Skoro sve što radimo u matematici temelji se, posredno ili neposredno, na pojmu skupa. Pojam skupa je intuitivno jasan: zamišljamo ga kao kolekciju nekih objekata. Termin kolekcija često koristimo kao sinonim za pojam skupa. Međutim, ukoliko na taj način posmatramo skupove, brzo nailazimo na probleme.
Berberinov paradoks: U nekom selu berberin brije sve stanovnike tog sela koji ne briju sami sebe. Postavlja se pitanje da li berberin brije sam sebe?
▶ ako je odgovor ne, dakle berberin ne brije sam sebe, tada je i on jedan od stanovnika sela koji se ne briju sami, pa mora brijati sam sebe, što je protivurečnost
▶ ako je odgovor da, opet dolazimo do protivurečnosti jer berberin brije isključivo ljude iz sela koji se ne briju sami
Paradoks laljivca: Filozof Epimenid (6 vek p.n.e.) sa Krita rekao je "Krićani uvek lažu". Da li je govorio istinu?
Druga verzija paradoksa lažljivca: Inspirisana je pričom o Pinokiju. Postavlja se pitanje šta će se desiti ako Pinokio kaže "Moj nos će sada porasti."?
Greling-Nelsonov paradoks: Postoje neki pridevi koji opisuju sebe, npr. petnaestoslovni, višesložan. . . Reči koje ne opisuju same sebe se zovu heterologičke. Da li je pridev "heterologički" heterologička reqč?
Prethodni primeri su u vezi sa čuvenim Raselovim paradoksom:
Posmatrajmo kolekciju S definisanu sa
$x \in S$ akko $x \not\in x$.
Da li $S \in S$?
▶ ako $S \in S$, na osnovu definicije kolekcije onda $S \not\in S$
▶ ako $S \not\in S$, opet na osnovu definicije kolekcije S zaključujemo da $S \in S$
Zaključak: Ovako definisanu kolekciju S ne možemo smatrati skupom u matematičkom smislu.

Formiranje skupova

Osnovna relacija među skupovima je relacija pripadnosti.
Skup A pripada skupu B zapisujemo sa $A \in B$. Kažemo da je A element od B.
Skupovi se zasnivaju (definišu) aksiomatski.
(Zermelo-Frenkelova (ZF) teorija skupova)

Aksioma ekstenzije

Dva skupa su jednaka ako imaju iste elmente. npr. skupovi $A = \{2, 3\}$ i $B = \{x \in R \mid x2 - 5x + 6 = 0\}$ su jednaki.

Aksioma praznog skupa

Postoji skup koji nema nijedan element.
Ovaj skup nazivamo prazan skup i oznaqavamo ga sa $\emptyset$. Prema aksiomi ekstenzije ovaj skup je jedinstven.

Aksioma para

Za sve skupove x i y postoji skup z čiji su jedini elementi x i y .
Skup z oznaqčavamo sa $z = \{x, y\}$. Važi sledeće:
$u \in \{x, y\}$ akko $u = x$ ili $u = y$.
Možemo formirati skup sa jednim elementom ako uzmeno da je $x = y$.
Prema aksiomi ekstenzije važi $\{x, x\} = \{x\}$.

Aksioma unije

Za svaki skup x postoji skup z tako da $u \in z$ ako i samo ako $u \in y$ za neki $y \in x$. Skup z predstavlja uniju članova skupa x i označavamo ga sa Ux.
Skup $z = Ux$ sastoji se od elemenata elemenata skupa x. Na primer, ako je $x = \{a, b\}$ tada je $z = U\{a, b\} = a \cup b$.

Definicija

Skup a je podskup skupa b, u oznaci $a \subseteq b$, ako za sve $x \in a$ važi da $x \in b$. Npr. skup $\emptyset$ je podskup svakog skupa.
Važi da je $N \subset Z \subset Q \subset R$.

Aksioma partitivnog skupa

Za svaki skup x postoji skup P(x), koji se sastoji od svih podskupova od x. Ako je $x = \{a, b\}$, tada je
$P(x) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.
Ako je $x = \emptyset$, tada je $P(x) = P(\emptyset) = \{\emptyset\}$. Ako X ima n elemenata, kada će P(x) imati 2^n elemenata (kardinalnost).

Aksioma izdvajanja podskupa (separacije)

Za svaki skup a i svaku formulu $\phi(x)$ važi da je $\{x \in a \mid \phi(x)\}$ skup.
Primene aksiome izdvajanja poskupa:
$A \cap B = \{x \in A \mid x \in B\}$ − presek skupova A i B
$A \setminus B = \{x \in A \mid x \not\in B\}$ − razlika skupova A i B
neka $A \subseteq U$, $A^c = \{x \in U \mid x \not\in A\}$ − komplement skupa A u skupu U
Osnovni skupovni identiteti:

1. $(A \cap B) \cap C = A \cap (B \cap C)$
2. $(A \cup B) \cup C = A \cup (B \cup C)$
3. $(A \triangle B) \triangle C = A \triangle (B \triangle C)$
4. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
5. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
6. $A \cap B = B \cap A$
7. $A \cup B = B \cup A$
8. $A \triangle B = B \triangle A$
9. $A \cap A = A$

10. $A \cup A = A$
11. $A \cap (A \cup B) = A$ (apsorbcija)
12. $A \cup (A \cap B) = A$ (apsorbcija)
13. $(A \cap B)^c = A^c \cup B^c$ (de Morganovi zakoni + 14.)
14. $(A \cup B)^c = A^c \cap B^c$
15. $(A^c)^c = A$
16. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
17. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

Dokazivanje identiteta:

$A = B$ akko $A \subseteq B$ i $B \subseteq A$

I 1) $x \in A$ proizvoljno
2) Dokazujemo da $x \in B$

II 1) $x \in B$ proizvoljno
2) Dokazujemo da $x \in A$

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

iz $(A \cap B)$ sledi $x \in A$ i $x \in B$.
iz $(A \cap B) \cap C$ sledi $x \in C$.
iz $x \in B$ i $x \in C$ sledi $x \in B \cap C$
iz $x \in B \cap C$ i $x \in A$ sledi $A \cap (B \cap C)$

iz $x \in A \cap (B \cap C)$ sledi $x \in A$ i $x \in B \cap C$
tj. sledi $x \in A$ i $x \in B$ i $x \in C$
iz $x \in A$ i $x \in B$ sledi $x \in A \cap B$
iz $x \in A \cap B$ i $x \in C$ sledi $x \in (A \cap B) \cap C$

Uređeni par

Tvrđenje: Za skupove a, b, c, d važi:
$\{a, b\} = \{c, d\}$ ako i samo ako $(a = c$ i $b = d)$ ili $(a = d$ i $b = c)$.

Dokaz: Ako važi neki od dva uslova sa desne strane, jasno je da je $\{a, b\} = \{c, d\}$.
S druge strane, pretpostavimo da je $\{a, b\} = \{c, d\}$.
Kako je $a \in \{a, b\}$, to je $a \in \{c, d\}$, pa je $a = c$ ili $a = d$. Neka je prvo $a = c$. Važi $d \in \{c, d\}$, pa $d \in \{a, b\}$, a time i $d = a$ ili $d = b$. Ako je $b = d$ važi desna strana. Ako je $a = d$, imamo da je $a = c = d$. Iz $b \in \{a, b\} = \{c, d\}$ sledi $b = c = d$, pa važi desna strana. Slično se dokazuje i drugi slučaj, kada je $a = d$.

Definicija

Uređeni par (a, b) skupova a i b je skup $\{\{a\}, \{a, b\}\}$.

Tvrđenje Za uređene parove (a, b) i (c, d) važi: $(a, b) = (c, d)$ akko $a = c$ i $b = d$.

Dokaz: Ako važi $a = c$ i $b = d$, onda je $(a, b) = \{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\} = (c, d)$. Naka je sad $(a, b) = (c, d)$.
Onda je $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. Prema prethodnom tvrđenju, važi da je $(\{a\} = \{c\}$ i $\{a, b\} = \{c, d\})$ ili $(\{a\} = \{c, d\}$ i $\{a, b\} = \{c\}.)$
Ako važi prvi deo, mora biti $a = c$. Takođe, važi $(a = c$ i $b = d)$ ili $(a = d$ i $b = c)$. U prvoj slučaju imamo $a = c$ i $b = d$. U drugom slučaju $d = a = c = b$, pa je specijalno i $a = c$ i $b = d$. Ako važi drugi deo, onda je $a = b = c = d$, pa opet važe tražene jednakosti.

Dekartov proizvod dva skupa

Definicija

Dekartov proizvod skupova A i B je skup
$A \times B = \{(a, b) \mid a \in A, b \in B\}$.
npr. Dekartov proizvod skupova $A = \{1, 2, 3\}$ i $B = \{x, y\}$ je
$A \times B = \{(1, x), (1, y), (2, x), (2, y), (3, x), (3, y)\}$.
Kako je $B \times A = \{(x, 1), (x, 2), (x, 3), (y, 1), (y, 2), (y, 3)\}$, vidimo da ne mora važiti jednakost između skupova $A \times B$ i $B \times A$.
napomena: $A \times B = \emptyset$ akko $A = \emptyset$ ili $B = \emptyset$
Osobine Dekartovog prizvoda:
$(A \cup B) \times C = (A \times C) \cup (B \times C)$
$(A \cap B) \times C = (A \times C) \cap (B \times C)$

Dekartov proizvod više skupova

Definicija

Uređena n-torka elemenata $a_1, a_2, \ldots, a_n$ je objekat $(a_1, a_2, \ldots, a_n)$
takav da važi
$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ akko $a_1 = b_1, a_2 = b_2, \ldots, a_n = b_n$.
uređena n-torka može se definisati preko pojma uređenog para:
$(a_1, a_2, \ldots, a_n) := (a_1, (a_2, (\ldots, (a_{n-1}, a_n) \cdots)))$
npr. $(a_1, a_2, a_3) := (a_1, (a_2, a_3))$
$(a_1, a_2, a_3, a_4) := (a_1, (a_2, (a_3, a_4)))$

Definicija

Dekartov proizvod skupova $A_1, A_2, \ldots, A_n$ je skup
$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots a_n \in A_n\}$.

Definicija

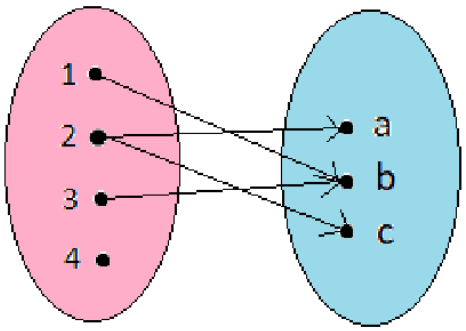
Dekartov stepen skupa A je skup:

$A^n := A \times A \times A \times \ldots \times A$, $n \geq 1$
Specijalno: $A^o := \{\emptyset\}$
Aksioma dobre zasnovanosti(aksioma regularnosti)
Svaki neprazan skup A sadrži element a takav da je $A \cap a = \emptyset$.
Tvrđenje
Ne postoji skup x takav da $x \in x$.
Dokaz. Ako bi skup x bio takav da $x \in x$, tada bi skup $A = \{x\}$ protivurečio aksiomi dobre zasnovanosti (kako $x \in x \cap A$, jedini element skupa A imao bi neprazan presek sa skupom A).

Čas 2
Neformalno rečeno, pojam relacije bavi ostvarivanjem veza između nekih elemenata skupova koje posmatramo.
Definicija: Neka su A i B skupovi. Relacija ρ sa skupa A u skup B je svaki podskup od $A \times B$. Dakle, $\rho \subseteq A \times B$. Ako je A = B onda kažemo da je ρ binarna relacija na skupu A.
Činjenicu da $(a, b) \in \rho$ pixemo i aρb.
Primer: $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$
$\rho = \{(1, b), (2, a), (2, c), (3, b)\}$ je jedna relacija sa skupa A na skup B.
$\sigma = \{(1, 3), (2, 1), (4, 2)\}$ je jedna binarna relacija na skupu A
Različiti načini predstavljanja relacija:
$\rho = \{(1, b), (2, a), (2, c), (3, b)\} \subseteq A \times B$

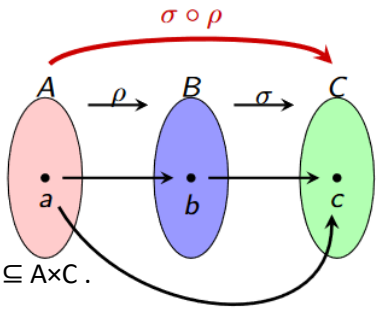
	a	b	c
1	0	1	0
2	1	0	1
3	0	1	0
4	0	0	0

табелари приказ

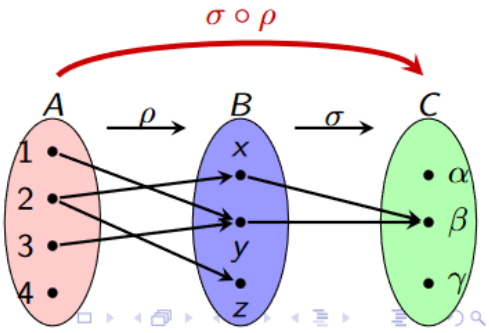


приказ помоћу дијаграма

Domen relacije $\rho \subseteq A \times B$:
$Dom(\rho) = \{a \in A \mid$ postoji $b \in B$ tako da je $(a, b) \in \rho\}$.
Slika relacije $\rho \subseteq A \times B$:
$Im(\rho) = \{b \in B \mid$ postoji $a \in A$ tako da je $(a, b) \in \rho\}$.
Inverzna relacija relacije $\rho \subseteq A \times B$:
$\rho^{-1} = \{(b, a) \in B \times A \mid (a, b) \in \rho\} \subseteq B \times A$.
Kompozicija relacija $\rho \subseteq A \times B$ i $\sigma \subseteq B \times C$:
$\sigma \circ \rho = \{(a, c) \in A \times C \mid$ postoji $b \in B$ tako da $(a, b) \in \rho$ i $(b, c) \in \sigma\} \subseteq A \times C$.



Primer:
$A = \{1, 2, 3, 4\}$, $B = \{x, y, z\}$, $C = \{\alpha, \beta, \gamma\}$
$\rho = \{(1, y), (2, z), (2, x), (3, y)\} \subseteq A \times B$,
$\sigma = \{(x, \beta), (y, \beta)\} \subseteq B \times C$
$Dom(\rho) = \{1, 2, 3\}$ $\rho^{-1} = \{(y, 1), (z, 2), (x, 2), (y, 3)\}$
$Im(\rho) = \{x, y, z\}$
Kompozicija relacija
Primer:
$A = \{1, 2, 3, 4\}$, $B = \{x, y, z\}$
$C = \{\alpha, \beta, \gamma\}$
$\rho = \{(1, y), (2, z), (2, x), (3, y)\} \subseteq A \times B$,
$\sigma = \{(x, \beta), (y, \beta)\} \subseteq B \times C$
$\sigma \circ \rho = \{(1, \beta), (2, \beta), (3, \beta)\}$
$a (\sigma \circ \rho) c$ akko $a \rho b$ i $b \sigma c$ za neko $b \in B$



Osobine inverzne relacije:

Neka su date relacije $\rho, \sigma \subseteq A \times B$ tada važi:

- Ako je $\rho \subseteq \sigma$, onda je $\rho^{-1} \subseteq \sigma^{-1}$.

I $(\rho^{-1})^{-1} = \rho$.

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

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

Dokazi:

I $(\rho^{-1})^{-1} = \rho$
$\rho \in A \times B$
$\rho^{-1} \in B \times A$
$(\rho^{-1})^{-1} \in A \times B$

1. inkluzija
$(a, b) \in (\rho^{-1})^{-1}$
$(b, a) \in \rho^{-1}$
$(a, b) \in \rho$ (na osnovu definicije inverzne relacije važi $(\rho^{-1})^{-1} \subseteq \rho$)

2. inkluzija
$(a, b) \in \rho$
$(b, a) \in \rho^{-1}$
$(a, b) \in (\rho^{-1})^{-1}$ $\rho \subseteq$ važi $(\rho^{-1})^{-1}$

II $(\sigma \cup \rho)^{-1} = \sigma^{-1} \cup \rho^{-1}$
$\sigma \cup \rho \subseteq A \times B$
$(\sigma \cup \rho)^{-1} \subseteq B \times A$
$\sigma^{-1} \subseteq B \times A$
$\rho^{-1} \subseteq B \times A$
$\sigma^{-1} \cup \rho^{-1} \subseteq B \times A$

1. inkluzija
$a \in A, b \in B$
$(b, a) \in (\sigma \cup \rho)^{-1}$
$(a, b) \in (\sigma \cup \rho)$
$(a, b) \in \sigma$ ili $(a, b) \in \rho$
$(b, a) \in \sigma^{-1}$ ili $(b, a) \in \rho^{-1}$
$(b, a) \in \sigma^{-1} \cup \rho^{-1}$

2. inkluzija
$(b, a) \in \sigma^{-1} \cup \rho^{-1}$
$(b, a) \in \sigma^{-1}$ ili $(b, a) \in \rho^{-1}$
$(a, b) \in \sigma$ ili $(a, b) \in \rho$
$(a, b) \in \sigma \cup \rho$
$(b, a) \in (\sigma \cup \rho)^{-1}$

Osobine kompozicije:

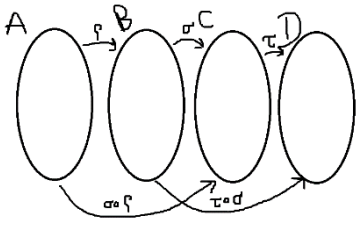
Neka je $\rho \subseteq A \times B$, $\sigma \subseteq B \times C$ i $\tau \subseteq C \times D$, tada važi:

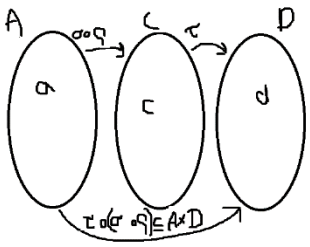
I $(\tau \circ \sigma) \circ \rho = \tau \circ (\sigma \circ \rho)$

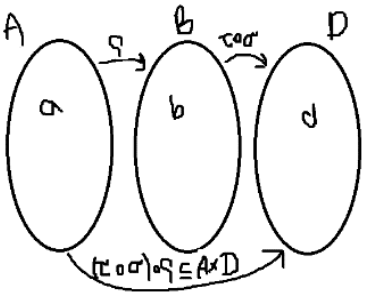
II $(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1}$

Dokazi I i II:

I $(\tau \circ \sigma) \circ \rho = \tau \circ (\sigma \circ \rho)$
$\rho \subseteq A \times B$, $\sigma \subseteq B \times C$, $\tau \subseteq C \times D$
$\tau \circ \sigma \subseteq B \times D$
$\sigma \circ \rho \subseteq A \times C$
1. inkluzija
$a \in A, d \in D$
$(a, d) \in (\tau \circ \sigma) \circ \rho$
postoji $b \in B$ tdj.
$(a, b) \in \rho$
$(b, d) \in \tau \circ \sigma$
postoji $c \in C$ tdj.
$(a, c) \in \sigma \circ \rho$
$(a, d) \in \tau \circ (\sigma \circ \rho)$
2. inkluzija
$\tau \circ (\sigma \circ \rho) \subseteq A \times D$
$a \in A, d \in D$
postoji $c \in C$ tdj.
$(a, c) \in \sigma \circ \rho$
$(c, d) \in \tau$ *
postoji $b \in B$ tdj.
$(a, b) \in \rho$ **
$(b, c) \in \sigma$ *
iz * $(b, d) \in \tau \circ \sigma$ **
iz ** $(a, d) \in (\tau \circ \sigma) \circ \rho$







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

$c \in C, a \in A$
$(c, a) \in (\sigma \circ \rho)^{-1}$ akko $(a, c) \in \sigma \circ \rho$
akko postoji $b \in B$ tdj.
$(a, b) \in \rho$ i $(b, c) \in \sigma$
akko $(b, a) \in \rho^{-1}$ i $(c, b) \in \sigma^{-1}$ onda
$(c, a) \in \rho^{-1} \circ \sigma^{-1}$
$(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1}$

Osobine preseka i unije:

I $\sigma \circ (\rho_1 \cup \rho_2) = (\sigma \circ \rho_1) \cup (\sigma \circ \rho_2)$
$\rho_1, \rho_2 \subseteq A \times B$, $\sigma \subseteq B \times C$
1. inkluzija
$(a, b) \in \rho_1 \cup \rho_2$ i $(b, c) \in \sigma$ za neko $b \in B$
$(a, b) \in \rho_1$ ili $(a, b) \in \rho_2$
slucaj I ako $(a, b) \in \rho_1$ i $(b, c) \in \sigma$, $b \in B$
onda $(a, c) \in \sigma \circ \rho_1$
pa $(a, c) \in (\sigma \circ \rho_1) \cup (\sigma \circ \rho_2)$
slucaj II ako $(a, b) \in \rho_2$ i $(b, c) \in \sigma$, $b \in B$
onda $(a, c) \in \sigma \circ \rho_2$
pa $(a, c) \in (\sigma \circ \rho_1) \cup (\sigma \circ \rho_2)$
2. inkluzija
neka $(a, b) \in (\sigma \circ \rho_1) \cup (\sigma \circ \rho_2)$
$(a, b) \in \sigma \circ \rho_1$ ili $(a, b) \in \sigma \circ \rho_2$
slucaj I $(a, c) \in \sigma \circ \rho_1$
tada $(a,b) \in \rho_1$ i $(b,c) \in \sigma$, $b \in B$
$(a, b) \in \rho_1 \cup \rho_2$ i $(b,c) \in \sigma, b \in B$
$(a, c) \in \sigma \circ (\rho_1 \cup \rho_2)$
slucaj II $(a, c) \in \sigma \circ \rho_2$
tada $(a,b) \in \rho_2$ i $(b,c) \in \sigma$, $b \in B$
$(a, b) \in \rho_1 \cup \rho_2$ i $(b,c) \in \sigma, b \in B$
$(a, c) \in \sigma \circ (\rho_1 \cup \rho_2)$

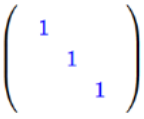
II $\sigma \circ (\rho_1 \cap \rho_2) \subseteq (\sigma \circ \rho_1) \cap (\sigma \circ \rho_2)$
$(a, c) \in \sigma \circ (\rho_1 \cap \rho_2)$
tada $(a, b) \in \rho_1 \cap \rho_2$ i $(b,c) \in \sigma$, za neko $b \in B$
$^1(a, b) \in \rho_1$ i $^2(a, b) \in \rho_2$ i $^{1,2}(b,c) \in \sigma$
iz $^1(a,c) \in \sigma \circ \rho_1$
iz ^{2} $(a,c) \in \sigma \circ \rho_2$
pa $(a, c) \in (\sigma \circ \rho_1) \cap (\sigma \circ \rho_2)$

Obrnuta inkluzija u opstem slucaju ne vazi
$A = \{a\}$, $B = \{b_1, b_2\}$, $C = \{c\}$
$\rho_1 = \{(a, b_1)\}$, $\rho_2 = \{(a, b_2)\}$
$\sigma = \{(b_1, c), (b_2, c)\}$
$\sigma \circ \rho_1 = \{(a, c)\}$ i $\sigma \circ \rho_2 = \{(a, c)\}$
tj $(\sigma \circ \rho_1) \cap (\sigma \circ \rho_2) = \{(a, c)\}$
$\rho_1 \cap \rho_2 = \emptyset \Rightarrow \sigma \circ (\rho_1 \cap \rho_2) =$

Definicija
Neka je ρ binarna relacija na skupu A. Kažemo da je ρ
- refleksivna, ako je $(a, a) \in \rho$ za svako $a \in A$;
- antirefleksivna, ako je $(a, a) \notin \rho$ za svako $a \in A$;
- simetrična, ako za sve $a, b \in A$ iz $(a, b) \in \rho$ sledi $(b, a) \in \rho$;
- antisimetrična, ako za sve $a, b \in A$ iz $(a, b) \in \rho$ i $(b, a) \in \rho$ sledi da je $a = b$;
- tranzitivna, ako za sve $a, b, c \in A$ iz $(a, b) \in \rho$ i $(b, c) \in \rho$ sledi da $(a, c) \in \rho$.

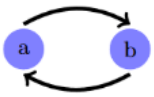
Neka je $\triangle A = \{(a, a) \mid a \in A\}$, relacija ρ je
- refleksivna, ako je $\triangle A \subseteq \rho$;
- antirefleksivna, ako je $\triangle A \cap \rho = \emptyset$;
- simetrična, ako je $\rho \subseteq \rho{-}1$;
- antisimetrična, ako je $\rho \cap \rho{-}1 \subseteq \triangle A$;
- tranzitivna, ako je $\rho \circ \rho \subseteq \rho$.

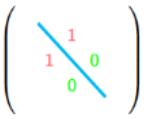
Рефлексивност:



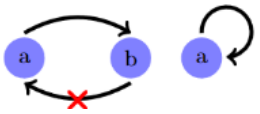
Антирефлексивност:

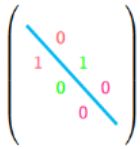
Симетричност:





Антисиметричност:





Примери:

	$\leq$ на $\mathbb{R}$	паралелност правих на скупу правих у простору	нормалност правих на скупу правих у простору
рефлексивност	да	да	не
антирефлексивност	не	не	да
симетричност	не	да	да
антисиметричност	да	не	не
транзитивност	да	да	не

≤ na R
R) $x \leq x$ važi AR) $x \not\leq x$, $x > x$ netačno S) $x \leq z \Rightarrow y \leq x$, $1 \leq 2$ ali $2 \not\leq 1$ AS) $x \leq y$, $y \leq x \Rightarrow x = z$ važi T) $x \leq y$, $y \leq z \Rightarrow x \leq z$ važi
Paralelnost pravih na skupu pravih u prostoru:
R) $a \| a$ T AR) $a \not\| a$ netačno S) $a \| b \Rightarrow b \| a$ T AS) $a \| b$, $b \| a \Rightarrow a = b$ netačno T) $a \| b$, $b \| c \Rightarrow a \| c$ T

Normalnost pravih u prostoru

R) $a \perp a$ netačno AR) $a\ !\perp a$ T S) $a \perp b \Rightarrow b \perp a$ T AS) $a \perp b, b \perp a \Rightarrow a=b$ netačno T) $a \perp b, b \perp c \Rightarrow a \perp c$ netačno

$A = \{a, b, c\}$
$\sigma = \{(a, c), (b, a)\} \subseteq A^2$
$\sigma^{-1} = \{(c, a), (a, b)\}$
$\sigma \circ \sigma = \{(b, c)\}$
$\rho = \{(a, a), (b, b), (a, b), (b, a)\} \subseteq A^2$
$\rho^{-1} = \{(a,a), (b,b), (b,a), (a,b)\}$
$\rho \circ \rho = \{(a,a), (b,b), (a, b), (b,a)\}$

	ρ	σ
рефлексивност	не	не
антирефлексивност	не	да
симетричност	да	не
антисиметричност	не	да
транзитивност	да	не

Ispitujemo ρ

R) $\Delta A = \{(a,a), (b,b), (c,c)\}$
$\Delta A \subseteq \rho$ Netačno (c,c ne pripada ρ)
AR) $\Delta A \cap \rho = \emptyset$ netačno
$\Delta A \cap \rho = \{(a,a), (b,b)\}$
S) $\rho \subseteq \rho^{-1}$ tačno
AS) $\rho \cap \rho^{-1} \subseteq \Delta A$
$\rho \cap \rho^{-1} = \rho = \rho^{-1} \neq \Delta A$
T) $\rho^2 \subseteq \rho$ tačno

Ispitujemo σ

R) $\Delta A \subseteq \sigma$ Netačno
AR) $\Delta A \cap \sigma = \emptyset$ Tačno
S) $\sigma \subseteq \sigma^{-1}$ netačno
AS) $\sigma \cap \sigma^{-1} \subseteq \Delta A$
$\sigma \cap \sigma^{-1} = \emptyset \subseteq \Delta A$
T) $\sigma^2 \subseteq \sigma$ Netačno

Neka $R, S \in Mn(\{0, 1\})$. Bulov proizvod matrica $R = [rij]_{i,j=1,n}$ i $S = [sij]_{i,j=1,n}$, u oznaci $R \otimes S$, je matrica $T = [tij]_{i,j=1,n}$ takva da je

$t_{ij} = (r_{i,1} \wedge s_{1,j}) \vee (r_{i,2} \wedge s_{2,j}) \vee \cdots \vee (r_{i,n} \wedge s_{n,j})$,

pri čemu su binarne operacije $\wedge, \vee : \{0, 1\} \times \{0, 1\} \to \{0, 1\}$
definisane na sledeći način:

∧	0	1
0	0	0
1	0	1

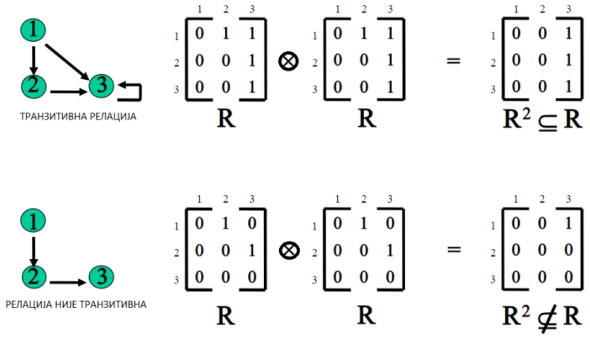
∨	0	1
0	0	1
1	1	1

Matricu relacije ρ označavaćemo sa M_ρ.

<u>Tvrđenje</u> Neka je ρ binarna relacija na proizvoljnom skupu A, tada je $M_{\rho\circ\rho} = M_\rho \otimes M_\rho$.

Dokaz: $A = \{a_1, a_2, ..., a_n\}$
$\rho \subseteq A^2$
$M_\rho^2 = M_\rho \otimes M_\rho$
$[M_\rho]_{ij} = m_{ij}$
$m_{ij} = 1$ akko $a_i \rho a_j$
Dokazujemo da je $[M_\rho^2]_{ij} = [M_\rho \otimes M_\rho]_{ij}$
1. $[M_\rho^2]_{ij} = 1 \Rightarrow a_i$ u relaciji ρ^2 sa a_j tj $a_i \rho^2 a_j \iff (a_i, a_j) \in \rho^2$
$\Rightarrow$ postoji $k \in \{1, 2, ..., n\}$ takav da $a_i \rho a_k$ i $a_k \rho a_j$
$\Rightarrow m_{ik} = 1, m_{ij} = 1$
$\Rightarrow [M_\rho \otimes M_\rho]_{ij} = (m_{i1} \wedge m_{1j}) \vee (m_{i2} \wedge m_{2j}) \vee ... \vee (m_{ik} \wedge m_{kj}) \vee ... \vee (m_{in} \wedge m_{nj}) = 1$ zbog $(m_{ik} \wedge m_{kj}) = 1 \wedge 1 = 1$
2. $[M_\rho^2]_{ij} = 0 \Rightarrow a_i$ nije $\rho^2 a_j$
$\Rightarrow$ ne postoji $k \in \{1, 2, ..., n\}$ takav da $a_i \rho a_k$ i $a_k \rho a_j$
$\Rightarrow$ ne postoji k za koje važi $m_{ik} = 1, m_{ij} = 1$
$\Rightarrow (m_{i1} \wedge m_{1j}) \vee (m_{i2} \wedge m_{2j}) \vee ... \vee (m_{ik} \wedge m_{kj}) \vee ... \vee (m_{in} \wedge m_{nj}) = 0 \vee 0 \vee ... \vee 0 \vee 0 = 0$
ρ je tranzitivna akko $\rho^2 \subseteq \rho$
$[M_\rho^2]_{ij} = 1 \Rightarrow [M_\rho]_{ij} = 1$ tj $(a_i, a_j) \in \rho^2 \Rightarrow (a_i, a_j) \in \rho$

Транзитивност и матрица релације



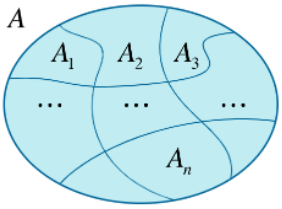
Dokaz: ρ◦ρ ⊆ ρ, tranzitivnost
pretpostavimo ρ je tranzitivna, dokazujemo
(a, b) ∈ ρ◦ρ => postoji c ∈ A tdj (a, c) ∈ ρ i (c, b) ∈ ρ
=> s obzirom da je ρ tranzitivna onda (a, b) ∈ ρ
Pretpostavimo da ρ◦ρ ⊆ ρ, dokazujemo
ρ je tranzitivna => (a, b) ∈ ρ i (b, c) ∈ ρ } (a, c) ∈ ρ◦ρ ⊆ ρ tj. (a, c) ⊆ ρ

Definicija Neka je ρ binarna relacija na skupu A. Kažemo da je ρ relacija ekvivalencije, ako je refleksivna, simetrična i tranzitivna. Relacija ρ je relacija ekvivalencije na skupu A akko važi
△A ⊆ ρ, $\rho = \rho^{-1}$, ρ ◦ ρ = ρ.
$\rho^{-1} \subseteq \rho$?
(y, x) ∈ ρ^{-1} => (x, y) ∈ ρ ⊆ ρ^{-1} => (x, y) ∈ ρ^{-1} => (y, x) ∈ ρ
ρ ◦ ρ = ρ ?
ρ je relacija ekvivalencije => ρ ◦ ρ = ρ iz ΔA⊆ ρ , $\rho = \rho^{-1}$, ρ ◦ ρ ⊆ ρ
Dokazujemo ρ ⊆ ρ ◦ ρ akko je ρ relacija ekvivalencije.
(x, y) ∈ ρ 1)
(y, y) ∈ ρ iz refleksivnosti 2) Iz 1 i 2 (x, y) ∈ ρ ◦ ρ
Primeri relacija ekvivalencije:
- Relacija jednakosti realnih brojeva.
- Relacija sliqnosti u skupu trouglova euklidske ravni.
- Neka je m ≥ 2. Relacija ≡m definisana na skupu Z sa:
x $\equiv_m$ y akko m | x – y je relacija ekvivalencije.

R) x $\equiv_m$ x ? m|x-x T
S) x $\equiv_m$ y y $\equiv_m$ x ?
m|x-y => m|y-x
x – y = m*k y-x
= m*k*(-1) T

T) x $\equiv_m$ y i y $\equiv_m$ z } x $\equiv_m$ z
m|x-y m|y-z } m|x-z?
x-y = k_1 * m ; y-z = k_2*m
m|m*(k_1 + k_2) T

Klase ekvivalencije
A – skup ljudi koji žive u jednoj državi X
A1, A2, . . . , An – skup gradova države X
Na skupu A definisana je relacija ∼⊆ A2 na sledeći način:
P1 ∼ P2 akko osoba P1 živi u istom gradu kao i osoba P2.



Definicija
Neka je ∼ relacija ekvivalencije na skupu A. Klasa ekvivalencije elementa a ∈ A je skup
C_a = {x ∈ A | a ∼ x} ⊆ A.
Označavamo je i sa [a] i kažemo da je element a predstavnik klase C_a.
∼ – relacija ekvivalencije na skupu A
Osobine relacije ∼:
1. Sve klase ekvivalencije su neprazni skupovi tj a ρ a pa je $C_a \neq \emptyset$
2. Neka je a, b ∈ A. Ako je Ca ∩ Cb=/= ∅, onda je Ca = Cb .

3. Unija svih klasa ekvivalencije je jednaka skupu A.
Dokaz:

1. $a \in A$
$C_a \neq \emptyset$
$\sim$ je refleksivna
$a \sim a \Rightarrow a \in C_a$
$C_a \neq \emptyset$ Tačno
2. $a, b \in A$
$C_a \cap C_b \neq \emptyset$
$\Rightarrow C_a = C_b$
Klase su disjunktne ili jednake

$C_a \cap C_b \neq \emptyset$ postoji $d \in A$ tdj
$d \in C_a \cap C_b$
$\Rightarrow d \in C_a$ i $d \in C_b$
$\Rightarrow a \sim d$ i $b \sim d$
tj. $d \sim b$ zbog S
$\Rightarrow a \sim b$ T
3. $C_a \subseteq C_b$
$x \in C_a \Rightarrow a \sim x$
zbog S $x \sim a$

iz 2) $a \sim b$
iz prethodna dva sledi zbog T
$x \sim b \overset{S}{\Rightarrow} b \sim x \Rightarrow x \in C_b$ Tacno
$C_b \subseteq C_a$
$x \in C_b \Rightarrow b \sim x$
zbog S $x \sim b$
iz 2) $a \sim b$
iz prethodna dva sledi zbog T
$a \sim x \overset{S}{\Rightarrow} x \sim a \Rightarrow x \in C_a$ Tacno

Osobine klasa:
I $a \rho b$ akko $C_a = C_b$
1. inkluzija Neka je $C_a = C_b$
$a \in C_a$, $C_a \subseteq C_b$ tj $a \in C_b$, a tada je $a \rho b$

2. inkluzija neka je $a \rho b$
$\underline{C_a \subseteq C_b}$
$x \in C_a \Rightarrow x \rho a$
$x \rho a$ i $a \rho b \overset{T}{\Rightarrow} x \rho b$ tj $x \in C_b$

$\underline{C_b \subseteq C_a}$
$x \in C_b \Rightarrow b \rho x$
$b \rho x$ i $a \rho b \overset{T}{\Rightarrow} a \rho x$ tj $x \in C_a$

II a nije ρ b akko $C_a \cap C_b = \emptyset$
1. inkluzija
Neka $C_a \cap C_b = \emptyset$
Kako su $C_a, C_b \neq \emptyset$ sledi da je $C_a \neq C_b$ pa a nije ρ b

2. inkluzija a nije ρ b
Pretpostavimo suprotno
$C_a \cap C_b \neq \emptyset$
tada postoji $x \in C_a \cap C_b$
$*x \in C_a \Rightarrow a \rho x$

$*x \in C_b \Rightarrow b \rho x$ pa i $x \rho b$
iz $* \overset{T}{\Rightarrow} a \rho b$ tj. $C_a = C_b$
Kontradikcija

<u>Definicija</u>
Količnički skup skupa A za relaciju ekvivalencije $\sim$ je
$A/\sim = \{Cx \mid x \in A\}$.
Primetimo da je $A/\sim \subseteq P(A)$, jer važi da je $Ca \subseteq A$, za sve $a \in A$.

Особине количничког скупа:

1. Ако $X, Y \in A/_\sim$ и $X \neq Y$, тада је $X \cap Y = \emptyset$.
2. Важи да је $\bigcup A/_\sim = \bigcup_{X \in A/_\sim} X = A$.

Dokazi:

1. neka $X, Y \in A/\sim$ i $X \neq Y$
tada je $x = C_a$ i $Y = C_b$ za neke $a,b \in A$
Kako je $C_a \neq C_b$ sledi $C_a \cap C_b = \emptyset$
tj $X \cap Y = \emptyset$

2. U $A/\sim = UX = A$, $(X \in A/\sim)$
1. inkluzija
Neka $X \in A/\sim$
tada $x \in X$
Vazi da je $X = C_a$ za neko $a \in A$

pa je $x \in C_a \subseteq A$
Dakle $x \in A$.
2. inkluzija
Tada $x \in C_x$, a $X_x \in A/\sim$ pa $x \in UA/\sim$

<u>Definicija</u>: Svaka relacija ekvivalencije deli skup na kome je definisana na neprazne, disjunktne skupove čija unija je jednaka celom skupu. Takva podela se naziva particija skupa. Particija skupa A je bilo koji podskup $P \subseteq P(A)$ koji zadovoljava sledeće uslove:
1. Ako $X, Y \in P$ i $X \neq Y$, važi $X \cap Y = \emptyset$
2. $UP = A$
3. Za svako $X \in P$ važi $X \neq \emptyset$
Na osnovu osobina $A/\sim$ zaključujemo da je $A/\sim$ particija skupa A.
Primer: Odrediti sve particije skupa $A = \{1, 2, 3\}$
$P_1 = \{\{1, 2, 3\}\}$ $P_2 = \{\{1\}, \{2, 3\}\}$ $P_3 = \{\{1, 2\}, \{3\}\}$ $P_4 = \{\{1, 3\}, \{2\}\}$ $P_5 = \{\{1\}, \{2\}, \{3\}\}$
Dakle na skupu A postoji 5 particija.
Tvrđenje: Neka je P particija na skupu A. Definišimo binarnu relaciju ρ na skupu A na sledeći način:
$a \rho b$ akko $a, b \in X$ za neko $X \in P$

Tada:
1. ρ je ekvivalencija na A
2. A/ρ = P
Dokazi:

1. (R) a ρ a za svako a∈A?
a∈A tada a∈UP tj a∈X za neko X∈P
a, a∈X => a ρ a Tacno
(S) a ρ b $=^{?}>$ b ρ a
a ρ b tada a, b∈X gde X∈P pa b ρ a
(T) a ρ b i b ρ c Da li a ρ c?

Kako a ρ b => a,b ∈ X gde X∈P
b ρ c => b, c ∈ Y gde Y∈P.
Dakle b ∈ X ∩ Y pa X∩Y ≠ ∅
Odnosno po definiciji particije
X = Y a, c ∈ X i X∈P pa sledi
a ρ c Tacno Jeste rel. ekviv

2. A/ρ = P
I inkluzija Neka X ∈ A/ρ = P
tada X = C_a za neko a ∈ A
kako je a ∈ A = UP to a ∈ X'
gde X' ∈ P
Dokazujemo C_a = X'
inkl 1.1 Neka x ∈ C_a tj x ρ a
x, a ∈ Y gde Y∈P
kako a∈Y∩X' to X' = Y pa x∈X'
inkl 1.2 neka x∈X'
tada a,x ∈ X' i X∈P pa a ρ x
tj x∈ C_a
Dakle X = C_a = X' ∈ P

II inkluzija Neka je X∈ P
Tada X ≠ ∅ pa biramo a∈X
Dokazujemo da je X = C_a
inkl 2.1 Neka x ∈ X
kako a,x ∈X sledi da je
a ρ x pa x∈C_a
inkl 2.2 Neka x∈C_a tj x ρ a
kako x ρ a, sledi x,a ∈ Z gde Z ∈P
a ∈X∩Z , X, Z ∈ P pa X = Z
Dakle x ∈ Z = X
Zakljucujemo, X = C_a ∈ A/ ρ

Pr.1: A = Z, $\equiv_m$, m ≥ 2
x $\equiv_m$ y akko m|x-y
Pokazali smo da jeste
relacija ekvivalencije.
a ∈ Z, C_a = ?
x $\equiv_m$ a akko m|x-a
akko za svako z ∈ Z tdj x-a = m*z
<=> x = a+m*z

x ∈ a+m*Z := {a + mz| z∈Z}
C_a = a+mZ
C_o = m*z = C_m = C_{2m} = C_{-5m} =...
C_1 = 1+mz
C_2 = 2+mz
C_{m-1} = (m-1) + mz
Ukupno imamo m klasa
Z/$\equiv_m$ = {mZ, 1+ mz, ..., (m-1)+mz} sadrzi skupove

Pr. 2: A = R^2, ρ⊆ $R^2 \times R^2$
(x_1, y_1) ρ (x_2, y_2) akko $x_1^2 + y_1^2 = x_2^2 + y_2^2$
Da li je relacija ekvivalencije?
R) (x, y) ρ (x, y)
$x^2 + y^2 = x^2 + y^2$ Jeste
S) (x_1, y_1) ρ (x_2, y_2) $=^{?}>$ (x_2, y_2) ρ (x_1, y_1)
$x_1^2 + y_1^2 = x_2^2 + y_2^2$ $=^{?}>$ $x_2^2 + y_2^2 = x_1^2 + y_1^2$ Jeste
T) [1] (x_1, y_1) ρ (x_2, y_2)
[2] (x_2, y_2) ρ (x_3, y_3)
Da li sledi (x_1, y_1) ρ (x_3, y_3)?

[1] $x_1^2 + y_1^2 = x_2^2 + y_2^2$
[2] $x_2^2 + y_2^2 = x_3^2 + y_3^2$
iz [1] i [2] $x_1^2 + y_1^2 = x_3^2 + y_3^2$ Jeste
(a, b) ∈ R^2
$C_{(a, b)}$ = ?
(x, y) ∈ $C_{(a, b)}$ akko (x, y) ρ (a, b)
akko $x^2 + y^2 = a^2 + b^2$
$r^2 := a^2 + b^2$
akko $x^2 + y^2 = r^2$
Dakle $C_{(a,b)}$ = {(x,y) ∈ R^2 | $x^2 + y^2 = r^2$}

Kruznica sa centrom (0,0)
$(x,y) \in C_{(0,0)}$ akko $(x,y)\ \rho\ (0,0)$
akko $x^2 + y^2 = 0$
akko $x = 0$ i $y = 0$
$C_{(0,0)} = \{(0, 0)\}$

$(x, y) \in C_{(3,4)}$ akko $(x,y)\ \rho\ (3,4)$
$x^2 + y^2 = 3^2 + 4^2 = 5^2$
$C_{(3,4)} = k((0,0), 5)$
$R^2/\rho = \{k(O, r) \mid r \in R \text{ i } r \geq 0\}$

Pr.3: $A=\{0, 1, 2\}$
$B = A \times A = A^2$
$\rho \subseteq B^2$
$(x_1, y_1)\ \rho\ (x_2, y_2)$ akko $x_1y_1 = x_2y_2$
ρ je ekvivalencija:
(R) $(x, y)\ \rho\ (x, y)$
$xy = xy$ Tacno
(S) $(x_1, y_1)\ \rho\ (x_2, y_2) =^{?}> (x_2, y_2)\ \rho\ (x_1, y_1)$
$x_1y_1 = x_2y_2 =^{?}> x_2y_2 = x_1y_1$ Tacno
(T) $^1(x_1, y_1)\ \rho\ (x_2, y_2)$
$^2(x_2, y_2)\ \rho\ (x_3, y_3)$
Da li sledi $(x_1, y_1)\ \rho\ (x_3, y_3)$
$^1x_1y_1 = x_2y_2$

$^2x_2y_2 = x_3y_3$
tj $x_1y_1 = x_3y_3$ Tacno
$C_{(a,b)} \in B$?
$(x, y) \in C_{(a,b)}$ akko $(x,y)\ \rho\ (a,b)$
akko $xy = ab$, ab je fiksirano
$C_{(0,0)} = \{ (x, y) \in B \mid xy = 0\}$
$= \{(0, 0), (0, 1), (0, 2), (1, 0), (2, 0)\}$
$= C_{(0, 1)} = C_{(0,2)} = C_{(1,0)} = C_{(2,0)}$
$C_{(1,1)} = \{ (x,y) \in B \mid xy = 1\} = \{(1,1)\}$
$C_{(1,2)} = \{ (x,y) \in B \mid xy = 2\} = \{(1,2), (2,1)\} = C_{(2,1)}$
$C_{(1,1)} = \{ (x,y) \in B \mid xy = 4\} = \{(2,2)\}$
$B/\rho = \{ (0, 0), (0, 1), (0, 2), (1, 0), (2, 0) \}, \{ (1,1) \}, \{ (1,2), (2,1) \}, \{ (2, 2) \} \}$

Čas 4. Relacije poretka

<u>Definicija</u>

Neka je ρ binarna relacija na skupu A. Kažemo da je ρ relacija parcijalnog uređenja ili poretka, ako je refleksivna, antisimetrična i tranzitivna.

Skup A na kome je definisana relacija parcijalnog uređenja ρ nazivamo parcijalno uređen skup ili poset.

Relacija ρ je relacija poretka na skupu A ako i samo ako važi:

$\triangle A \subseteq \rho$

$\rho \cap \rho^{-1} = \triangle A$

$\rho \circ \rho = \rho$.

Primeri relacija parcijalnog uređenja:

1. Relacija manje ili jednako na skupu realnih brojeva: $\leq$.
2. Relacija deljivosti na skupu prirodnih brojeva: $|$.
3. Relacija inkluzije na partitivnom skupu nekog skupa: $\subseteq$.

Dokaz 2:
$m|n$ akko postoji $k \in Z$ tkd $n = m*k$
$|$ je poredak na N
R) $m|m$
$m = 0$ tada je $0=0*k$, $k \in N$ vazi
antis) $m|n$ i $n|m =^{?}> m = n$?
$n = k*m$
$m = k'*n$, k i $k' \in N$
$n = k*k'*n \Rightarrow n(1-k*k') = 0$

$n = 0$ ili $kk' = 1$
akko je $n = 0 \Rightarrow m = k'*0 = 0 \Rightarrow m=n$
akko je $kk' = 1$ kako su k i $k' \in N$
onda $k=k'=1 \Rightarrow m=n$
T) $m|n$ i $n|l =^{?}> m = n$
$n = k*m$
$l = k'*n$ $k, k' \in N$
$\Rightarrow l = k'*k*m$ tj $m|l$ tacno

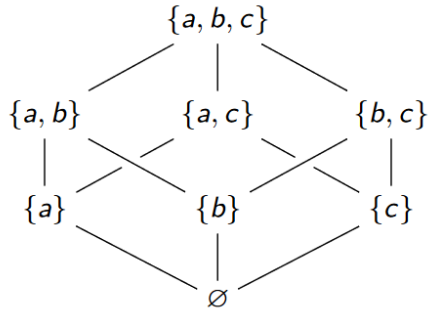
Dokaz 3:

$\subseteq$ je predak na $P(X)$ – X proizvoljan skup
R) $Y \in P(X)$
$Y \subseteq Y$ Tacno

Antis) $Y_1 \subseteq Y_2$ i $Y_2 \subseteq Y_1 \Rightarrow Y_1 = Y_2$ Tacno
T) $Y_1 \subseteq Y_2$, $Y_2 \subseteq Y_3 \Rightarrow Y_1 \subseteq Y_3$

Neka je $\rho \subseteq A^2$ poredak. Elementi a i b su uporedivi ako važi a ρ b ili b ρ a. U suprotnom, a i b su neuporedivi.
a ρ b čitamo: a je ρ-manje od b, odnosno, b je ρ-veće od a.
Poredak je linearan (totalan) ako su svaka dva elementa uporediva. Ukoliko nisu svaka dva elementa uporediva, poredak je parcijalan. Linearno uređen podskup nekog parcijalno uređen skup naziva se lanac. Podskupove parcijalno uređenog skupa u kojima su svaka dva elementa neuporediva nazivamo antilanci.
Primeri:
1. ≤ je linearan poredak na R, za sve a, b ∈ R važi a≤b ili b≤a.
2. | nije linearan poredak na N, skup $\{2^n \mid n \in N\}$ je jedan lanac na N
Npr 2∤3 i 3∤2, 2 i 3 nisu uporedivi
3. ⊆ nije linearan poredak na P(X), za proizvoljan skup X , skup svih jednočlanih podskupova od X je jedan antilanac u P(X)

Npr: X = {1,2} tada {1}, {2} ∈ P(X) => {1} /⊆ {2} i {2}/⊆{1} {1} i {2} su neuporedivi elementi.
Parcijalno uređeni skupovi mogu se predstaviti grafički pomoću Haseovog dijagrama. Ako je A skup na kome je dato parcijalno uređenje ρ, Haseov dijagram poseta A formira se na sledeći način:
- svakom elementu skupa A odgovara jedna tačka u ravni;
- tačke koje odgovaraju elementima x, y ∈ A su spojene linijom ako i samo ako je xρy , pri čemu se x nalazi niže na crtežu od y.
Primer: Neka je X = {a, b, c}. Skup P(X) uređen je relacijom ⊆ i u odnosu na ovu relaciju predstavlja se pomoću Haseovog dijagrama na sledeći način:



Definicija
Neka je ρ relacija parcijalnog poretka na skupu A i neka je B ⊆ A.
Kažemo da je a ∈ A:
- minimalan element skupa B ako a ∈ B i vaći: ako je x ρ a, onda je x = a, za sve x ∈ B;
- maksimalan element skupa B ako a ∈ B i važi: ako je a ρ x, onda je x = a, za sve x ∈ B;
- najmanji element (minimum) skupa B ako a ∈ B i za sve x ∈ B važi a ρ x;
- najveći element (maksimum) skupa B ako a ∈ B i za sve x ∈ B važi x ρ a.

	$\mathcal{P}(\{1,2,3\}), \subseteq$	$\mathcal{P}(\{1,2,3\}) \setminus \{\emptyset\}, \subseteq$	$\mathrm{N}, \mid$	$\mathrm{N} \setminus \{1\}, \mid$
минимум	$\emptyset$	нема	1	нема
максимум	$\{1,2,3\}$	$\{1,2,3\}$	0	0
минимални елемент(и)	$\emptyset$	$\{1\},\{2\},\{3\}$	1	прости бројеви
максимални елемент(и)	$\{1,2,3\}$	$\{1,2,3\}$	0	0

Važi sledeće:

1. Ako postoji najmanji element skupa B, onda je on jedinstven.
b i b' su minimumi skupa B; Vazi sledece b ρ b' jer je b minimum i b' ρ b jer je b' minimum
ρ je antisimetricna relacija pa je b = b'

2. Ako postoji najmanji element skupa B, tada i jedini minimalan element.

b je minimalan element u B
Neka x ρ b za neko x ∈ B
b ρ x jer je b najmanji
Zbog antisim. x = b
tj b je minimalan

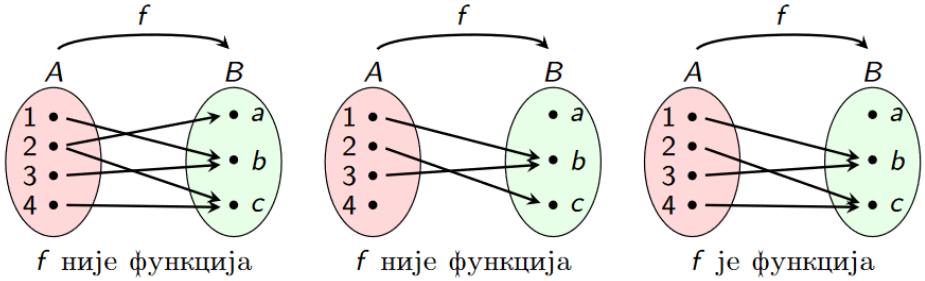
b je jedini minimalan element u B
pps neka je b' minimalan u B
b ≠ b'
vazi b ρ b' jer je b najmanji u B
b' je minimalan tj b = b'

3. Ukoliko postoji minimalan element, ne mora nužno postojati najmanji element.
Pr: B = $\{2^n \mid n \geq 1\} \cup \{5\}$ Minimalni elementi su 2 i 5, ali ne postoji najmanji element.
4. Ako postoji najveći element skupa B, onda je on jedinstven.
5. Ako postoji najveći element skupa B, tada i jedini maksimalan element.
6. Ukoliko postoji maksimalan element, ne mora nužno postojati najveći element.
Posledice:
-Ako nemamo minimalne elemente, nemamo ni najmanji element.
-Ako imamo bar dva minimalna elementa, nemamo najmanji element.
Primetimo:
Ako B ima jedan minimalan element, on ne mora biti najmanji element tj najmanji element ne mora postojati.
Analogno važi za najveći element: On je jedinstven ako postoji i jedini je maksimalan element.
Oznake:
max(B) – najveći element skupa B
min(B) - najmanji element skupa B
Definicija
Neka je ρ relacija parcijalnog uređenje na skupu A, $B \subseteq A$ i $a \in A$.
Kažemo da je element a
- donje ograničenje skupa B ako a ρ b za sve $b \in B$;
- gornje ograničenje skupa B ako b ρ a za sve $b \in B$.
Ako postoji najveće donje ograničenje, nazivamo ga infimum skupa B.
Ako postoji najmanje gornje ograničenje nazivamo ga supremum skupa B.
Infimum i supremum skupa B redom oznaqavamo sa inf(B) i sup(B).
Važi sledeće:
1. Ako postoji minimum u skupu B, onda je on jednak infinumu skupa B.
2. Ako postoji maksimum u skupu B, onda je on jednak supremumu skupa B.
Dokaz 1: Neka je b = min(B) => b jeste donje organičenje skupa B
Za sve $x \in B$ važi b ρ x
Potrebno je dokazati da je b najveće donje ograničenje od B. Neka je b' neko donje ograničenje tada je b' ρ-manje od svih elemenata iz B specijalno b' ρ b tj b jeste najveće donje ograničenje
Primeri:

1. R, ≤
B = (0,1) ⊂ R
skup donjih ograničenja od B: (-∞, 0]
skup gornjih ograničenja od B: [1, +∞)
0 najveći u (-∞, 0] => inf(B) = 0
1 najmanji u [1, +∞) => sup(B) = 1

2. A = R×R, ≤
(a, b) ≤ (u, v) akko a≤u, b≤v
≤ je uređenje na R×R
nije totalno(linearno) uređenje
Npr: (1,2) /≤ (2, 1) i (2,1) /≤ (1,2)
Tačke (1,2) i (2,1) su neuporedive

Čas 5 Funkcije
Definicija
Neka je $f \subseteq A \times B$ relacija. Kažemo da je f funkcija koja skup A slika u skup B ako za svako $a \in A$ postoji tačno jedno $b \in B$ tako da $(a, b) \in f$.
Element b nazivamo slika elementa a pri funkciji f i označavamo ga sa b = f (a).
Ako je $f \subseteq A \times B$ funkcija koja slika skup A u skup B pišemo $f : A \to B$ i kažemo da je A domen (oznaka Dom(f)) a B kodomen funkcije. Slika funkcije f je skup Im(f) = $\{f(a) \mid a \in A\} \subseteq B$.
Primer: A = {1, 2, 3, 4}, B = {a, b, c}, $f \subseteq A \times B$



f није функција f није функција f је функција

Ako je $f : A \to B$ funkcija, f^{-1} je inverzna relacija. Ali f^{-1} ne mora biti i funkcija.
Primer: Relacija $f \subseteq R \times R$ definisana sa $f = \{(x, x^2) \mid x \in R\}$ je funkcija.
Međutim, relacija $f^{-1} = \{(x^2, x) \mid x \in R\}$ nije funkcija.
Neka f: A-> B Tada:
-A je domen funkcije f, oznaka A = Dom(f)
-B je kodomen funkcije f
-Slika funkcije f je skup $Im(f) = \{ f(a) \mid a \in A\} \subseteq B$
Primer: Ako f: R -> R zadata sa $f(x) = x^2$ tada je Dom(f) = R, kodomen je R
$Im(f) = \{ f(x) \mid x \in R\} = \{x^2 \mid x \in R\} = [0, +\infty)$
Šta je f^{-1} ako je f funkcija?
-f^{-1} jeste relacija.
-f^{-1} ne mora biti funkcija.
Relacija $f^{-1} \subseteq B \times A$ je funkcija akko za svako $b \in Im(f)$ postoji tačno jedno $a \in A$ td $(b, a) \in f^{-1}$ odnosno akko za svako $b \in Im(f)$ postoji tačno jedno a takvo da je $(a, b) \in f$.
Definicija
-Funkcija $f : A \to B$ je surjekcija, ili "na" funkcija, ako važi:
za svako $b \in B$ postoji $a \in A$ tako da je $f(a) = b$.
-Funkcija $f : A \to B$ je injekcija, ili "1-1" funkcija, ako važi:
$f(a_1) = f(a_2) \Rightarrow a_1 = a_2$, za sve $a_1, a_2 \in A$.
Za funkciju $f : A \to B$ kažemo da je bijekcija ako je injekcija i surjekcija.
Primeri:
f: R-> R zadato sa $f(x) = x^2$
nije "1-1": $f(2) = f(-2)$, $2 \neq -2$
nije "na": ne postoji $x \in R$ tdj $f(x) = -2$
g: N->N zadato sa $g(n) = 2n$
jeste "1-1": $g(n_1) = g(n_2)$ tj $2n_1 = 2n_2$ tj $n_1 = n_2$
nije "na": ne postoji $n \in N$ tdj $g(n) = 3$
h: R-> R zadatu sa $h(x) = x + 1$
jeste "1-1": $h(x_1) = h(x_2)$ tj $x_1 + 1 = x_2 + 1$ tj. $x_1 = x_2$
jeste "na": za sve $x \in R$ važi $h(x-1) = x$
h je bijekcija.
Tvrđenje
Relacija f^{-1} je funkcija ako je f "1-1"
Dokaz: $b \in Im(f) <=>$ postoji $a \in A$ tdj $f(a) = b$
i tačno jedno a se slika u b ako je f "1-1" pa je f^{-1}: Im(f) -> A funkcija
ali f^{-1}: B -> A ne mora biti funkcija
Tvrđenje
Relacija $f^{-1} \subseteq B \times A$ je funkcija koja slika skup B u skup A ako i samo ako je $f : A \to B$ je bijekcija.
Dokaz:

1. inkluzija Neka f^{-1}: B -> A
f je "1-1"
$f(a_1) = f(a_2) =^{?}> a_1 = a_2$
$b = f(a_1) = f(a_2)$
$(a_1, b), (a_2, b) \in f => (b, a_1) , (b, a_2) \in f^{-1}$
f^{-1} je funkcija pa $a_1 = a_2$

f je "na"
neka $b \in B$
f^{-1} je funk. koja B slika u A pa
postoji $a \in A$ tdj
$f^{-1}(b) = a$ tj. $(b, a) \in f^{-1}$
$=> (a, b) \in f$ tj $b = f(a)$

2. inkluzija
neka je f: A -> B bijekcija
$b \in B$
f je "na" => postoji $a \in A$ tdj $f(a) = b$
odnosno $(a, b) \in f$ tj $(b,a) \in f^{-1}$

Da li je a jedinstveno?
pps. $(b, a) , (b, a') \in f^{-1}$ i $a \neq a'$
$=> (a, b)$ i $(a', b) \in f$
$f(a) = b = f(a')$ i $a \neq a'$
kontradikcija jer je f "1-1"

Tvrđenje

Ako su relacije $f \subseteq A \times B$ i $g \subseteq B \times C$ funkcije, onda je i relacija $g \circ f$ funkcija i važi $(g \circ f)(a) = g(f(a))$, za svako $a \in A$.

Dokaz:

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

Neka $(a, c_1), (a, c_2) \in g \circ f$

tada postoje $b_1, b_2 \in B$ tdj.

$(a, b_1) \in f$ i $(b_1, c_1) \in g$

$(a, b_2) \in f$ i $(b_2, c_2) \in g$

kako (a, b_1) i $(a, b_2) \in f$

f je funkcija => $b := b_1 = b_2$

g je funkcija i $(b, c_1), (b, c_2) \in g$

=> $c_1 = c_2$

Dakle $g \circ f$ jeste funkcija

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

$a \in Dom(g \circ f)$ tada $(a, c) \in (g \circ f)$ tj

postoji $b \in B$ tdj.

$(a, b) \in f$ i $(b,c) \in g$

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

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

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

Tvrđenje

Ako je f: A->B i g: B-> C tada $g \circ f$:A->C i važi $(g \circ f)(a) = g(f(a))$, za svako $a \in A$.

Dokaz:

$Dom(g \circ f) = A$?, uvek važi da je $Dom(g \circ f) \subseteq A$

2. inkluzija za svako $a \in A$ postoji $f(a) \in B$ jer f: A->B dalje postoji $g(f(a)) \in C$ jer g: B-> C

Dakle $a \in Dom(g \circ f)$

id_A: A -> A definisana sa $id_A(a) = a$ za sve $a \in A$

identitet na skupu A.

Neka je $f : A \rightarrow B$. Tada važi: f je bijekcija ako i samo ako postoji funkcija $g : B \rightarrow A$ tdj. $g \circ f = id_A$ i $f \circ g = id_B$. (u tom slučaju je $g = f^{-1}$)

Dokaz:

1. inkluzija

Ako je f bijekcija onda je f^{-1}: B -> A funkcija pa je $g = f^{-1}$

Neka je $f(a) = b$ => $f^{-1}(b) = a$

$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a$

tj. $f^{-1} \circ f = id_A$

$(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b$

tj. $f \circ f^{-1} = id_B$

2. inkluzija

f je "1-1"

$f(a_1) = f(a_2) \stackrel{?}{=>} a_1 = a_2$

$f(a_1) = f(a_2) \in B /_g$

$g(f(a_1)) = g(f(a_2))$

$id_A(a_1) = id_A(a_2)$

$a_1 = a_2$

f je "na"

$b \in B$

Neka je $a = g(b)$

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

dakle $b = f(a)$

Direktna i inverzna slika

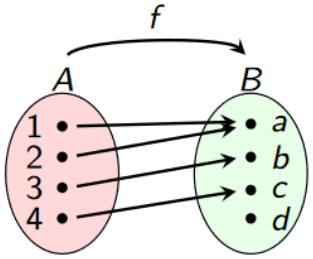
Definicija

Neka je $f : X \rightarrow Y$ i $A \subseteq X$. Direktna slika skupa A je skup $f[A] = \{f(x) \mid x \in A\}$.

Neka je $f : X \rightarrow Y$ i $B \subseteq Y$. Inverzna slika skupa B je skup $f^{-1}[B] = \{x \in X \mid f(x) \in B\}$.

Inverzna slika skupa $f^{-1}[B]$ je pojam koji je definisan bez obzira na to da li postoji inverzna funkcija f^{-1}.

Specijalno važi: f[x] = Im(f) i $f^{-1}[Y] = X$



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

Osobine direktne i inverzne slike:
Neka je $f : X \to Y$ i $A, A_1, A_2 \subseteq X$, $B, B_1, B_2 \subseteq Y$. Tada vai:
1. Ako je $A_1 \subseteq A_2$, onda je $f[A_1] \subseteq f[A_2]$.
2. Ako je $B_1 \subseteq B_2$, onda je $f^{-1}[B_1] \subseteq f^{-1}[B_2]$.
3. Važi da je $f^{-1}[f[A]] \supseteq A$. Ako je f injektivna, tada je $f^{-1}[f[A]] = A$.
4. Važi da je $f[f^{-1}[B]] \subseteq B$. Ako je f surjektivna, tada je $f[f^{-1}[B]] = B$.
Dokazi:

1. Neka je $A_1 \subseteq A_2$
Neka $y \in f[A_1]$
$\Rightarrow y = f(x)$ za neko $x \in A$
kako $x \in A_1$ i $A_1 \subseteq A_2$
$\Rightarrow x \in A_2$
$y = f(x)$ i $x \in A_2 \Rightarrow$
$f(x) \in f[A_2]$ tj
$y \in f[A_2]$

2. Neka $B_1 \subseteq B_2$ *
$x \in f^{-1}[B_1] \Rightarrow$
$f(x) \in B_1$ iz ovoga i * sledi
$f(x) \in B_2$ tj
$x \in f^{-1}[B_2]$

3. Neka $x \in A$
tada $f(x) \in f[A]$ pa
$x \in f^{-1}[f[A]]$
pretpostavimo da je f "1-1"
neka $x \in f^{-1}[f[A]] \Rightarrow f(x) \in f[A]$
kako je f "1-1" $\Rightarrow x \in A$
u suprotnom da f nije "1-1" mogao
bi da postoji $x' \not\in A$ tdj
$f(x') = f(x) \in f[A]$
Primer:
$x = 2$
$A = \{1\}$
$f(x) = f(2) = a \in f[A] = f[\{1\}] = \{a\}$
ali $2 \not\in \{1\}$ tj $x \not\in A$

4. neka $y \in f[f^{-1}[B]]$
$\Rightarrow y = f(x)$ za neko $x \in f^{-1}[B]$
tj $f(x) \in B \Rightarrow y = f(x) \in B$
pretpostavimo da je f "na"
neka $y \in B$
iz $y \in B \subseteq Y$ i f je "na"
postoji $x \in X$ tdj $f(x) = y$
$f(x) = y \in B \Rightarrow x \in f^{-1}[B]$
iz $x \in f^{-1}[B]$ i $y = f(x)$ dobijamo
$y \in f[f^{-1}[B]]$

Čas 6 Karakteristične funkcije skupova i kardinalnost
Definicija
Neka je X bilo koji skup i $A \subseteq X$. Karakteristična funkcija skupa A je
$\chi A : X \to \{0, 1\}$ takva da je
$\chi A(x) = (0, x \not\in A$ ili $1\ x \in A$
Primer: $X = \{a, b, c, d, e, f\}$, $A = \{c, d, f\} \subseteq X$. Karakteristična funkcija skupa A:

$\chi A : X \to \{0, 1\}$

$\chi A(a) = 0$
$\chi A(b) = 0$
$\chi A(c) = 1$
$\chi A(d) = 1$
$\chi A(e) = 0$
$\chi A(f) = 1.$

2 = {0, 1}

*	0	1	+	0	1
0	0	0	0	0	1
1	0	1	1	1	0

a, b, c ∈ **2**
a+b = b+a
a+(b+c) = (a+b)+c
a+0=a i a+a=0
a*b=b*a
a*(b*c) = (a*b)*c
a*a = a
a*1 = a i a*0 = 0

Tvrđenje
Za skupove A i B važi: A = B ako i samo ako $\chi A = \chi B$.
Dokaz:
1. inkluzija Neka je A = B
$\chi_A (a) = 1 <=> a \in A <=> a \in B <=> \chi_B (a) = 1$
2. inkluzija Neka je $\chi_A = \chi_B$
$a \in A <=> \chi_A (a) = 1 <=> \chi_B (a) = 1 <=> a \in B$ Dakle A = B
$Y^X = \{f \mid f : X \rightarrow Y \}$ - skup funkcija koje slikaju skup X u skup Y
Tvrđenje:
Funkcija $\Phi : P(X) \rightarrow \{0, 1\}^X$ definisana sa $\Phi(A) = \chi_A$ je bijekcija.
Dokaz:
{0, 1} = **2**
Da li je Φ injektivna?
$\Phi(A) = \Phi(B) => \chi_A = \chi_B <=> A=B$
Da li je Φ surjektivna?
$f \in \mathbf{2}^X => f: x -> \{0, 1\}$ Neka je $C := f^{-1}[\{1\}] \subseteq X$ $f = \chi_A$
Zbir f + g i proizvod f · g funkcija f , g ∈ {0, 1}X definisan je sa:
$(f + g)(x) =^{def} f (x) + g (x)$
$(f \cdot g)(x) =^{def} f (x) \cdot g (x)$.
Neka f , g , h ∈ $\{0, 1\}^X$. Tada važi:

f + g = g + f	f + (g + h) = (f + g) + h	f · (g + h) = f · g + f · h
f · g = g · f	f · (g · h) = (f · g) · h	(g + h) · f = g · f + h · f

Primenom prethodnih jednakosti na karakteristične funkcije dobijamo sledeće važne jednakosti:
1. $\chi_\emptyset = 0, \chi_X = 1$
2. $\chi_{A\cap B} = \chi_A\chi_B$
3. $\chi_{A\cup B} = \chi_A + \chi_B + \chi_A \chi_B$
4. $\chi_A c = 1 + \chi_A$
5. $\chi_{A\setminus B} = \chi_A + \chi_A \chi_B$
6. $\chi_{A\triangle B} = \chi_A + \chi_B$
7. $\chi_A + \chi_A = 0$
8. $\chi_A \chi_A = \chi_A$

Dokazi:
2. $\chi_{A\cap B} (x) = 1$ akko $x \in A\cap B$
akko $x \in A$ i $x \in B$
akko $\chi_A(x) = 1$ i $\chi_B(x) = 1$
$\chi_A (x) \chi_B (x) = 1$
akko $(\chi_A \chi_B) (x) = 1 => \chi_{A\cap B} = \chi_A \chi_B$
3. $\chi_{A\cup B} (x) = 1$ akko $x \in A\cup B$
akko $x \in A$ ili $x \in B$
Postoje tri slučaja:
I) $x \in A$ i $x \not\in B$ II) $x \not\in A$ i $x \in B$ III) $x \in A$ i $x \in B$
I) $\chi_A (x) = 1 \chi_B(x) = 0 \chi_{A\cap B} (x) = 0$ II) $\chi_A (x) = 0 \chi_B (x) = 1 \chi_{A\cap B} (x) = 0$ III) $\chi_A (x) = 1 \chi_B (x) = 1 \chi_{A\cap B} (x) = 1$
$\chi_A (x) + \chi_B(x) + \chi_{A\cap B}(x) = 1 => (\chi_A + \chi_B + \chi_A \chi_B) (x)$
4. $\chi_A c = 1 + \chi_A$
$\chi_A c (x) = 1 <=> x \in A^c <=> x \not\in A <=> \chi_A (x) = 0 <=> 1(x) + \chi_A (x) <=> (1 + \chi_A) (x) = 1$

5. $\chi_{A\setminus B} = \chi_A + \chi_A \chi_B$

$\chi_{A\setminus B} = \chi_{A\cap B^c} = \chi_A \chi_{B^c} = \chi_A(1 + \chi_B) = \chi_A + \chi_A \chi_B$

6. $\chi_{A\triangle B} = \chi_A + \chi_B$

$\chi_{A\triangle B} = \chi_{(A\setminus B)\cup(B\setminus A)} = \chi_{A\setminus B} + \chi_{B\setminus A} + \chi_{(A\setminus B)} \chi_{(B\setminus A)} = \chi_A + \chi_A\chi_B + \chi_B + \chi_A\chi_B + (\chi_A + \chi_A\chi_B)(\chi_B + \chi_A\chi_B) =$

$= \chi_A + \chi_A\chi_B + \chi_B + \chi_A\chi_B + \chi_A\chi_B + \chi_A\chi_A\chi_B + \chi_A\chi_B\chi_B + \chi_A\chi_B\chi_A\chi_B = \chi_A + \underline{\chi_A\chi_B} + \chi_B + \underline{\chi_A\chi_B} + \underline{\chi_A\chi_B} + \underline{\chi_A\chi_B} + \underline{\chi_A\chi_B} + \underline{\chi_A\chi_B} = \chi_A + \chi_B$

7. $\chi_A + \chi_A = 0$

$\chi_A(x) = 0 \Rightarrow (\chi_A + \chi_A)(x) = 0 + 0 = 0$

$\chi_A(x) = 1 \Rightarrow (\chi_A + \chi_A)(x) = 1 + 1 = 0$

8. $\chi_A \chi_A = \chi_A$

$\chi_A \chi_A = \chi_{A\cap A} = \chi_A$

Specijalni slučaj: $A \subseteq B$

$A\cap B = A$ $\qquad$ $A\cup B = B$

$\chi_{A\cap B} = \chi_A$ $\qquad$ $\chi_{A\cup B} = \chi_B$

$\chi_A \chi_B = \chi_A$ $\qquad$ $\chi_A + \chi_B + \chi_A \chi_B = \chi_B$

<u>Kantorova teorema</u>

Neka je X proizvoljan skup. Postoji injekcija iz X u P(X), ali ne postoji bijekcija između tih skupova.

Dokaz: Postoji injektivno preslikavanje X -> P(X)

$a \in A$

f: X -> P(X) tdj $f(a) = \{a\} \subseteq X$

$f(a) = f(b) \Rightarrow \{a\} = \{b\} \Rightarrow a=b$ tj f jeste injektivna

Ne postoji bijekcija X -> P(X)

Pps: Neka je g: X -> P(x) bijekcija

$a \in X \Rightarrow g(a) \subseteq X$

Definišemo novo preslikavanje $h(x) = \chi_{g(x)}(x) + 1$

h(x) = { 1, za $x/\in g(x)$ ili 0, za $x\in g(x)$ $\qquad \in \mathbf{2}^X$

$h = \chi_A$ gde je $A = \{x|x/\in g(x)\}$

Iz $A\subseteq P(X)$ i g je surjekcije zakljucujemo postoji $a_o \in X$ za koje je $g(a_0) = A$

$h(x) = \chi_{g(ao)}(a_0) + 1 = \chi_A(a_0) \Rightarrow 1 = 0$ kontradikcija

Kardinalnost skupova

<u>Definicija</u>

Neka su A i B skupovi.

- Kažemo da je skup A kardinalnosti manje ili jednake od B, i pišemo $|A| \leq |B|$, ako postoji funkcija $A \xrightarrow{"1-1"} B$.
- Kažemo da je kardinalnost skup A jednaka kardinalnosti skupa B, i pišemo $|A| = |B|$, ako postoji funkcija $A \xrightarrow{"1\text{-}1"\ "na"} B$
- Kažemo da je skup A kardinalnosti strogo manje od B, i pišemo $|A| < |B|$, ako je $|A| \leq |B|$ i $|A| \neq |B|$.

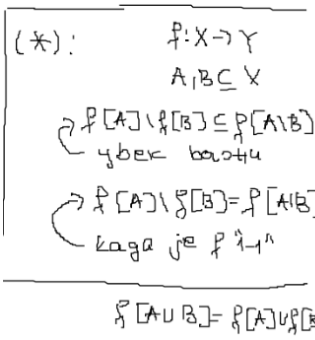
Osobine kardinalnosti:

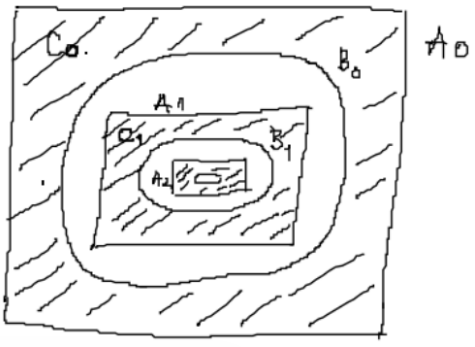
Neka su A, B, C skupovi. Tada važi:

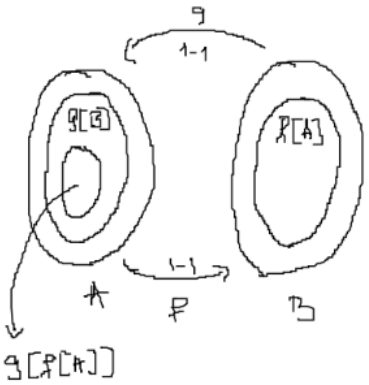
1. $|A| = |A|$. $id_A: A \xrightarrow{1\text{-}1}_{na} A$
2. Ako je $|A| = |B|$, onda je $|B| = |A|$

$f: A \xrightarrow{1\text{-}1}_{na} B \Rightarrow f^{-1}: B \xrightarrow{1\text{-}1}_{na} A$

3. Ako je |A| = |B| i |B| = |C |, tada je |A| = |C |
iz f: $A \xrightarrow{1\text{-}1}_{na} B$ i g: $B \xrightarrow{1\text{-}1}_{na} C$ sledi $g \circ f: A \xrightarrow{1\text{-}1}_{na} C$
$g \circ f$ je 1-1
$g \circ f(x_1) = g \circ f(x_2) \overset{?}{\Rightarrow} x_1 = x_2$
$g \circ f(x_1) = g \circ f(x_2) \Rightarrow g(f(x_1)) = g(f(x_2)) \overset{g \text{ je } 1\text{-}1}{\Rightarrow} f(x_1) = f(x_2) \overset{f \text{ je } 1-1}{\Rightarrow} x_1 = x_2$
$g \circ f$ je na
$z \in C$
g je na => postoji $y \in B$ td $g(y) = z$
f je na i $y \in B$ => postoji $x \in A$ td $f(x) = y$
Dakle $z = g(y) = g(f(x))$ $x \xrightarrow{g \circ f} z$
4. Ako je |A| = |B|, onda je $|A| \leq |B|$ i $|B| \leq |A|$
f: $A \xrightarrow{1\text{-}1}_{na} B$
f: $A \xrightarrow{1\text{-}1} B \Rightarrow |A| \leq |B|$
f^{-1}: $B \xrightarrow{1\text{-}1} A \Rightarrow |B| \leq |A|$
f^{-1} je 1-1
$f/f^{-1}(y_1) = f^{-1}(y_2) \overset{?}{\Rightarrow} y_1 = y_2$
$f(f^{-1}(y_1)) = f(f^{-1}(y_2))$
$f \circ f^{-1}(y_1) = f \circ f^{-1}(y_2) \Rightarrow id_B(y_1) = id_B(y_2) \Rightarrow y_1 = y_2$
5. Ako je $|A| \leq |B|$ i $|B| \leq |C|$, onda je $|A| \leq |C|$
f: $A \xrightarrow{1\text{-}1} B$
g: $B \xrightarrow{1\text{-}1} C$
$g \circ f$: $A \xrightarrow{1\text{-}1} C$
6. (<u>Kantor-Bernštajnova teorema</u>) Ako je $|A| \leq |B|$ i $|B| \leq |A|$, onda je $|A| = |B|$
Ako postoji $A \xrightarrow{1\text{-}1} B$ i $B \xrightarrow{1\text{-}1} A$ onda postoji $A \xrightarrow{1\text{-}1}_{na} B$
Pomoćna lema: $A_0 \supseteq B_0 \supseteq A_1$ i $|A_0| = |A_1|$ tada je $|A_0| = |B_0|$
Dokaz leme: Neka je f: $A_0 \xrightarrow{1\text{-}1}_{na} A_1$
$A_{n+1} := f[A_n]$
$B_{n+1} := f[B_n]$
$A_0 \supseteq B_0 \supseteq A_1 \;/_{f[\,]}$
$f[A_0] \supseteq f[B_0] \supseteq f[A_1] \Rightarrow A_1 \supseteq B_1 \supseteq A_2$
Generalno $A_n \supseteq B_n \supseteq A_{n+1}$
$C_n := A_n \setminus B_n$
$f[C_n] = f[A_n \setminus B_n] \overset{*}{\Rightarrow} f[A_n] \setminus f[B_n] = A_{n+1} \setminus B_{n+1} = C_{n+1}$
$C = \bigcup C_n \; (n \geq 0)$ sve šrafirano na slici
$D = A_0 \setminus C$ sve nešrafirano
$C' = \bigcup C_n \; (n \geq 1)$ sve šrafirano sem C_0
$f[C] = f[\bigcup C_n] \; (n \geq 0) = \bigcup f[C_n] \; (n \geq 0) = \bigcup C_{n+1} \; (n \geq 0) = \bigcup C_n \; (n \geq 1) = C'$
$A_0 = C \cup D$, $C \cap D = \emptyset$ $\quad B_0 = C' \cup D$, $C' \cap D = \emptyset$
g: $A_0 \xrightarrow{1\text{-}1}_{na} B_0$
$g = \{ f(x)$, za $x \in C$ $\quad x$, za $x \in D$
g je na
$y \in B_0 \Rightarrow y \in C'$ ili $y \in D$
ako $y \in C' \Rightarrow y \in A_1$
f je na
=> postoji $x \in A_0$ tdj $f(x) = y$
=> $g(x) = y$
ako $y \in D \Rightarrow g(y) = y$
g je 1-1
$g(x_1) = g(x_2) \in B_0$
$\Rightarrow g(x_1), g(x_2) \in C'$ ($g(x_1) = f(x_1)$, $g(x_2) = f(x_2)$ kako je f 1-1 onda $x_1 = x_2$)
ili
$\Rightarrow g(x_1) = g(x_2) \in D$ ($g(x_1) = x_1$, $g(x_2) = x_2$ onda $x_1 = x_2$)

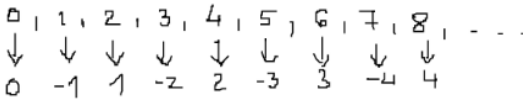






Dokaz K.B.T.
f: A-$^{1-1}$-> B
g: B-$^{1-1}$->A
f[A] ⊆ B/$_{g[\ ]}$
g[B] ⊆ A
g[f[A]] ⊆ g[B] ⊆A ($A_1 \subseteq B_0 \subseteq A_0$)
A_0 -$^{1-1}_{na}$-> f[A_0] -$^{1-1}_{na}$-> g[f[A_0]] = A_1
=> $|A_0|=|A_1|$
Kako je $A_0 \supseteq B_0 \supseteq A_1$ i $|A_0|=|A_1|$ primenom leme dobijamo:
$|A_0|=|B|=|g[B]|$
B-$^{1-1}_{na}$-> g[B] => $|g[B]| = |B|$
Dakle $|A|=|g[B]|=|B|$
7. (Berštajnova teorema) Za svaka dva skupa A i B važi $|A| \leq |B|$ ili $|B| \leq |A|$

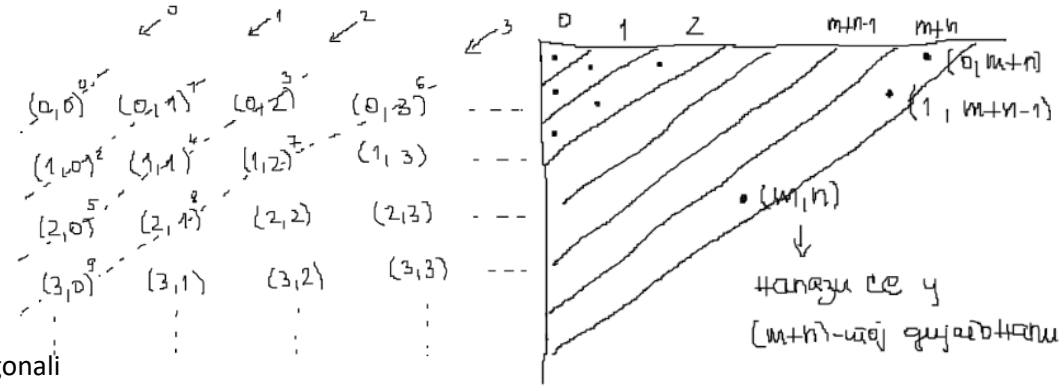
Čas 7 Prebrojivi i neprebrojivi skupovi
Definicija
Skup A je prebrojiv ako je iste kardinalnosti kao i skup prirodnih brojeva (tj. $|A| = |N|$). Oznaka za $|N| = \aleph_0$ (alef-nula)
Definicija
Skup A je konačan ako ima n elemenata, gde je n prirodan broj. Ako A nije konačan, kažemo da je beskonačan.
Skup A je beskonačan ako i samo ako postoji pravi podskup A' ⊂ A takav da su A i A' u bijekciji.
Tvrđenje
Skup prirodnih brojeva je beskonačan.
Dokaz: A = N/{0} ⊂ N
Da li postoji bijekcija N->A?
f(n) = n+1
f je 1-1
$f(n_1) = f(n_2) \Rightarrow n_1 + 1 = n_2 + 1 \Rightarrow n_1 = n_2$
f je na
n∈A (znamo da je n≠ 0)
f(n-1) = (n-1) + 1 = n ∈ N
=> N je beskonačan
Definicija
Ako je skup A konačan ili prebrojiv, kažemo da je najviše prebrojiv. Ako skup nije najviše prebrojiv, onda je neprebrojiv.
X – prebrojiv
f: N -$^{1-1}_{na}$-> X
f(0) = f_0 ; f(1) = f_1 ; f(2) = f_2 ... f(n) = f_n .... X = { f_0, f_1, f_2,...f_n,...} <- elemente skupa X možemo da indeksiramo
Pr. 1: Z je prebrojiv
f: N -$^{1-1}_{na}$-> Z
f(n) = { n/2, n je parno ili
-(n+1)/2 , n je neparno



Pr.2: Ako je A ⊆ N beskonačan, onda je A prebrojiv
Definišemo niz (A_n, a_n) n∈N

$A_0 = A$, $a_0 = \min(A_0)$
$A_1 = A_0 \backslash \{a_0\}$, $a_1 = \min(A_1)$
... $A_{n+1} = A_n \backslash \{a_n\}$, $a_{n+1} = \min(A_{n+1})$
Tada je $A = \{a_0, a_1, ... a_n, ...\} \subseteq N$
f: N-$^{1-1}_{na}$->A
$f(n) = a_n$

A = 2N (skup parnih brojeva) = {0, 2, 4, 6, 8, ...}
A_o = {0, 2, 4, 6,...} a_0 = 0
A_1 = {2, 4, 6,...} a_1 = 2
A_2 = {4, 6, 8...} a_2 = 4
A_3 = {6, 8,....} a_3 = 6
0->0 ; 1->2 ; 2->4 ; 3->6
f(n) = 2n



Pr. 3: N×N je prebrojiv
f: N×N -> N
f(m, n) = ?
broj parova pre (m, n):
1+2+...+(m+n)+m
1 je br el na 0. dijagonali
2 je br el na 1. dijagonali
m+n je br el na (m+n-1)oj dijagonali
u (m+n)toj dijagonali ima m elemenata pre (m, n)
=> (m,n) je 1+2+...+(m+n) + m + 1 po redu
Ako je neki par k-ti po redu, slika se u k-1 (npr (1,1) je 5. po redu a slika se u 4)
Dakle
f(m, n) = 1+2+...+(m+n)+m+1-1 = ½(m+n+1)(m+n) + m

1. Ako je $P_{fin}(X) = \{A \subseteq X \mid A \text{ je konačan}\}$ tada je $P_{fin}(N)$ prebrojiv tj vazi $|P_{fin}(N)| = |N|$
Dokazujemo primenom K.B.T.
$f: N \to P_{fin}(N)$
$f(n) = \{n\} \subseteq P_{fin}(N)$
$f(n) = f(n') \Rightarrow \{n\} = \{n'\} \Rightarrow n = n'$
$g: P_{fin}(N) \to N$
$g(\{a_1, a_2,...a_n\}) = 2^{a1} + 2^{a2} +...+2^{an}$
g je 1-1
$g(\{a_1, a_2,...a_n\}) = g(\{b_1, b_2,...b_l\}) =^{?}> \{a_1, a_2,...a_n\} = \{b_1, b_2,...b_l\}$
$2^{a1} + 2^{a2} +...+2^{an} = 2^{b1} + 2^{b2} +...+2^{bl}$
Možemo prepostaviti da je
$a_1 < a_2 <...< a_n$ i $b_1 < b_2 <...< b_l$
Tvrdimo da je $a_n = b_l$
pps $a_n \neq b_l$
Bez gubitka opstosti neka je $a_n < b_l$
$a_{n+1} \leq b_l$
$2^{an+1} \leq 2^{bl}$ *
$2^{a1} + 2^{a2} +...+2^{an} \leq 1 + 2 + 2^2 +...+2^{an}$
$\leq (1*(1-2^{an+1}))/(1-2) = 2^{an+1} - 1$
$\overset{*}{\leq} 2^{bl} - 1$
$< 2^{bl}$
$\leq 2^{b1} + 2^{b2} +...+2^{bl}$
$\Rightarrow 2^{a1} + 2^{a2} +...+2^{an} < 2^{b1} + 2^{b2} +...+2^{bl}$ Kontradikcija
Dakle $a_n = b_l$ Sada dokazujemo da $a_{n-1} = b_{l-1}$ na analogan nacin
$\Rightarrow \{a_1, a_2,...a_n\} = \{b_1, b_2,...b_l\}$ tj g je injektivna
$N \overset{1-1}{\to} P_{fin}(N)$ i $P_{fin} N \overset{1-1}{\to} N \overset{KBT}{\Rightarrow} N \overset{1-1}{\to}_{na} P_{fin}(N) \Rightarrow |N| = |P_{fin}(N)|$
2. Q je prebrojiv
$N \overset{1-1}{\to} Q$ $n \to n$ $|N| \leq |Q|$
$Q \overset{1-1}{\to} Z \times N$
$m/n \to (m, n)$ $m \in Z, n \in N$ m i n uzajamno prosti
$|Q| \leq |Z \times N|$
$Z \times N \overset{1-1}{\to} N \times N$
$f: Z \overset{1-1}{\to}_{na} N$
$(m, n) \to (f(m), n)$ $m \in Z, n \in N$
$|Z \times N| \leq |N \times N|$
$|N| \leq |Q| \leq |Z \times N| \leq |N \times N| = |N|$
$|N| \leq |Q|$ i $|Q| \leq |N| \overset{KBT}{\Rightarrow} |N| = |Q|$

3. R nije prebrojiv

Dovoljno je pokazati da skup (0,1) nije prebrojiv

pps (0,1) je prebrojiv tj (0,1) = $\{a_0, a_1, a_2,...\}$

$a_n \in (0,1)$ Dole je niz koji predstavlja sve elemente iz intervala (0,1)

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

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

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

$a_n = 0,a_{n0}\, a_{n1}\, a_{n2}...$

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

$\overline{a_{ii}} = \{0$, ako je $a_{ii} \neq 0$ 1, ako je $a_{ii} = 0$ za sve $i \in N$ (Ovo je Hanterov metod dijagonalizacije)

$a \in (0,1) = \{a_0, a_1,...\}$ => postoji $k \in N$ tdj $a = a_k$

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

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

$a_{kk} \neq \overline{a_{kk}}$ => $a \neq a_k$ kontradikcija

Dakle (0,1) nije prebrojiv pa ni R nije prebrojiv

4. $N \times N$ je prebrojiv

5. Z je prebrojiv

6. Ako je $A \subseteq N$ onda je A prebrojiv

7. P(Q) nije prebrojiv

8. P(N) nije prebrojiv

4. 2^N nije prebrojiv.

Pokazujemo sledeće:

$|N| = \chi_0$ – alef nula

$|R| = c$ – kontinuum

$\chi_0 < c$

Važi sledeće (+ dokaz): $|R| \leq |P(Q)| = |P(N)| = |2^N| \leq |R|$

1) $|R| \leq |P(Q)|$

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

$r \in R$

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

f je "1-1"

Neka je $r_1 \neq r_2$ ($r_1, r_2 \in R$) bez gubtika opstosti neka je $r_1 < r_2$

Postoji $q \in Q$ tdj $r_1 < q < r_2$ tada $q / \in f(r_1)$, $q \in f(r_2)$ pa je $f(r_1) \neq f(r_2)$

Zašto postoji racionalan broj između svaka dva realna broja?

$a, b \in R$ i $a<b \overset{?}{\Rightarrow}$ postoji $g \in Q$ tdj $a<q<b$ a_0 b_0

$a = a_0, a_1a_2...$ $a_0, b \in Z$ 11,5347 i 12,45198 q = 11,6

$b = b_0, b_1b_2...$ a_1, a_2, b_1, b_2 cifre iza zareza

ako je $a_0 < b_0$ trivijalno

ako je $a_0 = b_0$

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

$a=a_0,a_1a_2a_3...a_n$ + malo

$b=b_0,b_1b_2b_3...b_n$ + malo $b_n > a_n$ jer $b>a$

q ima konačno decimala => $q \in Q$ i $a<q<b$

ako je $b_{n+1}=b_{n+2}=...=0$ tražimo najmanje $m>n$ td. $a_m \neq 9$ (ako su sve 9tke posle a_n => a=b)

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

$a < q = a_o,a_1a_2...a_na_{n+1}...a_{m-1}\overline{a_m} < b$ i $q \in Q$

2. Pokazaćemo opštije tvrđenje Ako je |A|=|B| onda je |P(A)| = |P(B)| Dokaz:
$f:A\text{-}^{1\text{-}1}_{na}\text{->}B$, g: P(A)-->P(B)
$x \in P(A) \Rightarrow x \subseteq A$
$g(x) = f[x] \subseteq B \Rightarrow g(x) \in P(B)$
Da li je g bijekcija?
g je 1-1:
$g(x_1) = g(x_2) \overset{?}{\Rightarrow} x_1 = x_2 \quad x_1, x_2 \subseteq A$
ako je $g(x_1) = g(x_2) \Rightarrow f[x_1] = f[x_2]$
Pps $x_1 \neq x_2$
$x_1 \setminus x_2 \neq \emptyset$
To znam da postoji $a \in x_1 \setminus x_2$ tj $a \in x_1$ i $a/\in x_2$
$a \in x_1 \Rightarrow f(a) \in f[x_1] = f[x_2]$ tj $f(a) \in f[x_2]$
=> postoji $b \in x_2$ tdj $f(b) = f(a) \Rightarrow b = a \in x_2$ kontradikcija
f je $1 - 1 \Rightarrow x_1 = x_2$
g je na:
$y \in P(B)$ Da li postoji $? \in P(A)$ tdj $g(?) = N$ (neironicno pise znak pitanja)
$N \subseteq B$ i f je na => postoji $x \subseteq A$ tdj $f[x] = y$ pa je $g(x) = f[x] = y$
Specijalno za A = N i B=Q važiće $|N| = |Q| \Rightarrow |P(N)| = |P(Q)|$
3. $\Phi : P(X) \rightarrow \{0, 1\}^X$ definisana sa $\Phi(A) = \chi_A$ je bijekcija.
Dokaz:
$\{0, 1\} = \mathbf{2}$
Da li je Φ injektivna?
$\Phi(A) = \Phi(B) \Rightarrow \chi_A = \chi_B \Leftrightarrow A=B$
Da li je Φ surjektivna?
$f \in \mathbf{2}^X \Rightarrow f: x \rightarrow \{0, 1\}$ Neka je $C := f^{-1}[\{1\}] \subseteq X \quad f = \chi_A$
4. $|2^N| \leq |R| \quad f: 2^N \text{-}^{1\text{-}1}\text{-> } R$
$2^N = \{f | f:N \rightarrow \{0, 1\}\}$
$q \in 2^N \Rightarrow g:N \rightarrow \{0, 1\}$
$f(g) = 0,a_0a_1...a_n...$ gde je $a_i = g(i) \in \{0, 1\}$
Ako je $g_1 \neq g_2 \quad (g_1, g_2 \in 2^N)$ tada će $f(g_1)$ i $f(g_2)$ imati bar jednu različitu cifru iza zareza.
$\Rightarrow f(g_1) \neq f(g_2) \Rightarrow$ f jeste 1-1
<u>Definicija</u>
Skup A je moći kontinuuma ako je $|A| = |R|$. Oznaka za $|R| = c$.
Aksioma izbora
Tvrđenje
Neka je A neprazan skup. Postoji $A\text{-}^{1\text{-}1}\text{-> } B$ ako i samo ako $B\text{-}^{na}\text{->}A$.
Dokaz:
1. implikacija
Neka je f: $A\text{-}^{1\text{-}1}\text{->}B$, pokazimo da postoji $B\text{-}^{na}\text{->}A$.
Izaberimo $a_0 \in A$ takvo a postoji jer je A neprazan skup
definišimo g: $B\text{-}^{na}\text{->}A$
$g(b) = \{ a_0$ ako $b/\in f[A] \quad a$ ako $b \in f[A]$ pri čemu $f(a) = b$
f je 1-1 pa ne mogu dva različita elementa da se slikaju u b
g je dobro definisano
Ako je g(b) = a i g(b) = a' Pokažimo da je a = a'
I) ako $b \neq f[A] \Rightarrow a = a' = a_0$
II) ako b = f[A]
na osnovu definicije g
g(b) = a => f(a) = b iz ova dva f(a) = f(a') pa je a = a'
g(b) = a' => f(a') = b uslova f je 1-1
g je na, $x \in A$
$x = a_0$, svi elementi iz $B \setminus f[A]$ se slikaju u a_0 pri preslikavanju g
$x \neq a_0$, neka je b=f(x) tada je g(b) = x

2. implikacija
Neka je f: B-^{na}-> A
Pokazujemo da postoji
g:A->B takvo da je $f \circ g = id_A$ (ako je $f \circ g$ 1-1 onda je i g 1-1)
Za svaki $a \in A$ => $f^{-1}[\{a\}] \neq \emptyset$ jer je f na
izaberemo $b \in f^{-1}[\{a\}] \cap f^{-1}[\{a'\}]$
$b \in f^{-1}[\{a\}]$ => $f(b) = a$
$b \in f^{-1}[\{a'\}]$ => $f(b) = a'$ => $a' = a$
Drugim rečima $f^{-1}[\{a\}] \cap f^{-1}[\{a'\}] = \emptyset$ ako je $a \neq a'$ Za različite elemente $a \in A$ različiti su skupovi
$f^{-1}[\{a\}]$. Iz svakog od skupova $f^{-1}[\{a\}]$, $a \in A$ izaberemo po jedan element koji označavamo b_a.
Hoćemo g: A->B $g(a) = b_a$ -> izabrani element iz skupa $f^{-1}[\{a\}]$. Ako je $a \neq a'$, tada je
$f^{-1}[\{a\}] \cap f^{-1}[\{a'\}] = \emptyset$ => $b_a \neq b_{b'}$
$g(a) \neq g(a')$ g jeste 1-1
Koristili smo izbor po jednog elementa iz nepraznih međusobno disjunktivnih skupova $f^{-1}[\{a\}]$
Deluje očigledno da možemo to uraditi, ali nijedna od dosadašnjih aksioma nam to ne omogućava. To nam omogućava aksioma izbora.

<u>Aksioma izbora</u>

Neka je dat skupa F čiji su svi elementi neprazni i međusobno disjunktni skupovi. Tada postoji skup C takav da je $C \cap X$ jednočlan za sve $X \in F$. Taj skup se naziva izborni skup ili transverzala.

<u>Aksioma dobrog zasnivanja ili regularnosti</u>

Svaki neprazni skup A sadrži element a takav da je $A \cap a = \emptyset$

<u>Tvrđenje</u> (posledice aksiome regularnosti)

1. Ne postoji skup x takav da je $x \in x$
PPS postoji $x \in x$
Posmatramo $A = \{x\}, x \in A, x \in x\}$ $A \cap x \neq \emptyset$ X je jedini element skupa A i $A \cap x \neq \emptyset$
=> ovo je u kontradikciji sa aksiomom regularnosti
2. Ne postoje skupovi x i y takvi da $x \in y$ i $y \in x$
PPS Neka $x \in y$ i $y \in x$ za neke skupove x i y
Posmatrajmo skup $A = \{x, y\}$
$y \in x$ i $y \in A$ => $A \cap x \neq \emptyset$ Kontradikcija sa aksiomom dobrog zasnivanja jer su
$x \in y$ i $x \in A$ => $A \cap y \neq \emptyset$
3. Ne postoji niz skupova x0, x1 , x2 , . . . takvih da je $x0 \ni x1 \ni x2 \ni \ldots$
PPS postoji niz x_0, x_1, x_2 takav da je $x_0 \ni x_1 \ni x_2 \ni x_3 \ldots$
Neka je $A = \{ x_0, x_1, x_2 \ldots\}$ za svako $i \in \{0, 1, 2, \ldots\}$
$x_{i+1} \in x_i$ i $x_{i+1} \in A$ => $A \cap x_i \neq \emptyset$ Kontradikcija sa aksiomom dobrog zasnivanja
Tvrđenje: Ako je $x \cup \{x\} = y \cup \{y\}$, onda je x = y
Dokaz: PPS $x \neq y$
$x \in x \cup \{x\} = y \cup \{y\}$ => $x \in y$ ili $x \in \{y\}$ tj x = y
Kako je pretpostavka $x \neq y$ => $x \in y$
Slično,
$y \in y \cup \{y\} = x \cup \{x\}$ => $y \in x$ ili $y \in \{x\}$ tj y = x Kako pretpostavka $x \neq y$ => $y \in x$
Dakle $x \in y$ i $y \in x$ Kontradikcija sa 2. posledicom aksiome regularnosti

Čas 8 Prirodni brojevi

Peanove aksiome:
П1 0 je prirodan broj.
П2 Ako je x prirodan broj, onda je i x' prirodan broj.
П3 Ako su x i y prirodni brojevi i x' = y ', onda je x = y .
П4 Za svaki prirodan broj x važi x' ≠ 0.
П5 Neka je Φ svojstvo prirodnih brojeva za koje važi:
1) 0 ima svojstvo Φ;
2) Ako prirodan broj x ima svojstvo Φ, tada i x' ima svojstvo Φ.
Tada svaki prirodni broj ima svojstvo Φ.

0 - simbol konstante
' - unarni funkcijski simbol

Peanove aksiome opisuju prirodne brojeve ali ne govore na koju strukturu se tačno misli!
Fon Nojmanov model prirodnih brojeva zasnovan na teoriji skupova:
$0 := \emptyset$, $1 := \{0\}$, $2 := \{0, 1\}$, $3 := \{0, 1, 2\}, \ldots$
Preciznije, $0 := \emptyset$, $n' = n \cup \{n\}$ i $N := \{0, 1, 2, \ldots\}$.

Tvrđenje
Fon Nojmanov model prirodnih brojeva zadovoljava Peanove aksiome.
Dokaz: Aksiome П1 i П2 trivijalno važe.
Aksioma П3:
Ako je $m' = n' \Rightarrow mU\{m\} = nU\{n\} \overset{\text{prema tvrđenju iznad}}{\Rightarrow} m = n$
Aksioma П4:
$n \in N \quad n' = nU\{n\} \Rightarrow n \in n' \Rightarrow n' \neq \emptyset \Rightarrow n' = 0$
Aksioma П5:
Neka je Φ proizvoljno svojstvo prirodnih brojeva i neka važi:
1) Φ(0) je tačno
2) Za sve n ako je Φ(n) tačno, tada je i Φ(n') tačno
Da li je Φ(n) za sve prirodne brojeve n?
Neka postoji $m \in N$ takvo da Φ(m) nije tačno
$\Rightarrow m \neq 0 \Rightarrow$ postoji $m_1 \in N$ tdj $m_1' = m = m_1 U \{m_1\}$
Na osnovu svojstva 2) ako ne važi Φ(m) onda ne važi ni $\Phi(m_1)$ jer je $m_1' = m$
$\Rightarrow \Phi(m_1)$ ne važi pa $m_1 \neq 0$
$\Rightarrow$ postoji $m_2 \in N$ tdj $m_2' = m_1 \Rightarrow m_2 \in m_1$
Kako ne važi $\Phi(m_1)$ ne važi ni $\Phi(m_2)$
$\Rightarrow m_2 \neq 0$ pa postoji $m_3 \in N$ tdj $m_3 = m_2 \Rightarrow m_3 \in m_2$
Nastavkom dobijamo niz $m \ni m_1 \ni m_2 \ni m_3 \ldots$ Kontradikcija na osnovu posledice 3 aksiome regularnosti
Aksiomu П5 nazivamo aksiomom indukcije:
uslov 1) nazivamo baza indukcije
uslov 2) nazivamo induktivni korak

Princip matematičke indukcije
Neka je Φ svojstvo prirodnih brojeva za koje važi:
1) tačno je Φ(0);
2) ako za prirodni broj n tačno Φ(n), onda i tačno i Φ(n + 1).
Tada je za svaki prirodni broj n tačno Φ(n).
Uslov 1. se naziva baza indukcije, a uslov 2. induktivni korak. Formula Φ(n) u induktivnom koraku se naziva induktivna pretpostavka. Ima aritmetičkih tvrđenja koja nisu tačna za nekoliko najmanjih prirodnih brojeva, ali su tačna za sve ostale. U tim slučajevima možemo koristiti malo izmenjeni princip matamatičke indukcije, koji glasi ovako:
Neka je Φ svojstvo prirodnih brojeva za koje važi:
1) tačno je Φ(k);
2) ako za prirodni broj $n \geq k$ tačno Φ(n), onda i tačno i Φ(n + 1).
Tada je za svaki prirodni broj $n \geq k$ tačno Φ(n).
Princip potpune indukcije
Neka je Φ svojstvo prirodnih brojeva i neka važi: ako je Φ(0), Φ(1), . . . , Φ(n) tačno, tačno je i Φ(n'), za sve $n \in N$. Tada važi Φ(n) za sve prirodne brojeve n.

Za prirodne brojeve x i y operacija sabiranja definiše se sa:
$m + 0 := m$
$m + n' := (m + n)'$

Princip najmanjeg elementa

Ako je $A \subseteq N$ i $A \neq \emptyset$

Definišimo svojstvo $\Phi(n)$: $n \notin A$ tj $n \in N \setminus A$

Potpunom indukcijom dokazujemo da $\Phi(n)$ važi za sve $n \in N$:

Pretpostavimo da važi $\Phi(0), \Phi(1), \ldots \Phi(n)$ i dokazujemo da važi $\Phi(n')$ ako $\Phi(n')$ ne važi onda $n' \in A$, a kako $0,1,..,n \notin A$ (jer važi $\Phi(0), \Phi(1), \ldots \Phi(n)$) onda je n' najmanji element u A Kontradikcija

Dakle važi $\Phi(n')$

Princip potpune indukcije: $\Phi(n)$ važi za sve $n \in N$ tj $n \in N \setminus A$ za sve $n \in N$ $\Rightarrow N \setminus A = N$ pa je $A = \emptyset$ Kontradikcija

Tvrđenje(osobine sabiranja)

Za sve prirodne brojeve m, n i k važi:

1. $(m + n) + k = m + (n + k)$
2. $m + 0 = 0 + m = m$
3. $m + 1 = 1 + m$
4. $m + n = n + m$
5. $m + n = 0 \Rightarrow m = 0$ i $n = 0$
6. $m + k = n + k \Rightarrow m = n$

Dokazi:

1. $(m + n) + k$ Dokaz indukcijom po k $\Phi(k)$ $(m+n) + k = m + (n+k)$

Baza indukcije: $k = 0$ $(m+n)+0 = m+n$ i $m+(n+0) = m+n \Rightarrow (m+n)+0 = m+(n+0)$

Induktivni korak: $\Phi(k) =^{?}> \Phi(k')$

$(m+n)+k = m+(n+k)$

$(m+n)+k' = ((m+n)+k)' =^{ih}> (m+(n+k))' = m+(n+k)' = m+(n+k')$

2. $m+0=0+m=m$

$m+0 = m$ (važi na osnovu definicije)

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

Dokaz indukcijom po m

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

Induktivni korak $\Phi(m) =^{?}> \Phi(m')$

Važi $\Phi(m) = 0+m = m$ (ih)

Dokazujemo $\Phi(m') = 0+ m' = m'$

$0+m' = (0+m)' = m'$

3. $m+1 = 1+m = m'$

$m+1 = m+0' = (m+0)' = m'$

Dokazujemo $m+1 = 1+m = m'$ indukcijom po m

$\Phi(m)$: $m+1 = 1+m = m'$

Bi: $m = 0 \Rightarrow \Phi(0)$: $0 + 1 = 1 + 0 = 1$

$0+0' = (0+0)' = 0' = 1$ Važi

Ik: $\Phi(m) =^{?}> \Phi(m')$

Vazi $\Phi(m) = m+1 = 1+m$

Dokazujemo $\Phi(m') = m'+1 = 1+m'$

$1 + m' = (1+m)' =^{ih}= (m+1)' = m+1' = m + (1+1) = (m+1)+1 = m' + 1$

4. Analogno

5. $m + n = 0 \Rightarrow m = 0$ i $n = 0$

PPS $m \neq 0$ Tada postoji $m_1 \in N$ tdj $m = m_1'$

$m+n = n+m = n + m_1' = (n+m_1)' \neq 0$ Kontradikcija

6. $m + k = n + k \Rightarrow m=n$

Indukcija po k

$\Phi(k)$ ako $m+k = n+k$ onda je $n = m$

bi $k = 0$ $\Phi(0)$ $m + 0 = m$ $n+0 = n$ $m=n$

ik $\Phi(k) \Rightarrow$ Vazi $\Phi(k)$ ako je $m+k=n+k$ onda je $m=n$

$\Phi(k+1) = m + k' = n + k'$ $m+k' = (m+k)'$ i $n+k' = (n+k)'$ $\Rightarrow (m+k)' = (n+k)' \Rightarrow$ aksioma 3 $m+k = n+k =^{ih}> m = n$

Za brojeve x, y ∈ N za koje je x = y + z, za neko z ∈ N, definišemo razliku broja x i broja y kao
$x - y =^{def} z$

Za prirodne brojeve x i y operacija množenja definiše se sa:
$m \cdot 0 =^{def} 0$
$m \cdot n' =^{def} m \cdot n + m.$
Tvrđenje(osobine množenja)
Za sve prirodne brojeve m, m i k važi:
1. $m \cdot (n + k) = m \cdot n + m \cdot k$
Dokaz indukcijom po k
Φ(k): m*(n+k) = mn + mk
bi: k = 0 Φ(0): m(n+0) = mn = mn + 0 = mn + m0 T
ik: $\Phi(k) =^{?} > \Phi(k+1)$
Vazi: Φ(k): m(n+k) = mn + mk ih
Dokazujemo da vazi Φ(k'): m(n+k') = mn + mk'
m(n+k') = m(n+k)' = m(n+k) + m = (mn + mk) + m = mn + (mk + m) = mn + mk'
2. $(m \cdot n) \cdot k = m \cdot (n \cdot k)$
Dokaz indukcijom po k
Φ(k): (m*n)*k = m*(n*k)
bi: k = 0 Φ(0): (m*n)*0 = 0 = m*0 = m(n*0)
ik: Φ(k) => Φ(k') Vazi Φ(k): (m*n)*k = m(n*k) ih
Dokazujemo Φ(k') = (m*n)*k' = m(n*k')
$(m*n)*k' = (m*n)k + mn =^{ih} = m(n*k) + mn = m((n*k)+n) = m(n*k')$
3. $0 \cdot m = 0$
Φ(0): 0*0 = 0
ik: Φ(m) => Φ(m')
Vazi Φ(m) 0*m = 0 (ih)
$0*m' = 0*m + 0 =^{ih} = 0+0 = 0$
4. $1 \cdot m = m$
5. $(m + n) \cdot k = m \cdot k + n \cdot k$
6. $m \cdot n = n \cdot m$
7. $m \cdot n = 0 \Rightarrow m = 0 \vee n = 0$

Čas 9 Deljivost
Definicija
Neka su a, b ∈ N. Kažemo da a deli b ili da je b deljiv sa a i pišemo a | b ako postoji broj c ∈ N tako da je $b = a \cdot c$.
Teorema (o Euklidskom deljenju)
Neka su a, b ∈ N i b ≠ 0. Tada postoje brojevi q, r ∈ N koji su jedinstveno određeni tako da je $a = b \cdot q + r$, $0 \le r < b$.
Dokaz:
Jedinstvenost – PPS: Postoje q, r, q', r' ∈ N tdj.
a = b*q + r, $0 \le r < b$ i a = b*q' + r', $0 \le r' < b$
0 = b(q-q') + r – r'
r' – r = b(q-q') => b|r'-r
iz uslova r < b i r' < b sledi r'-r ∈ {-b+1, -b+2, ..., 0, ..., b-1}
iz dva prethodna uslova sledi r' – r = 0, r' = r Kontradikcija
0 = b(q-q'), b≠0 po definiciji, q-q' = 0 q' = q Kontradikcija
Egzistencija
S = {a-xb | x ∈ N, a-xb ∈ N}
S ⊆ N, S≠Ø jer a = a-0*b ∈ S => S ima najmanji element r na osnovu principa najmanjeg elementa
Neka je r = min(S) => postoji q ∈ N tdj r = a – qb odnosno a = qb + r
Treba pokazati $0 \le r < b$, r ∈ S => $0 \le r$
PPS $b \le r$ r' = r – b r = a-qb /+(-b)
r – b = a-qb-b = a – (q+1)b r' = a-b(q+1) Kontradikcija jer je r najmanji element u S.

Definicija

Neka su a, b ∈ Z. Kažemo da a deli b ili da je b deljiv sa a i pišemo a | b ako postoji broj c ∈ Z tako da je b = a · c.

Teorema

Neka su a, b ∈ Z i b ≠ 0. Tada postoje brojevi q, r ∈ Z koji su jedinstveno određeni tako da je
a = q · b + r , 0 ≤ r < |b|.

Dokaz:

Posmatramo sledeće slučajeve:

1. a≥0, b>0 svodi se na prethodnu teoremu
2. a≥0, b<0 tada je a≥0 i –b>0 pa primenimo prethodnu teoremu
Postoje q, r ∈ N tdj a = q(-b)+r, 0 ≤ r <|b|
3. a≤0, b>0 -a>0 primenimo prethodno tvrđenje na –a, b ∈ N
Postoje q, r ∈ N tdj –a = bq + r, 0 ≤ r < b
a = (-q)b – r, 0 ≥ -r > -b
a = -qb –r + b – b = (-q - 1)b + (b-r) -q-1 = q' b-r = r'
0 ≤ b-r < b = |b| => 0≤ r' < |b|
4. a≤0, b<0 -a>0 i -b > 0 Primenjujemo prethodnu teoremu na –a, -b ∈ N
=> postoje q, r ∈ N tdj –a = q(-b) + r, 0 ≤ r < -b
a = qb – r, b <-r ≤ 0
ako je r = 0 gotovo 0 ≤ 0 < |b|
ako je r>0
a = qb – r + b – r = (q+1)b + (-b-r) = q'b + r' b < -r < 0 /+(-b)
0 < -b-r < -b => 0 ≤ r' < |b|
Jedinstvenost se pokazuje isto kao u prethodnom tvrđenju

Definicija

Broj d ∈ N je zajednički delilac prirodnih brojeva a i b ako d | a i d | b. Za takav broj d kažemo da je najveći zajedniqki delilac brojeva a i b ako d' | d za svaki zajednički delilac d' tih brojeva.
U tom slučaju pišemo d = nzd(a, b)

Definicija

Broj s ∈ N je zajednički sadržalac prirodnih brojeva a i b ako a | s i b | s. Za takav broj s kažemo da je najmanji zajednički sadržalac brojeva a i b ako s | s' za svaki zajednički sadržalac s' tih brojeva. U tom slučaju pišemo
s = nzs(a, b).

Tvrđenje

Ako je a = bq + r onda je nzd(a, b) = nzd(b, r).

Dokaz:

D_1 – skup zajedničkih delilaca a i b D_2 – skup zajedničkih delilaca b i r
$D_1 = \{d \in Z \mid d|a, d|b\}$ $D_2 = \{d \in Z \mid d|b, d|r\}$
Dokazujemo da je $D_1 = D_2$

1. $D_1 \subseteq D_2$
$d \in D_1 \Rightarrow d|a, d|b$
r = a – bq
Kako d|a i d|b pa time i bq
$d|t \ (t = a – bq) \Rightarrow d \in D_2$

2. $D_2 \subseteq D_1$
$d \in D_2 \Rightarrow d|b, d|r$
a = bq + r
Kako d|r i d|b pa time i bq
$d|(bq+r)$ pa time $d|a \Rightarrow d \in D_1$

Iz 1 i 2 vidimo $D_1 = D_2 \Rightarrow \max(D_1) = \max(D_2)$ tj NZD(a,b) = NZD(b,r)

Euklidov algoritam

Euklidov algoritam predstavlja postupak za određivanje najvećeg zajedničkog delioca datih celih brojeva a i b ≠ 0. Sastoji se od uzastopnog primenjivanja teoreme o euklidskom deljenju za cele brojeve. Prvo, broj a pri deljenju sa b daje neki količnik q1 i ostatak r1. Ako je r1 ≠ 0, možemo podeliti b sa r1. U tom slučaju dobijamo količnik q2 i ostatak r2 . Ako je r2 ≠ 0 nastavljamo postupak sa brojevima r1 i r2. Postupak se završava kada dobijemo ostatak koji je jednak nuli. Algoritam možemo predstaviti shemom

$a = bq_1 + r_1 \quad 0 \le r_1 < |b|$

$b = r_1q_2 + r_2 \quad 0 \le r_2 < r_1$

$r_1 = r_2q_3 + r_3 \quad 0 \le r_3 < r_2$

...

$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1} \quad 0 \le r_{n-1} < r_{n-2}$

$r_{n-2} = r_{n-1}q_n + r_n \quad 0 \le r_n < r_{n-1}$

$r_{n-1} = r_nq_{n+1} + r_{n+1} \quad 0 \le r_{n+1} < r_n$

niz ostataka $|b| > r_1 > r_2 > ... > r_{n-1} > r_n > ... \ge 0$ je strogo opadajući ograničen nulom. Prema tome postoji $n \in N$ tdj $r_{n+1} = 0$ Na osnovu prethodnog algoritam se završava u konačno mnogo koraka. NZD(a, b) će biti poslednji ne-nula ostatak.

$NZD(a,b) = NZD(b, r_1) = NZD(r_1, r_2) = ... = NZD(r_{n-2}, r_{n-1}) = NZD(r_{n-1}, r_n) = NZD(r*q_{n+1}, r_n) = r_n$

Tvrđenje (Bezuova relacija)

Ako je nzd(a, b) = d, onda postoje brojevi x i y tkd ax + by = d.

Dokaz:

$NZD(a, b) = r_n = r_{n-2} - r_{n-1}q_n = r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n = -q_nr_{n-3} + (1+q_{n-1}q_n)r_{n-2} = ... = ax + by$

Neka a, b ∈ Z

$M_0 = \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$

M_{n+1} dobijamo od matrice M_n jednom od sledećih transformacija:

T_1: Množenje vrste celim brojem i dodavanje drugoj vrsti;

T_2: Množenje vrste sa -1;

T_3: Zamena mesta vrstama.

Tvrđenje

Neka je $M_n = \begin{bmatrix} x & p & q \\ y & s & t \end{bmatrix}$. Tada je x = ap + bq i y = as + bt.

Dokaz: Indukcijom po n:

n = 0 Iz matrice M_0 dobijamo x = a, p = 1, q = 0 i y = b, s = 0, t = 1

a = a*1 + b*0 i b = a*0 + b*1

n -> n + 1 $M_n = \begin{bmatrix} x & p & q \\ y & s & t \end{bmatrix}$ ——> $M_{n+1} = \begin{bmatrix} x' & p' & q' \\ y' & s' & t' \end{bmatrix}$

(ih) x = ap + bq dokazujemo x' = ap' + bq'

y = as + bt ——> y' = as' + bt'

Matricu M_{n+1} smo dobili na jedan od sledećih načina:

1. Zamenom vrsta

$\begin{bmatrix} x' & p' & q' \\ y' & s' & t' \end{bmatrix} = \begin{bmatrix} y & s & t \\ x & p & q \end{bmatrix}$ x' = y =^{ih}= as + bt = ap' + bq'

y' = x =^{ih}= ap + bq = as' + bt'

2. Množenjem jedne vrste sa -1 (bez gubitka opštosti pretpostavimo da smo prvu vrstu pomnožili sa -1)

$\begin{bmatrix} x' & p' & q' \\ y' & s' & t' \end{bmatrix} = \begin{bmatrix} -x & -p & -q \\ y & s & t \end{bmatrix}$ x' = -x = -(ap+bq) = a(-p) + b(-q) = ap' + bq'

3. Množenjem jedne vrste sa α ∈ Z i dodavanjem je drugoj(bez gubitka opštosti prvu ćemo pomnožiti i dodati drugoj)

$\begin{bmatrix} x' & p' & q' \\ y' & s' & t' \end{bmatrix} = \begin{bmatrix} x & p & q \\ y+\alpha x & s+\alpha p & t+\alpha q \end{bmatrix}$ x' = x, p' = p, q' = q => x' = x = ap+bq = ap' + bq'

y' = y + αx = as + bt + α(ap + bq) = a(s+αp) + b(t+αq) = as' + bt'

Tvrđenje

Neka je $M_n = \begin{bmatrix} x & p & q \\ y & s & t \end{bmatrix}$. Tada je NZD(a, b) = NZD(x, y).

Dokaz:

Indukcijom po n

Bi: n = 0 važi

$M_n = \begin{bmatrix} x & p & q \\ y & s & t \end{bmatrix}$ ——> $M_{n+1} = \begin{bmatrix} x' & p' & q' \\ y' & s' & t' \end{bmatrix}$

(ih) NZD(x, y) = NZD(a, b) ————> dokazujemo NZD(x', y') = NZD(a, b)

1. M_{n+1} dobijeno od M_n zamenom vrsta

NZD(x', y') = NZD(y, x) $=^{ih}$ NZD(a, b)

2. M_{n+1} dobijeno od M_n množenjem vrste sa -1

NZD(x', y') = NZD(-x, y) = NZD(x, y) $=^{ih}$ NZD(a, b)

3. M_{n+1} dobijeno od M_n množenjem vrste sa $\alpha \in Z$ i dodavanjem drugoj vrsti

NZD(x', y') = NZD(x + αy, y) = NZD(x, y) $=^{ih}$ NZD(a, b)

Dakle ako je $M_n = \begin{bmatrix} d & p & q \\ 0 & s & t \end{bmatrix}$ i d≥0, tada je NZD(a, b) = NZD(d, 0) = d i d = ap + bq

Definicija

Brojevi a, b ∈ Z su uzajamno prosti ako je NZD(a, b) = 1.

Tvrđenje

Ako a | bc i NZD(a, b) = 1 onda a | c.

Dokaz:

na osnovu Bezuove relacije postoje p, q ∈ Z tdj ap + bq = 1/ *c

apc + bqc = c kako a|apc i a | bqc sledi a|c

Tvrđenje

Neka je d = NZD(a, b), a = d*a', b = d * b' tada je NZD(a', b') = 1

Dokaz:

PPS: NZD(a', b') = d' > 1

a' = d' * a'' i b' = d' * b''

a = d * a' = d*d' * a'' i b = d * b' = d * d' * b''

=> d*d' |a,b i d'>1 => d*d' > d Kontradikcija jer je d = NZD(a, b)

Tvrđenje

Neka je d = NZD(a, b), tada je NZS(a, b) = |ab|/d

Dokaz:

S = |a*b|/d dokazujemo da S = NZS(a, b)

a = d*a' i b = d*b'

S = |d * a' * d * b'|/d = d*|a'|*|b'| => a|S i b|S => S jeste sadržalac

Da li je S najmanji sadržalac?

Neka je t neki drugi sadržalac brojeva a i b tj a|t i b|t

t = a*a'' = b*b''

t = d * a' * a'' = d * b' * b'' => a'a'' = b'b'' odnosno a'|b'b'' NZD(a', b') = 1 pa a'|b''

b'' = a' * l

t = d * b' * b'' = d * b' * a' * l i S = d*|b'|*|a'| => S|t

Dakle S = NZS(a, b)

Čas 10 Diofantove jednačine

Definicija
Diofantova jednačina je jednačina sa celobrojnim koeficijentima kod koje tražimo rešenja u skupu Z.
Primer: Jednačina ax = b, gde su a, b ∈ Z i a ≠ 0 je Diofantova jednačina. Ima rešenje u Z ako i samo ako a | b.
U nastavku ćemo posmatrati Diofantovu jednačinu oblika ax + by = c. (*)
Teorema
Jednačina ax + by = c, gde je a, b ≠ 0 ima celobrojna rešenja ako i samo ako NZD(a, b) | c. U tom slučaju opšte rešenje ove jednačine je

$x = p * \frac{c}{nzd(a,b)} + t * \frac{b}{nzd(a,b)}$ $y = q * \frac{c}{nzd(a,b)} - t * \frac{a}{nzd(a,b)}$, t ∈ Z

gde su p i q dobijeni pomoću (obrnutog) Euklidovog algoritma takvi da važi ap + bq = nzd(a, b).
Dokaz:

1. implikacija
Neka (*) ima rešenje
(x_0, y_0) – jedno rešenje $x_0, y_0 \in Z$
Neka je d = NZD(a, b)
$d|a, b \quad d|ax_0 + by_0 \Rightarrow d|c$

2. implikacija
Neka je d = NZD(a, b) | c
c = d*c'
postoje p, q ∈ Z tdj ap + bq = d/c'
a(pc') + b(qc') = c => (pc', qc') jedno rešenje (*)

Šta je opšte rešenje jednačine (*)?
Neka je $(x_0, y_0) = (pc', qc')$ gde je $c' = \frac{c}{NZD(a,b)}$ p, q su dobijeni iz Bezuove relacije NZD(a, b) = ap + bq

a = d*a'
b = d*b'
NZD(a', b') = 1
$ax_0 + by_0 = c$
ax + by = c
$a(x-x_0) + b(y-y_0) = 0$
$a(x-x_0) = -b(y-y_0) /d$
$a'(x-x_0) = -b'(y-y_0)$

$a'|b'(y-y_0)$, NZD(a', b') = 1 => $a'|y-y_0$
$b'|a'(x-x_0)$, NZD(a', b') = 1 => $b'|x-x_0$
$x – x_0 = b'*t \quad t \in Z$
$\Rightarrow x = x_0 + b'*t$
$a' * b' * t = -b'(y-y_0) / b'$
$a' * t = -y + y_0$
$\Rightarrow y = y_0 – a'$

Dakle opšte rešenje jednačine (*) je: x = p * c/d + t * b/d y = q * c/d - t * a/d
gde je d = NZD(a, b) i važi ap + bq = c

Prosti brojevi

Definicija
Ceo broj p > 1 je prost ako su jedini delioci tog broja 1 i p. Ceo broj n > 1 koji nije prost je složen.
Tvrđenje
Postoji beskonačno mnogo prostih brojeva.
Dokaz:
PPS da prostih brojeva ima konačno mnogo: $p_1, p_2, ..., p_n$ Posmatramo broj $k = p_1 * p_2 * ... * p_n + 1$ prema tome $p_i \nmid k \quad i \in \{1, 2, ..., n\}$ sledi da $k \neq p_i$, $i \in \{1,..., n\}$ prema tome k je složen broj.
=> postoji prost broj q koji deli p tada je $q = p_j$ za neko $j \in \{1, ..., k\}$ pa $p_j | k$ Kontradikcija

Tvrđenje
Ako je p prost broj i p | ab, onda je p | a ili p | b.
Dokaz:
Neka p|ab i pretpostavimo da pła dokazujemo da p|b
ako NZD(a, p) > 1 onda NZD(a, p) = p jer je p prost broj
Iz ovoga sledi p|a što nije tačno pa NZD(a, p) = 1
p|ab i NZD(p, a) => p|b
Važi i opštije: ako $p|a_1a_2...a_k \Rightarrow p|a_1$ ili $p|a_2$ ili ... ili $p|a_k$

Tvrđenje

Svaki prirodan broj veći od 1 je prost ili se može predstaviti kao proizvod prostih brojeva.

Dokaz:

Potpunom indukcijom po n. $\Phi(n)$: n je proizod prostih brojeva

Dokazujemo za sve $n \geq 2$ važi $\Phi(n)$ potpunom indukcijom po n

bi: n = 2, n = 3 prosti brojevi => važi $\Phi(2)$ i $\Phi(3)$

ih: Pretpostavimo da je za svaki prirodan broj manji od n zadovoljeno svojstvo Φ tj za svako $k < n$, k je proizvod prostih brojeva

Dokazujemo da je n proizvod prostih:

-ako je n prost broj: onda važi $\Phi(n)$

-ako je n složen: $n = m*k \quad 1<m \quad k<n$

po ih m i k su proizvodi prostih brojeva pa je $n = m * k$ proizvod prostih brojeva

Osnovna teorema aritmetike

Svaki prirodni broj veći od 1 može se predstaviti u obliku proizvoda prostih brojeva na jedinstven način (do na redosled prostih faktora).

Dokaz:

Na osnovu prethodne teoreme znamo da je svaki prirodan broj proizvod prostih, pokažimo da je zapis tog proizvoda jedinstven (do na redosled činilaca)

Neka je $n = p_1^{a1} p_2^{a2}...p_k^{ak} = q_1^{b1} q_2^{b2}...q_l^{bl} \quad a_i, b_i \geq 1$

$p_1 < p_2 < p_3 < ... < p_k , \quad q_1 < q_2 < ... < q_l$

za svako $i \in \{1, ..., k\}$ $p_i | n = q_1^{b1} q_2^{b2}...q_l^{bl}$

Postoji $j \in \{1,..., l\}$ td $p_i | q_j$ pa $p_i = q_j$

Dakle $\{p_1, ..., p_k\} \subseteq \{q_1, ..., q_l\}$

Analogno se dokazuje da je $\{q_1, q_2, ..., q_l\} \subseteq \{p_1, p_2, ..., p_k\}$

=> $\{p_1, ..., p_k\} = \{q_1, ..., q_l\}$ pa je k = l

Kako je $p_1<p_2<...<p_k$ i $q_1<q_2<...<q_l$ zaključujemo $p_1 = q_1, p_2 = q_2, ..., p_k = q_l$

Za sada imamo:

$n = p_1^{a1}p_2^{a2}...p_k^{ak} = p_1^{b1}p_2^{b2}...p_k^{bk}/p_1^{a1}$

ako je npr $a_1 < b_1$

$\underline{p_2^{a2}...p_k^{ak}} = \underline{p_1^{b1-a1} p_2^{b2}...p_k^{bk}} \quad b_1 - a_1 \geq 1$

$p_1 \nmid \qquad p_1 | \qquad$ Kontradikcija

Dakle $a_1 = b_1$ pa važi

$p_2^{a2} ... p_k^{ak} = p_2^{b2}...p_k^{bk}$ i nastavkom postupka dobijamo $a_2 = b_2, ..., a_k = b_k$

Kongruencije po modulu

Definicija

Neka je m prirodni broj veći od 1. Kažemo da su brojevi $a, b \in Z$ kongruentni po modulu m i pišemo

$a \equiv b \pmod m$ ili $a \equiv_m b$ ako $m \mid (a - b)$.

Tvrđenje

Relacija $\equiv_m$ je relacija ekvivalencije.

Dokaz:

(R) $a \equiv_m a$ jer $m | a-a = 0$

(S) $a \equiv_m b \quad =^{?}> \quad b \equiv_m a$

$a \equiv_m b \quad => \quad m | a-b \quad => \quad m | b-a = -(a-b)$

$=> b \equiv_m a$

(T) $a \equiv_m b \quad i \quad b \equiv_m c \quad => \quad a \equiv_m c$?

$m | a-b \quad i \quad m | b-c$

$=> m | a-c = (a-b)+(b-c) => a \equiv_m c$

Tvrđenje

Ako je a ≡ a1 (mod m) i b ≡ b1 (mod m) onda je:

1) $a + b \equiv a_1 + b_1 \pmod m$

2) $ab \equiv a_1b_1 \pmod m$

3) $a^n \equiv a_1^n \pmod m$, za sve $n \geq 1$.

Dokaz:

1) $m \mid a-a_1$ i $m \mid b-b_1 \Rightarrow m \mid (a-a_1) + (b-b_1) \Rightarrow m \mid (a+b) - (a_1 + b_1) \Rightarrow a+b \equiv a_1 + b_1$

2) $ab - a_1b_1 = ab - a_1b + a_1b - a_1b_1 = a_1(b-b_1) + b(a-a_1) \Rightarrow m \mid ab - a_1b_1$ tj. $ab \equiv_m a_1b_1$

3) Indukcijom po n:

n = 1 $a^1 = a$, $b^1 = b$

$a \equiv_m b$ (dato)

(ih) Neka je $a^n \equiv_m b^n$

n –> n+1:

$a^{n+1} = a^n * a$

$a^n \equiv_m b^n$ i $a \equiv_m b \Rightarrow a^n * a \equiv_m b^n * b$

$a^{n+1} \equiv_m b^{n+1}$

Tvrđenje

Neka $d \mid a, b, m$ i neka je $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ i $m' = \frac{m}{d}$. Tada je $a \equiv_m b$ akko $a' \equiv_{m'} b'$

Dokaz:

1. implikacija

Neka je $a \equiv_m b$

$m \mid a-b$

$a-b = m*k$ za neko $k \in Z$

$da' - db' = dm'*k/d$

$a' - b' = m'k$

pa $m' \mid a'- b'$

tj. $a' \equiv_{m'} b'$

2. implikacija

Neka je $a' \equiv_{m'} b'$

$m' \mid a' - b'$

$a' - b' = m'*l$ za neko $l \in Z$

$da' - db' = dm'l$

$a - b = ml$

pa $m \mid a-b$ tj $a \equiv_m b$

Jednačine sa kongruencijama

Posmatrajmo jednačinu $ax \equiv b \pmod m$ gde su $a, b \in Z$?

Kada jednačina ima rešenja i šta su rešenja te jednačine?

$ax \equiv_m b$ akko $m \mid ax - b$

akko $ax - b = m(-k)$ za neko $k \in Z$

akko $ax + mk = b$, za neko $k \in Z$

$ax \equiv_m b$ ima rešenje akko $ax + mk = b$ ima rešenje akko $NZD(a, m) \mid b$

Neka $d = NZD(a, m) \mid b$ Šta su rešenja $ax \equiv_m b$?

Prema prethodnom tvrđenju, dovoljno je da rešimo

$\frac{a}{d}x \equiv_{m/d} \frac{b}{d}$ tj. $a'x \equiv_{m'} b'$ gde je $NZD(a', m') = 1$

$\frac{a}{d} = a'$, $\frac{b}{d} = b'$, $\frac{m}{d} = m'$

Iz $NZD(a', m') = 1$

$\Rightarrow 1 = a'p + m'q$ za neke $p, q \in Z$

$\Rightarrow 1 \equiv_{m'} a'p \ /*b'$

$b' \equiv_{m'} a'(pb')$

Pokažimo: $a'x \equiv_{m'} b'$ akko $x \equiv_{m'} pb'$

=>: $a'x \equiv_{m'} b'$ i $p \equiv_{m'} p$ =^{2}> $a'px \equiv_{m'} pb'$ $a'p \equiv_{m'} 1$

$x \equiv_{m'} pb'$

<=: $x \equiv_{m'} pb'$ i $a' \equiv_{m'} a'$ =^{2}> $a'x \equiv_{m'} a'pb'$ $a'p \equiv_{m'} 1$ $a'x \equiv_{m'} b'$

Skup rešenja jednačine $a'x \equiv_{m'} b'$ su $x \equiv_{m'} pb'$ tj rešenja su $\{pb' + m't \mid t \in Z\}$ (samo jedno rešenje je ≥ 0 i $<m'$)

$ax \equiv_m b$ gde $d = NZD(a, m) \mid b$

Koliko ova jednačina ima rešenja ≥ 0 i $<m$?

Ima ukupno d rešenja u intervalu $[0, m)$ ima po jedno rešenje u svakom od sledećih intervala:

$[0, m'), [m', 2m'), ..., [(d-1)m', dm')$ $dm' = m$

<u>Vilsonova teorema</u>

Ako je p prost broj tada je $(p - 1)! \equiv -1 \pmod p$.

Dokaz:

za $p = 2$ $(2-1)! = 1! = 1$ $1 \equiv -1 \pmod 2$ jer $2 \mid 1 - (-1) = 2$

za $p = 3$ $(3-1)! = 2! = 2$ $2 \equiv -1 \pmod 3$ jer $3 \mid 2 - (-1) = 3$

Kada je $p \geq 5$

Neka $a \in \{2, 3, 4, ... p - 2\}$

Posmatramo jednačinu $ax \equiv 1 \pmod p$

$NZD(a, p) = 1$ => jednačina ima jedinstveno rešenje u intervalu $[0, p)$ Neka je to rešenje x_a:

Pokažimo da $x_a \in \{2, 3, 4, ... p - 2\}$

PPS: $x_a = 0$ $a*0 \equiv 1 \pmod p$ Kontradikcija

$x_a = 1$ $a*1 \equiv 1 \pmod p$ $p \mid a-1$ $(a-1) \in \{1, 2, 3, 4, ... p - 3\}$ Kontradikcija

$x_a = p-1$ $a*(p-1) \equiv 1 \pmod p$ $ap - a \equiv 1$ $a \equiv -1$ $p \mid a+1$ $(a+1) \in \{3, 4, 5,... p - 1\}$ Kontradikcija

Pokažimo da je $a \neq x_a$ za sve $a \in \{2, 3, 4, ... p - 2\}$

PPS $a = x_a$ za neko $a \in \{2, 3, 4, ... p - 2\}$

$a*x_a = a^2 \equiv 1 \pmod p$

$p \mid a^2 - 1$

$p \mid (a-1)(a+1)$ => $p \mid (a-1)$ ili $p \mid (a+1)$

$(a-1) \in \{1, 2, 3, 4, ... p - 3\}$ i $(a+1) \in \{3, 4, ... p - 1\}$

Među brojevima 2, 3, ..., p-2 imamo ukupno $\frac{p-3}{2}$ parova (a, x_a)

$(p-1)! = 1*2*3*...*(p-2)*(p-1) = 1*(2x_2)*(3x_3)*...*(p-1) \equiv_p 1*1*1*1*....*(p-1) \equiv_p p-1 \equiv_p -1$

Dodatno objašnjenje: (a, x_a) i (b, x_b) Ako je $a \neq b$ da li može biti $x_a = x_b$?

Pretpostavimo da je $x_a = x_b$

$a*x_a \equiv 1 \pmod p$

$b*x_b = b*x_a \equiv 1 \pmod p$

$a*x_a \equiv b*x_a \pmod p$

$p \mid a*x_a - bx_a = x_a(a-b)$

$NZD(p, x_a) = 1$ $\Rightarrow$ $p \mid a-b$

$a-b \in \{-p+4, -p+5, ..., 0, 1, 2, ..., p-4\}$

$p \mid a-b$ => $a = b$ Kontradikcija

<u>Kineska teorema o ostacima</u>

Sistem kongruencija

$x \equiv a1 \pmod{m_1}$

$x \equiv a2 \pmod{m_2}$

$x \equiv a_3 \pmod{m_3}$

. . .

$x \equiv a_k \pmod{m_k}$

ima rešenje ako $NZD(m_i, m_j) \mid (a_i - a_j)$ za sve $i \neq j$. Ako je x neko rešenje tog sistema, onda je opšte rešenje oblika $x = x + NZS(m_1, \ldots m_k) \cdot t$, gde je $t \in Z$.

Dokaz za opšti slučaj (2022):
Indukcijom po n
bi: k = 1
$x \equiv a_1 \pmod{m_1}$ dakle ova jednačina uvek ima rešenje i njeno opšte rešenje je oblika: $x = a_1 + m_1 t$, $t \in Z$
ih: Tvrđenje važi za sistem sa k jednačina
ik: Pokažimo da tvrđenje važi i za sistem sa k+1 jednačina

$$\left.\begin{array}{l} x \equiv a_1 \pmod{m_1} \\ \ldots \\ x \equiv a_k \pmod{m_k} \end{array}\right\} (*)$$

$x \equiv a_{k+1} \pmod{m_{k+1}}$
Neka je $x = x_0 + NZS(m_1, m_2, ..., m_k)*t \quad t \in Z$ rešenje sistema *
$x_0 + NZS(m_1, m_2, ..., m_k)*t \equiv a_{k+1} \pmod{m_{k+1}}$
$NZS(m_1, m_2, ..., m_k)*t \equiv a_{k+1} - x_0 \pmod{m_{k+1}}$

Ova jednačina ima rešenje kada $NZD(NZS(m_1, m_2, ..., m_k), m_{k+1}) \mid a_{k+1} - x_0$
(Dokazujemo $NZS(NZD(m_1, m_{k+1}), NZD(m_2, m_{k+1}), ..., NZD(m_k, m_{k+1}))$)
Dovoljno je pokazati da $NZD(m_i, m_{k+1}) \mid a_{k+1} - x_0$ za sve $i \in \{1, 2, ..., k\}$
Ako važi $NZD(m_i, m_{k+1}) \mid a_i - a_{k+1}$
$a_{k+1} - x_0 = a_{k+1} - a_i + a_i - x_0$ $NZD(m_i, m_{k+1}) \mid a_{k+1} - a_i$ $m_i \mid a_i - x_0$

Ako $NZD(m_i, m_j) \mid a_i - a_j$ za sve $i, j \in \{1, 2, ..., k+1\}$ $i \neq j$
Tada sistem od k+1 jednačina ima rešenje.

Neka je x' jedno rešenje sistema od k+1 jednačine:

$x' \equiv a_1 \pmod{m_1}$	$x \equiv a_1 \pmod{m_1}$
$x' \equiv a_2 \pmod{m_2}$	$x \equiv a_2 \pmod{m_2}$
...	...
$x' \equiv a_{k+1} \pmod{m_{k+1}}$	$x \equiv a_{k+1} \pmod{m_{k+1}}$

$\Rightarrow x' \equiv x \pmod{m_1}$ i $x' \equiv x \pmod{m_{k+1}}$
$m_1 \mid x-x'$, $m_2 \mid x-x'$ .... $m_{k+1} \mid x-x'$ $\Rightarrow NZS(m_1, m_2, ..., m_{k+1}) \mid x - x'$
$x-x' = NZS(m_1, m_2, ..., m_{k+1})*t$
$x = x' + NZS(m_1, m_2, ..., m_{k+1})*t \quad t \in Z$

Dokaz konkretni (2021):
Neka je $m = m_1 m_2 ... m_n$
$M_1 = \frac{m}{m1} = m_2 m_3 ... m_n$ $M_2 = \frac{m}{m2} = m_1 m_3 ... m_n$ ... $M_n = \frac{m}{mn} = m_2 m_3 ... m_{n-1}$

m_i je uzajamno prosto sa $m_1, m_2, ..., m_{i-1}, m_{i+1}, ..., m_n$
$\Rightarrow NZD(m_i, m_i) = 1$ za sve $i \in \{1, ..., n\}$
pa je $1 = p_i*m_i + q_i*M_i$ za sve $i \in \{1, ..., n\}$
Primetimo da je:
$q_i M_i \equiv_{mi} 1$ za sve $i \in \{1, ..., n\}$ $q_i M_i \equiv_{mj} 0$ za sve $j \neq i$ jer $m_j \mid M_i$
Neka je:
$x = a_1 q_1 M_1 + a_2 q_2 M_2 + ... + a_n q_n M_n$
$x \equiv_{mi} a_1 q_1 M_1 + a_2 q_2 M_2 + ... + a_{i-1} q_{i-1} M_{i-1} + a_i q_i M_i + a_{i+1} q_{i+1} M_{i+1} + ... + a_n q_n M_n$
$x \equiv_{mi} a_i$
Dakle x jeste rešenje sistema
Neka je x_0 ostatak pri deljenju x sa m, tj.
$x_0 \equiv_m x \quad i \quad 0 \leq x_0 < m$
Tada je $x_0 \equiv_{mi} x \equiv_{mi} a_i \Rightarrow x_0 \equiv_{mi} a_i$ za sve $i \in \{1, ..., n\}$ pa je x_0 rešenje sistema
Neka je x_1 proizvoljno rešenje, tada je $x_1 \equiv_{mi} a_i \equiv_{mi} x_0$ pa $m_i \mid x_1 - x_0$ za sve $i \in \{1, ..., n\}$
Kako su $m_1, m_2, ..., m_n$ u parovima uzajamno prosti
$\Rightarrow m \mid x_1 - x_0$ tj. $x_1 \equiv_m x_0$
$x_1 = x_0 + m*t$, $t \in Z$

Čas 12

Ojlerova funkcija

$n \geq 1$

$\varphi(n) = \{a \in N \mid 1 \leq a \leq n, NZD(a, n) = 1\}$

$\varphi(5) = \{1, 2, 3, 4\}$

Definicija

Neka je $n > 1$ prirodan broj. Sa $\varphi(n)$ označavamo broj prirodnih brojeva m tako da $1 \leq m < n$ i $NZD(m, n) = 1$. Funkcija φ se naziva Ojlerova funkcija.

$\varphi(n) = ?$ p – prost broj

$\varphi(p) = ?$

$\phi(p) = \{1, 2, 3, ..., p-1\} \Rightarrow \varphi(p) = p-1$

$\varphi(p^2) = ?$

$NZD(a, p^2) \in \{1, p, p^2\}$ za sve $a \in N$

1	2	3	...	p-1	p
p+1	p+2	p+3	...	2p-1	2p
....					
p^2-p+1				p^2-1	p^2

} p vrsta

$NZD(a, p) = 1$ akko $NZD(a, p^2) \notin \{p, p^2\}$ akko $p \nmid a$

$\varphi(p^2) = p(p-1) = p^2-p = p^2(1 - 1/p)$

$\varphi(p^n) = ?$ $n \in N$

$NZD(a, p^n) \in \{1, p, p^2, ..., p^n\}$

$NZD(a, p^n) = 1$ akko $NZD(a, p^n) \notin \{p, p^2, ..., p^n\}$ akko $p \nmid a$

1	2	3	...	p-1	p
p+1	p+2	p+3	...	2p-1	2p
....					
p				p^{n-1}	p^n

} p^{n-1} vrsta

$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p - 1) = p^n(1 - 1/p)$

Tvrđenje

Neka su $m, n > 1$ prirodni brojevi takvi da je $NZD(m, n) = 1$. Tada je $\varphi(mn) = \varphi(m)\varphi(n)$.

Dokaz:

Neka je $NZD(m, n) = 1$

$\rho_n(k)$:= ostatak pri deljenju k sa n, $\rho_n(k) \in \{0, 1, ..., n-1\}$

Posmatrajmo funkciju:

$F: \phi(mn) \to \phi(m) \times \phi(n)$ definisanu sa $F(a) = (\rho_m(a), \rho_n(a))$ i pokazujemo da je bijekcija

1. Da li je F dobro definisano?

za $a \in \phi(mn)$ treba da pokažemo da $\rho_m(a) \in \phi(m)$ i $\rho_n(a) \in \phi(n)$

$NZD(a, mn) = 1 \Rightarrow NZD(a, m) = 1$ i $NZD(a, n) = 1$

$a = mq + r$ gde je $r = \rho_m(a)$ $0 \leq r < m$

$1 = NZD(a, m) = NZD(m, r) = NZD(m, \rho_m(a)) \Rightarrow \rho_m(a) \in \phi(m)$

$a = nq + r$ gde je $r = \rho_n(a)$ $0 \leq r < n$

$1 = NZD(a, n) = NZD(n, r) = NZD(n, \rho_n(a)) \Rightarrow \rho_n(a) \in \phi(n)$

F jeste dobro definisamo

2. F je 1-1

$F(a) = F(b) \stackrel{?}{\Rightarrow} a = b$

$(\rho_m(a), \rho_n(a)) = (\rho_m(b), \rho_n(b))$

$\rho_m(a) = \rho_m(b) \Rightarrow a \equiv_m b \Rightarrow m \mid a-b$

$\rho_n(a) = \rho_n(b) \Rightarrow a \equiv_n b \Rightarrow n \mid a-b$

Kako je $NZD(m, n) = 1 \Rightarrow a \equiv_{mn} b$ tj $mn \mid a-b$ $0 \leq a, b < mn$

$-mn < a-b < mn$ i $mn \mid a-b \Rightarrow a-b = 0$ tj $a = b$

3. F je na

Neka $(r, s) \in \phi(m) \times \phi(n)$

Pokazujemo da postoji $a \in \phi(mn)$ td. $F(a) = (r, s)$ odnosno $(\rho_m(a), \rho_n(a)) = (r, s)$

Posmatramo sistem:

$x \equiv_m r$ i $x \equiv_n s$

Kako je NZD(m, n) = 1 Prema Kineskoj teoremi postoji a tdj:

$0 \leq a < mn$ i $a \equiv_m r$ i $a \equiv_n s$

Zašto $a \in \phi(mn)$?

iz $a \equiv_m r$ => NZD(r, m) = 1 => NZD(a, m) = 1

iz $a \equiv_n s$ => NZD(s, n) = 1 => NZD(a, n) = 1

} NZD(a, mn) = 1 tj. $a \in \phi(mn)$

$| \phi(mn) | = | \phi(m) | * | \phi(n) |$ tj $\varphi(mn) = \varphi(m) * \varphi(n)$

Posledica: Ako je $n = p_1^{\alpha 1} * p_2^{\alpha 2} \ldots p_k^{\alpha k}$ onda je $\varphi(n) = n(1 - 1/p_1)(1 - 1/p_2) \cdot \cdot \cdot (1 - 1/p_k)$.

Neka je $n > 1$ prirodni broj. Skup $\{r1, \ldots, rn\}$ prirodnih brojeva je potpuni sistem ostataka po modulu n ako je svaki ceo broj konguentan po modulu n tačno jednom od brojeva r_i.

Možemo primetiti da je r_i nije kongruentno po modulu n broju rj , za $i \neq j$. Jedan primer za potpuni sistem ostataka po modulu n je $\{0, 1, 2, \ldots, n-1\}$.

Ojlerova teorema

(Ojlerova teorema) Neka su a i n pozitivni prirodni brojevi, takvi da NZD(a, n) = 1. Tada važi $a^{\varphi(n)} \equiv 1 \pmod n$.

Dokaz:

$k = \varphi(n)$

$\phi(n) = \{r_1, r_2, \ldots, r_k\}$ i $NZD(r_i, n) = 1$ za sve $i \in \{1, \ldots, k\}$

$NZD(r_i, n) = 1$ $NZD(a, n) = 1$ => $NZD(ar_i, n) = 1$ pa $\rho_n(ar_i) \in \phi(n)$ (*)

Posmatramo $a*r_i$

Neka je $S_i = \rho_n(ar_i)$ Pokažimo da je $\phi(n) = \{S_1, S_2, \ldots, S_k\}$

Na osnovu (*) znamo da $S_i \in \phi(n)$

Potrebno je pokazati da je $S_i \neq S_j$ za $i \neq j$

Neka je $S_i = S_j$

$\rho_n(ar_i) = \rho_n(ar_j)$

$n | ar_i - ar_j$

$n | a(r_i - r_j)$ kako je NZD(a, n) = 1 => $n | r_i - r_j$

$1 \leq r_i, r_j < n$ pa je $-n < r_i - r_j < n$

Sledi $r_i - r_j = 0$ tj $r_i = r_j$ $i = j$

$ar_1 \equiv_n S_1$

$ar_2 \equiv_n S_2$

$\ldots ar_k \equiv_n S_k$ Pomnožimo

$a^k r_1 r_2 * \ldots * r_k \equiv_n S_1 S_2 \ldots S_k$ $r_1 * r_2 * \ldots * r_k = x$ $S_1 * S_2 * \ldots * S_k = x$

$a^k * x \equiv_n x$

Da bismo mogli da skratimo x mora važiti da je NZD(n, x) = 1

$NZD(n, r_i) = 1$ za sve $i \in \{1, \ldots, k\}$ => $NZD(n, r_1 r_2 \ldots r_k) = 1$ tj $NZD(n, x) = 1$

$a^k x \equiv_n x$ /x

$a^k \equiv_n 1$

$a^{\varphi(n)} \equiv_n 1$

Posledica: Mala Fermaova teorema: Ako je p prost broj tada je $a^p \equiv_p a$

Dokaz:

1. $p | a$

$a^p \equiv_p 0$

$a \equiv_p 0$

$a^p \equiv_n 1$

2. $p \nmid a$

NZD(a, p) = 1 Ojlerovom teoremom dobijamo:

$a^{\varphi(p)} \equiv_p 1$

$a^{p-1} \equiv_p 1$ /a

$a^p \equiv_p a$

Bulove algebre

Uveo ih je Džordž Bul sredinom 19. veka.
Definicija
Algebarska struktura B = (B, $\curlyvee$, $\curlywedge$,' , 0, 1), gde je B≠∅, 0, 1 ∈ B, $\curlyvee$ i $\curlywedge$ su binarne a ' je unarna operacija na skupu B, je Bulova algebra ukoliko su zadovoljene sledeće aksiome:
A1: x $\curlyvee$ y = y $\curlyvee$ x,
A2: x $\curlywedge$ y = y $\curlywedge$ x,
A3: x $\curlyvee$ (y $\curlywedge$ z) = (x $\curlyvee$ y) $\curlywedge$ (x $\curlyvee$ z),
A4: x $\curlywedge$ (y $\curlyvee$ z) = (x $\curlywedge$ y) $\curlyvee$ (x $\curlywedge$ z),
A5: x $\curlyvee$ 0 = x,
A6: x $\curlywedge$ 1 = x,
A7: x $\curlyvee$ x' = 1,
A8: x $\curlywedge$ x' = 0,
A9: 0 ≠ 1
za svako x, y , z ∈ B.
Operacije $\curlyvee$, $\curlywedge$ i ' redom nazivamo bulovska disjunkcija, bulovska konjunkcija i bulovski komplement. Kada je u nekom kontekstu jasno da se radi o bulovskim operacijama tada ih kraće nazivamo konjunkcija, disjunkcija i komplement. Skup B nazivamo domen. Ukoliko je skup B konačan, tada je kažemo da je Bulova algebra B konačna, inače kažemo da je beskonačna.

Primeri Bulovih algebri
Primer 1: (Prekidačka algebra) Algebarska struktura 2 = ({0, 1}, ∨, ∧, ¬, 0, 1), gde su operacije ∨, ∧ i ¬ definisane na sledeći način je Bulova algebra.

∨	0	1
0	0	1
1	1	1

∧	0	1
0	0	0
1	0	1

¬	
0	1
1	0

Ovako definisane operacije su, u stvari, logička disjunkcija (∨), logička konjunkcija (∧) i negacija (¬).

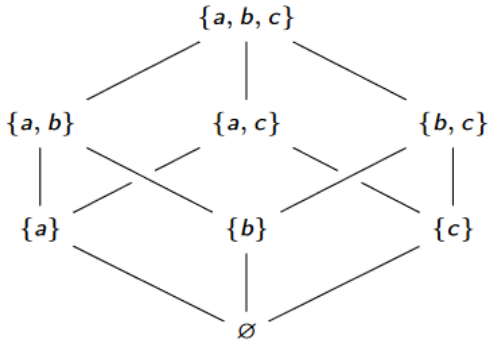
Primer 2: (Algebra partitivnog skupa) Neka je X proizvoljan neprazan skup i P(X) partitivni skup skupa X . Skup P(X) zajedno sa operacijama unije, preseka i skupovnog komplementiranja (u
odnosu na skup X) i istaknutim elementima ∅ i X qini Bulovu algebru P(X) = (P(X), ∪, ∩,c , ∅, X).
Ako A, B, C ∈ P(X), jednakosti Bulove algebre
A1: A ∪ B = B ∪ A,
A2: A ∩ B = B ∩ A,
A3: A ∪ (B ∩ C) = (A ∪ B) ∩ (A ∪ C),
A4: A ∩ (B ∪ C) = (A ∩ B) ∪ (A ∩ C),
A5: A ∪ ∅ = A,
A6: A ∩ X = A,
A7: A ∪ A^c = X ,
A8: A ∩ A^c = ∅,
A9: X≠ ∅.
su poznati skupovni identiteti.

Princip dualnosti
Identiteti F_1 i F_2 su dualni ako se identitet F_2 može dobiti od identiteta F1 tako što se svako pojavljivanje operacije $\curlyvee$ zameni sa $\curlywedge$, svako pojavljivanje operacije $\curlywedge$ zameni sa $\curlyvee$, svako pojavljivanje 0 zameni sa 1 i svako pojavljivanje 1 zameni sa 0.
Primer: Identiteti (x $\curlyvee$ y) $\curlywedge$ y ' = x i (x $\curlywedge$ y) $\curlyvee$ y ' = x su dualni identiteti, kao i identiteti (x $\curlywedge$ 0) $\curlywedge$ (1 $\curlyvee$ x) = x' $\curlyvee$ 0 i (x $\curlyvee$ 1) $\curlyvee$ (0 $\curlywedge$ x) = x' $\curlywedge$ 1.
Neka je ϕ($\curlyvee$, $\curlywedge$,' , 0, 1) proizvoljan Bulov iskaz. Tada je ϕ($\curlyvee$, $\curlywedge$,' , 0, 1) teorema akko je ϕ($\curlywedge$, $\curlyvee$,' , 1, 0) teorema.
Aksiome su dualne i princip dualnosti je direktna posledica toga.

Tvrđenje (osnovni zakoni Bulovih algebri)
U proizvoljnoj Bulovoj algebri B = (B, ∨, ∧,' , 0, 1) za sve x, y , z ∈ B važe sledeći identiteti:
1. 0' = 1, 1' = 0;
2. x ∨ x = x, x ∧ x = x (zakon idempotecije);
x $=^{5}$= x∨0 $=^{8}$= x∨(x∧x') $=^{3}$= (x∨x)∧(x∨x') $=^{7}$= x ∨ x

x $=^{6}$= x∧1 $=^{7}$= x∧(x∨x') $=^{4}$= (x∧x)∨(x∧x') $=^{8}$= (x∧x)∨0 $=^{5}$= x∧x
3. x ∨ (x ∧ y) = x, x ∧ (x ∨ y) = x (zakon apsorpcije);
4. Ako je x ∨ y = 1 i x ∧ y = 0, tada je x = y ' . (jedinstvenost komplementa)
5. (x')' = x (zakon involucije);
6. x ∨ (y ∨ z) = (x ∨ y) ∨ z, x ∧ (y ∧ z) = (x ∧ y) ∧ z (zakon asocijativnosti);
7. (x ∧ y)' = x' ∨ y ' , (x ∨ y)' = x' ∧ y ' (De Morganovi zakoni)

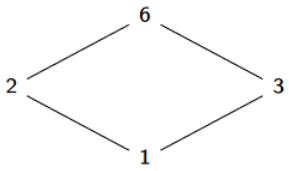
Bulovo uređenje
Neka je struktura B = (B, ∨, ∧,' , 0, 1) Bulova algebra. Na skupu B možemo definisati relaciju parcijalnog uređenja na sledeći način: x ≼ y akko x ∧ y = x
≼ je relacija poretka:
R: x ∈ B x≼x? x∧x = x T na osnovu idempotencije
AS: x ≼ y i y≼x => x=y?
x = x∧y = y∧x = y
T: x ≼ y i y≼z => x≼z?
x∧y = x i y∧z = y $=^{?}$> x∧z = x?
x∧z = x∧y∧z = x∧(y∧z) = x∧y = x
Par (B, ≼) je parcijalno uređeni skup. Ukoliko je domen B konačan, Bulovu algebru B možemo predstaviti grafički pomoću Haseovog dijagrama.
Primer: Posmatrajmo Bulovu algebru: P({a, b, c}) = (P({a, b, c}), ∪, ∩,c , ∅, {a, b, c}).
Važi da je P({a, b, c}) = {∅, {a}, {b}, {c}, {a, b}, {a, c}, {b, c}, {a, b, c}}. Na skupu P({a, b, c}) definisano je Bulovo uređenje ≼ sa:
A ≼ B akko A ∩ B = A akko A ⊆ B.
Bulovu algebru P({a, b, c}) predstavljamo pomoću Haseovog dijagrama na sledeći način:



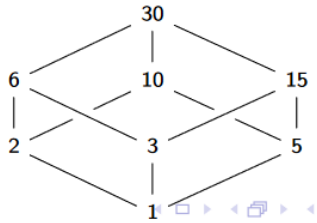
Primer: Na skupu D30 = {1, 2, 3, 5, 6, 10, 15, 30} (tj. skupu delilaca broja 30), definisane su binarne operacije nzs(x, y) i nzd(x, y), kao i unarna operacija 30/x, za sve x, y ∈ B. Struktura D30 = (D30, nzs, nzd, 30/, 1, 30) je Bulova algebra.Za sve x, y ∈ D30, ispunjeni su sledeći uslovi:
A1: nzs(x, y) = nzs(y , x),
A2: nzd(x, y) = nzd(y , x),
A3: nzs(x, nzd(y , z)) = nzd(nzs(x, y), nzs(x, z)),
A4: nzd(x, nzs(y , z)) = nzs(nzd(x, y), nzd(x, z)),
A5: nzs(x, 1) = x,
A6: nzd(x, 30) = x,
A7: nzs(x, 30/x) = 30,
A8: nzd(x, 30/x) = 1,
A9: 1⁄= 30.

Generalno, ukoliko je prirodan broj n proizvod različitih prostih brojeva i D_n skup svih delilaca broja n, tada je struktura $D_n = (D_n , nzs, nzd, n/, 1, n)$ Bulova algebra. Bulovo uređenje $\preccurlyeq$ na skupu D_n definisano je sa:
$x \preccurlyeq y$ akko $nzd(x, y) = x$ akko $x \mid y$.
Haseovi dijagrami parcijalno uređenih skupova $(D_6, |)$ i $(D_{30}, |)$. ($D_6 = \{1, 2, 3, 6\}$ i $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$)

D_6 :



D_{30} :



Uređenje $\preccurlyeq$ je saglasno sa operacijama:

1. $x \preccurlyeq y$ onda je $x \curlywedge z \preccurlyeq z \curlywedge y$
Dokaz: vazi $x \preccurlyeq y$ tj. $x \curlywedge y = y$
Dokazujemo $x \curlywedge y \preccurlyeq y \curlywedge z$ tj. $(x \curlywedge z) \curlywedge (y \curlywedge z) = x \curlywedge z$
$(x \curlywedge z) \curlywedge (y \curlywedge z) = x \curlywedge y \curlywedge z \curlywedge z = x \curlywedge z$

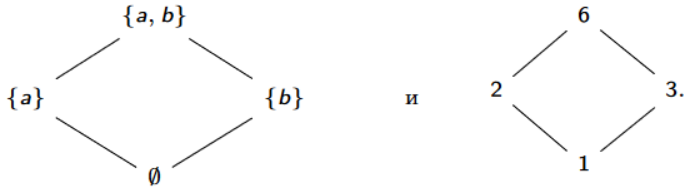
2. $x \preccurlyeq y$ onda je $x \curlyvee z \preccurlyeq y \curlyvee z$
Dokaz: vazi $x \preccurlyeq y$ tj. $x \curlywedge y = y$
Dokazujemo $x \curlyvee z \preccurlyeq y \curlyvee z$ tj. $(x \curlyvee z) \curlywedge (y \curlyvee z) = x \curlyvee z$
$(x \curlyvee z) \curlywedge (y \curlyvee z) = (x \curlywedge y) \curlyvee z = x \curlyvee z$

Atomi
Definicija
Neka je $B = (B, \curlyvee, \curlywedge, ', 0, 1)$ proizvoljna Bulova algebra. Element $a \in B$ je atom ukoliko važi sledeće:
1) $0 \prec a$;
2) ako postoji $y \in B$ takvo da je $0 \preccurlyeq y \preccurlyeq a$, tada je $y = 0$ ili je $y = a$.
U generalnom slučaju, Bulova algebra ne mora da sadrži atome. Ukoliko Bulova algebra ne sadrži nijedan atom, kažemo da je bezatomična. Konačne Bulove algebre uvek imaju atome. Šta više, svaki element proizvoljne konačne Bulove algebre može se predstaviti kao bulovska disjunkcija atoma.
Tvrđenje
Neka je $B = (B, \curlyvee, \curlywedge, ', 0, 1)$ konačna Bulova algebra, tada važi sledeće:
1. Ako je $x \neq 0$ i $x \in B$, tada postoji atom $a \in B$ takav da je $a \preccurlyeq x$.
2. Ako je $x \neq 0$ i $x \in B$, tada je $x = \curlyvee\{a \mid a \in B$ je atom i $a \preccurlyeq x\}$.
Dokaz 1:
Neka je $x \in B$ tada postoji element $a \in B$ tdj $a \leq x$ Ako je x atom onda je $a = x$.
ako x nije atom onda postoj $x' \in B$ tdj $0<x'<x$ ako je x' atom onda $a=x'$ u suprotnom postoji $x'' \in B$ tdj $0<x''<x'<x$
analiziramo x'' i nastaljamo proces B je konačan skup pa se proces mora završiti u konačno mnogo koraka.
2. Neka je $x \in B$ tada je $x = \{a \mid a \in B$ atom i $a \leq x\}$
Neka je $y = \curlyvee\{a \mid a \in B$ atom i $a \leq x\}$ Pokažimo da je $y = x$ $\{a \mid a \in B$ atom i $a \leq x\} = \{a_1, a_2, ..., a_k\}$
$y = a_1 \curlyvee a_2 \curlyvee a_3 \curlyvee ... \curlyvee a_k$ i važi $a_i \leq x$ tj. $a_i \curlyvee x = a_i$ za sve $i \in \{1, ..., k\}$
$y \curlywedge x = (a_1 \curlyvee a_2 \curlyvee a_3 \curlyvee ... \curlyvee a_k) \curlywedge x = (a_1 \curlywedge x) \curlyvee (a_2 \curlywedge x) \curlyvee ... \curlyvee (a_k \curlywedge x) = a_1 \curlyvee a_2 ... \curlyvee a_k = y$
$\Rightarrow y \leq x$
PPS. $y \neq x$ tj. da je $y<x$
Posmatrajmo element $y' \curlywedge x$ $y' \curlywedge x \geq 0$ uvek vazi Pokazimo da je $y' \curlywedge x > 0$
Ako bi bilo $y' \curlywedge x = 0$ tada bi
$x \curlywedge y = (x \curlywedge y) \curlyvee 0 = (x \curlywedge y) \curlyvee (x \curlywedge y') = x \curlywedge (y \curlyvee y') = x \curlywedge 1 = x \Rightarrow x \leq y$ Kontradikcija!
Dakle $y' \curlywedge x > 0$ pa postoji atom $c \in B$ tdj c atom i $c \leq y' \curlywedge x$
$c \curlywedge y' \curlywedge x = c$
$c \curlywedge y' = (c \curlywedge y \curlywedge x) \curlywedge y' = c \curlywedge x \curlywedge y' \curlywedge y' = c \curlywedge x \curlywedge y' = c \Rightarrow c \leq y'$
$c \curlywedge x = (c \curlywedge y' \curlywedge x) \curlywedge x = c \curlywedge y' \curlywedge x \curlywedge x = c \curlywedge y' \curlywedge x = c \Rightarrow c \leq x$
Kako je $c \leq x$, c je atom $\Rightarrow c = a_i$ za neko i iz $\{1,...,k\}$
$c \curlywedge y = a_i \curlywedge (a_1 \curlyvee a_2 \curlyvee ... \curlyvee a_i \curlyvee ... \curlyvee a_k) = a_i = c \Rightarrow c \leq y$
Zakljucili smo da je $c \leq y'$ i $c \leq y$: $c \curlywedge y' = c$ $c \curlywedge y = c$
$c = c \curlywedge c = (c \curlywedge y') \curlywedge (c \curlywedge y) = c \curlywedge c \curlywedge y' \curlywedge y = c \curlywedge 0 = 0$ Kontradikcija c je atom pa ne moze biti 0 Dakle $x = y$

Izomorfizam Bulovih algebri

Haseovi dijagrami Bulovih algebri

P({a, b}) = (P({a, b}), ∪, ∩,C , ∅, {a, b}) i D6 = ({1, 2, 3, 6}, nzs, nzd, 6/, 1, 6)



Prethodna dva dijagrama su identična (do na oznaku elemenata). Tabele operacija ovih Bulovih algebri razlikuju se do na oznaku elemenata i oznaku operacija.

∪	∅	{a}	{b}	{a, b}
∅	∅	{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

∩	∅	{a}	{b}	{a, b}
∅	∅	∅	∅	∅
{a}	∅	{a}	∅	{a}
{b}	∅	∅	{b}	{b}
{a, b}	∅	{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
∅	{a, b}
{a}	{b}
{b}	{a}
{a, b}	∅

⟷

x	$6/x$
1	6
2	3
3	2
6	1

Izomorfizam Bulovih algebri

<u>Definicija</u>

Bulove algebre B = (B, ϒ, ʌ,’ , 0, 1) i B^* = (B^* , $ϒ^*$, $ʌ^*$,’* , 0^* , 1^*) su izomorfne ukoliko postoji bijekcija f : B → B^* za koju važi:

1) f (x ϒ y) = f (x) $ϒ^*$ f (y),

2) f (x ʌ y) = f (x) $ʌ^*$ f (y),

3) f (x’) = f (x)’*,

za sve x, y ∈ B. Izomorfizam Bulovih algebri B i B∗ oznaqavamo sa: B ∼= B^* .

<u>Stonova teorema</u>

Ako je B = (B, ϒ, ʌ,’ , 0, 1) konaqna Bulova algebra tada postoji konaqan skup S takav da je

B ∼= P(S).

Dokaz:

Za svaku konačnu Bulovu algebru B = (B, ϒ, ʌ,’ , 0, 1) postoji skup S takav da postoji preslikavanje f : B → P(S) koje je bijekcija i za koju važi:

1) f (x ϒ y) = f (x) U f (y)

2) f (x ʌ y) = f (x) ∩ f (y),

3) f (x’) = f $(x)^c$ = x \ f(x)

Dokaz:

x ∈ B S = {a ∈ B | a je atom u B} x = ϒ{ a ∈ B | a je atom i a ≤ x} = a_1 ϒ a_2 ϒ...ϒ a_n

f(x) := {a_1, a_2, ..., a_n}

1. f je homomorfizam

1) f(x ϒ y) = f(x) U f(y) ?

a ∈ f(x ϒ y) => a je atom a ≤ x ϒ y

a ʌ (x ϒ y) = a

(a ʌ x) ϒ (a ʌ y) iz ova dva sledi (a ʌ x) ϒ (a ʌ y) = a pa mora vaziti: a ʌ x = a ili a ʌ y = a

tj a ≤ x ili a ≤ y <=> a ∈ f(x) ili a ∈ f(y) Dakle a ∈ f(x) U f(y)

2) $f(x \wedge y) = f(x) \cup f(y)$?
$a \in f(x \wedge y) \Rightarrow a$ je atom $a \leq x \wedge y$
$a \wedge x \wedge y = a$
$a \leq x$ i $a \leq y$ $\Leftrightarrow$ $a \in f(x)$ i $a \in f(y)$ Dakle $a \in f(x) \cap f(y)$

3) $f(x') = X \setminus f(x)$
$a \in f(x)$
a je atom i $a \leq x'$
Ako je $a \leq x$ tada je $a = a \wedge a = (a \wedge x') \wedge (a \wedge x) = a \wedge a \wedge x' \wedge x = a \wedge 0 = 0$ Kontradikcija sa a je atom
Dakle $a > x$ pa $a \notin X \setminus f(x)$

2. f je "na"
Neka $A \subseteq X$ $A \in P(X)$
Da li postoji $x \in B$ tdj $f(x) = A$?
$x = \{a \mid a \in A\}$
$A = \{a_1, a_2, ..., a_k\}$
$X = a_1 \vee a_2 \vee ... \vee a_k$

$A \subseteq f(x)$:
$a \in A \Rightarrow a = a_i$ za neko $i \in \{1, ..., k\}$
$a_i \wedge x = a_i \wedge (a_1 \vee a_2 \vee ... \vee a_k) = a_i$
$a_i \leq x$ a_i je atom $a_i = a$ $\Rightarrow$ $a \in f(x)$

$f(x) \subseteq A$:
Neka $b \in f(x)$
b je atom i $b \leq x$
$b \wedge x = b \wedge (a_1 \vee a_2 \vee ... \vee a_k) = (b \wedge a_1) \vee (b \wedge a_2) \vee ... \vee (b \wedge a_k) = b$
pa za bar jedno $i \in \{1, ..., k\}$ vazi $(b \wedge a_i)$ $\Rightarrow$ $b \leq a_i$ b, a_i atomi $\overset{\text{iz ova dva}}{\Rightarrow}$ $b = a_i \in A$

3. f je "1-1"
$f(x) = f(y) \overset{?}{\Rightarrow} x = y$
Pokažimo da iz $f(x) \subseteq f(y) \Rightarrow x \leq y$:
pps: $x \not\leq y$
postoji atom $a \leq x$ i $a \not\leq y$
$\Rightarrow a \in f(x)$ i $a \notin f(y) \Rightarrow f(x) \not\subseteq f(y)$ Kontradikcija jer jeste podskup
Dakle iz sledeca dva dobijamo
$f(x) \subseteq f(y) \Rightarrow x \leq y$
$f(y) \subseteq f(x) \Rightarrow y \leq x \Rightarrow x = y$

Konačnu Bulova algebru moguće je konstruisati samo na skupovima koji imaju 2^m elemenatam, gde je $m \geq 1$.