККНФ (узимамо све вредности у којима је формула нетачна)

$F \equiv (p \vee \neg q \vee r) \wedge (p \vee q \vee r)$