RASELOV PARADOKS
$S = \{x \mid x \notin x\}$ – Ako $S \in S$, onda $S \notin S$ i obrnuto.

AKSIOMA EGZISTENCIJE
Dva skupa su jednaka ako imaju iste elemente.

AKSIOMA PRAZNOG SKUPA
Postoji skup koji nema nijedan element. Označavamo sa $\emptyset$. Prazan skup je jedinstven. Prazan skup je podskup svakog skupa.

PODSKUP
Skup A je podskup skupa B (oznaka $A \subseteq B$) ako za sve $x \in A$ važi da $x \in B$.

AKSIOMA PARTITIVNOG SKUPA
Za svaki skup X postoji skup $\mathcal{P}(x)$ koji se sastoji od svih podskupova skupa X.
$\mathcal{P}(x) = \{Y \mid Y \subseteq X\}$

AKSIOMA IZDVAJANJA PODSKUPA (AKSIOMA SEPARACIJE)
Ako je A skup i P(x) neka formula, onda postoji skup $\{x \in A \mid P(x)\}$.

AKSIOMA UNIJE
Za svaki skup X postoji postoji skup Z tako da $u \in Z$ ako i samo ako $u \in Y$ za neko $Y \in X$.
Skup Z predstavlja uniju članova skupa X i označavamo ga sa $\cup X$.
$\cup \{A, B\} = A \cup B$

INDEKSIRANA FAMILIJA SKUPOVA
Indeksirana familija skupova je familija skupova $\mathcal{F}$ koja je oblika $\mathcal{F} = \{A_i \mid i \in I\}$ gde je I indeksni skup.

UREDJENI PAR
Uredjeni par elemenata a i b je objekat (a, b) koji zadovoljava osobinu $(a, b) = (c, d)$ akko $a = c$ i $b = d$.
Uredjeni par možemo definisati:
$(a, b) \coloneqq \{\{a\}, \{a, b\}\}$

DEKARTOV PROIZVOD SKUPOVA
Dekartov proizvod skupova A i B je skup $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

UREDJENA N-TORKA
Uredjena n-torka elemenata $a_1, a_2, \dots, a_n$ je objekat $(a_1, a_2, \dots, a_n)$ takav da važi:
$(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_n)$ ako i samo ako $a_1 = b_1, a_2 = b_2, \dots, a_n = b_n$.

REKURZIVNA DEFINICIJA UREDJENE N-TORKE
$(a_1, a_2, \dots, a_n) \coloneqq \Big(a_1, \big(a_2, (\dots, (a_{n-1}, a_n) \dots)\big)\Big)$.

DEKARTOV STEPEN SKUPA
$A^n \coloneqq A \times A \times \dots \times A \quad (n \geq 1)$
Specijalno: $A^0 \coloneqq \{\emptyset\}$

BINARNA RELACIJA

Binarna relacija izmedju skupova A i B je bilo koji podskup $\rho \subseteq A \times B$. Pišemo $a\rho b$ $(a \in A, b \in B)$.
Ako je $A = B$, tj. ako $\rho \in A^2$, kažemo da je ρ binarna relacija na skupu A.

N-ARNA RELACIJA

N-arna relacija izmedju skupova $A_1, \dots, A_n$ je bilo koji podskup $\rho \subseteq A_1 \times A_2 \times \dots \times A_n$.
Ako je $A_1 = A_2 = \cdots = A_n = A$, tj. ako $\rho \in A^n$, kažemo da je ρ n-arna relacija na skupu A.

Za $n = 1$, $\rho \subseteq A$ je unarna relacija na A.

DOMEN RELACIJE

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

IMIDŽ/SLIKA RELACIJE

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

INVERZNA RELACIJA

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

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

KOMPOZICIJA RELACIJA

Ako $\rho \subseteq A \times B, \sigma \subseteq B \times C$:
$\sigma \circ \rho = \{(a, c) \in A \times C \mid (a, b) \in \rho,\ (b, c) \in \sigma,\ b \in B\} \subseteq A \times C$ je kompozicija ρ i σ.

RELACIJE NA SKUPU A

$\rho \subseteq A \times A$
Kažemo da je ρ:

- **refleksivna** ako za $\forall a \in A$ važi $a\rho a$ $((a, a) \in \rho)$
- **antirefleksivna** ako za $\forall a \in A$ NE važi $a\rho a$
- **simetrična** ako za $\forall a, b \in A$: $a\rho b \Longrightarrow b\rho a$
- **antisimetrična** ako za $\forall a, b \in A$: $a\rho b \wedge b\rho a \Longrightarrow a = b$
- **asimetrična** ako za $\forall a, b \in A$: $a\rho b \Longrightarrow$ NE važi $b\rho a$
- **tranzitivna** ako za $\forall a, b, c \in A$: $a\rho b \wedge b\rho c \Longrightarrow a\rho c$

RELACIJA DIJAGONALA

$\Delta_A \subseteq A \times A$
$\Delta_A = \{(a, a) \mid a \in A\}$ – dijagonala

RELACIJA EKVIVALENCIJE

Relacija $\rho \subseteq A^2$ je ekvivalencija ako je refleksivna, simetrična i tranzitivna.

KLASA EKVIVALENCIJE

Neka je $\rho \subseteq A^2$ ekvivalencija. Klasa ekvivalencije elementa $a \in A$ je skup:
$C_a = a_{/\rho} = [a]_\rho = \{x \in A \mid a\rho x\}$
Zbog simetričnosti važi $[a]_\rho = \{x \in A \mid x\rho a\}$.

KOLIČNIČKI SKUP EKVIVALENCIJE

Neka je $\rho \subseteq A^2$ relacija ekvivalencije. Količnički skup ekvivalencije ρ je skup:
$A_{/\rho} = \{C_a \mid a \in A\} \subseteq \mathcal{P}(A)$

PARTICIJA SKUPA

Particija skupa A je bilo koji podskup $P \subseteq \mathcal{P}(A)$ koji zadovoljava sledeće uslove:

1. Ako $X, Y \in P$ i $X \neq Y$, važi $X \cap Y = \emptyset$
2. $\cup P = A$
3. Za svako $X \in P$ važi $X \neq \emptyset$

$A_{/\rho}$ je particija skupa A.

RELACIJA PORETKA

Refleksivna, antisimetrična, tranzitivna.

Elementi a i b su uporedivi ako važi $a\rho b$ ili $b\rho a$. Inače su neuporedivi.

LINEARNI (TOTALNI) POREDAK

Poredak je linearan ako su svaka dva elementa uporediva. Inače, poredak je parcijalan.

MINIMALNI, MAKSIMALNI, NAJMANJI I NAJVEĆI ELEMENT

Neka je ρ uredjenje na skupu A i neka je $B \subseteq A$.
$a\rho b$ čitamo "a je ρ-manje od b."

- b je **najmanji** element (***minimum***) skupa B ako $b \in B$ i za sve $x \in B$ važi $b\rho x$.
- b je **najveći** element (***maksimum***) skupa B ako $b \in B$ i za sve $x \in B$ važi $x\rho b$.
- b je **minimalan** element skupa B ako $b \in B$ i važi:
  ako $x\rho b$, onda je $x = b$ za sve $x \in B$ (ne postoji ništa ρ-manje od b).
- b je **maksimalan** element skupa B ako $b \in B$ i važi:
  ako $b\rho x$, onda je $x = b$, za sve $x \in B$ (ne postoji ništa ρ-veće od b).

OGRANIČENJE SKUPA

Neka je $\rho \subseteq A^2$ poredak, $B \subseteq A$ i $a \in A$.

- a je **donje ograničenje** skupa B ako $a\rho x$ za sve $x \in B$.
- a je **gornje ograničenje** skupa B ako $x\rho a$ za sve $x \in B$.
- **infimum** ($\inf(B)$) je najveće donje ograničenje od B (ako postoji).
- **supremum** ($\sup(B)$) je najmanje gornje ograničenje od B (ako postoji).

Ako postoji minimum od B, onda je on inf(B).
Ako postoji maksimum od B, onda je on sup(B).

FUNKCIJA

Relacija $f \subseteq A \times B$ je funkcija ako i samo ako: za svaki element $a \in A$ postoji tačno jedan element $b \in B$ tako da je afb (tj. $(a, b) \in f$). Pišemo $f: A \to B$.

A je domen funkcije f, a B je kodomen funkcije.
Slika funkcije f je skup $Im(f) = \{f(a) \mid a \in A\} \subseteq B$.

INVERZNA FUNKCIJA

Relacija $f^{-1} \subseteq B \times A$ je funkcija ako i samo ako: za svako $b \in Im(f)$ postoji tačno jedno $a \in A$ takvo da $(b, a) \in f^{-1}$, odnosno akko za svako $b \in Im(f)$ postoji tačno jedno a takvo da je $(a, b) \in f$.
f^{-1} je funkcija ako i samo ako je f "1-1". $f^{-1}: B \to A$ ako i samo ako je f bijekcija.

"1-1" FUNKCIJA

f je "1-1" (injektivna) ako za sve $a_1, a_2 \in A$ važi:
Ako je $f(a_1) = f(a_2)$, tada je $a_1 = a_2$.

"NA" FUNKCIJA

f je "NA" (surjektivna) ako za sve $b \in B$ postoji $a \in A$ takvo da je $b = f(a)$.
Odnosno, $Im(f) = B$.

BIJEKCIJA

f je bijekcija ako je i "1-1" i "NA".

KOMPOZICIJA FUNKCIJA

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

IDENTITET

$id_A: A \to A$ je definisana sa $id_A(a) = a$ za sve $a \in A$.

DIREKTNA I INVERZNA SLIKA SKUPA

Neka $f: X \to Y, A \subseteq X, B \subseteq Y$

- Direktna slika skupa A pri preslikavanju f je skup $f[A] = \{f(x) \mid x \in A\} \subseteq Y$.
- Inverzna slika skupa B pri preslikavanju f je skup $f^{-1}[B] = \{x \in X \mid f(x) \in B\} \subseteq X$.

KARAKTERISTIČNE FUNKCIJE

Neka je U skup (univerzum) za $A \subseteq U$ definišemo funkciju $\chi_A: U \to 2$ na sledeći način:

$$\chi_A \begin{cases} 0, x \notin A \\ 1, x \in A \end{cases}$$

Funkciju χ_A zovemo karakteristična funkcija.

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

$A = B$ ako i samo ako $\chi_A = \chi_B$.

KARDINALNOST

Neka su A i B skupovi:

1. Kažemo da je skup A kardinalnosti manje ili jednake od B, oznaka $|A| \leq |B|$, ako postoji "1-1" funkcija $f: A \to B$.
2. Kažemo da je A jednake kardinalnosti sa B, $|A| = |B|$, ako postoji bijekcija $f: A \to B$.
3. Kažemo da je kardinalnost od A strogo manja od B, $|A| < |B|$, ako $|A| \leq |B| \wedge |A| \neq |B|$.

KANTOROVA TEOREMA

Za svaki skup X važi $|X| < |\mathcal{P}(X)|$.

PREBROJIV SKUP

Skup A je prebrojiv ako je iste kardinalnosti kao skup prirodnih brojeva (tj. $|A| = |\mathbb{N}|$).

KONAČAN SKUP

Skup A je konačan ako ima *n* elemenata, gde je *n* prirodan broj. Ako A nije konačan, onda je beskonačan.

A je beskonačan akko postoji pravi podskup $A' \subset A$ takav da su A i A' u bijekciji. Skup $\mathbb{N}$ je beskonačan.

Ako je skup konačan ili prebrojiv, kažemo da je najviše prebrojiv. Inače je neprebrojiv.

KANTOR-BERNŠTAJNOVA TEOREMA

Ako postoji injekcija $A \to B$ i surjekcija $A \to B$, onda postoji bijekcija $A \to B$.

AKSIOMA IZBORA

Neka je dat skup F čija su svi elementi neprazni skupovi i medjusobno disjunktni. Tada postoji skup C takav da je $C \cap X$ jednočlan za sve $x \in F$. Taj skup se naziva izborni skup (transverzala).

AKSIOMA DOBROG ZASNIVANJA (REGULARNOSTI)

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

Posledice:

- Ne postoji skup X takav da je $X \in X$.
- Ne postoje skupovi X i Y takvi da $X \in Y$ i $Y \in X$.
- Ne postoji niz skupova $X_0, X_1, \ldots$ takvih da $X_0 \ni X_1 \ni X_2 \ni \cdots$

PEANOVE AKSIOME

- Π_1: 0 je prirodan broj.
- Π_2: Ako je x prirodan broj, onda je i x' (njegov naslednik) prirodan broj.
- Π_3: Ako su x i y prirodni brojevi i $x' = y'$, onda je $x = y$.
- Π_4: Za svaki prirodan broj x važi $x' \neq 0$.
- Π_5: 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 prirodan broj ima svojstvo Φ.

FON NOJMANOV MODEL PRIRODNIH BROJEVA

$0 \coloneqq \emptyset$
$n' \coloneqq n \cup \{n\}$

$1 \coloneqq 0' = 0 \cup \{0\} = \emptyset \cup \{\emptyset\} = \{\emptyset\} = \{0\}$
$2 \coloneqq 1' = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\}$
$3 \coloneqq 2' = 2 \cup \{2\} = \{2\} \cup \{0, 1\} = \{0, 1, 2\}$
…
$n + 1 = n' = n \cup \{n\} = \{0, 1, \dots, n-1\} \cup \{n\} = \{0, 1, 2, \dots, n\}$

AKSIOMA INDUKCIJE

Peanovu aksiomu Π_5 nazivamo aksiomom indukcije.
Uslov 1. nazivamo baza indukcije. Uslov 2. nazivamo induktivni korak.

PRINCIP POTPUNE INDUKCIJE

Neka je Φ svojstvo prirodnih brojeva i neka važi: ako je tačno $\Phi(0), \Phi(1), \dots, \Phi(\mathrm{n})$ tačno je i $\Phi(\mathrm{n}')$ za sve $n \in \mathbb{N}$ (dakle, Φ(n) važi za sve prirodne brojeve).

PRINCIP NAJMANJEG ELEMENTA

Ako je $A \subseteq \mathbb{N}$ i $A \neq \emptyset$ onda A ima najmanji element.

DELJIVOST

U $\mathbb{N}$:
$a|b$ akko $b = a \cdot q$ za neko $q \in \mathbb{N}$. | je relacija poretka.

DELJENJE U $\mathbb{Z}$

Neka su $a, b \in \mathbb{Z}$ i $b \neq 0$. Tada postoje jedinstveni $q, r \in \mathbb{Z}$ takvi da je:
$a = b \cdot q + r$, gde je $0 \leq r < |b|$.

NZD

Neka $a, b \in \mathbb{Z}$.
Broj $d \geq 0$ je najveći zajednički delilac od a i b, kraće NZD(a, b), ako zadovoljava sledeće uslove:

- $d|a$ i $d|b$
- ako $e|a$ i $e|b$, onda $e|d$.

NZS

Neka $a, b \in \mathbb{Z}$.
Broj $s \geq 0$ je najmanji zajednički sadržalac od a i b, kraće NZS(a, b), ako zadovoljava sledeće uslove:

- $a|s$ i $b|s$
- ako $a|t$ i $b|t$, onda $s|t$.

DIOFANTOVE JEDNAČINE

Jednačina oblika:
$ax + by = c \quad (a, b, c \in \mathbb{Z};\ a, b \neq 0)$
Ima rešenje akko $NZD(a, b) \mid c$.

PROSTI BROJEVI

Broj $p > 1$ je prost ako su mu jedini delioci 1 i p.
Ako $p|ab$ onda $p|a$ ili $p|b$, odnosno ako $p|a_1 a_2 \dots a_k \Longrightarrow p|a_1\ ili\ p|a_2\ ili \dots ili\ p|a_k$.
Svaki prirodan broj $n > 1$ je prost ili se može predstaviti kao proizvod prostih brojeva.

OSNOVNA TEOREMA ARITMETIKE

Svaki prirodan broj $n > 1$ se (do na redosled članova) na jedinstven način zapisuje kao proizvod prostih.

KONGRUENCIJA PO MODULU

Neka je $m \geq 2$. Definišemo binarnu relaciju $\equiv_m$ na $\mathbb{Z}$ sa: $a \equiv_m b\ \ akko\ \ m|(a - b)$.

VILSONOVA TEOREMA

Ako je p prost broj, tada je $(p - 1)! \equiv_p -1$

KINESKA TEOREMA O OSTACIMA

Neka su $m_1, m_2, \dots, m_n \geq 2$ uzajamno prosti u parovima i neka su $a_1, a_2, \dots, a_n \in \mathbb{Z}$.
Tada sistem kongruencija $\begin{cases} x \equiv_{m1} a_1 \\ \quad \cdots \\ x \equiv_{mn} a_n \end{cases}$ ima rešenje, jedinstveno u intervalu $[0, m_1 m_2 \dots m_n)$.
Opšte rešenje je oblika $x_0 + t \cdot m_1 m_2 \dots m_n$ gde $t \in \mathbb{Z}$, a $x_0 \in \big[0, NZS(m_1, \dots, m_n)\big)$.

OJLEROVA FUNKCIJA

Ojlerov skup: $\Phi(n) = \{a \mid 1 \leq a \leq n,\ NZD(a, n) = 1\}$ za $n \geq 1$.
Na primer: $\Phi(12) = \{1, 5, 7, 11\};\ \Phi(5) = \{1, 2, 3, 4\}$; itd.

Ojlerova funkcija: $\varphi(n) = |\Phi(n)|$ – broji koliko ima elemenata koji su uzajamno prosti sa n.
Na primer: $\varphi(5) = \varphi(12) = 4$

p – prost broj:

$\varphi(p) = p - 1$
$\varphi(p^n) = p^n \left(1 - \frac{1}{p}\right)$

Ojlerova funkcija je multiplikativna, tj. $\varphi(mn) = \varphi(m) \cdot \varphi(n)$ kad god $NZD(m, n) = 1$

OJLEROVA TEOREMA

Neka je $NZD(a, n) = 1$, tada je $a^{\varphi(n)} \equiv_n 1$.

MALA FERMAOVA TEOREMA

Ako je p prost broj, tada je $a^p \equiv_p a$.

BULOVA ALGEBRA

Bulova algebra je algebarska struktura $\mathbb{B} = (B, \vee, \wedge, ', 0, 1\}$ koja zadovoljava sledeće aksiome:

1. $x \vee y = y \vee x$
2. $x \wedge y = y \wedge x$
3. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$
4. $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
5. $x \vee 0 = x$
6. $x \wedge 1 = x$
7. $x \vee x' = 1$
8. $x \wedge x' = 0$
9. $0 \neq 1$

za svako $x, y, z \in \mathbb{B}$.

PRINCIP DUALNOSTI

Formule F_1 i F_2 su dvojne ako se F_2 može dobiti od formule F_1 tako što se svako pojavljivanje $\wedge$ zameni sa $\vee$ i obrnuto, svako pojavljivanje 1 zameni sa 0 i obrnuto.

BULOVO UREDJENJE

Na proizvoljnoj Bulovoj algebri $\mathbb{B} = (B, \vee, \wedge, ', 0, 1\}$ možemo uvesti uredjenje na sledeći način:
$x \leq y \iff x \wedge y = x$
Važi da je $x \wedge y = y$.

$(\mathbb{B}, \leq)$ je parcijalno uredjen skup (skup kod kojeg postoji relacija za koju važe antisimetričnost, tranzitivnost i refleksivnost.

ATOM

Element x Bulove algebre $\mathbb{B} = (B, \vee, \wedge, ', 0, 1\}$ je atom ukoliko $x > 0$ i ako važi: ako postoji $y \leq x$ tada je $y = x$ ili $y = 0$.

STONOVA TEOREMA

Za svaku konačnu Bulovu algebru $\mathbb{B} = (B, \vee, \wedge, ', 0, 1\}$ postoji skup X takav da postoji bijekcija:
$\mathcal{F}: \mathbb{B} \to \mathcal{P}(X)$
za koju važi:
$f(x \vee y) = f(x) \vee f(y)$
$f(x \wedge y) = f(x) \wedge f(y)$
$f(x') = f(x)^c = x \backslash f(x)$

Konačnu Bulovu algebru moguće je konstruisati na skupu koji ima 2^m elemenata, $m \in \mathbb{N}$.

JEZIK ISKAZNE ALGEBRE

- P – prebrojiv skup promenljivih
- C = {T, ⊥} – skup logičkih konstanti
- logički veznici: ¬,∧,∨, ⟹, ⟺, ↑, ↓, ⊻
- zagrade: (,)

VALUACIJA

Valuacija je preslikavanje $v: P \to \{0,1\}$.

INTERPRETACIJA

Interpretacija pri valuaciji *v* je preslikavanje $I_v: For\mathcal{L} \to \{0,1\}$, gde je For$\mathcal{L}$ skup svih formula jezika iskazne algebre $\mathcal{L}$.

ZADOVOLJIVA/PORECIVA FORMULA

Formula F je zadovoljiva ako postoji bar jedna valuacija *v* tdj. $I_v(F) = 1$. $(v \vDash F)$
Formula F je poreciva ako postoji bar jedna valuacija *v* tdj. $I_v(F) = 0$. $(v \nvDash F)$

TAUTOLOGIJA

Ako za sve valuacije *v* važi da je $I_v(F) = 1$, F je tautologija.

KONTRADIKCIJA

Ako za sve valuacije *v* važi da je $I_v(F) = 0$, F je kontradikcija.

ZADOVOLJIV SKUP

$\Gamma \subseteq For\mathcal{L}$
Skup Γ je zadovoljiv ako postoji valuacija $v: P \to \{0, 1\}$ td. za sve $F \in \Gamma$ važi $I_v(F) = 1$.
Pišemo $v \vDash \Gamma$.

F je logička posledica skupa Γ (pišemo $\Gamma \vDash F$) ako za svaku valuaciju *v* za koju važi $v \vDash \Gamma$ važi $v \vDash F$.

LOGIČKI EKVIVALENTNE FORMULE

Formule A i B su logički ekvivalentne ako $A \vDash B$ i $B \vDash A$. (Zapis $A \equiv B$)

KONJUKTIVNA NORMALNA FORMA

Formula je u KNF ako je oblika $A_1 \wedge A_2 \wedge \ldots \wedge A_n$, gde su A_i disjunkcije iskaznih slova.
Na primer $(p \vee q) \wedge (p \vee r) \wedge (q \vee \neg r) \wedge \neg p$ je u KNF.

DISJUNKTIVNA NORMALNA FORMA

Formula je u DNF ako je oblika $A_1 \vee A_2 \vee \ldots \vee A_n$, gde su A_i konjukcije iskaznih slova.