# O P Š T A  A L G E B R A

(prvi deo)

po predavanjima
Dr. S. B. Prešića.

BEOGRAD
April 1968

U realizaciji skripta sudelovali su

Ašić Miroslav
Bokan Neda
Bulatović Jelena
Vukomanović Đorđe
Jovanović Boško
Savić Vladimir
Udovičić Enes

studenti III-godine matematike A smer

i

Frankl Milan

student II-godine matematike.

# ISKAZI, ISKAZNE FORMULE, TAUTOLOGIJE. HIPOTEZE I POSLEDICE

## Iskazi i operacije sa njima

Iskazi su jedna vrsta rečenica koje se najčešće javljaju u matematici.

Iskaz je ona rečenica koja je ili tačna (istinita) ili netačna (neistinita). Kažemo takodje da je iskaz rečenica koja ima jednu i samo jednu (potpuno odredjenu) istinitosnu vrednost. Iskaze čemo označavati slovima p,q, r, ... (dakle: p,q,r,... nisu iskazi nego samo oznake za neke iskaze), a vrednosti tih iskaza sa v (p), v (q), v(r), .... Znači: ako je p oznaka za ma koji iskaz tada je v(p) = ⊤ ili v (p) = ⊥ , gde su ⊤ , ⊥ redom oznake za "tačan", odnosno "netačan".

Sledeće rečenice su iskazi:

1. Postoji broj koji je istovremeno manji od 2 i veći od 3.
2. Rešenja jednačine $x^2 + 2x - 3 = 0$ su realna i različita.
3. Kvadrat je četvorougao.
4. Svi skupovi su jednoelementni.

Iskazi 1. i 4. su netačni, a 2. i 3. su tačni.

Sa iskazima se prave novi iskazi pomoću tzv. logičkih operacija. Logičke operacije su: konjunkcija, disjunkcija, implikacija, ekvivalencija i negacija.

Ako su p i q oznake nekih iskaza onda je

| | | |
|---|---|---|
| konjunkcija | redom iskaza, čije su oznake p i q, iskaz | p i q |
| disjunkcija | | p ili q |
| implikacija | | ako p onda q |
| ekvivalencija | | ako p onda q i ako q onda p |

Negacija iskaza p je iskaz ne p .

Iskaz "ako p onda q" ima isto značenje kao i sledeće rečenice:

1. Iz p sledi q.
2. p je pretpostavka za q.
3. p je dovoljan uslov za q.
4. q je neophodan uslov za p.

Iskaz "ako p onda q i ako q onda p" ima isto značenje kao i sledeće rečenice:

1. p je ekvivalentno sa q.
2. p je neophodan i dovoljan uslov za q.
3. p je ako i samo ako je q.

Istinitosna vrednost svakog novog iakaza zavisi od iskaza pomoću kojih je obrazovan. Konjunkcija redom iskaza p i q je tačna onda i samo onda kada su i p i q tačni. Disjunkcija redom iskaza p i q je tačna ako je bar jedan od iskaza p i q tačan. Implikacija redom iskaza p i q je netačna jedino tada kada je p tačan, a q netačan iskaz, a ako p i q imaju druge istinitosne vrednosti implikacija redom tih iskaza je tačna. Ekvivalencija redom iskaza p i q je tačna, ako p i q imaju iste istinitosne vrednosti, a netačna ako su im istinitosne vrednosti različite. Negacija tačnog iskaza je netačan iskaz, a negacija netačnog je tačan iskaz.

Označimo konjukciju, disjunkciju, implikaciju i ekvivalenciju (redom) iskaza p i q (redom) oznakama $p \wedge q$, $p \vee q$, $p \Rightarrow q$, $p \Leftrightarrow q$ i negaciju iskaza p oznakom $\neg p$. Tada sledeće tablice prikazuju zavisnost vrednosti novog iskaza od vrednosti iskaza pomoću kojih je ovaj obrazovan uz pomoć navedenih logičkih operacija:

| p | q | $p \wedge q$ | $p \vee q$ | $p \Rightarrow q$ | $p \Leftrightarrow q$ |
|---|---|---|---|---|---|
| $\top$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ |
| $\top$ | $\bot$ | $\bot$ | $\top$ | $\bot$ | $\bot$ |
| $\bot$ | $\top$ | $\bot$ | $\top$ | $\top$ | $\bot$ |
| $\bot$ | $\bot$ | $\bot$ | $\bot$ | $\top$ | $\top$ |

| p | $\neg p$ |
|---|---|
| $\top$ | $\bot$ |
| $\bot$ | $\top$ |

Iskazne formule

Uvedimo jedan novi pojam, pojam iskazne formule.

Iskazne formule su odredjene reči[1] čija su slova elementi prethodno odredjenih skupova. Ti skupovi su: skup iskaznih slova, skup operacijskih simbola i skup pomoćnih simbola. Skup iskaznih slova može biti proizvoljan, ali prebrojiv. Dogovorimo se da iskazna slova budu sledeći simboli:

$$p, q, r, p_1, q_1, r_1, \ldots, p_n, q_n, r_n, \ldots$$

Operacijskih simboli će biti

$$\wedge\ ,\ \vee\ ,\ \Rightarrow\ ,\ \Leftrightarrow\ ,\ \neg$$

Pomoćni simboli su

$$(\ ,\ )\ .$$

Sada uočimo skup čiji su elementi iskazna slova, operacijski simboli i pomoćni simboli. Ovaj skup nazovimo azbukom. Dakle, iskazne formule se formiraju od slova ove azbuke i to na određeni način.

Definicija iskazne formule:

1. Iskazna slova su iskazne formule.
2. Ako su A i B (oznake za) iskazne formule onda su i $(A \wedge B)$, $(A \vee B)$, $(A \Rightarrow B)$, $(A \Leftrightarrow B)$, $\neg A$ iskazne formule.
3. Iskazne formule se mogu obrazovati samo pomoću konačnog broja primena 1. i 2.

(Ovo je rekurzivna definicija jer se pomoću formula manjih dužina obrazuju formule većih dužina.)

Prema ovoj definiciji $\neg(p \Rightarrow \neg q)$, $((p \wedge q) \vee r)$, $(\neg p \vee (q \Leftrightarrow r))$ jesu formule, dok $\neg)$, $p \neg p$, $(p \vee \neg q$, to nisu.

Radi što jednostavnijeg pisanja formula usvajamo razne konvencije.

Konvencija 1. Ako su A i B formule, onda formule $(A \wedge B)$, $(A \vee B)$, $(A \Rightarrow B)$, $(A \Leftrightarrow B)$ označavamo redom sa $A \wedge B$, $A \vee B$, $A \Rightarrow B$, $A \Leftrightarrow B$.

Konvencija 2. Operacijski simbol $\Leftrightarrow$ najjače razdvaja zagrade. Za njim, po jačini razdvajanja dolaze $\Rightarrow$, $\vee$, $\wedge$. Ukoliko se simbol odnosi na pot formolu u kojoj ima više iskaznih slova onda se ta potformula mora pisati u zagradama. Shodno konvenciji 2. i uz konvenciju 1. formulu $A \wedge B \vee C \wedge D$ ćemo shvatiti kao $(A \wedge B) \vee (C \wedge D)$, a formulu $A \vee B \Rightarrow C \wedge D$ kao $(A \vee B) \Rightarrow (C \wedge D)$.

Konvencija 3. Ako su $A_1, A_2, \ldots, A_n$ neke formule onda reč $A_1 \wedge A_2 \wedge \ldots \wedge A_n$ je zamena za formulu $A_1$ ako je $n = 1$, odnosno zamena za $(A_1 \wedge A_2 \wedge \ldots \wedge A_{n-1}) \wedge A_n$ ako je $n > 1$. Slično usvajamo za $A_1 \vee A_2 \vee \ldots \vee A_n$.

Ako su $p_1, p_2, \ldots, p_n$ redom n različitih iskaznih slova pa ako svako od njih "zamenimo" jednim od

---

(1) Ako su $a_1, a_2, \ldots$ elementi nekog skupa onda reč čija su slova redom $a_1, a_2, \ldots, a_n$, u oznaci $a_1 a_2 \ldots a_n$, shvatamo kao preslikavanje $\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ a_1 & a_2 & a_3 & \ldots & a_n \end{pmatrix}$.

simbola $\top$ , $\bot$ onda dobijemo tzv. vrednost redom slova $p_1$, $p_2$, ..., $p_n$ (u oznaci $v(p_1)$, $v(p_2)$,..., $v(p_n)$ ). To je, po definiciji, uredjena n - torka simbola $\top$, $\bot$. Ako je broj razlocitih iskaznih slova n onda je broj odgovarajućih vrednosti $2^n$.

Neka je A formula koja je, na odredjeni način, obrazovana pomoću slova $p_1$, $p_2$, ..., $p_n$. Svakoj vrednosti tih slova odgovara vrednost formule (u oznaci v(A) ), koja je takodje $\top$ ili $\bot$. Znači: $v(A) \in \{\top, \bot\}$.

Ako su A i B neke formule onda definišemo:

$v((A \wedge B)) = v(A) \wedge v(B)$

$v((A \vee B)) = v(A) \vee v(B)$

$v((A \Rightarrow B)) = v(A) \Rightarrow v(B)$

$v((A \Leftrightarrow B)) = v(A) \Leftrightarrow v(B)$

$v(\neg A) = \neg v(A)$

gde su simboli $\wedge$, $\vee$ , $\Rightarrow$ , $\Leftrightarrow$ , $\neg$ , na levoj strani elementi uvedenog skupa operacijskih simbola, a simboli $\wedge$ , $\vee$ , $\Rightarrow$ , $\Leftrightarrow$ , $\neg$ , na desnoj strani su operacije skupa $\{\top, \bot\}$ definisane tablicama (*) (na sledećoj strani) .

Znači; vrednost v formule je preslikavanje čiji su orginali formule, a slike su elementi skupa $\{\top, \bot\}$ .

## Interpretacija

Navešćemo dve interpretacije formula i elemenata $\top$, $\bot$ .

I interpretacija. Iskazna slova interpretirajmo kao elemente skupa $\{\top, \bot\}$ , a operacijske simbole $\wedge$ , $\vee$ , $\Rightarrow$ $\Leftrightarrow$ , $\neg$ inprepretirajmo kao operacije koje ćemo označavati istim znacima, a koje se definišu sledećim tablicama:

| $\wedge$ | $\top$ | $\bot$ |
|---|---|---|
| $\top$ | $\top$ | $\bot$ |
| $\bot$ | $\bot$ | $\bot$ |

| $\vee$ | $\top$ | $\bot$ |
|---|---|---|
| $\top$ | $\top$ | $\top$ |
| $\bot$ | $\top$ | $\bot$ |

| $\Rightarrow$ | $\top$ | $\bot$ |
|---|---|---|
| $\top$ | $\top$ | $\bot$ |
| $\bot$ | $\top$ | $\top$ |

| $\Leftrightarrow$ | $\top$ | $\bot$ |
|---|---|---|
| $\top$ | $\top$ | $\bot$ |
| $\bot$ | $\bot$ | $\top$ |

| | $\neg$ |
|---|---|
| $\top$ | $\bot$ |
| $\bot$ | $\top$ |

Ovom interpretacijom smo doboili tzv. iskaznu algebru.

Iskaznu algebru možemo uvesti i formalno: kažemo da je to uredjena šestorka čiji je prvi član skup, a ostali članovi su operacije: ( $\{\top, \bot\}$ , $\wedge$ , $\vee$ , $\Rightarrow$ , $\Leftrightarrow$ , $\neg$ ).

U skupu $\{\top,\bot\}$ posmatrali smo operacije $\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg$,. Da ove operacije nisu medjusobno nezavisne tvrdi sledeći

Stav. Svaka operacija skupa $\{\top,\bot\}$ se može definisati formulom koja kao jedine operacije sadrži: 1. $\wedge$ , $\neg$.; 2. $\vee$ , $\neg$ ; 3. $\Rightarrow$, $\neg$.

Vidimo da se ne mogu pomoću jedne od navedenih pet operacija izraziti ostale. No, postoje dve operacije, Sheffer-ova i Łukasiewicz-ova, redom u oznaci $\uparrow$ i $\downarrow$ , od kojih svaka ima osobinu da se samo pomoću nje mogu izraziti operacije $\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg$. Operacije $\uparrow$ i $\downarrow$ se definišu pomoću sledećih tablica

| $\uparrow$ | $\top$ | $\bot$ |
|---|---|---|
| $\top$ | $\bot$ | $\top$ |
| $\bot$ | $\top$ | $\top$ |

| $\downarrow$ | $\top$ | $\bot$ |
|---|---|---|
| $\top$ | $\bot$ | $\bot$ |
| $\bot$ | $\bot$ | $\top$ |

Neposredno se dokazuju da izmedju operacija $\uparrow$ i $\downarrow$ i operacija $\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg$ postoje sledeće veze

1. $p \uparrow q = \neg(p \wedge q)$ , $p \downarrow q = \neg(p \vee q)$
2. $\neg p = p \uparrow p$ , $p \wedge q = (p \uparrow q) \uparrow (p \uparrow q)$ , $p \vee q = (p \uparrow p) \uparrow (q \uparrow q)$
3. $\neg p = p \downarrow p$ , $p \wedge q = (p \downarrow p) \downarrow (q \downarrow q)$ , $p \vee q = (p \downarrow q) \downarrow (p \downarrow q)$

gde su p i q elementi skupa $\{\top,\bot\}$.

Zanimljivo je da važi

Stav. Jedine binarne operacije pomoću kojih se može izraziti svaka formula su $\uparrow$ i $\downarrow$.

Dokaz. Pretpostavimo suprotno, tj. da postoji bnarna operacija h takva da se pomoću nje mogu izraziti operacije $\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg$. Konstruišimo tablicu ove operacije h. Ako bi bilo h $(\top,\top) = \top$ onda se pomoću h nebi mogla izraziti negacija; dakle je h $(\top,\top) = \bot$ . Iz istih razloga je h $(\bot,\bot) = \top$ . Na preostala dva mesta ne možemo staviti $\top$ (ili $\bot$ ) jer bi tada dobili Sheffer - ovu (odnosno Łukasiewicz-ovu) operaciju. Dakle, postoje mogućnosti: 1. $h(\bot,\top) = \top$ , $h(\top,\bot) = \top$ ; 2. $h(\bot,\top) = \bot$ , $h(\top,\bot) = \top$ ; no, u prvom slučaju je zapravo $h(p,q) = \neg q$, a u drugom $h(p,q) = \neg p$ (gde su $p,q \in \{\top,\bot\}$), a samo pomoću $\neg$ se ne mogu izraziti ostale operacije. Dakle: pomoću h se ne mogu izraziti ostale operacije što je i trebalo dokazati.

II interpretacija. Iskazna slova $p,q,r,p_1,q_1,r_1,\ldots$ $p_n,q_n,r_n,\ldots$ se interpretiraju kao rečenice koje su ili tačne (u oznaci $\top$) ili netačne (u oznaci $\bot$), simboli ( , ) se interpretiraju kao leva, odnosno desna zagrada, a operacijski simboli $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\neg$ se interpretiraju redom kao konjukcija, disjunkcija, implikacija, ekvivalencija, negacija (i pri tom se za ove operacije zadržavaju gornje oznake, uzete tim redom).

Tautologije

Definicija. Za formulu A kažemo da je tautologija ako ima vrednost $\top$ za sve vrednosti svojih iskaznih slova.

Neka $\models A$ znači da je A tautologija.

Za formulu A kažemo da je kontradikcija ako ima vrednost $\bot$ za sve vrednosti svojih iskaznih slova.

Jedna od mogućnosti da se dokaže da je neka formula tautologija je da se obrazuje tablica vrednosti koje ona prima pri svim mogućim vrednostima svojih iskaznih slova.

Obeležimo sa A formulu.

$$(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$$

i dokažimo, obrazovanjem tablice, da je ona tautologija

| $p$ | $q$ | $r$ | $q \Rightarrow r$ | $p \Rightarrow q$ | $p \Rightarrow r$ | $p \Rightarrow (q \Rightarrow r)$ | $(p \Rightarrow q) \Rightarrow (p \Rightarrow r)$ | $A$ |
|---|---|---|---|---|---|---|---|---|
| $\top$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ |
| $\top$ | $\top$ | $\bot$ | $\bot$ | $\top$ | $\bot$ | $\bot$ | $\bot$ | $\top$ |
| $\top$ | $\bot$ | $\top$ | $\top$ | $\bot$ | $\top$ | $\top$ | $\top$ | $\top$ |
| $\top$ | $\bot$ | $\bot$ | $\top$ | $\bot$ | $\bot$ | $\top$ | $\top$ | $\top$ |
| $\bot$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ |
| $\bot$ | $\top$ | $\bot$ | $\bot$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ |
| $\bot$ | $\bot$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ |
| $\bot$ | $\bot$ | $\bot$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ |

Na ovaj način se za svaku formulu može utvrditi da li je tautologija ili ne.

Za formulu oblika $A \Rightarrow B$ (tu su A i B takodje neke formule) postoji još jedan način za odredjivanje da li je ona tautologija ili ne. U ovom postupku se traže takve vrednosti

njenih iskaznih slova pri kojima sama formula ima vrednost $\bot$. Ako se pokaže da takve vrednosti ne postoje onda je dokazano da je ta formula tautologija. No, formula oblika $A \Rightarrow B$ može imati vrednost $\bot$ tada i samo tada kada je $v(A) = \top$, $v(B) = \bot$. Ako se pokaže da za kakve vrednosti iskaznih slova ne može biti $v(A) = \top$ i $v(B) = \bot$ znači da je data formula tautologija.

Navodimo primer: dokažimo da je formula

$$(p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p)$$

tautologija. Predpostavimo da ona nije tautologija tj. da za neke vrednosti iskaznih slova ima vrednost $\bot$. Tada je $v(p \Rightarrow q) = \top$ i $v(\neg q \Rightarrow \neg p) = \bot$. Ovo drugo je ispunjeno samo ako je $v(\neg q) = \top$, tj. $v(q) = \bot$ i $v(\neg p) = \bot$, tj. $v(p) = \top$. No, tada je $v(p \Rightarrow q) = \bot$ što je suprotno učinjenoj pretpostavci. Znači: data formula ni za kakvu vrednost iskaznih slova ne može imati vrednost $\bot$ pa je ona tautologija.

Za objašnjavanje trećeg postupka kojim utvrdjujemo da li je neka formula tautologija ili ne biće nam potrebne sledeće tautologije koje navodimo bez dokaza:

(1) $\neg\neg p \Leftrightarrow p$ (Zakon dvojne negacije)

(2) $(p \Leftrightarrow q) \Leftrightarrow (p \Rightarrow q) \wedge (q \Rightarrow p)$

(3) $(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$

(4) $\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$
$\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$ } (De Morganovi zakoni)

(5) $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ (Zakon distributivnosti $\vee$ prema $\wedge$.)

(6) $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$ (Zakon asocijativnosti za $\wedge$)

Cilj ovog postupka je da se dobije formula ekvivalentna [1] sa polaznom koja je oblika $A_1 \wedge A_2 \wedge \ldots \wedge A_n$ gde su formule $A_1, A_2, \ldots, A_n$ oblika $p_1 \vee p_2 \vee \ldots \vee p_k$; ovde su $p_1, p_2, \ldots p_k$ iskazna slova ili njihove negacije. Tada je data formula tautologija ako i samo ako su $A_1, A_2, \ldots, A_n$ tautologije, a one su tautologije ako i samo ako bar sa jednim slovom sadrže i njegovu negaciju.

---

(1) Definicija. Formule A i B su ekvivalentne tada i samo tada ako imaju istu vrednost pri istim vrednostima učestvujućih iskaznih slova, tj. tada i samo tada kada je formula $A \Leftrightarrow B$ tautologija.

Sam postupak se izvodi ovako. Prvo, koristeći se tautologijom (2) od date formule prelazimo na formulu koja ne sadrži $\Leftrightarrow$. Zatim, pomoću tautologije (3) dobijemo formulu koja ne sadrži ni $\Rightarrow$. Pomoću tautologija (1) i (4) najzad dobijamo formulu koja ima samo operacijske simbole $\wedge$, $\vee$, $\neg$ i simbol $\neg$ stoji samo uz slova. Na kraju, primenom (5) i (6) dolazimo do formule traženog oblika koja je ekvivalentna polaznoj.

Ilustrujmo ovo sledećim primerom. Neka je A formula $(\neg p \Rightarrow \neg q) \Rightarrow (q \Rightarrow p)$. Tada je

$\models A \Leftrightarrow (\neg\neg p \vee \neg q) \Rightarrow (\neg q \vee p)$ (zbog (3))

$\models A \Leftrightarrow \neg(p \vee \neg q) \vee \neg q \vee p$ (zbog(1) i (3))

$\models A \Leftrightarrow (\neg p \wedge q) \vee \neg q \vee p$ (zbog (4))

$\models A \Leftrightarrow (\neg p \vee \neg q \vee p) \wedge (q \vee \neg q \vee p)$,

a oda-vde se lako vidi da je formula A tautologija.

Hipoteze, Posledice.

Neka je $\mathcal{F}$ skup iskaznih formula i F neka formula toga skupa.

Za formulu F kažemo da je (semantička) posledica formula skupa $\mathcal{F}$ ako je ispunjen uslov: ako za neku vrednost iskaznih slova formula skupa $\mathcal{F}$ te formule dobijaju vrednost $\top$ tada i formula F dobija vrednost $\top$.

Formule skupa $\mathcal{F}$ zovemo hipoteze za formulu F, a $\mathcal{F} \models F$ je oznaka da je F (semantička) posledica formula skupa $\mathcal{F}$.[1] Ako je $\mathcal{F} = \{F_1, F_2, \ldots, F_n\}$ pišemo $F_1, F_2, \ldots F_n \models F$.

Važe sledeći stavovi:

Stav 1. Formula $(F_1 \wedge F_2 \wedge \ldots \wedge F_n) \Rightarrow F$ je tautologija ako i samo ako je formula F posledica formula $F_1, F_2, \ldots, F_n$, tj. $\models (F_1 \wedge F_2 \ldots \wedge F_n) \Rightarrow F$ je ekvivalentno sa $F_1, \ldots, F_n \models F$.

Dokaz. Pretpostavimo da je formula $(F_1 \wedge F_2 \wedge \ldots \wedge F_n) \Rightarrow F$ tautologija. To znači: za one vrednosti slova za koje leva strana dobija vrednost $\top$ i desna strana dobija vrednost $\top$, a pošto leva strana ima vrednost $\top$ tada i samo tada

---

(1) Ako je skup $\mathcal{F}$ prazan onda je formula F tautologija (uporedi sa definicijom tautologije).

kada svaka od formula $F_1, F_2, \ldots, F_n$ ima vrednost $\top$ znači da je $F_1, F_2, \ldots, F_n \models F$.

Neka je sada $F_1, F_2, \ldots, F_n \models F$. Tada, za one vrednosti slova za koje formule $F_1, F_2, \ldots, F_n$ dobijaju vrednost $\top$ i formula $F$ dobija vrednost $\top$. Onda kada bar jedna od formula $F_1, F_2, \ldots, F_n$ dobije vrednost $\bot$ i formula $(F_1 \wedge F_2 \wedge \ldots \wedge F_n) \Rightarrow F$ opet ima vrednost $\top$. Dakle je $\models (F_1 \; F_2 \; \ldots \; F_n) \Rightarrow F$.

Stav 2. Formula

(1) $\big((F_1 \wedge F_2 \wedge \ldots \wedge F_n) \Rightarrow F\big) \Leftrightarrow \big(F_1 \Rightarrow (F_2 \Rightarrow (\ldots \Rightarrow (F_n \Rightarrow F)\ldots))\big)$ ($n$)

je tautologija.

Dokaz izvedimo indukcijom. Za $n = 1$ imamo formulu $(F_1 \Rightarrow F) \Leftrightarrow (F_1 \Rightarrow F)$, a ona je očigledno tautologija. Pretpostavimo da je formula

$\big((F_1 \wedge F_2 \wedge \ldots \wedge F_{n-1}) \Rightarrow F\big) \Leftrightarrow \big(F_1 \Rightarrow (F_2 \Rightarrow (\ldots \Rightarrow (F_{n-1} \Rightarrow F)\ldots))\big)$ ($n-1$)

tautologija i dokažimo da je i (1) tada tautologija. Neka formule $F_1, F_2, \ldots, F_n, F$ imaju ma koje vrednosti. Postoje dve mogućnosti: 1) $v(F_n) = \top$, 2) $v(F_n) = \bot$. Lako se proverava da u oba slučaja formula (1) ima vrednost $\top$. Dakle: (1) je tautologija.

Ovaj stav se može dokazati i 1) koristeći tautologiju $(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$ gde su $p$ i $q$ oznake za ma kakve formule; ili 2) pokazujući da leva strana ekvivalencije (1) ima vrednost $\bot$ tada i samo tada kada i desna strana ima vrednost $\bot$.

Stav 3. Formula $F$ je posledica formula $F_1, \ldots, F_n$ tada i samo tada kada je formula $(F_1 \Rightarrow (F_2 \Rightarrow (\ldots \Rightarrow (F_n \Rightarrow F)\ldots))$ ($n$) tautologija, tj. $F_1, F_2, \ldots F_n \models F$ je ekvivalentno sa $\models (F_1 \Rightarrow (F_2 \Rightarrow (\ldots \Rightarrow (F_n \Rightarrow F)\ldots))$ ($n$) (1).

Ovaj stav je neposredna posledica prethodna dva stava.

Posledica:

$F_1, F_2, \ldots, F_n \models F$ je ekvivalentno sa $F_1, F_2, \ldots, F_{n-1} \models F_n \Rightarrow F$.

Koristeći se nekim od gore navedenih stavova dokažimo da je formula

---

(1) Ovaj stav se naziva teorema dedukcije (za tautologije).

$$(p \Rightarrow q) \Rightarrow ((\neg p \Rightarrow q) \Rightarrow q) \qquad (1)$$

Tautologije.

Da bismo pokazali da je ova formula tautologija pokažimo da je

$$p \Rightarrow q,\ \neg p \Rightarrow q \models q \qquad (2)$$

Hipoteze su, dakle, formule $p \Rightarrow q$ i $\neg p \Rightarrow q$ i one imaju vrednost $\top$ samo ako je $v(q) = \top$ (pri tom $v(p)$ može biti bilo $\top$ bilo $\bot$ ) pa znači da je q stvarno posledica formula $p \Rightarrow q$, $\neg p \Rightarrow q$. Prema stavu 3 (2) je ekvivalentno sa tim da je formula (11) tautologija.

Napomena. Kada imamo formulu

$$(F_1 \Rightarrow (F_2 \Rightarrow (\ldots \Rightarrow (F_n \Rightarrow \overbrace{F \ldots}^{n}))))$$

dovoljno je pokazati da je $\models F$ pa je tada sigurno $F_1, F_2, \ldots, F_n \models F$. No, da bi se pokazalo da je $F_1, F_2, \ldots, F_n \models \models F$ nije i potrebno pokazati da je $\models F$ jer F ne mora biti tautologija, a da je ipak posledica formula $F_1, F_2, \ldots, F_n$.

U narednom tekstu dokazujemo dva osnovna svojstva tautologija. U tu svrhu skup svih iskaznih formula obeležimo sa $\mathcal{F}$ , a skup tautologija sa $\mathcal{T}$ .

1) Neka je $F(p_1, p_2, \ldots, p_n)$ iskazna formula čija su iskazna slova $p_1, p_2, \ldots, p_n$ i neka su $A_1, A_2, \ldots, A_n$ bilo koje iskazne formule. Označimo sa $F(A_1, A_2, \ldots, A_n)$ formulu dobijenu iz prethodne zamenom slova $p_i$ $(i=1,\ldots,n)$ formulom $A_i$ $(i=1,\ldots,n)$. Tada važi tzv. pravilo supstitucije koje glasi: ako je $F(p_1, p_2, \ldots, p_n) \in \mathcal{T}$ onda je i $F(A_1, A_2, \ldots, A_n) \in \mathcal{T}$.

Ovo pravilo je očigledno jer: ako za sve moguće vrednosti slova $p_1, p_2, \ldots, p_n$ $(F(p_1, p_2, \ldots, p_n) \in \mathcal{T}$ onda i $F(A_1, A_2, \ldots, A_m) \in \mathcal{T}$ jer formule $A_1, A_2, \ldots, A_n$ imaju najviše onoliko različitih vrednosti koliko i slova $p_1, p_2, \ldots, p_n$ (mogu imati i manje vrednosti jer neke od formula $A_1, A_2, \ldots, A_m$ mogu biti tautologije ili kontradikcije).

2) Ako su formule A i $A \Rightarrow B$ tautologije onda je i formula B tautologija. Ovo svojstvo se zove modus ponens.

Dokaz izvedimo indirektno. Pretpostavimo da, pri nekoj vrednosti slova koja učestvuju u B, može biti $v(B) = \bot$. No, pošto je formula $A \Rightarrow B$ tautologija, tj. $v(A \Rightarrow B) = \top$ za sve vrednosti učestvujućih slova, to je i $v(A) = \bot$ , a ovo ne može biti jer je formula A tautologija. Dakle, ni za jednu vrednost slova koja učestvuju u B, ne može biti $v(B) = \bot$ , tj.

B je tautologija.

Postavlja se pitanje: koja su svojstva karakteristična za skup $\mathcal{T}$, tj. pomoću kojih svojstava se ovaj skup može potpuno opisati? Da bismo odgovorili na ovo pitanje uvešćemo pojam teoreme, tj. skupa teorema T.

Definicija teoreme:

$1^{o}$ Ako su A,B,C neke formule onda su $A \Rightarrow (B \Rightarrow A)$, $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$, $(\neg A \Rightarrow \neg B) \Rightarrow (B \Rightarrow A)$ teoreme.

$2^{o}$ Ako su A i $A \Rightarrow B$ teoreme onda je i B teorema.

$3^{o}$ Teoreme su samo one formule koje se dobijaju konačnom primenom $1^{o}$ i $2^{o}$.

Očigledno je da $T \subset \mathcal{T}$.

Stav (semantičke potpunosti). Svaka tautologija je i teorema i obrnuto, svaka teorema je tautologija. tj. $\mathcal{T} = T$.

Ovo je jedan od osnovnih stavova u tzv. iskaznom računu.

Na osnovu definicije teoreme i ovoga stava skup tautologija možemo uvesti sintaktički, tj. odredjenim pravilima. Ta karakterizacija tautologija je:

Ako su A,B,C ma kakve formule tada su formule

$1^{o}$ $A \Rightarrow (B \Rightarrow A)$

$2^{o}$ $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

$3^{o}$ $(\neg A \Rightarrow \neg B) \Rightarrow (B \Rightarrow A)$

tautologije.

# KVANTIFIKATORSKI RAČUN PRVOG REDA

U ovom računu značajnu ulogu imaju tzv. kvantifikatori koji se inače u običnom jeziku uzimaju kao zamjenice : "svaki", "neki", "bilo koji", "ma koji",... Često se simboli $\forall$ odnosno $\exists$ upotrebljavaju umesto zamenica , "svaki", odnosno "neki".

Usvajamo da je $\forall$ univerzalni kvantifikator, dok je $\exists$ egzistencijalni kvantifikator. Kvantifikatori $\forall$, $\exists$ učestvuju u nekim formulama računa koji ćemo posmatrati , i to uvek u obliku $(\forall u),(\exists u)$, gde je slovo $u$ oznaka za tzv. promenljivu.

Navodimo primere zaključivanja sa kvantifikatorima.

Primer 1.

Iz pretpostavki

Svi prosti brojevi su prirodni ($p_1$)

5 je prost broj ($p_2$)

Zaključujemo : 5 je prirodan broj ($z$)

Primer 2.

Iz pretpostavki

Bilo koji Markov prijatelj je Jovanov prijatelj ($p_1'$)

Petar nije Jovanov prijatelj ($p_2'$)

Zaključujemo : Petar nije Markov prijatelj. ($z'$)

Navedeni i slični primeri mogu biti opisani tzv. formulskim rečenicama. Ilustrujmo to na primeru 1.

$(\forall x)(\alpha(x)\Rightarrow\beta(x))$

$\alpha(5)$

$\beta(5)$

U ovom primeru x je promenljiva a 5 je konstanta.

- Dogovorimo se da rečenicu "x ima svojstvo $\alpha$" označavamo sa $\alpha(x)$. U našem primeru neka $\alpha(x)$ znači "x je prost broj", a $\beta(x)$ "x je prirodan broj".

Zaključivanje u primeru 1 možemo opisati i sledećom formulom : $(\forall x)(\alpha(x)\Rightarrow\beta(x))\wedge\alpha(5)\Rightarrow\beta(5)$.

Navodimo primere prevođenja na formulski jezik nekih poznatih matematičkih tvrđenja.

Primer 3.

Iz $x>y$ i $y>z$ sledi $x>z$ ($x,y,z$, su realni brojevi)

Ako sa $\downarrow(x,y)$ označimo činjenicu "broj x je veći od broja y", onda navedenom tvrđenju odgovara formula:

$$(\alpha(x,y)\wedge\alpha(y,z))\Rightarrow\alpha(x,z)$$

Primer 4.

Ako je $x>y$ onda postoji broj z takav da je $x>z$ i $z>y$.

Uvodeći oznaku kao u prethodnom primeru imamo :

Primer 5.

U skupu realnih brojeva važi: Za svaki par brojeva x i y ispunjena je jedna i samo jedna od relacija $x=y$, $x>y$, $x<y$.

Uz iste oznake imamo ($\beta(x,y)$ znači "x jednako y")

$$(\forall x)(\forall y)\Big((\beta(x,y)\wedge\neg\alpha(x,y)\wedge\neg\alpha(y,x))\vee(\neg\beta(x,y)\wedge\alpha(x,y)\wedge\neg\alpha(y,x))\vee(\neg\beta(x,y)\wedge\neg\alpha(x,y)\wedge\alpha(y,x))\Big)$$

Primer 6.

Za svaki par različitih tačaka x i y postoji treća tačka z tako da je y između x i z.

Uvodeči oznake : $\delta'(x,y)$ označava "x različito od y"

$\delta(x,y,z)$ označava "y je između x i z i tačke x,y,z su različite"

dobijemo odgovarajuču formulu :

$$(\forall x)(\forall y)(\delta'(x,y)\Rightarrow(\exists z)\,\delta(x,y,z))$$

## FORMULE KVANTIFIKATORSKOG RAČUNA. GLAVNA INTERPRETACIJA. MODEL. VALJANE FORMULE.

Polazni simboli su dogovorno : $\Rightarrow$ $\neg$ , ( ) $\forall$

Zatim promenljive : $x,y,z,\ x_1,y_1,z_1,\ldots,x_n,y_n,z_n,\ldots$

i Relacijska slova : $R_1^i$, $R_2^i$, ..., $R_i^j$, . . (i,j - prirodni brojevi)

gde je gornji indeks tzv. dužina relacijskog slova.

Definicija 1.

Neka su $u_1$, $u_2$, ..., $u_n$, (oznake za) promenljive i neka je $\emptyset$ (takođe oznaka za ) relacijsko slovo dužine n. Tada reč :

$\emptyset(u_1, u_2, \ldots u_n)$ nazivamo elementarna formula.

Dajemo definiciju formule kvantifikatorskog računa prvog reda ( u daljem izlaganju : formula ).

Definicija 2.

1) Elementarna formula je formula.

2) Ako su A i B formule onda su i : $(A\Rightarrow B)$ , $\neg A$ , $(\forall u)A$ formule , gde je u izvesna promenljiva.

3) Formule se mogu dobiti jedino konačnom primenom 1) i 2)

Definicija 3.

Ako su A i B neke formule onda

$(A\wedge B)$ je zamena za $\neg(A\Rightarrow\neg B)$

$(A\vee B)$ je zamena za $(\neg A\Rightarrow B)$

$(A\Leftrightarrow B)$ je zamena za $(A\Rightarrow B)\wedge(B\Rightarrow A)$

$(\exists u)A$ je zamena za $\neg(\forall u)\neg A$.

Prema usvojenim definicijama sledeče reči su formule:

$R_1^1(x)$, $(R_2^2(x,y)\Rightarrow R_2^1(z))$, $((\forall x)R_4^2(x,y)\wedge(\exists y)R_7^1(y))$

ali reči $R_1^1(x,y)$, $(\forall x)\wedge(\exists y)$ nisu formule.

Usvajamo slične konvencije o brisanju zagrada kao u slučaju iskaznih formula.
Kratkoće radi, relacijska slova $R_i^j$, ćemo ubuduće označavati malim grčkim slovima $\alpha, \beta, \gamma, \ldots$ pri čemu će iz same formule biti jasna dužina slova.
Pojavljivanje promenljive u u formuli F nazivamo vezano pojavljivanje ako je:
1) to pojavljivanje oblika $(\forall u)$ ili $(\exists u)$ ili
2) postoji formula A u kojoj u ima pojavljivanje i pri tome $(\forall u)A$ ili $(\exists u)A$ su podformule formule F.
Ono pojavljivanje promenljive u koje nije vezano nazivamo slobodno pojavljivanje.
Ako u ima slobodno pojavljivanje onda promenljivu u zovemo slobodna promenljiva. Formulu A, koja eventualno ima slobodnu promenljivu u, označavamo sa A(u).
Naprimer, ako je A formula : $(\forall x)\alpha(x) \Rightarrow (\beta(y) \vee \alpha(z))$
onda su u njoj y i z slobodne promenljive, dok x ima samo vezano pojavljivanje. Formulu A možemo označiti sa A(x), A(y), A(z).
Postavlja se pitanje : zašto, pri takvim proizvoljnostima, uvodimo oznaku A(u). Razlog je sledeći: neka je v neka promenljiva, tada uzimamo da A(v) označava formulu koja se dobije kada sva slobodna pojavljivanja u u formuli A zamenimo sa v.
Naprimer, ako je formula A iz prethodnog primera bila označena sa A(y) onda je A(z) sledeca formula: $(\forall x)\alpha(x) \Rightarrow (\beta(z) \vee \alpha(z))$
Ako je ta formula bila označena sa A(x) onda je A(v) formula A ma kakva bila promenljiva v.

Glavna interpretacija. (u daljem izlaganju : interpretacija)
Domen D interpretacije I je bilo koji neprazan skup.
Promenljive interpretiramo kao elemente skupa D, a relacijska slova kao relacije odgovarajuće dužine skupa D.
Simbole : $, \Rightarrow, \neg, \vee, \wedge, \Leftrightarrow$ Interpretiramo kao odgovarajuće operacije iskazne algebre.
Simbole $\forall$ odnosno $\exists$ interpretiramo kao "svaki" odnosno "neki".
Dajemo strogu definiciju interpretacije.
Definicija 4.
Interpretacija formule F je uređen par čije su komponente redom: domen interpretacije D, preslikavanje f .
Dakle , ako sa I označimo interpretaciju onda je $I \overset{def.}{=} (D, f)$.
gde je f sledece preslikavanje : $f = \begin{pmatrix} R_1 & R_2 & R_3 & \ldots & R_\rho \\ \bar{R}_1 & \bar{R}_2 & \bar{R}_3 & \ldots & \bar{R}_\rho \end{pmatrix}$

Pri tome su $R_1, R_2, \ldots R_\rho$ , sva različita upotrebljena relacijska slova u formuli F, a $\bar{R}_1, \bar{R}_2, \ldots \bar{R}_\rho$, relacije odgovarajuće dužine skupa D.

Primer.

Neka je data formula $\alpha(x,y) \Rightarrow \beta(x,y)$ (2)

Jedna od mogućih interpretacija navedene formule je sledeća.

Neka je domen skup Z celih brojeva, a $\bar{\alpha}$ i $\bar{\beta}$ interpretacije relacijskih slova $\alpha$ i $\beta$ :

$\bar{\alpha}(x,y) \longleftrightarrow$ " x-y deljivo sa 4 "

$\bar{\beta}(x,y) \longleftrightarrow$ " x-y deljivo sa 2 "

Interpretacija je dakle uređen par

$$\left(Z, \begin{pmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{pmatrix}\right) \qquad (3)$$

Primetimo da formula (2) ima pri navedenoj interpretaciji uvek vrednost T ma kako interpretirali promenljive x,y. Kažemo da je formula (2) tačna za interpretaciju (3).

Precizirajmo taj pojam.

Pri interpretaciji I formuli F odgovara Zavisno od interpretacije promenljivih, jedan od simbola $\top$ ili $\bot$ , tzv. vrednost formule F.

Za formulu F kažemo da je tačna u odnosu na interpretaciju I sa domenom D i utvrđenim interpretacijama relacijskih slova , ukoliko je vrednost formule uvek T bez obzira na interpretaciju njenih promenljivih.

Formula F je netačna (pri interpretaciji I ) ako je formula $\neg$F tačna ( pri interpretaciji I).

Ako je formula F tačna pri interpretaciji I onda I zovemo Model te formule.

U malo pre navedenom primeru model formule (2) je interpretacija (3), jer je ona tačna za tu interpretaciju .

Formula je valjana ako je tačna pri svakoj interpretaciji.

Prema usvojenim definicijam valjane su sledeće formule:

$$(\alpha(x,y) \wedge \alpha(y,x)) \vee \neg(\alpha(x,y) \wedge \alpha(y,x))$$

$$(\forall x)(\exists y)\,\alpha(x,y) \Rightarrow (\beta(y,y) \Rightarrow (\forall x)(\exists y)\,\alpha(x,y)) \qquad (4)$$

Ma kako izabrali skup D i ma kako interpretirali relacijska slova $\alpha, \beta$ formule (4) uvek imaju vrednost T.

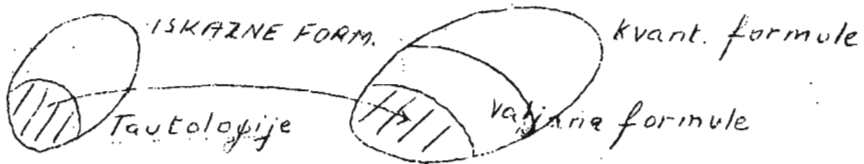
Neka je sada F izvestan skup formula i neka su to tačne formule u odnosu na interpretaciju I koju čini domen D i izvesne njegove relacije kao interpretacije odgovarajućih relacijskih slova, pri čemu se ista relacijska slova u raznim formulama interpretiraju na isti način. Tada algebarsku strukturu koju čini domen D u odnosu na pomenute relacije zovemo model skupa formula F.

Iz rečenog sledi da je u slučaju valjanih formula model bilo koja algebarska struktura, određena nekim domenom i nekim njegovim relacijama.

Primer.
Neka je dat skup formula : $F = \{ \alpha(x,x),\ \alpha(x,y) \Rightarrow \alpha(y,x) \wedge \alpha(y,z) \Rightarrow \alpha(x,z) \}$
Model skupa formula F je bilo koji neprazan skup D sa nekom svojom relacijom ekvivalencije, kao interpretacijom relacijskog slova $\alpha$.

Neka svojstva valjanih formula.

U primeru (4) valjane formule su konstruisane koristeći tautologije : $p \vee \neg p$ , $p \Rightarrow (q \Rightarrow p)$ , gde smo iskazna slova p i q zamenili kvantifikatorskim formulama. Slično važi i u opštem slučaju.
Neka je A iskazna formula čija su sva različita iskazna slova $u_1, u_2, \ldots, u_n$ i neka je F formula koja se dobija kada se slova $u_1, u_2, \ldots, u_n$ zamene nekim formulama kvantifikatorskog računa (ista slova zamene se istim formulama) i pri tome se , $\Rightarrow$ , $\neg, \vee, \wedge$ $\Leftrightarrow$ zamene odgovarajućim znacima kvantifikatorskog računa.
tada važi sledeći stav :
Stav 1. Ako je A tautologija, onda je F valjana formula.
Međutim, na ovaj način se može dobiti samo jedan deo klase valjanih formula.




Navedimo primere valjanih formula koje se mogu dobiti iz tautologija na opisani način.
1) $\alpha(x) \Rightarrow (\exists x)\, \alpha(x)$
2) $(\forall x)(A \wedge B) \Leftrightarrow (\forall x)\, A \wedge (\forall x)\, B$
3) $(\exists x)(A \wedge B) \Rightarrow (\exists x)\, A \wedge (\exists x)\, B$
4) $(\exists x)(A \vee B) \Leftrightarrow (\exists x) A \vee (\exists x)\, B$
5) $(\forall x)(A \vee B) \Leftarrow (\forall x)\, A \vee (\forall x)\, B$
gde su A,B neke kvantifikatorske formule.
Može se pomisliti da je i formula $(\forall u)\, A(u) \Rightarrow A(v)$ (5)
gde su u,v promenljive, A kvantifikatorska formula, valjana.
Međutim sledeći primer će nas uveriti da to nije tačno.
Neka je A sledeća formula : $(\exists y)\, \alpha(x,y)$
Tada formula (5) postaje : $(\forall x)\, (\exists y)\, \alpha(x,y) \Rightarrow (\exists y)\, \alpha(y,y)$ (6)
Navedimo interpretaciju za koju formula (6) nije tačna (prema tome nemože biti valjana).
Neka je domen D skup prirodnih brojeva, a relacijsko slovo $\alpha$ interpretirajmo kao relaciju $<$ (manje). Interpretacija formule (6) je sledeća : $(\forall x)(\exists y)(x < y) \Rightarrow (\exists v)(v < y)$ (7)
Leva strana u (7) ima vrednost T, a desna $\perp$, pa cela formula ima vrednost : $T \Rightarrow \perp = \perp$

Stav 2. Formula (5) je valjana ukoliko formula A ispunjava sledeći uslov : U formuli A(u) promenljiva u se nigde ne nalazi pod dejstvom kvantifikatora $(\forall v)$, $(\exists v)$.

Dokaz.

Pretpostavimo da formula (5) nije valjana. Tada pri nekoj interpretaciji I formula (5) ima vrednost $\perp$ . U tom slučaju formula $(\forall u)A(u)$ ima vrednost T , dok formula A(v) ima vrednost $\perp$ Po pretpostavci promenljiva u u formuli A ne nalazi se nigde pod dejstvom kvantifikatora $(\forall v),(\exists v)$. Stoga zaključujemo da, ako promemenlive u i v dobiju pri interpretaciji I istu vrednost, onda će i vrednosti formula A(u) i A(v) biti iste. Znači , za ovu određenu interpretaciju promenljive u , formula A(u) ima vrednoost $\perp$, dok prema pretpostavci formula A(u) ima vrednost T za svako u. Dobijena kontradikcija dokazuje tvrđenje.

Navedimo još dva svojstva valjanih formula.

Stav 3. Ako su A, $A \Rightarrow B$ valjane formule onda je i B valjana formula.

Stav 4. Ako je A valjana formula onda je i $(\forall u)A(u)$ valjana formula.

Hipoteze i posledice.

Definicija 1.

Neka je F skup formula i F neka formula. Kažemo da je F semantička posledica skupa formula, u oznakom $F \models F$ , ako je za svaku interpretaciju I skupa svih tih formula ispunjen sledeći uslov: Kada su sve formule skupa F tačne tada je i formula F tačna. Formule skupa F zovu se hipoteze.

Kratkoće radi, umesto semantička posledica , reći ćemo kratko posledica.

Umesto $\{F_1, F_2, \ldots, F_n\} \models F$ pisaćemo $F_1, F_2, \ldots, F_n \models F$.

Prema usvojenoj definiciji važi sledeće :

$F_1 \models F_1$ , $F_1, F_2 \models F_1$ , $F_1 \wedge F_2 \models F_1$ , $F_1 \models F_1 \vee F_2$ , $F_1 \models (\forall u)F_1$ .

gde su $F_1, F_2$ proizvolne formule, a u promenljiva.

U iskaznoj algebri smo imali $A \models B$ ako i samo ako $\models A \Rightarrow B$

U kvantifikatorskom računu analogno ne važi, jer naprimer :

$\alpha(x) \models (\forall x)\alpha(x)$ , ali nije $\models \alpha(x) \Rightarrow (\forall x)\alpha(x)$ (8)

Navodimo interpretaciju za formulu (8) za koju ona nije tačna. Neka je D skup N prirodnih brojeva, a relacijsko slovo $\alpha$ interpretirajmo kao relaciju dužine 1 :"biti paran broj". Desna strana je netačna, leva je tačna ako x interpretiramo kao broj 2. Tada formula (8) ima vrednost $T \Rightarrow \perp = \perp$, pa (8) nije valjana formula

Karakterizacija valjanih formula.

Uvedimo skup $\underline{T}$ tzv. teorema.

Definicija.

1) Ako su A,B,C proizvoljne kvantifikatorske formule , tada su sledeće formule teoreme.

I $A \Rightarrow (B \Rightarrow A)$

II $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

III $(\neg A \Rightarrow \neg B) \Rightarrow (B \Rightarrow A)$

IV $(\forall u)A(u) \Rightarrow A(V)$

u formuli A(u) promenljiva u se nigde ne nalazi pod dejstvom kvantifikatora $(\forall v)$, $(\exists v)$.

V $(\forall u)(A \Rightarrow B) \Rightarrow (A \Rightarrow (\forall u)B)$

(promenljiva u nije slobodna promenljiva formule A)

2) (a) Ako su A, $A \Rightarrow B$ teoreme, onda je B teorema.

(b) Ako je A teorema onda je i $(\forall u)A(u)$ teorema , gde je u promenljiva.

3) Teoreme se mogu dobiti samo konačnom primenom 1) i 2) ove definicije.

Prema usvojenoj definiciji očigledno je da je svaka teorema valjana formula. Ako skup svih valjanih formula označimo sa V onda imamo sledeću inkluziju : $\underline{T} \subseteq V$.

Međutim, inkluzija važi i u drugom smeru, pa imamo sledeći,

Gödel-ov stav.

Skup $\underline{T}$ svih teorema poklapa se sa skupom V svih valjanih formula odnosno $\underline{T} = V$.

Ovaj stav je od izuzetnog značaja, jer dozvoljava da se skup valjanih formula uvede sa manje intuicije i bez pominjanja interpretacije i semantičkih pojmova : "tačan","netačan".

Inače, ovaj stav se naziva stav o potpunosti predikatskog računa.

Napomena. Kvantifikatorski račun prvoga reda, koji smo posmatrali je tzv. čisti kvantifikatorski račun, za razliku od opšteg kvantifikatorskog računa u kome se pored simbola koje smo mi upotrebili, upotrebljavaju još konstante i funkcijska slova, i na osnovu njih definišu tzv. termi.

Svi izloženi rezultati u čistom kvantifikatorskom računu lako se prenose (sa izvesnim izmenama) i na slučaj opšteg kvantifikatorskog računa. Nakon uvođenja neophodnih definicija objasnićemo to na primeru.

Za konstante uzimamo simbole : $a_1, a_2, \ldots, a_n, \ldots$

Za funkcijska slova : $f_1^1, f_2^1, \ldots, f_i^1, \ldots$

gde je gornji indeks oznaka za tzv. dužinu slova.

Dajemo definiciju terma.

Definicija.

1) Promenljive i konstante su termi.
2) Ako su $t_1, t_2, \ldots, t_n$ termi i ako je f operacijsko slovo dužine n, onda je i reč $f(t_1, t_2, \ldots t_n)$ term.
3) Termi se mogu obrazovati samo posle konačno mnogo primena 1) i 2) ove definicije.

Termi su naprimer : x, $a_1$, $f_1^5(x,y,z,a_1,a_2)$, $f_1^2(f_1^1(x), f_1^2(a_1,a_2))$.
Međutim, reči : $f_1^3(x,y)$, $f_1^1(f_1^1)$, $f_2^1(a_1,a_2)$ nisu termi.
Definicije formula uvode se analogno kao u čistom kvantifikatorskom računu sa tim što umesto promenljivih dolaze termi. Isto važi i za pojam interpretacije. Pri tome se konstante interpretiraju kao fiksirani elementi domena, a funkcijska slova kao operacije domena odgovarajuće dužine.
Razjasnimo rečeno na sledećem primeru.
Neka je data formula: (9)

$$(\forall x)(\forall y)\alpha(f_1^1(f_1^2(x,y)), f_1^2(f_2^2(f_1^1(x), f_2^1(y)), f_2^2(f_2^1(x), f_1^1(y))))$$

Za domen interpretacije uzmimo skup R realnih brojeva, relacijsko slovo $\alpha$ dužine dva interpretirajmo kao "jednakost", a funkcijska slova $f_1^1$, $f_2^1$, $f_1^2$, $f_2^2$, redom kao sin, cos, + , . , tada formula (9) postaje : $(\forall x)(\forall y)(\sin(x+y) = \sin x.\cos y + \cos x.\sin y)$.
Ova formula ima vrednost T. Kažemo, kao i ranije, da je formula (9) tačna pri interpretaciji I, $I = \left(R, \left(\underset{\sin}{f_1^1}\ \underset{\cos}{f_2^1}\ f_1^2\ f_2^2\right)\right)$.
Valjane formule se definišu analogno, a vredi i slična karakterizacija (Godel-ov stav).
Postavlja se pitanje kakav je značaj valjanih formula u matematici uopšte.
Matematičke teorije (danas) uglavnom se zasnivaju tzv. potpuno aksiomatski na sledeći način.
Polazni termini i aksiome se iskazuju korišćenjem navedenog formulskog jezika. Može se reći : termini i aksiome se prevode na taj jezik. Teoreme matematičke teorije su onda : aksiome, valjane formule (koje se obično uvode pomoću navedenih karakterističkih svojstva I,II,III,IV,V i zovu teoreme predikatskog računa) kao i sve formule koje se izvode iz njih primenom pravila izvođenja.
Ta pravila izvođenja su : modus ponens (iz A i $A \Rightarrow B$ proizlazi B), generalizacija (iz A proizlazi $(\forall u)A$, gde je u promenljiva.)
Kao što ćemo kasnije videti, svako korektno zaključivanje (dedukcija) je izvestan niz čiji su elementi hipoteze ili valjane formule ili se dobijaju iz nekih prethodnih članova niza primenom tzv. pravila izvođenja.

# FORMALNE TEORIJE

Po analogiji s običnim matematičkim teorijama uvode se formalne teorije i pojmovi : dokaz, teorema, hipoteza, posledica itd. Ovi pojmovi sadrže i neka bitna preciziranja koja obično nisu naglašena u neformalnim teorijama.

Formalna teorija u oznaci $\mathcal{T}$, određena je kad su ispunjeni sledeći uslovi :

1) Dat je najviše prebrojiv skup simbola, tzv. osnovnih simbola teorije $\mathcal{T}$.
2) U skupu svih reči sa osnovnim simbolima određen je pod skup, tzv. skup formula teorije $\mathcal{T}$. Uz to je dat i efektivan postupak za odlučivanje dali je neka reč formula ili nije.
3) U skupu svih formula određen je jedan podskup čije elemente zovemo aksiome . . Ako je još dat i efektivan postupak za određivanje dali je neka formula aksioma ili nije, onda teoriju $\mathcal{T}$ zovemo aksiomatskom teorijom.
4) Dat je konačan broj tzv. pravila izvođenja. Svako pravilo izvođenja je izvesna relacija u skupu formula teorije $\mathcal{T}$. Ako je $\alpha$ jedno pravilo izvođenja dužine n , naprimer, onda ma kakve bile formule $A_1, A_2, \ldots, A_{n-1}, A_n$ postoji efektivan postupak za odlučivanje dali su redom formule $A_1, A_2, \ldots, A_n$ u relaciji ili nisu. Ako su redom formule $A_1, A_2, \ldots, A_n$ u relaciji $\alpha$ onda kažemo i: $A_n$ je direktna posledica redom formula $A_1, A_2, \ldots A_{n-1}$, po pravilu izvođenja $\alpha$, i pišemo :

$$\frac{A_1, A_2, \ldots, A_{n-1}}{A_n}$$

Označimo redom sa $S(\mathcal{T})$, $\mathcal{F}(\mathcal{T})$, $A(\mathcal{T})$, $R(\mathcal{T})$, Skupove osnovnih simbola, formula, aksioma i pravila izvođenja teorije $\mathcal{T}$. Navedeni skupovi određuju formalnu teoriju pa se teorija $\mathcal{T}$ može striktno definisati kao uređena četvorka $(S(\mathcal{T}), \mathcal{F}(\mathcal{T}), A(\mathcal{T}), R(\mathcal{T}))$

Umesto formalna teorija kažemo i formalni račun.

Definicija. Konačan niz formula $B_1, B_2, \ldots, B_n$ zovemo izvođenje (dedukcija dokaz) u teoriji $\mathcal{T}$ ako svaka formula $B_i$ ( $1 \leq i \leq n$) tog niza ispunjava uslov :

1) $B_i$ je aksioma , ili
2) $B_i$ je direktna posledica nekih prethodnih formula po izvesnom pravilu izvođenja teorije $\mathcal{T}$.

Definicija. Formulu $B_m$, formalne teorije $\mathcal{T}$ zovemo teorema u teoriji $\mathcal{T}$ u oznaci $\vdash_{\mathcal{T}} B_m$ , (Ili samo $\vdash B_m$) ako postoji bar jedan niz $B_1, B_2, \ldots B_m$ koji je izvođenje u teoriji $\mathcal{T}$. U ovom slučaju kažemo i da je taj niz izvođenje teoreme $B_m$. Dokazati teoremu $B_m$, u teoriji $\mathcal{T}$ znači konstruisati niz $B_1, B_2, \ldots, B_m$, koji je izvođenje u ovoj teoriji.

Pojam dokaza u formalnoj teoriji uveden je po ugledu na obične matematičke dokaze. Dokaz u običnoj matematičkoj teoriji je konačan niz čiji svaki član je: aksioma , ranije dokazana teorema ili se dobija iz nekih prethodnih članova po izvesnom pravilu izvođenja (ta se pravila obično ne e pliciraju).

Naprimer u sistemu ne negativnih realnih brojeva, niz

1) $x + y = x + y$ (aksioma)

2) $0 \leq 2\sqrt{xy}$ (dokazana teorema)

3) $x + y \leq x + 2\sqrt{xy} + y$ ("sabiranjem" 1 i 2)

4) $(\sqrt{x + y})^2 \leq (\sqrt{x} + \sqrt{y})^2$ (iz 3)

5) $\sqrt{x + y} \leq \sqrt{x} + \sqrt{y}$ (iz 4, korenovanjem)

predstavlja dokaz tvrđenja : Ako su x , y ne negativni realni brojevi onda je $\sqrt{x+y} \leq \sqrt{x} + \sqrt{y}$

Primer formalne teorije.

Neka su slova a i r osnovni simboli teorije $\mathcal{T}$. Dogovorno reči a , aaa, .. označimo sa $a^1$, $a^3$, (dakle $a^1$ je a, $a^{n+1} = a^n a$., n= 1,2. Neka su formuše reči oblika $a^1 r a^2$, $a^1 r a^3$, $a^1 r a^5$,...odnosno sve reči oblika $a^m r a^n$, gde su m i n pozitivni prirodni brojevi. Za aksiome uzimamo formule : $a^1 r a^1$, $a^3 r a^1$, a za pravila izvođenja :

$$\alpha : \frac{a^m r a^n}{a^n r a^m} \quad ; \quad \beta : \frac{a^m r a^n}{a^{m+1} r a^{n+1}} \quad , \quad \gamma : \frac{a^m r a^n,\ a^p r a^q}{a^{m+p} r a^{n+q}}$$

od kojih su $\alpha$ i $\beta$ dužine dva a $\gamma$ je dužine tri. Tada niz formula: I) $a^3 r a^1$, 2) $a^4 r a^2$ 3) $a^5 r a^3$ 4) $a^5 r a^1$ pretstavlja izvođenje u teoriji jer : 1 je aksioma, 2 dobijeno iz 1 pomoću pravila $\beta$ 3 dobijeno iz 2 pomoću pravila $\beta$, 4 dobijeno iz 3 i 1 pomoću pravila $\gamma$ .

Prema tome formula $a^5 r a^1$ je teorema teorije $\mathcal{T}$.

Takođe su i formule $a^2 r a^2$, $a^2 r a^4$, $a^6 r a^2$, $a^3 r a^3$, teoreme.

Uopšte ako je m + n paran broj tada je formula $a^m r a^n$ teorema teorije $\mathcal{T}$. Dokazaćemo da važi i sledeće: Ako je $a^m r a^n$ teorema teorije $\mathcal{T}$ onda je zbir m + n paran broj.

Neka se formula $a^m r a^n$ zove parna formula ako je m + n paran broj. Aksiome $a^1 r a^1$, $a^3 r a^1$ su parne formule. Ako su $a^m r a^n$ parne formule onda su i formule $a^{m+1} r a^{n+1}$, $a^{m+p} r a^{n+q}$, takođe parne. Slično ako su $a^m r a^n$ i $a^p r a^q$ parne formule onda je formula $a^{m+p} r a^{n+q}$ parna, kratko kažemo : aksiome su parne formule i pravila izvođenja čuvaju parnost formula. Zbog ovoga svi članovi $B_1, B_2, \ldots, B_n$ nekog izvođenja u teoriji $\mathcal{T}$ moraju biti parne formule. Zaključak : Teorema računa $\mathcal{T}$ mora biti parna formula . Dakle u slučaju navedene teorije $\mathcal{T}$ tačan je iskaz : Formula A teorije $\mathcal{T}$ je teorema ako i samo ako je A parna formula.

Za odlučivanje tačnosti neke formule postoji efektivan postupak. Otuda postoji efektivan postupak za odlučivanje dali je neka formula teorije $\mathcal{T}$ teorema ili nije. Iz ovog razloga za teoriju $\mathcal{T}$ kažemo da je odlučiva.

Uopšte, neka formalna teorija $\mathcal{T}$ je odlučiva ako postoji efektivan postupak kojim se može za proizvolnu formulu A te teorije odlučiti dali je teorema teorije $\mathcal{T}$ ili nije.

Definicija.

Neka je $\mathcal{F}$ neki skup formula neke formalne teorije $\mathcal{T}$, i neka je A određena formula iz te teorije. Kažemo : formula A je posledica skupa formula $\mathcal{F}$ ako postoji konačan niz formula $B_1, B_2, \ldots B_n$ ( $B_n = A$) , čija svaka formula $B_i$ ispunjava uslove :

1) $B_i$ je aksioma, ili
2) $B_i$ je iz skupa $\mathcal{F}$
3) $B_i$ je direktna posledica nekih prethodnih formula niza po izvesnom pravilu izvođenja teorije $\mathcal{T}$.

Ako je A posledica skupa formula $\mathcal{F}$, onda pišemo $\mathcal{F} \vdash_{\mathcal{T}} A$ ili $\mathcal{F} \vdash A$ , a elemente skupa $\mathcal{F}$ zovemo hipoteze (premise, pretpostavke). Pomenuti niz $B_1, B_2, \ldots, B_n$ zovemo izvođenje formule A iz skupa hipoteza $\mathcal{F}$. Ako je $\mathcal{F}$ konačan skup , onda umesto : $\{A_1, A_2, \ldots, A_n\} \vdash A$ pišemo i $A_1, A_2, \ldots, A_n \vdash A$

Izvođenja iz hipoteza imaju sledeća značajna svojstva :

1) Ako je $\mathcal{F}_1 \subseteq \mathcal{F}_2$ i $\mathcal{F}_1 \vdash A$ onda $\mathcal{F}_2 \vdash A$
2) $\mathcal{F} \vdash A$ ako i samo ako postoji konačan podskup $\mathcal{F}_1$ skupa $\mathcal{F}$ takav da je $\mathcal{F}_1 \vdash A$
3) Neka $\mathcal{F}_1 \vdash B$ gde je B proizvolna formula iz skupa $\mathcal{F}_2$. Ako $\mathcal{F}_2 \vdash A$ onda $\mathcal{F}_1 \vdash A$.

Formalne teorije obrazuju jednu klasu matematičkih teorija. Ostale matematičke teorije zovemo obične matematičke teorije. Za opisivanje i izgrađivanje neke formalne teorije koristi se izvesna obična matematička teorija , koju zovemo metateorija te formalne teorije . Formalnu teoriju u tom slučaju zovemo i objekt-teorija. Meta-teorija nužno sadrži osnove logike i odgovarajući deo logike sa kvantifikatorima.

Jedan od tvoraca formalnih teorija , D. Hilbert, u svome programu izgrađivanja formalnih teorija postavio je zahtev korišćenja striktne finitnosti u meta-teoriji, odnosno ne korišćenja , naprimer, Zorn-ove leme, aksiome izbora, aktualne beskonačnosti i slično. Ali pomoću takve meta-teorije nije moguće dokazati, naprimer, neprotivrečnost formalne teorije brojeva. To je rezultat K. Godel-a, tzv. druga Godel-ova teorema.

Međutim ako se meta-teorija proširi teorijom ordinalnih brojeva, odnosno neelementarnom teorijom skupova, onda se neprotivrečnost formalne teorije brojeva dokazuje (G.Gentzen) .
Za neki rezultat koji se odnosi na formalnu teoriju veoma je značajno pomoću koje metateorije je dobijen . Ako se o ovome ne vodi računa mogu nastati razni nesporazumi.
Metateorija se izlaže korišćenjem jednog dela običnog jezika proširenog odgovarajućom matematičkom terminologijom. Taj jezik zovemo meta-jezik. I formalna teorija ima svoj jezik tzv. objekt-jezik. To je skup čiji su elementi polazni simboli formalne teorije reči sastavljene od tih polaznih simbola , kao i konačni nizovi tih reči. Prema tome, formule, aksiome i izvođenja pripadaju objekt jeziku. U prethodno navedenoj teoriji formule ara, araa,.. su u objekt-jeziku dok je iskaz : "Formula ara je teorema " , u meta-jeziku. U meta-teoriji koristili smo i izvesne elemente teorije prirodnih brojeva.
Tvrđenje koje se odnosi na neku formalnu teoriju zovemo meta-teorema. Tako :"formula ara je teorema" jeste meta-teorema.
Obične matematičke teorije izgrađuju se na sledeći način.
Polazi se od jednog skupa polaznih (osnovnih) termina i određenog skupa rečenica sa tim terminima, tzv, aksioma. Za teoreme se onda uzimaju rečenice koje su tačne pri onim interpretacijama pri kojima su i aksiome tačne, isto tako teoreme su i sve rečenice koje se dobijaju iz aksioma primenom izvesnih logičkih pravila ( koja se obično ne ističu ) . Za prvi slučaj kažemo da se teoreme izvode semantički a sa drugi sintaktički. Kod običnih matematičkih teorija često se prepliću ta dva načina dobijanja teorema.
Osim toga postoji i jak stepen intuicije o skupu.
Kod formalnih teorija upotreba intuicije svodi se na neizbežni minimum, a takođe se preciziraju pojmovi aksioma, teorema, izvodjenje i slično.
Formalne teorije se obrazuju sa ciljem tzv. potpunog aksiomatskog zasnivanja neke obične matematičke teorije. Radi toga se formalna teorija tako izabere da elementima njenog objekt-jezika odgovaraju objekti matematičke teorije koju formalno izgradujemo. Preciziranjem rečenog dobija se pojam glavnih interpretacija.
Inače interpretacija neke formalne teorije je svako preslikavanje objekt-jezika te teorije u klasu objekata neke druge matematičke teorije.
Navodimo dve interpretacije posmatrane formalne teorije.

Prvu smo obrazovali inspirišući se sledećim tvrdenjima iz teorije celih brojeva :

a) $-1 = -1$ , $-1 = (-1)^3$

b) ako je $(-1)^i = (-1)^j$ onda je $(-1)^j = (-1)^i$ , gde su i i j prirodni brojevi.

Stim u vezi pri njenoj glavnoj interpretaciji imamo : interpretacija slova a je broj -1, interpretacija slova r je relacija "jednakost", a interpretacija reči a je broj $(-1)$ , itd...

Za isti primer druga interpretacija u oznaci g jeste sledeće preslikavanje objekt jezika u skup prirodnih brojeva :

1) $g(a) = 1$, $g(r) = 3$, $g(aa) = 11$, $g(araa) = 1311$ ,

odnosno $g(s_1, s_2, \ldots, s_k)$ ( gde su $s_i$ slova a i r ) jeste prirodan broj čija su cifra u dakadnom sistemu redom $g(s_1), g(s_2), \ldots, g(s_k)$.

2) Ako su $g(w_1), g(w_2), \ldots, g(w_n)$ prirodni brojevi dodeljeni redom rečima $w_1, w_2, \ldots, w_n$ onda nizu reči $w_1, w_2, \ldots, w_n$ dodeljujemo prirodan broj u oznaci $g(w_1)2g(w_2)2\ldots2g(w_n)$ čije su cifre redom cifre brojeva $g(w_i)$ i 2.

Naprimer nizu ara, a ra dodeljujemo broj 131112111131.

Korišćenjem slične interpretacije Gödel je dokazao neke svoje poznate stavove.

Primeri formalnih teorija.

1) Iskazni račun.

polazni simboli su $p, q, r, p_1 q_1 r_1 \ldots p_n q_n r_n$ , $( ) \Rightarrow \neg$

Formule se definišu na poznati način.

Aksiome su

1) $A \Rightarrow (B \Rightarrow A)$

2) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

3) $(\neg A \Rightarrow \neg B) \Rightarrow (B \Rightarrow A)$

gde su A,B,C proizvolne formule.

Pravilo izvodenja je modus ponens : $\frac{A,\ A \Rightarrow B}{B}$

Iskazni račun je odlučiva teorija. To sledi iz činjenice da je skup teorema jednak skupu tautologija (to je ujedno osnovni stav u ovoj teoriji).

2) Čisti predikatski račun prvoga reda.

Polazni simboli su :

promenljive $x, y, z, x_1, y_1, z_1, \ldots$

relacijska slova $R_1^1, R_2^1, \ldots, R_m^1, \ldots, R_i^j, \ldots$

Aksiome su :

1) $A \Rightarrow (B \Rightarrow A)$

2) $(\neg A \Rightarrow \neg B) \Rightarrow (B \Rightarrow A)$

3) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

4) $(\forall u)A(u) \Rightarrow A(v)$, ako se u formuli A(u) promenljiva u ne nalazi u oblasti dejstva $(\forall v)$ ili $(\exists v)$

Međutim ako se meta-teorija proširi teorijom ordinalnih brojeva, odnosno neelementarnom teorijom skupova, onda se neprotivrečnost formalne teorije brojeva dokazuje (G.Gentzen) .
Za neki rezultat koji se odnosi na formalnu teoriju veoma je značajno pomoću koje metateorije je dobijen . Ako se o ovome ne vodi računa mogu nastati razni nesporazumi.
Metateorija se izlaže korišćenjem jednog dela običnog jezika proširenog odgovarajućom matematičkom terminologijom. Taj jezik zovemo meta-jezik. I formalna teorija ima svoj jezik tzv. objekt-jezik. To je skup čiji su elementi polazni simboli formalne teorije reči sastavljene od tih polaznih simbola , kao i konačni nizovi tih reči. Prema tome, formule, aksiome i izvođenja pripadaju objekt jeziku. U prethodno navedenoj teoriji formule ara, araa,.. su u objekt-jeziku dok je iskaz : "Formula ara je teorema " , u meta-jeziku. U meta-teoriji koristili smo i izvesne elemente teorije prirodnih brojeva.
Tvrđenje koje se odnosi na neku formalnu teoriju zovemo meta-teorema. Tako :"formula ara je teorema" jeste meta-teorema.
Obične matematičke teorije izgrađuju se na sledeći način.
Polazi se od jednog skupa polaznih (osnovnih) termina i određenog skupa rečenica sa tim terminima, tzv, aksioma. Za teoreme se onda uzimaju rečenice koje su tačne pri onim interpretacijama pri kojima su i aksiome tačne, isto tako teoreme su i sve rečenice koje se dobijaju iz aksioma primenom izvesnih logičkih pravila ( koja se obično ne ističu ) . Za prvi slučaj kažemo da se teoreme izvode semantički a sa drugi sintaktički. Kod običnih matematičkih teorija često se prepliću ta dva načina dobijanja teorema.
Osim toga postoji i jak stepen intuicije o skupu.
Kod formalnih teorija upotreba intuicije svodi se na neizbežni minimum, a takođe se preciziraju pojmovi aksioma, teorema, izvodjenje i slično.
Formalne teorije se obrazuju sa ciljem tzv. potpunog aksiomatskog zasnivanja neke obične matematičke teorije. Radi toga se formalna teorija tako izabere da elementima njenog objekt-jezika odgovaraju objekti matematičke teorije koju formalno izgradujemo. Preciziranjem rečenog dobija se pojam glavnih interpretacija.
Inače interpretacija neke formalne teorije je svako preslikavanje objekt-jezika te teorije u klasu objekata neke druge matematičke teorije.
Navodimo dve interpretacije posmatrane formalne teorije.

Prvu smo obrazovali inspirišući se sledećim tvrdenjima iz teorije celih brojeva :

a) $-1 = -1$ , $-1 = (-1)^3$

b) ako je $(-1)^i = (-1)^j$ onda je $(-1)^j = (-1)^i$ , gde su $i$ i $j$ prirodni brojevi.

Stim u vezi pri njenoj glavnoj interpretaciji imamo : interpretacija slova a je broj -1, interpretacija slova r je relacija "jednakost", a interpretacija reči a je broj (-1) , itd...

Za isti primer druga interpretacija u oznaci $g$ jeste sledeće preslikavanje objekt jezika u skup prirodnih brojeva :

1) $g(a) = 1$, $g(r) = 3$, $g(aa) = 11$, $g(araa) = 1311$ ,

odnosno $g(s_1, s_2, \ldots, s_k)$ ( gde su $s_i$ slova a i r ) jeste prirodan broj čija su cifra u dakadnom sistemu redom $g(s_1), g(s_2), \ldots, g(s_k)$.

2) Ako su $g(w_1), g(w_2), \ldots, g(w_n)$ prirodni brojevi dodeljeni redom rečima $w_1, w_2, \ldots, w_n$ onda nizu reči $w_1, w_2, \ldots, w_n$ dodeljujemo prirodan broj u oznaci $g(w_1)2g(w_2)2\ldots2g(w_n)$ čije su cifre redom cifre brojeva $g(w_i)$ i 2.

Naprimer nizu ara, a$^3$ra dodeljujemo broj 13111211131.

Korišćenjem slične interpretacije Gödel je dokazao neke svoje poznate stavove.

Primeri formalnih teorija.

1) Iskazni račun.

polazni simboli su $p, q, r, p_1, q_1, r_1, \ldots p_n, q_n, r_n$ , $( ) \Rightarrow \neg$

Formule se definišu na poznati način.

Aksiome su

1) $A \Rightarrow (B \Rightarrow A)$

2) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

3) $(\neg A \Rightarrow \neg B) \Rightarrow (B \Rightarrow A)$

gde su A,B,C proizvolne formule.

Pravilo izvodenja je modus ponens : $\frac{A,\ A \Rightarrow B}{B}$

Iskazni račun je odlučiva teorija. To sledi iz činjenice da je skup teorema jednak skupu tautologija (to je ujedno osnovni stav u ovoj teoriji).

2) Čisti predikatski račun prvoga reda.

Polazni simboli su :

promenljive $x, y, z, x_1, y_1, z_1, \ldots$

relacijska slova $R_1^1, R_2^1, \ldots, R_n^1, \ldots, R_i^j, \ldots$

Aksiome su :

1) $A \Rightarrow (B \Rightarrow A)$

2) $(\neg A \Rightarrow \neg B) \Rightarrow (B \Rightarrow A)$

3) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

4) $(\forall u)A(u) \Rightarrow A(v)$, ako se u formuli $A(u)$ promenljiva u ne nalazi u oblasti dejstva $(\forall v)$ ili $(\exists v)$

5) $(\forall u)(A \Rightarrow B) \Rightarrow (A \Rightarrow (\forall u)B)$ , ako u nije slobodna promenljiva u A.

Pravila izvodenja su :

Modus ponens $\dfrac{A,\ A \Rightarrow B}{B}$

Generalizacija $\dfrac{A}{(\forall u)\ A}$

Predikatski račun nije odlučiva teorija. To je dokazao Church 1936 god. Predikatski račun je neprotivrečna teorija.

3) Kvantifikatorski račun.

Ova formalna teorija predstavlja proširenje prethodne. Izlaganje o njoj dobija se iz izlaganja o predikatskom računu prvoga reda ukoliko se na odredeni način promenljive zamene termima. Formule ovog kvantifikatorskog računa su "podesnije" za opisivanje matematičkih tekstova. Tu treba tražiti osnovni razlog njegovog uvodenja. Možemo međutim (često vrlo "komplikovano") i pomocu formula predikatskog računa prvoga reda da opisujemo matematičke tak stove.

## AKSIOMATIZACIJA MATEMATIČKIH TEORIJA POMOĆU KVANTIFIKATORAKOG RAČUNA

Neka je T izvesna (intuitivna) matematička teorija. Njenim polaznim terminima - relacijskim i operacijskim , možemo dodeliti po jedan relacijski odnosno operacijski simbol. Aksiomama te teorije T možemo dodeliti izvesne formule kvantifikatorskog računa. Drukčije rečeno, aksiome možemo prevesti na formulski jezik kvantifikatorskog računa. Označimo sa For skup svih kvantifikatorskih formula u koje ne ulaze drugi operacijski i relacijski simboli već samo oni koji odgovaraju polaznim terminima. Skup $Ax \subseteq For$ je onda skup formula koje odgovaraju aksiomama teorije T.

Preciziranjem skupa For i skupa Ax je izvršena aksiomatizacija matematičke teorije T u okviru kvantifikatorskog računa. Tako smo odredili jednu formalnu teoriju, koju ćemo označiti istim simbolom T.

Aksiome teorije T su :

1) svi elementi skupa Ax - tzv. sobstvene aksiome teorije T.
2) sve logičke aksiome iz skupa For - u stvari sve valjane formule iz skupa For.

Teoreme teorije T su one formule $F \in For$ koje imaju <u>dokaz</u> (<u>izvodjenje</u>) - izvestan konačan niz $F_1, F_2, \ldots, F_{n-1}, F$ čiji je svaki član aksioma ili se može dobiti iz nekih prethodnih članova niza primenom MP (modus ponens) ili Gen (generalizacija).

MP : $\dfrac{A \ , \ A \Rightarrow B}{B}$ (čita se : iz A i $A \Rightarrow B$ proizlazi B)

Gen : $\dfrac{A}{(\forall u)A}$ ( u je promenljiva ).

Jedan od osnovnih problema teorije T je problem neprotivurečnost teorije T.

<u>Definicija 1.</u>

Teorija T je neprotivurečna ukoliko u skupu For formula te teorije nema dve formuše oblika A i $\neg A$ koje su obe teoreme teorije T.

Ukoliko je teorija T protivurečna onda joj je svaka formula teorema. Zaista onda su izvesne formule A i $\neg A$ teoreme pa ako je $B \in For$ bilo koja formula onda na osnovu logičke aksiome :

$A \Rightarrow (\neg A \Rightarrow B)$ dvostrukom primenom MP dobijamo da je formula B teorema.

Šta više, ukoliko teorija T ima bar jednu formulu koja nije teorema te teorije onda je ta teorija neprotivurečna. Stoga se može dati i sledeča definicija neprotivurečnosti :

Definicija 2.

Teorija T je neprotivurečna ukoliko ima bar jednu formulu koja nije teorema te teorije.

U današnje vreme nemamo za mnoge značajne matematičke teorije dokaz neprotivurečnosti. Na osnovu poznate Gödelove teoreme koristeći se u meta-teoriji samo finitnim sredstvima nije moguče , na primer, dokazati neprotivurečnost formalne aritmetike - čije aksiome dalje navodimo. Neprotivurečnost aritmetike moguče je dokazati (Rosser) korišćenjem teorije skupova. Opravdano je pitanje koliko smo uvereni u takav dokaz sa toliko snažnom meta-teorijom odnosno intuicijom.

Navodimo primere.

I Formalna aritmetika A.

Ta teorija ima relacijski simbol $\propto$ - dužine 2, jednu konstantu a, jedan operacijski simbol f - dužine 1, dva operacijska simbola g i h - dužine 2.

Umesto : $\propto(t_1,t_2)$, a , $f(t_1)$, $g(t_1,t_2)$, $h(t_1,t_2)$ gde su $t_1$ i $t_2$ neki termi, pišemo : $t_1 = t_2$, 0 , $t_1'$, $t_1 + t_2$, $t_1 . t_2$.

Sobstvene aksiome aritmetike su :

$(x = y \wedge x = z) \Rightarrow y = z$

$x = y \Leftrightarrow x' = y'$, $\neg(x' = 0)$, $x + 0 = x$, $x + y' = (x + y)'$;

$x . y' = x . y + x$

$(A(0) \wedge (\forall x)(A(x) \Rightarrow A(x'))) \quad (\forall x)(A(x))$

gde je A - proizvoljna formula te teorije.

Jedan model je odredjen skupom prirodnih brojeva 0,1,2,... relacijom =, operacijama + i . , operacijom $x' = x + 1$, i konstantom 0. To je tzv. Standardni model. Prihvatanjem tog modela, odnosno prihvatanjem toliko intuicije, možemo zaključiti da je teorija A neprotivurečna.

Napomenimo da su teoreme teorije A razne, dobro poznate formule, koje"izražavaju dobro poznata svostva operacija + , . , ', kao i relacije =". Navodimo primere.

$0 . x = 0$, $0 + x = x$, $x' . y = x . y + y$, $x + y = y + x$,

$x . y = y . x$, $x + (y + z) = (x + y) + z$, $x . (y + z) = x . y + x.z$

$(x.y).z = x.(y.z)$, $x.y = y.x$,... .

Medjutim ostalo je otvoreno pitanje dali postoje prirodni brojevi takvi da je za $x,y,z,n$ $(x > 0, y > 0, z > 0, n > 2)$

$$x^n + y^n = z^n$$

## II. Aksiomatske teorije skupova.

U svojim prvim istraživanjima tvorac teorije skupova Cantor nije se eksplicitno pozivao na neke aksiome o skupovima.

Medjutim, analizom njegovih dokaza može se zaključiti da se skoro sve teoreme koje je on dobio mogu izvesti iz sledećih aksioma :

1) Dva skupa su jednaka ako imaju iste elemente.
2) Za unapred dato svojstvo postoji skup čiji su elementi baš oni koji imaju to svojstvo (Aksioma apstrakcije).
3) Za svaki neprazan skup postoji bar jedna funkcija čiji su originali neprazni podskupovi tog skupa, a slike su elementi originala (Aksioma izbora).

Aksiomu apstrakcije prvi je formulisao G.Frege (1893). B.Russell je 1901. godine iz te aksiome izveo kontradikciju posmatranjem skupa svih skupova koji imaju svojstvo da nisu sami sebi elementi.

Neka je, dakle po pretpostavci, U skup svih skupova V, koji imaju svojstvo $V \notin V$ . Za skup U postoji jedna od dve mogućnosti :

1) $U \in U$. U tom slučaju je U jedan od V-ova, odnosno elemenata skupa U, pa ima svojstvo $U \notin U$.
2) $U \notin U$. U tom slučaju U nije jedan od elemenata skupa U, pa nema svojstvo $U \notin U$ , odnosno jeste $U \in U$.

Označimo sa P iskaz $U \in U$. Prema tome, izveli smo tačnost iskaza : $P \to$ ne P, ne $P \to P$, odakle na osnovu pravila istinitosti za implikaciju proizlazi da su i P i ne P istiniti.

Primedba. Neka je A oznaka za neko predikatsko slovo dužine dva. Formula $(\forall y)(\exists x)\,\neg(A(x,y) \Leftrightarrow \neg A(x,x))$ je valjana, što se neposredno dokazuje.

Negacija te formule je ekvivalentna sa sledećom formulom :

(K) $\qquad (\exists y)(\forall x)(A(x,y) \Leftrightarrow \neg A(x,x))$

Formula (K) je, prema tome, uvek netačna. Uočimo sledeću interpretaciju :

Domen je bilo koji skup i A se interpretira kao relacija $\in$. Tada prema (K) zaključujemo da nije tačno

$$(\exists y)(\forall x)(x \in y \Leftrightarrow \neg(x \in x)),$$

odnosno da ne postoji skup čiji su elementi skupovi koji nisu sebi elementi.

Istorijski, Burali-Forti je prvi 1987. otkrio paradoks u jednom delu teorije skupova - u teoriji ordinalnih brojeva.

Ubrzo zatim (1899) Cantor je našao sličan paradoks u teoriji kardinalnih brojeva.

Iako su matematičari bili jednodušni u pitanju neophodnosti izmena u samim osnovama matematike, u pitanju načina ostvarivanja tih izmena došlo je do dubokih razmimoilaženja.

Prema formalističkom gledištu zasnivanje neke matematičke teorije ne sme da se temelji na intuiciji, već je potrebno stvoriti aksiomatsku bazu i tada je matematička istina jedino ono što proizlazi iz aksioma bez obzira na moguća značenja takvog tvrdjenja.

Dakle, za formaliste rešenje problema se sastojalo u izgradnji aksiomatske teorije skupova, iz koje izlaze svi rezultati Cantorove teorije skupova, a istovremeno u onemogućivanju postojanja "skupova" koji dovode do otkrivenih paradoksa.

Mnogi su nastojali da izbegnu paradokse proičavajući dublje njihovu strukturu. Tako je Russell svojom teorijom tipova uspešno otklonio uočene paradokse. Strogim prihvatanjem njegove teorije mnogi rezultati matematike postaju neobično složeni. Medjutim zajednička odlika navedenih načina rešavanja je nastojanje da se sačuvaju svi postojeći rezultati teorije skupova.

Nasuprot takvim shvatanjima razvio se pravac intuicionizam, čijim koncepcijama se uklanjaju paradoksi, ali se zato dovode u pitanje čitave grane klasične matematike.

Jezikom formula predikatskog računa uvode se razne tzv. aksiomatske teorije skupova. Te teorije su specialni kvantifikatorski računi.

Medjutim, ni za jednu od poznatih aksiomatskih teorija ne znamo da li je neprotivurečna.

Navodimo prethodno tzv. NBG. sistem, koji je prvobitno uveo von Neumann (1925,1928), a koji su zatim dopunili R.Robinson (1937),P.Bernays (1937-1954) i K. Gödel (1940).

Račun NBG je specijalni kvantifikatorski račun prvog reda koji ima samo jedno relacijsko slovo $R_2^2$ (obično se $R_2^2(u,v)$ zamenjuje sa u v i konačno monogo (individualnih) aksioma. Izuzetno pri opisivanju tog računa promenljive su $X_1, X_2, \ldots,$ dok za njihove oznake uzimamo $X, Y, Z, \ldots$. Promenljive $X_1, X_2, X_3, \ldots, X_n, \ldots$ interpretiramo kao klase, a klasa je odredjena svojstvom koje poseduju njeni elementi. Inače, ne zahtevamo da svakom svojstvu odgovara klasa . To pretpostavljamo samo za ona svojstva koja su u skladu sa aksiomama računa NBG. Samo neke klase su skupovi, odnosno uvodimo sledeće definicije.

Definicija 1.

$M(X_i)$ je zamena za $(\exists X_{i+1})(X_i \in X_{i+1})$, gde je $i = 1,2,3,\ldots$ .

$M(X_i)$ čitamo : $X_i$ je skup.

Definicija 2.

$x_i$ je zamena za $M(X_i)$ $(i=1,2,\ldots)$.

Na taj način $x_1,x_2,x_3,\ldots,x_n,\ldots$ je niz promenljivih kojima u interpretaciji odgovaraju skupovi. Za njihove oznake uzimamo x, y, z, u, v, w, ... .

Formule

$$(\forall X_i)(M(X_i) \Rightarrow A(X_i)),\quad (\exists X_i)(M(X_i) \wedge A(X_i))$$

ozhačavamo dogovorno redom

$$(\forall x_i)A(x_i),\quad (\exists x_i)A(x_i),\ \text{gde je}\ i = 1,2,\ldots .$$

Navodimo aksiome i osnovne definicjie računa NBG, dajući pri tom i komentare koji su u skladu sa interpretacijom promenljivih $X_i$, $x_i$ kao klasa, odnosno skupova, i sa interpretacijom simbola relacijom koju možemo zvati "biti element od".

Definicija 3.

$X = Y$ je zamena za $(\forall Z)(Z \in X \Leftrightarrow Z \in Y)$

(Z je prva promenljiva niza $X_1,X_2,\ldots,X_n,\ldots$ koja se razlikuje od X i Y).

Definicija 4.

$X \subseteq Y$ je zamena za $(\forall Z)(Z \in X \Rightarrow Z \in Y)$

(Z je prva promenljiva niza $X_1,X_2,\ldots,X_n,\ldots$ koja se razlikuje od X i Y).

Definicija 5.

$X \subset Y$ je zamena za $X \subseteq Y \wedge X \neq Y$.

Definicijama 3, 4, 5 uvedene su jednakost i inkluzije (neprava i prava).

Aksioma T.(Aksioma ektenzije)

$$X_1 = X_2 \Rightarrow (X_1 \in X_3 \Leftrightarrow X_2 \in X_3).$$

Aksioma P.(Aksioma egzistencije para)

$$(\forall x_1)(\forall x_2)(\exists x_3)(\forall x_4)(x_4 \in x_3 \Leftrightarrow x_4 = x_1 \vee x_4 = x_2).$$

Za bilo koje skupove $x_1,x_2$ postoji skup $x_3$ tako da su $x_1$, $x_2$ jedini elementi tog skupa.

Aksioma N. (aksioma egzistencije praznog skupa)

$$(\exists x_1)(\forall x_2)(x_2 \notin x_1).$$

Iz navedenih aksioma izvode se sledeće teoreme :

$X = X$, $X = Y \Leftrightarrow (X \subseteq Y \wedge Y \subseteq X)$, $X = Y \Rightarrow Y = X$,

$(X = Y \wedge Y = Z) \Rightarrow X = Z$, $X = Y \Rightarrow (Z \in X \Leftrightarrow Z \in Y)$,

$X \in Y \Rightarrow M(X)$, $X = Y \Leftrightarrow (\forall z)(z \in X \Leftrightarrow z \in Y)$,

$(\forall x)(\forall y)(\exists z)(\forall u)(u \in z \Leftrightarrow u = x \vee u = y)$, $(\exists x)(\forall y)(y \notin x)$.

Na osnovu njih zaključujemo da je NBG račun sa jednakošću. Poslednje dve navedene teoreme opravdaju uvodjenje jedne nove konstante, u oznaci $\emptyset$ , i novog operacijskog slova za skupovne promenljive , u oznaci .

Definicija 6.

$z = \{x, y\}$ je zamena za $(\forall u)(u \in z \Leftrightarrow u = x \vee u = y)$, gde je u prva medju promenljivim niza $x_1, x_2, \ldots, x_n, \ldots$ koja se razlikuje od x, y i z.

Definicija 7.

$x_1 = \emptyset$ je zamena za $(\forall x_2)(x_2 \notin x_1)$.

Definicija 8.

$(x,y)$ je zamena za $\{\{x\}, \{x,y\}\}$.

$(x,y)$ zovemo uredjen par redom za x i y. Mogli smo staviti $(x,y) \overset{def}{=} \{\{x\}, \{x,y\}\}$.

Inače, $\{x\}$ je zamena za $\{x,x\}$.

Uredjenu trojku $(x,y,z)$ definišemo kao zamenu za $((x,y),z)$. Slično, rekurzivno definišemo $(u_1, u_2, \ldots, u_n)$.

Navodimo niz tzv. aksioma o egzistenciji klasa, u kojima se govori o egzistenciji klasa i skupova čiji elementi zadovoljavaju neke uslove.

Aksioma B 1. $(\exists X_1)(\forall x_2)(\forall x_3)((x_2, x_3) \in X_1 \Leftrightarrow x_2 \in x_3)$.

Aksioma B 2. $(\forall X_1)(\forall X_2)(\exists X_3)(\forall x_4)(x_4 \in X_3 \Leftrightarrow x_4 \in X_1 \wedge x_4 \in X_2)$.

Aksioma B 3. $(\forall X_1)(\exists X_2)(\forall x_3)(x_3 \in X_2 \Leftrightarrow x_3 \notin X_1)$.

Aksioma B 4. $(\forall X_1)(\exists X_2)(\forall x_4)(x_4 \in X_2 \Leftrightarrow (\exists x_3)((x_4, x_3) \in X_1))$.

Aksioma B 5. $(\forall X_1)(\exists X_2)(\forall x_3)(\forall x_4)((x_3, x_4) \in X_2 \Leftrightarrow x_3 \in X_1)$.

Aksioma B 6.

$(\forall X_1)(\exists X_2)(\forall x_3)(\forall x_4)(\forall x_5)((x_3, x_4, x_5) \in X_2 \Leftrightarrow (x_4, x_5, x_3) \in X_1)$.

Aksioma B 7.

$(\forall X_1)(\exists X_2)(\forall x_3)(\forall x_4)(\forall x_5)((x_3, x_4, x_5) \in X_2 \Leftrightarrow (x_3, x_5, x_4) \in X_1)$.

Koristeći aksiomu T mogu se iz Aksioma $B_2, B_3, B_4$ dobiti teoreme, koje se razlikuju od tih aksioma jedino u tome što u njima stoji $(\exists X_2)$, $(\exists X_3)$ umesto $(\exists X_2)$, $(\exists X_3)$. To opravdava uvodjenje novih operacijskih slova u oznaci
redom : presek, komplement, domen.

Definicija 9.

$Z = X \cap Y$ je zamena za $(\forall u)(u \in Z \Leftrightarrow u \in X \wedge u \in Y)$.

$Z = \bar{X}$ je zamena za $(\forall u)(u \in Z \Leftrightarrow u \notin X)$.

$Z = \mathcal{D}(X)$ je zamena za $(\forall u)(u \in Z \Leftrightarrow (\exists v)((u,v) \in X))$,

gde je $\underline{u}$ prva medju promenljivim $x_1, x_2, \ldots x_n, \ldots$ čiji se indeks razlikuje od indeksa : u prvom slučaju od X, Y, Z, u drugom slučaju od X i Z, u trećem slučaju od X, Z, v.

Definicija 10.

X U Y je zamena za $\overline{(\bar{X} \cap \bar{Y})}$.

V je zamena za $\bar{\emptyset}$.

X - Y je zamena za $X \cap \bar{Y}$ .

Navodimo neke teoreme koje se izvode pomoću izloženih aksioma.

$\{x,y\} = \{z,u\} \Leftrightarrow (x = z \wedge y = u) \vee (x = u \wedge y = z)$,

$(x,y) = (z,u) \Leftrightarrow (x = z \wedge y = u)$,

$(\forall u)(u \in X \cup Y \Leftrightarrow u \in X \vee u \in Y)$,

$(\forall u)(u \in V)$, $X \cap X = X$, $X \cup X = X$, $X \cap Y = Y \cap X$, $X \cup Y = Y \cup X$,

$X \cap \emptyset = \emptyset$, $X \cap V = X$, $X \cup \emptyset = X$, $X \cup V = V$,

$(X \cap Y) \cap Z = X \cap (Y \cap Z)$, $(X \cup Y) \cup Z = X \cup (Y \cup Z)$,

$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$, $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$,

$\overline{X \cup Y} = \bar{X} \cap \bar{Y}$, $\overline{X \cap Y} = \bar{X} \cup \bar{Y}$, $X - X = \emptyset$, $\bar{\bar{X}} = X$,

$V - X = \bar{X}$, $\bar{V} = \emptyset$,

$(\forall X)(\exists Y)(\forall u)(\forall v)((u,v) \in Y \Leftrightarrow (v,u) \in X)$

Aksioma U (Aksioma egzistencije sume skupa)

$$(\forall x_1)(\exists x_2)(\forall x_3)(x_3 \in x_2 \Leftrightarrow (\exists x_4)(x_3 \in x_4 \wedge x_4 \in x_1)).$$

Može se dokazati da važi teorema dobijena iz te aksiome na taj način što se $(\exists x_2)$ zameni sa $(\exists_1 x_2)$. Na osnovu toga možemo uvesti tzv. SUMU skupa x, u oznaci U(x) ili $\bigcup_{v \in x} v$ na sledeći način :

$$u \in U(x) \Leftrightarrow (\exists v)(u \in v \wedge v \in x).$$

Aksioma S (Aksioma o podskupovima)

$$(\forall x_1)(\forall X_2)(\exists x_3)(\forall x_4)(x_4 \in x_3 \Leftrightarrow x_4 \in x_1 \wedge x_4 \in X_2).$$

Za bilo koji skup $x_1$ i klasu $X_2$ postoji skup $x_3$, čiji su elementi zajednički elementi skupa $x_1$ i klase $X_2$, tj. presek skupa i klase je skup.

Aksioma W (Aksioma o partitivnom skupu)

$$(\forall x_1)(\exists x_2)(\forall x_3)(x_3 \in x_2 \Leftrightarrow x_3 \subseteq x_1).$$

Teorema je i ona formula koja se dobija iz aksiome W kada se $(\exists x_2)$ zameni sa $(\exists_1 x_2)$. Tako, možemo uvesti novo operacisko slovo, dužine 1, u oznaci $\mathcal{P}(x)$ na sledeći način :

$$y \in \mathcal{P}(x) \Leftrightarrow y \subseteq x.$$

U tom slučaju su, na primer, teoreme sledeće formule :

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

$= \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}\}\}$.

Definicija 11.

$Un(X_i)$ je zamena za

$$(\forall x_{i+1})(\forall x_{i+2})(\forall x_{i+3})((x_{i+1},x_{i+2}) \in X_i \wedge (x_{i+1},x_{i+3}) \in X_i \Rightarrow x_{i+2} = x_{i+3})$$

$(i = 1,2,3,\ldots)$.

$Un(X_i)$ čitamo : klasa X je **jednoznačna.**

Aksioma R (Aksioma zamene)

$$(\forall x_1)(Un(X_5) \Rightarrow (\exists x_2)(\forall x_3)(x_3 \in x_2 \Leftrightarrow (\exists x_4)((x_4,x_3) \in X_5 \wedge x_4 \in x_1))).$$

Dakle, ako je X jednoznačna klasa, tada klasa svih drugih komponenti uredjenih parova koji su elementi te klase jeste skup ako je i klasa prvih komponenti neki skup.

Aksioma I (Aksioma beskonačnosti)

$$(\exists x_2)(\emptyset \in x_2 \wedge (\forall x_1)(x_1 \in x_2 \Rightarrow x_1 \cup \{x_1\} \in x_2)).$$

Dakle postoji skup $x_2$ koji ima element $\emptyset$ i sa svakim elementom $x_1$ sadrži i element $x_1 \cup \{x_1\}$.

Tako su aksiome računa NBG potpuno navedene. Aksiome su T, P, N, S, U, W, R, I, B1 - B7 .

Inače, aksiome N i S mogu se izvesti iz ostalih aksioma.

Aksiomatska teorija skupova ZSF (Zermelo-Skolem-Fraenkel) u stvari je podteorija teorije NBG, i to onaj deo koji se odnosi na skupove.

Promenljive su $x_1,x_2,x_3,\ldots$, a jedino relacijsko slovo je $\in$ Aksiome su : T, P, N, U, W, I i jedna shema — aksioma koja odgovara aksiomi R.

Ako je $F(x,y)$ bilo koja formula, onda je aksioma formula $P \Rightarrow Q$, gde su P i Q redom sledeće formule :

$$(\forall x_1)(\forall x_2)(\forall x_3)(F(x_1,x_3) \wedge F(x_1,x_2) \Rightarrow x_3 = x_2),$$

$$(\exists x_5)(\forall x_3)(x_3 \in x_5 \Leftrightarrow (\exists x_1)(x_1 \in x_4 \wedge F(x_1,x_3))).$$

Svaka formula računa ZSF može se smatrati i kao formula računa NBG. Dokazano je da je ZSF neprotivurečan račun ako i samo ako je NBG neprotivurečan.

Aksiomu izbora nismo uključili ni u jedan od tih računa. Za zasnivanje teorije skupova usvaja se i ta aksioma.

Ta aksioma glasi $P \Rightarrow Q$ gde su P i Q redom sledeće formule :

$$(\forall x_1)(x_1 \in x_2 \Rightarrow x_1 \neq \emptyset \wedge (\forall x_3)(x_3 \in x_2 \wedge x_3 \neq x_1 \Rightarrow x_3 \cap x_1 = \emptyset)),$$

$$(\exists x_4)(\forall x_1)(x_1 \in x_4 \Rightarrow (\exists x_5)(x_5 \in x_1 \cap x_4)).$$

Dakle, ako je $x_2$ skup medjusobno disjunktnih nepraznih skupova, onda postoji skup $x_4$ koji sadrži tačno po jedan element tih nepraznih skupova.

U teoriji skupova je dugo bio nerešen tzv. PROBLEM KONTINUUMA. Da bi se on prikazao, potrebno je uvesti izvesne definicije, na primer "skup x je beskonačan", "skup x je ekvivalentan sa skupom y". Zadovoljavamo se da običnim rečima opišemo drugu definiciju :

Kažemo de je skup x ekvivalentan sa skupom y ako postoji bar jedno 1-1 preslikavanje skupa x na skup y.

Pitanje je da li je tačan sledeći iskaz :
"Ako je x beskonačan skup i $\mathcal{P}(x)$ njegov partitivan skup, onda ne postoji skup y koji ima sledeće svojstvo : skup x je ekvivalentan sa nekim podskupom skupa y, skup y je ekvivalentan sa nekim podskupom skupa $\mathcal{P}(x)$ i pri tome skup y nije ekvivalentan ni sa skupom x ni sa skupom $\mathcal{P}(x)$".

Odgovor na taj problem (uopšteni problem kontinuuma) dao je P.Cohen, 1964.g.(The independence of the continuum hypothesis ; Proc.Nat.Acad.Sci.USA,I - 1963, 50, 1143 - 1148 ; II - 1964, 51, 105 - 110).

Označimo sa C formulu koja na formulskom jeziku predikatskog računa odgovara iskazu pod znacima " " u navedenom pitanju. P.Cohen dokazao je da ni C ni $\neg$C nisu teoreme ZSF sistema (u koji je uključena aksioma izbora), odnosno nezavisnost hipoteze kontinuuma od ostalih aksioma sistema ZSF (u koji je uključena aksioma izbora).

Prema tome, možemo proučavati aksiomatske teorije skupova koje imaju aksiomu C, kao i one koje imaju aksiomu $\neg$C.

Primedba. Na kraju ove tačke napominjemo da u daljem tekstu za simbolizovanje matematičkih misli češće upotrebljavamo običan jezik nego navedeni formulski jezik.

Naravno moguće je prevodjenje skoro čitavog matematičkog teksta (sem minimalne metateorije) na taj formulski jezik.

## PRESLIKAVANJ

Obisno rečeno, preslikavanje skupa A u skup B, je svaki postupak dogovor, pravilo koji se svakom elementu x skupa A dodeljuje tačno po jedan element y skupa B. Uopšte svako preslikavanje se može jednoznačno odrediti pomoću skupa uredjenih parova (x,y), gde je $x \in A$ a y odgovarajući element skupa B.
Prethodno definišemo uredjen par.

Definicija 1.

Uredjen par redom elementa x i y, u oznaci (x,y), jeste sledeći skup $\{\{x\},\{x,y\}\}$. U uredjenom paru (x,y) element x zovemo prva komponenta a y - druga komponenta. Mogučnost ovakvog definisanja uredjenog para otkriva sledeće svojstvo koje ima $\{\{x\},\{x,y\}\}$.

$$\{\{x\},\{x,y\}\} = \{\{z\},\{z,u\}\} \iff (x = z,\ y = u)$$

što se inače neposredno dokazuje.
Uredjenu trojku redom elemenata x,y,z definišemo kao ((x,y),z), odnosno, uopšte uredjenu n - torku redom elemenata $x_1,x_2,\ldots,x_n$, je $((x_1,x_2,\ldots,x_{n-1}),x_n)$ $(n \geq 3)$.
Da bismo pojam preslikavanja definisali uvodimo još neke pojmove.

Definicija 2.

Direktan proizvod redom skupova A i B u oznaci $A \times B$, jeste skup svih uredjenih paraova (a,b) gde je $a \in A$, $b \in B$. Ako je A = B, onda umesto AxB pišemo i $A^2$.
Na sličan način uvodimo i direktan proiuvod redom skupova $A_1,A_2,\ldots,A_n$ u oznaci $A_1 \times A_2 \times \ldots \times A_n$ kao skup svih uredjenih n torki $(a_1,a_2,\ldots,a_n)$ gde je $a_i \in A$ $(i = 1,2,\ldots,n)$.

Definicija 3.

Preslikavanje skupa A u skup B u oznaci $f : A \to B$ jeste podskup f skupa $A \times B$ koji ima sledeća svojstva :
1) Skup svih prvih komponenti elemenata skupa f, tzv. domen za f, u oznaci D(f), jeste skup A.
2) Ako $(x,y) \in f$, $(x,z) \in f$ onda je y = z.

Definicija 4.

Kažemo da je f preslikavanje
1) Postoje skupovi A i B i
2) $f : A \to B$.
Ako je $f : A \to B$ i ako je $(x,y) \in f$, onda x zovemo original a y slika tog originala. u oznaci y = f(x).
Sem uvedenih oznaka uobičajne su i sledeće :

$$y = xf,\quad f = \{(a_1,b_1),(a_2,b_2),\ldots,(a_n,b_n)\},\quad f = \begin{pmatrix} x \\ xf \end{pmatrix}_{x \in A}$$

$$f = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix}$$

Primeri :

1) $f = \{(1,8),(2,9)\}$ nije preslikavanje skupa $A = \{1,2,3,4\}$ u skup $B = \{8,9,10\}$ jer nije ispunjen uslov 1.

2) Ako su A i B skupovi iz prethodnog primera onda (1,8),(2,9), (3,8),(4,10),(3,10) nije preslikavanje A u B jer nije ispunjen uslov 2.

3) Neka je A = B = R skup svih realnih brojeva. Onda su : $\{(x,x^2),/\ x\in R\}$ , $\{(x,\sin x)\ /\ x\in R\}$ primeri preslikavanja R u R.

Definicija 5.

Preslikavanje $f : A \to B$ je 1-1 preslikavanje ako je ispunjen uslov $f(x_1) = f(x_2) \longrightarrow x_1 = x_2$ za sve elemente $x_1$, x skupa A.

Na primer, preslikavanje $f : R \to R$ definisano na sledeći način $f = \{(x, |x|)\ /x\in R\}$ nije 1-1 preslikavanje jer je $|x| = |-x|$ dok je $x \neq -x$ za sve realne brojeve, dok $f = \{(x,\operatorname{tg}x)\ /\ x \in [-\pi/2, \pi/2]\}$ jeste preslikavanje 1-1 skupa $[-\pi/2, \pi/2]$ u skup R svih realnih brojeva.

Definicija 6.

Preslikavanje $f : A \to B$ je preslikavanje A na skup B ako je svaki element skupa B slika bar jednog elementa skupa A.

Preslikavanje $f = \{(x,e^x)\ /x\in R\}$ nije preslikavanje skupa R na skup R jer naprimer -2 nema svoj original.

Definicija 7.

Preslikavanje $f : A \to A$ je permutacija skupa A ako je f 1-1 preslikavanje skupa A na skup A. Ako f još ispunjava uslov $f(x) = x$ za svaki element x skupa A onda f zovemo identičko preslikavanje skupa A.

Definicija 8.

Preslikavanje $f : A \to B$ je konstantno preslikavanje skupa A u skup B ako za sve elemente skupa A ispunjava uslov : $f(x) = b$ gde je b neki fiksirani element iz B.

Primeri preslikavanja.

1) Niz skupa A je preslikavanje $f : N \to A$ skupa prirodnih brojeva u skup A. Ako je $n\in N$ onda f(n) označavamo sa $x_n$ i zovemo n-ti član niza f.

2) Reč dužine n skupa A je preslikavanje skupa $\{1,2,\ldots,n\}$ u A. Obično A zovemo alfabet.

reč $f = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$ označavamo i $a_1 a_2 \ldots a_n$.

Primeri.

a) $f = \begin{pmatrix} 1 & 2 & 3 \\ x & = & 1 \end{pmatrix}$ ili u drugoj oznaci $x = 1$ je reč dužine tri čija su slova simboli : x, = , 1.

b) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ ( & 2 & + & x & ) \end{pmatrix}$ ili (2+x) je reč dužine pet.

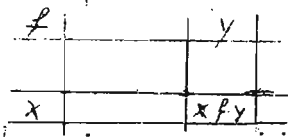
Direktan proizvod familije skupova $F = \{A_i / i \in I\}$ je skup u oznaci $\prod_{i\in I} A_i$, svih preslikavanja $f : I \to A$, gde je $A = \bigcup_{i\in I} A_i$, takvih da je $f(i) \in A_i$ za svaki $i \in I$.
Na primer ako je $I = \{1,2,\ldots,n\}$ onda je $f \in \prod_{i=1}^{n} A_i \leftrightarrow f = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$
tj. $f = a_1a_2\ldots a_n$ je reč dužine n koja ispunjava uslov $a_i \in A_i$ $i \in I$.
Ranije smo definisali $\prod_{i=1}^{n} A_i$ pomoću uredjenih n-torki. Mogli smo da usvojimo i prethodno uvedenu definiciju.

Definicija 9.
Operacija dužine n skupa A je preslikavanje skupa $A^n$ u skup A.

primeri.
1) $\{(x,x^2) / x\in R\}$, $\{(x,e^x) / x\in R\}$ jesu operacije dužine 1 skupa realnih brojeva. Ove operacije smo mogli opisati i pomoću jednakosti : $y = x$, $y = e^x$ kao što se inače često čini.
2) Neka je $A = \{1,2,3\}$ i neka je $*$ sledeći skup :
$$* = \{((1,1),2),((1,2),3),((1,3),3),((2,1),1),((2,2),2),((2,3),1),((3,1),3),((3,2),2),((3,3),1)\}.$$
Ovaj skup je preslikavanje skupa $A^2$ u skup A, odnosno $*$ je operacija dužine 2 (binarna) skupa A. U slučaju binarne operacije bilo kog skupa A uobičajeno je da se umesto $f(x_1,x_2) = y$ (original $(x_1,x_2)$, slika y, $x_1,x_2 \in A$) piše $x_1 f x_2 = y$. U ovom primeru imamo prema tome $1*1 = 2$, $1*2 = 3$, $1*3 = 3$, $2*1 = 1$, $2*2 = 2$, $2*3 = 1$, $3*1 = 3$, $3*2 = 2$, $3*3 = 1$, što se još preglednije prikazuje pomoću tzv. Cayley-eve tablice te operacije :

| $*$ | 1 | 2 | 3 |
|---|---|---|---|
| 1 | 2 | 3 | 3 |
| 2 | 1 | 2 | 1 |
| 3 | 3 | 2 | 1 |

Slično se ma kojoj binarnoj operaciji na nekom konačnom skupu, dodeljuje izvesna Cayley-eva tablica čiji karakterističan detalj navodimo :




3) Skup $\{((x_1,x_2,x_3), x_1^2 - x_2 + x_3 / x_1,x_2,x_3 \in R\}$ je operacija dužine tri skupa R realnih brojeva. Možemo reći da nju odredjuje obrazac $y = x_1^2 - x_2 + x_3$.

Proizvod preslikavanja.
Neka je f preslikavanje skupa A u skup B a g preslikavanje skupa B u skup C, u oznaci $f : A \to B$, $g : B \to C$.
Proizvod preslikavanja f sa preslikavanjem g je preslikavanje skupa A u skup C odredjeno na sledeći način :
original x - slika (xf)g. Inače ovako definisano preslikavanje označavamo fg (zovemo ga i desni proizvod) i pišemo $x(fg) = (xf)g$.
Primeri :
1) $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 3 \end{pmatrix}$ $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ $fg = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 4 & 4 \end{pmatrix}$

2) $f = \begin{pmatrix} x \\ \sin x \end{pmatrix}$ $x \in R$ $\quad g = \begin{pmatrix} x \\ \cos x \end{pmatrix}$ $x \in R$ $\quad fg = \begin{pmatrix} x \\ \cos(\sin x) \end{pmatrix}$ $x \in R$

3) $f = \begin{pmatrix} x \\ 1/x \end{pmatrix}$ $x \in R \setminus \{0\}$ $\quad g = \begin{pmatrix} x \\ x-1 \end{pmatrix}$ $x \in R$ $\quad fg = \begin{Bmatrix} x \\ 1/x-1 \end{Bmatrix}$ $x \in R \setminus \{0\}$

Levi proizvod preslikavanja g sa preslikavanjem f je po definiciji desni proizvod f sa g. Označavamo ga sa gof.
Dakle gof = fg.
U slučaju levog proizvoda piše se : (gof)(x) = g(f(x)).
Levi proizvod ima sledeća svojstva :
1) ho(gof) = (hog)of
2) Neka $f : A \to B$ , $g : B \to C$ i h = gof.
Tada važi :
a) Ako je h preslikavanje skupa A na skup C tada je g preslikavanje skupa B na skup C.
b) Ako je h 1-1 preslikavanje skupa A u skup C tada je f 1-1 preslikavanje skupa A u skup B.
3) $f : A \to B$ je "1-1" i "na" preslikavanje skupa A u skup B postoje preslikavanja $g : B \to A$ i $h: B \to A$ takva da su proizvodi gof i foh identička preslikavanja redom skupa A i B.

Inverzne grane preslikavanja i inverzne funkcije.

Definicija 10.
Neka je S neprazan skup i $f : \overset{*}{P}(S) \to S$ gde je $\overset{*}{P}(S)$ skup svih nepraznih podskupova skupa S. Tada f zovemo funkcija izbora ako ispunjava uslov : $A \in \overset{*}{P}(S) \longrightarrow Af \in A$ $\quad (*)$
Primeri.
1) $S = \{1,2,3\}$ $\quad f = \begin{pmatrix} \{1\} & \{2\} & \{3\} & \{1,2\} & \{1,3\} & \{2,3\} & \{1,2,3\} \\ 1 & 2 & 3 & 1 & 3 & 2 & 3 \end{pmatrix}$
je jedna funkcija izbora.
Medjutim, i preslikavanje f definisano na sledeći način

$$f = \begin{pmatrix} \{1\} & \{2\} & \{3\} & \{1,2\} & \{1,2\} & \{2,3\} & \{1,2,3\} \\ 1 & 2 & 3 & 2 & 1 & 3 & 3 \end{pmatrix}$$

ispunjava uslov (*) pa je i f funkcija izbora. Jasno je da u ovom slučaju to nisu jedine mogućnosti.
2) Ako je N skup svih prirodnih brojeva, N je dobro uredjen u odnosu na relaciju $\leq$, pa ta osobina omogućava sledeću definiciju funkcije izbora f : $M \in \overset{*}{P}(N)$ : $Mf = \min M$ .
Postavlja se pitanje dali svaki neprazan skup ima funkciju izbora. Za prebrojive skupove odgovor je potvrdan, jer se jedna takva funkcija uvek može definisati kao u primeru 2). Medjutim kod realnih brojeva ne znamo algoritam za konstrukciju funkcije izbora f.. U teoriji skupova se u mnogim teoremama koristi

pretpostavka o eksistenciji funkcije izbora proizvolnog skupa S, odnosno koristi aksioma izbora :
Za svaki neprazan skup S postoji funkcija izbora f.
Ili u drugoj formulaciji :
Ako je A skup medjusobno disjunktnih nepraznih skupova, onda postoji skup B koji sadrži po tačno jedan element tih nepraznih skupova.
Korišćenjem te aksiome u matematici često dokazujemo egzistenciju izvesnih objekata ali pri tom ne znamo dali postoji algoritam za njihovu konstrukciju.
Ona je ekvivalentna sa Zornovom lemom, Haussdorfovom teoremom i još nekim iskazima o čemu će biti reči kasnije.
Neka je $f : A \to B$ . U skupu A definišemo relaciju $\sim$ na sledeći način : $x,y \in A$, $x \sim y \overset{def}{\Leftrightarrow} xf = yf$ . Neposredno se dokazuje da je $\sim$ relacija ekvivalencije skupa A, pa njoj, na osnovu osobine proizvoljne relacije ekvivalencije, odgovara razbijanje skupa A na neprazne disjunktne podskupove (klase ekvivalencije). Znači da preslikavanjem f svi elementi iz klase Cx imaju istu sliku, u oznaci xf.

Definicija 11.

Inverzna grana preslikavanja $f : A \to B$ je preslikavanje $g : Af \to A$ koje ima sledeća svojstvo : $(xg)f = x$ $(x \in Af)$

Tvrdjenje. Svako preslikavanje ima bar jednu inverznu granu.
Ovo sledi iz aksiome izbora.

Primeri.

1) Ako je $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & a & c & b \end{pmatrix}$ inverzne grane su : $g = \begin{pmatrix} a & b & c \\ 1 & 2 & 4 \end{pmatrix}$

$g = \begin{pmatrix} a & b & c \\ 1 & 5 & 4 \end{pmatrix}$ $g = \begin{pmatrix} a & b & c \\ 3 & 2 & 4 \end{pmatrix}$ $g = \begin{pmatrix} a & b & c \\ 3 & 5 & 4 \end{pmatrix}$

2) Ako je f preslikavanje definisano na sledeći način : $f = \begin{pmatrix} x \\ x^2 \end{pmatrix}_{x \in R}$
jedna inverzna grana je : $g = \begin{cases} -\sqrt{x}, & 0 \leq x \leq 1 \\ +\sqrt{x}, & 1 < x < \infty \end{cases}$
Sve inverzne grane definisane su sledećom formulom: $g = \begin{pmatrix} x \\ \alpha(x)(+\sqrt{x}) \end{pmatrix}_{x \in R^+}$
gde je $\alpha(x) \in \{1,-1\}$ , odnosno $\alpha : R^+ \setminus \{0\} \to \{-1,1\}$ bilo koje preslikavanje.

3) $f = \begin{pmatrix} x \\ \sin x \end{pmatrix}$ jedna grana tog preslikavanja je $g = \begin{pmatrix} x \\ \arccos x \end{pmatrix}$
koje zadovoljava uslov $\arcsin a = y \Leftrightarrow \sin y = a$ i $-\frac{\pi}{2} \leq y \leq \frac{\pi}{2}$

Ako je $f : A \to B$ 1-1 preslikavanje skupa A u skupB onda su klase ekvivalencije u odnosu na napred definisanu relaciju $\sim$ , jednočlane , pa postoji samo jedna inverzna grana preslikavanja f, koju u tom slučaju zovemo inverzna funkcija (preslikavanje) i označavamo $f^{-1}$ . Dakle inverzna funkcija je definisana samo za 1-1 preslikavanja.

Zadaci.

1) Ako je $A \subseteq X$ i $B \subseteq Y$ dokazati da je :
   a) $A \times B \subset X \times Y$
   b) $(X \times Y) \setminus (A \times B) = [(X \setminus A) \times Y] \cup [X \times (Y \setminus B)]$

2) Ako je $A \subset X$, $B \subset Y$, $C \subset X$, $D \subset Y$, dokazati da važi :
   a) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$
   b) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$
   Naći kontraprimer u kome nevaži jednakšot u b).

3) Ako $f : X \to Y$ i $A \subset X$ i $B \subset X$ onda važi :
   a) $f(A \cup B) = f(A) \cup f(B)$
   b) $f(A \cap B) \subseteq f(A) \cap f(B)$
   U slučaju b) ne važi obrnuta inkluzija što se vidi iz sledečeg primera : $X = \{a, b\}$ , $Y = \{y\}$ , $A = \{a\}$ , $B = \{b\}$ i $f : X \to Y$ definisano pomoću , $f = \begin{pmatrix} a & b \\ y & y \end{pmatrix}$ tada je $f(A \cap B) = f(\emptyset) = \emptyset$
   $f(A) \cap f(B) = Y$

4) Neka je $f : X \to Y$ i $A, B \subset Y$ . Označimo sa $f^{-1}(A)$ sledeči skup : $\{x \in X \ / \ f(x) \in A\}$ (f nije ovde oznaka za inverznu funkciju, jer nigde nije pretpostavljeno da je f 1-1 preslikavanje).
   Dokazati da važi :
   a) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$
   b) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$
   c) $f^{-1}(A \setminus B) = f^{-1}(A) \setminus f^{-1}(B)$.

5) $f: X \to Y$, $g: Y \to Z$ , $A \subset X$ i $C \subset Y$ tada važi :
   a) $(g \circ f)(A) = g(f(A))$
   b) $(g \circ f)^{-1}(C) = f^{-1}(g^{-1}(C))$

6) $f: X \to Y$ , $A \subset X$ , $B \subset Y$ . Dokazati :
   a) $f^{-1}(f(A)) \supset A$
   b) $f(f^{-1}(B)) \subset B$
   c) $f(X \setminus A) \supset f(X) \setminus f(A)$
   d) $f^{-1}(Y \setminus B) = X \setminus f^{-1}(B)$
   e) $f(A \cap f^{-1}B) = f(A) \cap B$ gde su $f(A)$ i $f^{-1}(B)$ oznake za skupove $f(A) = \{xf \ / \ x \in A\}$ , $f^{-1}(B) = \{x \in X \ / \ f(x) \in B\}$ .

7) Ako je X dati skup a $A \subset X$, preslikavanje $\chi_A$ $X \to R$ (R skup realnih brojeva) definisano pomoću : $\chi_A(x) = \begin{cases} 1 & \text{za } x \in A \\ 0 & \text{za } x \in X \setminus A \end{cases}$ zovemo karakteristična funkcija skupa A.
   Dokazati da važi :
   a) $\chi_{A \cap B}(x) = \chi_A(x) \chi_B(x)$
   b) $\chi_{A \cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_A(x) \chi_B(x)$
   c) $\chi_{A \setminus B}(x) = \chi_A(x)(1 - \chi_B(x))$ .

# RELACIJE

1). Ako za svaki elemant x iz skupa M postoji samo jedna od mogućnosti : a) x jeste u relaciji $\rho$
b) x nije u relaciji $\rho$
tada ćemo kazati da je u skupu M definisana relacija $\rho$ dužine 1.

Primer.1
U skupu prirodnih brojeva N, svaki od brojeva 3,6,9,12,...,3n,.. jeste u relaciji $\rho$ , koja u ovom slučaju označava svojstvo : "biti deljiv sa 3", dok ostali prirodni brojevi nisu u relaciji.

Primer. 2
U skupu prirodnih brojeva N interpretirajmo relaciju $\rho$ dužine 1 kao :" biti prost broj". Tada je svaki od brojeva 2,3,5,7,11,... itd. u relaciji $\rho$ , dok recimo, nijedan od brojeva 1,4,6,8,10,.. nije u relaciji $\rho$ .
Analogno u nepraznom skupu M definišemo relaciju $\rho$ dužine 2 ako svaki uredjen par (x,y) iz MxM=M postoji samo jedna od mogućnosti:
a) x,y tim redom jesu u relaciji $\rho$
b) x,y tim redom nisu u relaciji $\rho$

Primer. 3
Neka je M skup svih pravih u Euklidskom prostoru R i neka relacija $\rho$ dužine 2 u M bude :"prave su ortogonalne".

Primer.4
U skupu Z celih brojeva kazačemo da je par (x,y) u relaciji $\rho$ ako i samo ako je x - y = ck gde je k iz Z i c fiksiran ceo broj. (ova relacija se zove kongruencija po modulu c. Umesto x$\rho$y pišemo i $x \equiv y \pmod c$.

Primer. 5
U skupu R realnih brojeva možemo da definišemo na sledeći način relaciju $\rho$ : x,y tim redom jesu u relaciji $\rho$ ako i samo ako $x \leqslant y$ . Tako su sledeći parovi u relaciji $\rho$: (2,5),(3,3),(4/7,1),.. dok parovi (5,2),(-2,-7/3),.. nisu u relaciji $\rho$ .
Relaciju dužine 2 obično nazivamo binarna relacija.
Za primere 1 i 2 karakteristično je dali neki element "jeste u relaciji $\rho$" ili "nije u relaciji $\rho$". Analogno smo u primerima 3,4,5, posmatrali dali parovi "jesu u relaciji $\rho$" ili "nisu u relaciji $\rho$".
Analognim postupkom možemo uopštiti pojam relacije definisane u nekom skupu i tako dolazimo do opšte definicije relacije.

2). Definicija 1.
Relacija $\rho$ dužine n skupa M je svako preslikavanje skupa $M^n$ u skup $\{T, \perp\}$ .

Neka je $\rho : M^n \longrightarrow \{T, \perp\}$
Ako je : $\rho(x_1, x_2, \ldots, x_n) = T$ onda kažemo : $x_1, x_2, \ldots, x_n$ tim redom jesu u relaciji $\rho$, a ako je $\rho(x_1, x_2, \ldots, x_n) = \perp$ onda kažemo : $x_1, x_2, \ldots, x_n$ tim redom nisu u relaciji $\rho$ .
Za n =1 kažemo samo "x jeste u relaciji $\rho$" ili "x nije u relaciji $\rho$ ".
Ako je n = 2 obično kažemo $x_1$ je u relaciji $\rho$ sa $x_2$ i pišemo $x_1 \rho x_2$
Relacija dužine nula proisvolnom skupu M su simboli $T, \perp$ .
Napomena. Intuitivno opisana relacija je karakterisana (odredjena) poznavanjem skupa svih x koji jesu u relaciji. To pruža mogučnost da se uvede sledeča definicija relacije.
Relaciju $\rho$ dužine n u skupu M možemo definisati i kao neki podskup skupa $M^n$, tj. $\rho \subseteq M^n$.
U primeru 1 elemanti iz podskupa 3,6,9,..,3n,.. jesu u relaciji $\rho$, dok elemanti koji nisu u tom podskupu nisu u relaciji $\rho$ .
Ako tako uvedemo relaciju $\rho$, onda proučavanje relacija u nekom skupu ne odvajamo od proučavanja podskupova toga skupa. Specijalno možemo govoriti o uključivanju relacije $\rho_1$ u $\rho_2$, $\rho_1 \subseteq \rho_2$, zatim o preseku, uniji relacija itd.
Neka je $\rho$ binarna relacija definisana u mnoštvu M. Onda je:
a) refleksivna, ako je za svako $x \in M$, $x \rho x$
b) tranzitivna, ako iz $x \rho y$ i $y \rho z$ sledi $x \rho z$
c) simetrična , ako iz $x \rho y$ sledi $y \rho x$
d) anti-simetrična, ako iz $x \rho y$ i $y \rho x$ sledi $x = y$
3). U ovom delu obradjujemo one binarne relacije koje poseduju neke od prethodno navedenih osobina.
Definicija 2.
Binarna relacija skupa M u oznaci $\sim$ jeste relacija ekvivalencije ako je : refleksivna, simetrična i tranzitivna.
U primeru 4 je definisana jedna relacija ekvivalencije.
U skupu M u kome je definisana relacija ekvivalencije $\sim$ uvodimo i pojam klase ekvivalencije elementa x. To je skup , u oznaci Cx , svih elementa $y \in M$, skupa M, takvih da je $x \sim y$ .
Stav 1.
Ako su x i y proizvolni elementi skupa M, onda $x \sim y \Leftrightarrow Cx = Cy$
dokaz: Zaista, ako je $x \sim y$, tada za proizvolno $z \in Cx$ , po definiciji klase Cx , sledi da je $z \sim x$, zbog osobine 3 , iz $z \sim x$ i $x \sim y$ sledi $z \sim y$, pa je zbog 2 i definicije Cy , $z \in Cy$. Analogno se dokazuje ako $z \in Cy$ , tada $z \in Cx$, pa je na osnovu definicije jednakosti skupova Cx = Cy
Obrnuto, ako je Cx = Cy , tada $y \in Cy$ prema osobini 1, pa $y \in Cx$, tj. $x \sim y$.

Stav 2.

Klase ekvivalencije Cx i Cy skupa M u odnosu na relaciju ekvivalencije $\sim$ ili se poklapaju ili su disjunktne.

dokaz: Ako su klase Cx i Cy bez zajedničkih elemenata stav je dokazan. Ako nije tako onda neka je z njihov zajednički element tj. $z \in Cx$ i $z \in y$, pa je po definiciji klase ekvivalencije $x \sim z$ i $y \sim z$. Odatle zbog 2 i 3 sledi da je $x \sim y$. Prema stavu 1, je $Cx = Cy$. Dakle ako klase Cx i Cy imaju bar jedan zajednički element tada se one poklapaju.

Skup čiji su elementi klase ekvivalencije zove se količnik skup.

Simbolički : $M/\sim = \{ Cx \ / \ x \in M \}$

Prema definiciji 2, stavu 1,2 elementi Cx skupa $M/\sim$ poseduju sledeća svojstva :

a) Nijedan podskup Cx nije prazan.

b) Različiti podskupovi su bez zajedničkih elementa.

c) Unija svih podskupova Cx je skup M.

Zbog ovih osobina skupa $M/\sim$ kažemo da je to razbijanje skupa M

U primeru 4 klase ekvivalencije su sledeći skupovi :

$Co = \{ ck, k \in Z \}$, $Cl = \{ ck+1, k \in Z, \} \ldots$, $Ck-1 = \{ ck+(c-1), k \in Z \}$

Tako dobijamo da je $Z/\sim = \{ Co, Cl, \ldots, Ck-1 \}$.

Stav 3.

Svako razbijanje P skupa M odredjuje u skupu M izvesnu relaciju ekvivalencije $\sim$.

dokaz: Stvarno, ako za $x,y \in M$ stavimo da je $x \sim y$, tada i samo tada ako x i y pripadaju istoj klasi razbijanja P, onda u skupu M dobijamo binarnu relaciju $\sim$ za koju se neposredno dokazuje da ispunjava sve definisane zahteve relacije ekvivalencije.

Drugi veoma važan tip binarne relacije je relacija delimičnog poretka ili relacija poretka.

Definicija 3.

Binarna relacija $\rho$ skupa M je relacija poretka ako je : refleksivna, tranzitivna i antisimetrična.

Za relaciju poretka često se koristi i oznaka $\leqslant$. Ako su $x,y \in M$ i $x \leqslant y$, tada u zavisnosti od situacije , to ćemo čitati : x je manje ili jednako y, x se sadrži u y, x prethodi y. Ako je $x \leqslant y$ i $x \neq y$ pisaćemo $x < y$ , $<$ nije relacija poretka, što se neposredno proverava.

-Parcijalno uredjen sistem $(M, \leqslant)$ čija su svaka dva elementa uporediva, zovemo linearno ( potpuno ) uredjen sistem ili lanac.

- Elementi skupa M su uporedivi ako je $x \leqslant y$ ili $y \leqslant x$.
- Linearno uredjen skup ili lanac je onaj skup u kome su svaka dva elementa uporediva.

Neka je M skup i $\leq$ njegova relacija poretka. Tada $(M, \leq)$ zovemo parcijalno uredjen sistem. Ako je $(M, \leq)$ parcijalno uredjen sistem onda kažemo i : skup M je parcijalno uredjen relacijom $\leq$ .
U primeru 5 je definisana jedna relacija poretka . Tako uredjen skup R je i lanac.

Primer 6.

Skup prirodnih brojeva možemo urediti delimično ( ali ne i linearno) sledećom relacijom $\leq$ : $a \leq b$ tada i samo tada ako je b deljivo sa a bez ostatka.
Ako postoji obostrano jednoznačno prelikavanje f uredjenog skupa $(M_1, \leq_1)$ na uredjen sistem $(M_2, \leq_2)$, takvo da je za $x, y \in M_1$

$$x \leq_1 y \iff xf \leq_2 yf$$

tada kažemo da je f jedan izomorfizam izmedju $(M_1, \leq_1)$ i $(M_2, \leq_2)$, a da su skupovi izomorfni s obzirom na svoju relaciju poretka.
Kada nas , u skupovima, samo poredak interesuje , tada možemo identifikovati izomorfne skupove u odnosu na poredak.
Kažemo da se delimično uredjen sistem M izomorfno potapa u delimično uredjen sistem N ako je M izomorfan nekom podskupu N' skupa N. Pri tom je relacija delimičnog uredjenja u N' inducirana relacijom delimičnog uredjenja u N .

Stav 4.

Svaki delimično uredjen sistem M izomorfno se potapa u partitivni skup P(N) nekog skupa N koji je delimično uredjen relacijom inkluzije skupova.

dokaz: Neka je skup N baš sam M. Preslikavanje f : $M \to P(M)$ definišemo na sledeći način. Za svako a iz M neka je

$$f(a) = \{x \mid x \leq a\} = A$$

Ako je $a, b \in M$ i A, B odgovarajući podskupovi ( elementi skupa P(M)) dobijeni preslikavanjem f, tada iz činjenice da je A = B, sledi $a \leq b$ $b \leq a$ . Odatle zaključujemo da je a = b, tj. preslikavanje f je 1-1. Neka je dalje $a \leq b$ , tada zbog $x \leq a$ dobijamo da je $x \leq b$ tj. $f(a) \subseteq f(b)$. Obrnuto ako je $A \subseteq B$ tada je $a \in B$ pa prema tome kako je definisano f sledi $a \leq b$ Pošto f održava poredak, stav je u celini dokazan.

4) . Operacije sa relacijama.

Uvodimo sledeće operacije : $\vee, \wedge, \Rightarrow, \Leftrightarrow, \neg, \exists, \forall$ sa skupom relacija R definisanih u skupu M. Operacije $\wedge, \vee, \Rightarrow, \Leftrightarrow$ su binarne, dok su operacije $\forall, \exists, \neg$ unarne (tj. dužine 1 ).

Definicija 4.

Neka su $\alpha(x_1, x_2, \ldots, x_m)$ i $\beta(y_1, y_2, \ldots, y_n)$ dve relacije definisane u skupu M dužine m i n. $(m, n \geq 1)$. Tada je :

$$\alpha(x_1,x_2,\ldots,x_n)\vee\beta(y_1,y_2,\ldots,y_m)=\gamma_1(x_1,x_2,\ldots,x_n,y_1,y_2,\ldots,y_m)$$
$$\alpha(x_1,x_2,\ldots,x_n)\wedge\beta(y_1,y_2,\ldots,y_m)=\gamma_2(x_1,x_2,\ldots,x_n,y_1,y_2,\ldots,y_m)$$
(1) $$\alpha(x_1,x_2,\ldots,x_n)\Rightarrow\beta(y_1,y_2,\ldots,y_m)=\gamma_3(x_1,x_2,\ldots,x_n,y_1,y_2,\ldots,y_m)$$
$$\alpha(x_1,x_2,\ldots,x_n)\Leftrightarrow\beta(y_1,y_2,\ldots,y_m)=\gamma_4(x_1,x_2,\ldots,x_n,y_1,y_2,\ldots,y_m)$$
$$\neg\alpha(x_1,x_2,\ldots,x_n)=\gamma_5(x_1,x_2,\ldots,x_n)$$

gde su $\gamma_1$, $\gamma_2$, $\gamma_3$, $\gamma_4$, $\gamma_5$ relacije skupa M definisane jednakostima :

$$\gamma_1(x_1',x_2',\ldots,x_n',y_1',\ldots,y_m')=\alpha(x_1',x_2',\ldots,x_n')\vee\beta(y_1',\ldots,y_m')$$
$$\gamma_2(x_1',x_2',\ldots,x_n',y_1',\ldots,y_m')=\alpha(x_1',x_2',\ldots,x_n')\wedge\beta(y_1',\ldots,y_m')$$
(2) $$\gamma_3(x_1',x_2',\ldots,x_n',y_1',\ldots,y_m')=\alpha(x_1',x_2',\ldots,x_n')\Rightarrow\beta(y_1',\ldots,y_m')$$
$$\gamma_4(x_1',x_2',\ldots,x_n',y_1',\ldots,y_m')=\alpha(x_1',x_2',\ldots,x_n')\Leftrightarrow\beta(y_1',\ldots,y_m')$$
$$\gamma_5(x_1',x_2',\ldots,x_n')=\neg\alpha(x_1',x_2',\ldots,x_n')$$

pri tome su $x_i'$, $y_j'$ elementi skupa M interpretacije za $x_i$, $y_j$.
U (1) $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\neg$, jesu znaci novouvedenih operacija medju relacijam,dok su simboli navedeni u (2) znaci operacija algebre $(T,\perp)$.

Primer 7.

Neka su u skupu prirodnih brojeva N definisane relacije : $\alpha$ dužine 3 i $\beta$ dužine 2 na sledeći način :

$\alpha(x,y,z) = T \iff$ 2x+5y+z je paran broj

$\beta(x,y) = T \iff$ x+4y je potpun kvadrat.

Na osnovu toga kako smo definisali relacije $\gamma_1$, $\gamma_2$, $\gamma_3$, $\gamma_4$, $\gamma_5$, imamo da je : $\gamma_1(1,2,3)=\alpha(1,2,3)\vee\beta(1,2)=\perp\vee T=T$

$\gamma_1(1,2,3) = \alpha(1,2,3)\wedge\beta(1,2) = \perp\wedge T=\perp$

$\gamma_2(1,6,2) = \alpha(1,6,2)\wedge\beta(1,6) = T\wedge T=T$

$\gamma_3(5,1,1) = \alpha(5,1,1)\Rightarrow\beta(5,1) = T\Rightarrow T=T$

$\gamma_4(2,4,3) = \alpha(2,4,3)\Leftrightarrow\beta(2,4) = \perp\Leftrightarrow\perp=T$

$\gamma_5(3,2,2) = \neg\alpha(3,2,2) = \neg T=\perp$

Ako je : $\gamma(x,y,z)=(\alpha(x,z,z)\wedge\alpha(y,y,y))\Rightarrow(\beta(x,y)\vee\alpha(x,y,y))$
tada je na primer:

$$\gamma(4,2,3)=(\alpha(4,3,3)\wedge\alpha(2,2,2))\Rightarrow(\beta(4,2)\vee\alpha(4,2,2))=$$
$$=(T\wedge T)\Rightarrow(\perp\vee T)=T\Rightarrow T=T$$

U skupu $\{T,\perp\}$ uvedimo relaciju poretka $\leq$ tako da je $\perp\leq T$.
Neka su :
$\min\{\perp\}$, $\min\{T\}$, $\min\{\perp,T\}$, $\max\{\perp\}$, $\max\{T\}$, $\max\{\perp,T\}$
dogovorene oznake redom za $\perp$, $T$, $\perp$, $\perp$, $T$, $T$.

Definicija 5.

Neka je $\alpha(x_1,x_2,\ldots,x_n)$ relacija skupa M čija je dužina n, gde je x jedna od promenljivih $x_1,x_2,\ldots,x_n$, tada je:

$$(\exists x)\alpha(x_1,x_2,\ldots,x_n)=\max\{\alpha(x_1,x_2,\ldots,x_n)\ /\ x\in M\}$$
$$(\forall x)\alpha(x_1,x_2,\ldots,x_n)=\min\{\alpha(x_1,x_2,\ldots,x_n)\ /\ x\in M\}$$

Kada x nije jedna od promenljivih $x_1, \ldots x_n$, dogovorno uzimamo:

$(\exists x)\alpha(x_1, x_2, \ldots, x_n) = \alpha(x_1, x_2, \ldots, x_n)$

$(\forall x)\alpha(x_1, x_2, \ldots, x_n) = \alpha(x_1, x_2, \ldots, x_n)$

Primer 8.

Neka je $\alpha$ binarna relacija skupa prirodnih brojeva za koju:

$$\alpha(x,y) = T \Leftrightarrow 2x-3y = 5$$

Tada za relacije $\beta$ $\gamma$ definisane jednakostima

$\beta(y) = (\exists x)\alpha(x,y)$ , $\gamma(x,y) = (\forall x)\alpha(x,y) \Rightarrow \alpha(x,x)$ imamo:

$\beta(3) = (\exists x)\alpha(x,3) = T$

$\beta(4) = \bot$ $\beta(6) = \bot$

$\gamma(3,4) = (\forall x)\alpha(x,4) \Rightarrow \alpha(4,4) = \bot \Rightarrow \bot = T$

$\gamma(1,3) = (\forall x)\alpha(x,3) \Rightarrow \alpha(1,1) = \bot \Rightarrow \bot = T$

operac. *

U skupu binarnih relacija F definisanih na skupu $M$ $(\neq \emptyset)$ uvodimo koju zovemo proizvod binarnih relacija. Ako su $\rho$ i $\sigma$ dve binarne relacije u skupu M njihov proizvod je binarna relacija $\tau = \rho * \sigma$ u M saglasna tome $\tau(x,y) = T$ za $x,y \in M$ tada i samo tada ako postoji element $z \in M$ takav da je $\rho(x,z) = T$ i $\sigma(z,y) = T$. Ili simbolički :

$$(\tau(x,y) = T,\ x,y \in M) \Leftrightarrow (\exists z)(z \in M \wedge \rho(x,z) = T \wedge \sigma(z,y) = T)$$

## USLOVI MINIMALNOSTI

- Element a delimično uredjenog skupa M je <u>minimalni element</u> toga skupa ako u M nema ni jednog elementa x takvog da je $x \leq a$. (ili : a je minimalan element $\Longleftrightarrow$ $(x \leq a \Rightarrow x = a)$. Dualno se definiše <u>maximalni</u> element.)

Naprimer u sistemu $(\mathbb{P}X, \subseteq)$ jedini minimalni element je prazan skup. U skupu svih nepraznih podskupova skupa X minimalni elementi su svi jednočlani podskupovi od X.

Medjutim sistem $(Z, \leq)$ gde je Z skup celih brojeva nema minimalnog elementa.

Pojam minimalnog elementa se koristi za definisanje klase delimično uredjenih skupova, koji zadovoljavaju sledeće medju sobom ekvivalentne uslove :

<u>Uslov minimalnosti --Min.</u>

Svaki neprazan podskup N nekog delimično uredjenog skupa M ima bar jedan svoj minimalni element.

<u>Uslov prekida opadajućih lanaca. -P.</u>

Svaki strogo opadajući lanac elemenata delimično uredjenog skupa M : $a_1 > a_2 > a_3 > a_4 > \ldots > a_n > \ldots$ prekida se na konačnom mestu . Drugim rečima : $a_1 \geq a_2 \geq a_3 \geq \ldots \geq a_n \geq$ . postoji takav indeks n, tako da je $a_n = a_{n+1} = \ldots$.

<u>Uslov induktivnosti- Ind.</u>

Svi elementi parcijalno uredjenog skupa M imaju neko svojstvo ako :

1) To svojstvo imaju svi minimalni elementi toga skupa (ako postoje).

2) Iz važenja tog svojstva za sve elemente koji su manji od nekog elementa a može se i zvesti važenje tog svojstva za sam element a.

Dokaz ekvivalentnosti ovih iskaza izvodimo po ovoj šemi :

Min $\Longrightarrow$ Ind $\Longrightarrow$ P $\Longrightarrow$ Min

a) Iz uslova <u>minimalnosti</u> sledi uslov <u>induktivnosti</u>.

Neka su za neki delimično uredjen skup M ispunjeni : uslov Min i neka su za neko svojstvo $\mathcal{E}$ ispunjene indukcijske hipoteze 1 i 2. Treba da dokažemo da svaki element ima svojstvo $\mathcal{E}$.

Pretpostavimo suprotno, tj. da postoji neprazan skup $S \subset M$ elemenata koji nemaju svojstvo $\mathcal{E}$. Po uslovu minimalnosti skup S ima minimalnih elemenata. Neka je a jedan od tih elemenata. Element a nemože da bude minimalni elemant skupa M prema prvoj hipotezi uslova Ind. pošto svi elementi koji su strogo manji od a imaju svojstvo $\mathcal{E}$. Po drugoj hipotezi uslova Ind. i sam

element a mora da svojstvo $\mathcal{E}$ . Tako smo došli do protivrečnosti,

b) Iz uslova Ind. sledi uslov P.

Neka je M delimično uredjen skup koji zadovoljava uslov Ind. Primenimo uslov Ind. na svojstvo $\mathcal{E}$ koje je definisano na sledeći način: element a M ima svojstvo $\mathcal{E}$ ako se svi opadajući nizovi koji počimju sa a , prekidaju na konačnom mestu.

1) svojstvo $\mathcal{E}$ poseduju svi minimalni elementi ako postoje (lanac se tada prekida na prvom mestu)

2) neka svi elementi koji su strogo manji od a imaju svojstvo $\mathcal{E}$. To znači da se svaki lanac koji počinje ma kojim od tih elemenata prekida na konačnom mestu. Ta osobina važi i kada tim lancima dodamo element a, tj. svaki lanac koji počinje sa elementom a prekida se na konačnom mestu, odnosno a ima svojstvo $\mathcal{E}$ . Na osnovu uslova induktivnosti sledi da se svaki lanac prekida na konačnom mestu a to je upravo uslov P.

c) Iz uslova P sledi uslov Min.

Treba da dokažemo da svaki neprazan podskup skupa M koje je parcijalno uredjen, ima minimalni element, Pretpostavimo suprotno. Neka postoji neprazan podskup N skupa M koji nema minimalnih elemenata. Po aksiomi izbora , iz svakog nepraznog podskupa skupa N možemo izabrati po jedan element.

Obrazujemo niz $a_n$ $(n = 1,2,..)$ na sledeći način : ako je $\varphi$ birajuća funkcija, neka je $a_1 = \varphi(N)$

$a_{n+1} = \varphi(A_n)$ gde je

$A_n = \{ x / x < a_n \text{ i } x \in N \}$

kako skup N nema minimalnih elemenata, skup $A_n$ je neprazan za svaki n, i na ovaj način smo dobili beskonačan strogo opadajući lanac : $a_1 > a_2 > a_3 > \ldots > a_n > \ldots$,

što je suprotno pretpostavci da je svaki strogo opadajući lanac konačan.

Linearno uredjen skup koji ispunjava uslov minimalnosti je dobro uredjen skup. Naprimer $( N, \leq )$.

-Svaki podskup dobro uredjenog skupa i sam je dobro uredjen.

-Iz definicije dobro uredjenog skupa sledi da on ima jedinstven minimalni element.

-U dobro uredjenom skupu svaki elemant a ili je maksimalni element ili ima svog neposrednog naslednika. Element a može da nema neposrednog prethodnika, kao na primer u skupu $1,3,5,7,..2,4,..$ 2 nema neposrednog prethodnika.

## TEOREME EKVIVALENTNE AKSIOMI IZBORA

Ako je N podskup skupa M parcijalno uredjenog relacijom poretka tada za svaki element $a \in M$ koji zadovoljava uslov $x \leqslant a$ za svaki $x \in N$ kažemo da je gornja medja tog skupa N.
U skupu svih lanaca parcijalno uredjenog skupa M može se uvesti parcijalno uredjenje relacijom skupovne inkluzije. Maksimalne elemente tog skupa, ako postoje, nazivamo maksimalnim lancima.

Sledeće teoreme su ekvivalentne aksiomi izbora :

Zermelova teorema.
Svaki skup se može dobro urediti.

Haussdorfova teorema.
Svaki lanac delimično uredjenog skupa sadrži se u nekom maksimalnom lancu.

Teorema Zorn-Kuratovskog.
Ako svaki lanac delimično uredjenog skupa M ima gornju medju tada je svaki element skupa M manji (ili jednak) od nekog maksimalnog.
Napomena. To ne znači da su svi elementi skupa M $\leqslant$ od nekog fiksiranog elementa m (jer M može imati više različitih maksimalnih elemenata).
Pre nego što dokažemo ekvivalentnost ovih stavova i aksiome izbora uvodimo još neke pojmove koji su potrebni za dokaz.
Ako je A neki dobro uredjen skup tada svaki podskup B skupa A koji ima osobinu da uz svaki svoj elemenat sdrži i sve one elemente koji su manji od njega, zove se odsečak skupa A.
Skup svih elemenata strogo manjih od nekog elementa $a \in A$ je pravi odsečak $A'$ $(A' \neq A)$.
Ovom konstrukcijom se iscrpljuju svi pravi odsečci.
Odsečak B se sastoji iz svih elemenata strogo manjih od minimalnog elementa razlike $A \setminus B$, tj. definisan je tim elementom.

Dokaz.

a) Iz aksiome izbora sledi Zermelova teorema.
Neka je M proizvoljan skup. Prema aksiomi izbora , u svakom nepraznom podskupu N skupa M možemo da odredimo po jedan element $\varphi(N)$ gde je $\varphi$ birajuća funkcija. Ako podskup A ima svojstva :
1) može se dobro urediti nekom relacijom poretka
2) svaki element $a \in A$ ima oblik $a = \varphi(M \setminus A')$, gde je $A'$ pravi odsečak definisan elementom a,
tada kažemo da je A istaknut podskup.
Istaknuti podskupovi u M postoje, takv je naprimer $\{\varphi(M)\}$.

Neka su A i B dva istaknuta podskupa. A i B su dobro uredjeni pa imaju najmanje elemente, redom

$a_0 = \varphi(M \setminus A_0') = \varphi(M \setminus \emptyset) = \varphi(M)$, i

$b_0 = \varphi(M \setminus B_0') = \varphi(M)$

Dakle : $a_0 = b_0$.

Uočimo skup svih zajedničkih odsečaka D skupova A i B takvih da su elementi $(D_1, \leq_A)$ i $(D_1, \leq_B)$ izomorfni.

Taj skup nije prazan jer $\varphi(M)$ je takav odsečak.

Obeležimo sa C uniju svih takvih zajedničkih odsečaka. C je odsečak u svakom od skupova A i B i to najveći koji je zajednički Ako se C ne poklapa ni sa jednim od podskupova A I B, po definiciji istaknutosti postoji element koji se nalazi i u A i u B i oblika je $\varphi(M \setminus C)$, tako da definiše odsečak C. Tada bi A i B imali zajednički odsečak veći od C : $C = C' \cup \{\varphi(M \setminus C)\}$ koji očigledno zadovoljava uslov $(C_1', \leq_A) = (C_1', \leq_B)$, a to je u protivrečnosti sa definicijom odsečka C. Dakle, jedan od istaknutih podskupova je odsečak drugoga.

Neka je A odsečak od B. Pri tome se sistem $(A, \leq_A)$ izomorfno potapa u $(B, \leq_B)$.

Po uslovu induktivnosti koji je ispunjen jer je B $(\supset A)$ dobro uredjen pa ispunjava uslov minimalnosti ekvivalentan uslovu induktivnosti, izlazi da su im uredjenja jednaka.

Označimo sa L uniju svih istaknutih podskupova skupa M.

Dokažimo da je L istaknut podskup.

Neka su a i b ma koja dva elementa iz L, koji pripadaju redom istaknutim podskupovima A i B, tada prema prethodnom dokazano, sledi da pripadaju većem od njih , naprimer skupu A.

Neka je $a \leq_A b$ . Kako se za svaka dva elementa iz L može naći istaknut podskup kome oni pripadaju ( i koji je dobro uredjen) oni su uporedivi pa je L linearno uredjen skup. Svaki strogo opadajući lanac iz L ceo pripada nekom istaknutom podskupu $A \subset L$ u kome se on na osnovu uslova P prekida na konačnom mestu. Prema tome taj lanac se prekida na konačnom mestu i u skupu L, tj. L je dobro uredjen skup. Za svaki $a \subset L$ postoji podskup $A \subseteq L$ tako da $a \subset A$ pri čemu je $a = \varphi(M \setminus A')$ . Element a je i u L takvog oblika pa je L zaista istaknut podskup.

Na kraju dokažimo da je $L = M$.

Pretpostavimo suprotno, tj. da je $M \neq L$, pa skup $M \setminus L$ nije prazan. Pošto je L istaknut podskup on je i odsečak koji je definisan elementom $\varphi(M \setminus L)$. Tada le $L \cup \{\varphi(M \setminus L)\}$ novi istaknut podskup koji ne pripada L jer je veći od L, a to je nemoguće na osnovu definicije istaknutog podskupa L.

Dakle $M \setminus L = \emptyset$ pa se M i L poklapaju.

b) Iz Zermelove teoreme sledi Haussdorf-ova teorema.

Neka je M delimično uredjen skup u kome je A proizvoljan lanac. Ako je $A = M$ stav neposredno sledi jer je tada A maksimalan lanac. Zato pretpostavimo da je $M \setminus A = B$ neprazan podskup.

Po Zermelovoj teoremi skup B se može dobro urediti, ali je to uredjenje različito od parcijalnog uredjenja skupa B kao podskupa skupa M . Neka je b minimalni element skupa B. Elemente skupa B delimo u dve klase i to tako da b pripada prvoj klasi ako je on u relaciji delimičnog poretka sa svakim elementom lanca A, inače je u drugoj klasi. Ako je b B proizvoljan elemenat tada ako smo sve njegove prethodne već podelili u klase stavimo b u prvu klasu ako je on uporediv sa svakim elementom lanca A i svakim njegovim prethodnikom koji je u prvoj klasi. U protivnom slučaju b pripada drugoj klasi. Pošto je B dobro uredjen skup na osnovu uslova induktivnosti sledi da svaki element skupa B na jednoznačan način pripada prvoj ili drugoj klasi.

Skup elemenata lanca A i prve klase označimo sa C. C je lanac u M jer su svi elementi u njemu uporedivi. To je i maksimalni lanac jer nijedan elemenat druge klase skupa B prema konstrukciji nije uporediv ni sa jednim elentom skupa C. Ovo je upravo tvrdjenje Haussdorfove teoreme.

c) Iz Haussdorfove teoreme sledi teorema Zorn-Kuratovskog.

Neka je M takav parcijalno uredjen skup u kome svaki lanac ima gornju medju. Ako je a proizvoljan elemenat skupa M, on je rada i lanac, pa po Haussdorfovoj teoremi on se sadrži u maksimalnom lancu C. Po hipotezi teoreme Zorn-Kuratovskog C ima gornju medju c, pa je prema definiciji gornje medje $a \prec c$. Ako c nije maksimalni element, tada postoji $c'$ M takav da je $c \prec c'$.

Prema definiciji gornje medje $x \preccurlyeq c$ za svaki $x \in C$, a zbog toga je i $x \prec c$, odnosno $C \cup \{c'\}$ je veći lanac od C, a to je u suprotnosti sa tim da je C maksimalan lanac. Dakle , c ne postoji, pa je stav dokazan.

d) Iz teoreme Zorn-Kuratovskog sledi aksioma izbora.

Neka je dat proizvoljan skup M. Uočimo sve familije nepraznih podskupova skupa M , takvih da je na njima moguće zadati birajuću funkciju. Takve familije postoje, jedna od njih je na primer familija sastavljena od jednog nepraznog podskupa. Skup svih familija $\varphi$ koje odgovaraju familijama S označimo sa $\emptyset$ . U skupu $\emptyset$ relaciju delimičnog poretka $\preccurlyeq$ definišimo na sledeći način :

ako su $\varphi$ i $\psi$ dve funkcije iz skupa $\emptyset$ zadane redom familijama S i T , gde je $S \subseteq T$ i na S se poklapaju, tada je $\varphi \leq \psi$.
Neka je $\Gamma$ neki lanac sastavljen od familija $\varphi_\alpha$ iz skupa $\emptyset$, koje su zadane na familijama $S_\alpha$ . Na familji $F = \bigcup_\alpha S_\alpha$ definišemo funkciju f koja se poklapa na svakoj familiji $S_\alpha$ sa funkcijom $\varphi_\alpha$. To je moguće jer je T unija familija $S_\alpha$ . $f \in \emptyset$ i f je gornja medja lanca $\Gamma$, pa po teoremi Zorn-Kuratovskog, skup $\emptyset$ ima maksimalnih elemenata. Neka je jedan od njih $\chi$ , i neka je U familija podskupova na kojoj je ta funkcija zadana. Ako U ne sadrži neki podskup A skupa M, tada na familiji $U \cup A$ možemo zadati funkciju $\chi_1$ , strogo veću od $\chi$ koja se sa $\chi$ poklapa na U, a u skupu A odredjuje jedan njegov element. No , ovo je protivrečno sa tim da je $\chi$ maksimalni element, pa familija U obuhvata sve neprazne podskupove skupa M. Znači $\chi$ je birajuća funkcija za čitav skup M.

# UNIVERZALNE ALGEBRE

## I. Prve definicije.Homomorfizmi. Kongruencije.

### 1. Grupoid.

Jedan od najvažnijih algebarskih pojmova je pojam algebarske operacije. To je preslikavanje oblika $A^n \to A$, gde je $n = 1,2,...$ i A neki skup.

Svaki skup na kome je definisana neka binarna operacija, slobodnije rečeno, naziva se grupoid. Grupoid se strogo definiše kao uredjen par $(G,+)$ skupa G i binarne operacije $+ : G^2 \to G$ . On se, prema tome, sastoji iz skupovnog i operacijskog dela. Često $(x,y)+$, $x,y \in G$, obično se piše $x+y$ .

Specijalni grupoidi se zovu grupe, podgrupe,...

### 2. Univerzalne algebre.

Izmedju mnogih delova teorije grupa i teorije prstena postoji paralelizam. Često je pogodno ne razmatrati grupe i prstene odvojeno već graditi jedinstvenu teoriju čiji rezultati vrede i za grupe i za prstene. S tim ciljem je započeno izučavanje proizvoljnih algebarskih struktura, sa proizvoljnim brojem algebarskih operacija koje ne moraju obavezno biti binarne. OpisnoOpisno rečeno, skup G naziva se univerzalnom algebrom ako je u njemu zadat neki skup $\Omega$ n-arnih operacija, pri čemu za različite operacije $w \in \Omega$ brojevi n mogu biti kako različiti tako i jednaki ($n = 0,1,2,...$). Ovaj skup može biti i beskonačan - naprimer kod vektorskih prostora nad beskonačnim poljima postoji jedna binarna operacija, sabiranje, i beskonačan skup unarnih operacija množenje elementima osnovnog polja.

Specijalno, nularnom operacijom skupa G nazivamo neki odredjeni element skupa G. Prema tome, nularnih operacija može biti onoliko koliko ima elemenata u skupu G.

Univerzalna algebra ima skupovni deo G (skup G na kome su definisane izvesne operacije), i operacijski deo (skup izvesnih operacija $w_i$ , kada $i \in I$ gde je I neki pomočni skup indeksa).

U stvari , $(G, \{w_i / i \in I\})$ zovemo univerzalna algebra.

Prema prethodnoj definiciji u univerzalne algebre spadaju grupoidi grupe, kvazi grupe, prsteni, itd. Primetimo da grupu, kao univerzalnu algebru, možemo posmatrati na dva načina: s jedne strane to je skup s trima binarnim operacijama -"množenje"i"levo i desno deljenje", s druge strane, to je skup s jednom nularnom operacijom "jedinicom", jednom binarnom operacijom "množenjem" i jednom unarnom operacijom ,"nalaženje inverznog elementa". Primetimo

takodje da tela možemo smatrati uneverzalnim algebrama samo ako u razmatranju dopustimo algebarske operacije koje nisu definisane na čitavom osnovnom skupu, jer su takve levo i desno deljenje u telu i nalaženje inverznog elementa.

Neka je data univerzalna algebra G sa skupom operacija $\Omega$. Podskup $A \subseteq G$ nazivamo podalgebrom univerzalne algebre G, ako za svaku n-arnu operaciju $w \in \Omega$ iz $a_1, a_2, \ldots, a_n \in A$ uvek sledi $(a_1, \ldots, a_n)w \in A$ i ako A sadrži sve nularne operacije algebre G.

Specijalni skučajevi ovog pojma su, očigledno, podgrupoid grupoida podgrupa grupe, podprsten prstena. Primetimo, takodje, da ako prsten R ima jedinični element i posmatramo ga kao univerzalnu algebru čija je jedna nularna operacija jedinica, tada su pod algebre samo oni podprsteni prstena R koji sadrže jedinicu prstena R a ne ma koji podprsteni, čak i ako imaju sopstvenu jedinicu.

Lako se dokaže da je presek ma koga skupa podalgebri univerzalne algebre G, ako nije prazan, takodje podalgebra te algebre.

Otuda sledi, da ako u univerzalnoj algebri G uzmemo proizvoljan neprazan podskup M, tada postoji jednoznačno odredjena podalgebra $\{M\}$, minimalna medju podalgebrama koje sadrže M. To je presek svih podalgebri iz G koje sadrže M . (jedna od njih je i sama algebra G). Ako je $\{M\} = G$ kažemo da je M skup generatornih elemenata za G.

## 3. Homomorfizmi. Kongruencije. Količničke strukture.

### Homomorfizmi.

Univerzalne algebre $\mathcal{A} = (A, \{w_i / i \in I\})$ i $\mathcal{B} = (B, \{w'_j / j \in J\})$ ($w_i$ i $w'_j$ su oznake za neke operacije skupova A, odnosno B) nazivamo jednakotipnim ako postoji 1-1 i "na" preslikavanje $f : I \to J$ takvo da odgovaraće operacije $w_i$ i $w'_{f(i)}$ imaju jednake dužine.

**Definicija 1.**

Ako su $\mathcal{A} = (A, \{w_i / i \in I\})$ i $\mathcal{B} = (B, \{w'_j / j \in J\})$ dve jednakotipne univerzalne algebre i f preslikavanje skupa A u skup B takvo da je za svake dve odgovarajuće operacije w i w' univerzalnih algebri $\mathcal{A}$, odnosno $\mathcal{B}$ ispunjen uslov :

$((x_1, x_2, \ldots, x_n)w)f = (x_1 f, x_2 f, \ldots, x_n f)w'$ za sve $x_1, \ldots, x_n \in A$

kažemo da je f homomorfizam $\mathcal{A}$ u $\mathcal{B}$.

- Homomorfizam koji je 1-1 i "na" nazivamo izomorfizam.
- Homomorfizam univerzalne algebre u samu sebe nazivamo endomorfizam.
- Izomorfizam univerzalne algebre na samu sebe nazivamo automorfizam.

Primer :

Neka su $\mathcal{G}_1 = (\{a_1,a_2,a_3,b_1,b_2\}, \circ)$ i $\mathcal{G}_2 = (\{\alpha,\beta\}, *)$ dva grupoida s operacijama definisanim na sledeći način :

| $\circ$ | $a_1$ | $a_2$ | $a_3$ | $b_1$ | $b_2$ |
|---|---|---|---|---|---|
| $a_1$ | $a_1$ | $a_1$ | $a_1$ | $b_2$ | $b_1$ |
| $a_2$ | $a_2$ | $a_3$ | $a_3$ | $b_1$ | $b_2$ |
| $a_3$ | $a_1$ | $a_3$ | $a_2$ | $b_1$ | $b_1$ |
| $b_1$ | $b_2$ | $b_1$ | $b_2$ | $b_1$ | $b_1$ |
| $b_2$ | $b_1$ | $b_2$ | $b_1$ | $b_1$ | $b_1$ |

| $*$ | $\alpha$ | $\beta$ |
|---|---|---|
| $\alpha$ | $\alpha$ | $\beta$ |
| $\beta$ | $\beta$ | $\beta$ |

Tada je preslikavanje $f = \begin{pmatrix} a_1 & a_2 & a_3 & b_1 & b_2 \\ \alpha & \alpha & \alpha & \beta & \beta \end{pmatrix}$ jedan homomorfizam grupoida $\mathcal{G}_1$ u grupoid $\mathcal{G}_2$.

Kongruencije univerzalnih algebri.

Definicija 2.

Neka je $\mathcal{A} = (A, \{w_i\}_{i\in I})$ univerzalna lagebra i w jedna njena operacija dužine n. Kažemo da je relacija ekvivalencije skupa A saglasna s operacijom w ako iz

$$\left.\begin{array}{l} x_1 \sim y_1 \\ x_2 \sim y_2 \\ x_n \sim y_n \end{array}\right\} \text{ sledi } (x_1,x_2,\ldots,x_n)w \sim (y_1,y_2,\ldots,y_n)w$$

Ako je $\sim$ saglasna sa svakom operacijom univerzalne algebre kažemo da je $\sim$ kongruencija univerzalne algebre .

Primeri :

1) Neka je $(Z,+,\cdot)$ prsten celih brojeva i $\sim$ relacija skupa Z definisana na sledeći način :

$$x \sim y \text{ ako je } \operatorname{sgn}x = \operatorname{sgn}y$$

Lako se vidi da je $\sim$ relacija ekvivalencije skupa Z koja je saglasna s operacijom $\cdot$ , a nije saglasna s operacijom +. Za semigrupu $(Z,\cdot)$ je $\sim$ kongruencija.

2) Za prsten celih brojeva je relacija $\equiv \bmod m$ , definisana na sledeći način :

$$x \equiv y \pmod m \iff (\exists z)(z\in Z \wedge (y-x = mz))$$

kongruencija, jer je saglasna sa obe operacije + i $\cdot$.

$$\left.\begin{array}{l} x \equiv y \pmod m \\ z \equiv u \pmod m \end{array}\right\} \Rightarrow \begin{array}{l} x+z \equiv y+u \pmod m \\ x\cdot z \equiv y\cdot u \pmod m \end{array}$$

3) Neka je $\Gamma = \{a,b\}$ i $W = \{a,b,ab,ba,aa,\ldots,bab,\ldots\}$ skup reči sa simbolima a i b. U skup W uvodimo operaciju "dopisivanje", u oznaci $\cdot$ , na sledeći način :

$$w_1 \cdot w_2 = w_1 w_2 \quad : \quad w_1 , w_2 \in W$$

Tako dobijamo semigrupu $(W,\cdot)$. Jedna njena kongruencija je relacija $\sim$ , definisana na sledeći način:

$w_1 \sim w_2$ ako je $d(w_1) = d(w_2)$ (tj. ako reči $w_1$ i $w_2$ imaju jednake dužine ).

Sledeće relacije su takodje kongruencije semigrupe (W,.):

a) $w_1 \sim w_2$ ako je $d(w_1) \equiv d(w_2) \pmod m$

b) $w_1 \sim w_2$ ako je broj a-ova u reči $w_1 w_2$ paran.

c) $w_1 \sim w_2$ ako se iz $w_1$ može dobiti $w_2$ konačnom primenom zakona xy = yx ( gde su x i y elementi skupa W.

4) Ako u skupu W = {a,b,ab,aa,ba,bb} uvedemo operaciju "dopisivanje sa skraćivanjem na dužinu dva", u oznaci . , dobijamo grupoid (W,.) .

| . | a | b | aa | ab | ba | bb |
|---|---|---|---|---|---|---|
| a | aa | ab | aa | aa | ab | ab |
| b | ba | bb | ba | ba | bb | bb |
| aa | aa | aa | aa | aa | aa | aa |
| ab | ab | ab | ab | ab | ab | ab |
| ba | ba | ba | ba | ba | ba | ba |
| bb | bb | bb | bb | bb | bb | bb |

Relacija $\sim$ , definicana na sledeći način :

$w_1 \sim w_2$ ako je $d(w_1) = d(w_2)$ , je jedna kongruencija grupoida (W,.) .

Kongruencije su sledeće trivijalne relacije :

$w_1 \sim w_2$ ako je $w_1 = w_2$

$w_1 \sim w_2$ za svake $w_1, w_2$ iz W.

Definicija 3.

Neka je $\mathcal{A} = (A, \{w_{i/i \in I}\})$ univerzalna algebra i $\sim$ njena kongruencija . Svakoj operaciji strukture $\mathcal{A}$ na sledeći način dodeljujemo po jednu operaciju skupa klasa $A/\sim$ :

1. Konstanti a ( odnosno nularnoj operaciji skupa A) dodeljujemo klasu $C_a$ (nularnu operaciju skupa $A/\sim$ ).

2. Operaciji w (dužine $n \geq 1$) strukture $\mathcal{A}$ dodeljujemo operaciju $\circledcirc$ (iste dužine) skupa $A/\sim$ definisanu na sledeći način :

$$(C_{x_1}, C_{x_2}, \ldots, C_{x_n}) \circledcirc = C_{(x_1, x_2, \ldots, x_n)w}$$

Na taj način prelazimo na tzv. količničku strukturu $\mathcal{A}/\sim$ čiji je skupovni deo $A/\sim$ i operacije $C_a$ i $\circledcirc$ (gde a i w "predju" preko svih operacija strukture $\mathcal{A}$).

Iz definicije kongruencije proizlazi :

Ako $C_{x_1} = C_{y_1}$ , $C_{x_2} = C_{y_2}$ , ..., $C_{x_n} = C_{y_n}$ onda

$(C_{x_1}, C_{x_2}, \ldots, C_{x_n})\circledcirc = (C_{y_1}, C_{y_2}, \ldots, C_{y_n})\circledcirc$ pa je prethodna definicija operacije $\circledcirc$ korektna.

Osnovna teorema o homomorfizmima.

Ova teorema uspostavlja vezu izmedju homomorfizama i kongruencija univerzalnih algebri.

1) Neka je $\sim$ kongruencija univerzalne algebre $\mathcal{A}$.
Tada je količnička struktura $\mathcal{A}/\sim$ homomorfna slika algebre $\mathcal{A}$.
Jedan homomorfizam je preslikavanje $x \to C_x$ (tzv. prirodni homomorfizam).

2) Obrnuto : ako je $\mathcal{A}'$ homomorfna slika univerzalne algebre $\mathcal{A}$ tada ova ima bar jednu kongruenciju $\sim$ takvu da su strukture $\mathcal{A}/\sim$ i $\mathcal{A}'$ izomorfne .

Dokaz.

1) Neka je f preslikavanje definisano sa $xf = C_x$ .
f je preslikavanje skupa A na skup $A/\sim$ .
Prema definiciji operacije $w$ je :

$$(C_{x_1}, C_{x_2}, \ldots, C_{x_n})w = C_{(x_1, x_2, \ldots, x_n)w}$$

odnosno, uzimajući u obzir definiciju f :

$(x_1 f, x_2 f, \ldots, x_n f)w = ((x_1, x_2, \ldots, x_n)w)f$ , za svaku operaciju w strukture $\mathcal{A}$. Prema tome f je homomorfizam algebre $\mathcal{A}$ na $\mathcal{A}/\sim$ .

2) Obrnuto : neka je f homomorfizam univerzalne algebre $\mathcal{A}$ na $\mathcal{A}'$.
Definišimo relaciju $\sim$ na sledeći način :

$x, y \in A$ , $x \sim y$ ako je $xf = yf$ .

je relacija ekvivalencije skupa A :

$xf = xf \iff x \sim x$

$x \sim y \Rightarrow xf = yf \Rightarrow yf = xf \Rightarrow y \sim x$

$x \sim y$ i $y \sim z \Rightarrow xf = yf$ i $yf = zf \Rightarrow xf = zf \Rightarrow x \sim z$

$\sim$ je i kongruencija univerzalne algebre $\mathcal{A}$, jer je za svaku njenu operaciju w :

$x_i \sim y_i (i = 1, 2, \ldots, n) \iff x_i f = y_i f \Rightarrow$

$\Rightarrow (x_1 f, x_2 f, \ldots, x_n f)w' = (y_1 f, y_2 f, \ldots, y_n f)w'$ (gde je w' odgovarajuća operacija strukture $\mathcal{A}$ ).

$\iff ((x_1, x_2, \ldots, x_n)w)f = ((y_1, y_2, \ldots, y_n)w)f \iff$

$\iff (x_1, x_2, \ldots, x_n)w \sim (y_1, y_2, \ldots, y_n)w$

Uvedimo sada skup $A/\sim = \{C_x / x \in A\}$ i odgovarajuću količničku strukturu $\mathcal{A}/\sim$ .
Definišimo preslikavanje $\varphi$ na sledeći način : $\varphi = \begin{pmatrix} C_x \\ xf \end{pmatrix}_{x \in A}$

$\varphi$ je preslikavanje $A/\sim$ na $A'$

$\varphi$ je 1-1 preslikavanje : $C_x \neq C_y$ $x \not\sim y \iff xf \neq yf \iff$

$\iff (C_x)\varphi \neq (C_y)\varphi$

$\varphi$ je saglasno s odgovarajućim operacijama univerzalnih algebri $\mathcal{A}/\sim$ i $\mathcal{A}'$ :

$$((C_{x_1}, C_{x_2}, \ldots, C_{x_n})w)\varphi = C_{(x_1, x_2, \ldots, x_n)w}\varphi =$$

$$= ((x_1, x_2, \ldots, x_n)w)f = (x_1 f, x_2 f, \ldots, x_n f)w' =$$

$$= (C_{x_1}\varphi, C_{x_2}\varphi, \ldots, C_{x_n}\varphi)w'$$

Znači $\varphi$ je izomorfizam, odnosno strukture $\mathcal{A}/\sim$ i $\mathcal{A}'$ su izomorfne .

Razni primeri kongruencija i količničkih algebri.

Kongruencija grupe.

Svaka grupa $\mathcal{G}=(G,.)$ predstavlja univerzalnu algebru koja ima tri operacije : jednu binarnu . , jednu unarnu $()^{-1}$, i jednu nularnu - e (jedinični element grupe). S obzirom na ovo , kongruencija grupe može se definisati kao relacija ekvivalencije $\sim$ skupa G koja ima sledeća svojstva :

1) $\left.\begin{matrix} x \sim y \\ z \sim u \end{matrix}\right\} \Rightarrow \quad x.z \sim y.u$

2) $x \sim y \quad \Rightarrow \quad x^{-1} \sim y^{-1}$

Lako se medjutim dokazuje da je uslov 2) posledica uslova 1) pa se zato kongruencija grupe može definisati i samo pomoću uslova 1).

Definicija 4.

Za podskup H skupa G kažemo da je podgrupa grupe $\mathcal{G}=(G,.)$ ako ispunjava sledeće uslove :

1) $x,y \in H \Rightarrow x.y \in H$

2) $x \in H \Rightarrow x^{-1} \in H$

3) $e \in H$

Ovi uslovi su ekvivalentni sa jednim jedinim :

$(x,y\ H \Rightarrow xy^{-1} \in H)$ i $(H \neq \emptyset)$

Za podgrupu (H,.) grupe (G,.) kažemo da je normalna ako ispunjava uslov : $(\forall x)(x \in G \Rightarrow x.H = H.x)$

ili neki od ekvivalentnih uslova :

$(\forall x)(x \in G \Rightarrow x.H.x^{-1} = H)$ , $(\forall x)(x \in G \Rightarrow x^{-1}.H.x \subseteq H)$

Kongruencija po modulu podgrupe.

Ako je (H,.) podgrupa grupe (G,.) lako se dokazuje da su relacije $\equiv \mod_l H$ i $\equiv \mod_d H$ , definisane na sledeći način

$x \equiv y \ (\mod_l H)$ ako $(\exists h)(h \in H$ i $y = xh)$

$x \equiv y \ (\mod_d H)$ ako $(\exists h)(h \in H$ i $y = hx)$

relacije ekvivalencije skupa G.

Važi sledeća teorema :

- $(H,.)$ je normalna podgrupa grupe $(G,.)$ ako i samo ako je $\equiv \mathrm{mod}_d H$ jednaka $\equiv \mathrm{mod}_l H$ (tada se ova relacija označava samo sa $\equiv \mathrm{mod}\ H$ ).

-Teorema o kongruencijama grupa :

1) Ako je $(H,.)$ normalna podgrupa grupe $(G,.)$ tada je relacija $\equiv \mathrm{mod}\ H$ skupa G kongruencija grupe $(G,.)$

2) Obrnuto, ako je $\sim$ kongruencija grupe $(G,.)$ tada ova ima normalnu podgrupu H takvu da je $\sim$ jednaka $\equiv \mathrm{mod}\ H$ .

Dokaz.

1) Neka je $(H,.)$ normalna podgrupa grupe $(G,.)$ .Tada je $\equiv \mathrm{mod}\ H$ relacija ekvivalencije:

$x \equiv x \ (\mathrm{mod}H)$ jer $e \in H$ i $x = ex$

$x \equiv y \ (\mathrm{mod}H) \Rightarrow (\exists h)(h \in H \wedge y = hx) \Rightarrow x = h^{-1}y \ , \ h^{-1} \in H \Rightarrow$

$\Rightarrow y \equiv x \ (\mathrm{mod}H)$

$x \equiv y \ (\mathrm{mod}H)$ i $y \equiv z \ (\mathrm{mod}H) \Rightarrow (\exists h_1)(h_1 \in H \wedge y = h_1 x) \wedge$

$\wedge (\exists h_2)(h_2 \in H \wedge z = h_2 y) \Rightarrow$

$\Rightarrow z = h_2 h_1 x \ , \ h_2 h_1 \in H$

$\Rightarrow x \equiv z \ (\mathrm{mod}H)$

$\equiv (\mathrm{mod}\ H)$ je i kongruencija grupe $(G,.)$ :

$$\left.\begin{array}{l} x \equiv y \ (\mathrm{mod}H) \\ z \equiv u \ (\mathrm{mod}H) \end{array}\right\} \Rightarrow \begin{array}{l} y = h_1 x \\ u = h_2 z \end{array} \ ; \ h_1 \ , \ h_2 \in H \Rightarrow$$

$\Rightarrow y.u = h_1 x . h_2 z = h_1 h' x . z \ , \ h' \in H, \ h_1 . h' \in H$

$\Rightarrow xz \equiv yu \ (\mathrm{mod}H)$

tj. $\equiv (\mathrm{mod}H)$ je kongruencija grupe $(G,.)$ .

2) Neka je $\sim$ kongruencija grupe $(G,.)$ .

Definišimo skup $H = \{ x / \ x \in G \wedge x \sim e \}$

gde je e jedinični element grupe .

$(H,.)$ je podgrupa grupe $(G,.)$ .

$H \neq \emptyset$ jer je $e \in H$

$$x,y \in H \quad \begin{array}{l} x \sim e \\ y \sim e \end{array} \Rightarrow \begin{array}{l} x \sim e \\ y \sim e \end{array} \Rightarrow x.y^{-1} \sim e \Rightarrow x.y^{-1} \in H$$

$(H,.)$ je normalna podgrupa :

Neka $h \in H$ i $x \in G$ . Tada je

$$\left.\begin{array}{l} x^{-1} \sim x^{-1} \\ h \sim e \\ x \sim x \end{array}\right\} \text{ sledi : } x^{-1}hx \sim e \text{ tj. } x^{-1}hx \in H \text{ odnosno } x^{-1}Hx \subseteq H .$$

Dokažimo da je $\equiv \mathrm{mod}\ H$ jednaka sa $\sim$ :

$x \equiv y \ (\mathrm{mod}H) \Rightarrow (\exists h)(h \in H \wedge y = hx) \Rightarrow yx^{-1} = h \in H \Rightarrow yx^{-1} \sim e \Rightarrow$

$\Rightarrow y \sim x \Rightarrow x \sim y$

Obrnuto : $x \sim y \Rightarrow x \sim y \wedge x^{-1} \sim x^{-1} \Rightarrow e \sim yx^{-1} \Rightarrow yx^{-1} \sim e \Rightarrow$

$\Rightarrow yx^{-1} \in H \Rightarrow x \equiv y \ (\mathrm{mod}H)$ .

Prema tome zaista je $\equiv \mathrm{mod}\ H$ jednaka $\sim$ .

Količnička grupa.

Grupu $\mathcal{G}$ i njenoj normalnoj podgrupi $\mathcal{H}$, odnosno njenoj kongruenciji $\equiv \bmod H$, odgovara količnička grupa $\mathcal{G}/\equiv \bmod H$. Najčešće se ova količnička grupa označava kratko sa $\mathcal{G}/\mathcal{H}$.

Osnovna teorema o homomorfizmima grupa.

Koristeći raniji stav o vezi izmedju kongruencija i homomorfizama univerzalnih algebri, kao i prethodni stav o vezi kongruencija grupa i njenih normalnih podgrupa, zaključujemo da važi sledeći stav :

1) Neka je H normalna podgrupa grupe $\mathcal{G}$ i $\mathcal{G}/\mathcal{H}$ odgovarajuća količnička grupa. Grupa $\mathcal{G}/\mathcal{H}$ je homomorfna slika grupe $\mathcal{G}$. Jedan homomorfizam je preslikavanje $\nu$: $x \to Hx$ (tzv. prirodni homomorfizam).

2) Obrnuto, ako je $\mathcal{G}'$ homomorfna slika grupe $\mathcal{G}$ onda grupa $\mathcal{G}$ ima bar jednu normalnu podgrupu $\mathcal{H}$ takvu da su grupe $\mathcal{G}/\mathcal{H}$ i $\mathcal{G}'$ izomorfne. Ako je f homomorfizam grupe $\mathcal{G}$ na grupu $\mathcal{G}'$ tada je jedna takva podgrupa jezgro homomorfizma f. definisano na sledeći način : $\ker f = \{x \mid x \in G \wedge xf = e'\}$ ($e'$ je jedinični element grupe $\mathcal{G}'$).

Kongruencija prstena .

Svaki prsten $\mathcal{R} = (R,+,.)$ prestavlja univerzalnu algebru koja ima četiri operacije : dve binarne - + , . - , jednu unarnu : $-()$, i jednu nularnu : 0 (nularni element u odnosu na +). Sobzirom na ovo kongruencija prstena $\mathcal{R}$ se može definisati kao relacija ekvivalencije $\sim$ skupa R koja ima sledeća svojstva :

1. $\left.\begin{matrix} x \sim y \\ z \sim u \end{matrix}\right\} \Rightarrow \quad x+z \sim y+u$

2. $\left.\begin{matrix} x \sim y \\ z \sim u \end{matrix}\right\} \Rightarrow \quad x.z \sim y.u$

3. $x \sim y \quad \Rightarrow \quad -x \sim -y$

Lako se medjutim dokazuje da je uslov 3. posledica uslova 1., pa se zato kongruencija prstena definiše samo pomoću 1. i 2. .

Definicija 5.

Za neprazan skup I skupa R kažemo da je ideal prstena $\mathcal{R} = (R,+,.)$ ako ispunjava sledeće uslove :

1. $x,y \in I \Rightarrow x-y \in I$

2. $x \in I$ , $y \in R \Rightarrow x.y \in I \wedge y.x \in I$ .

Kongruencija po modulu ideala :

Ako je $\mathcal{R} = (R,+,.)$ prsten i I njegov ideal tada je relacija $\equiv \bmod I$ definisana na sledeći način: $x \equiv y \bmod I \Leftrightarrow x-y \in I$

$\mathcal{R}/\mathcal{J} = (R/I,+,.)$ ; $R/I = \{I+x \ / \ x \in R\}$

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

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

$-(I+x) = I + (-x)$

Osnovna teorema o homomorfizmima za prstene glasi :

1. Ako je I ideal prstena $\mathcal{R}$ tada je prsten $\mathcal{R}/\mathcal{J}$ homomorfna slika prstena $\mathcal{R}$.

2. Obrnuto, ako je $\mathcal{R}'$ homomorfna slika prstena $\mathcal{R}$ tada $\mathcal{R}$ ima bar jedan ideal $\mathcal{J}$ takav da su prsteni $\mathcal{R}/\mathcal{J}$ i $\mathcal{R}'$ izomorfni.

## II. Primitivne klase univerzalnih algebri. Zakoni. Posledice.

### 1. Zakoni klase Z. Model tih zakona.

Jedan od važnih algebarskih pojmova je pojam algebarskog zakona. Pod tim podrazumevamo formulu (reč) oblika $t_1 = t_2$ , gde su $t_1$ i $t_2$ termi.

Kažemo da u univerzalnoj algebri $\mathcal{G} = (G, \Omega)$ važi zakon $t_1 = t_2$ ako kada sve operacijske simbole koji se pojavljuju u $t_1$ i $t_2$ interpretiramo kao odredjene operacije algebre $\mathcal{G}$ termi $t_1$ i $t_2$ dobijaju istu vrednost za sve interpretacije promenljivih, koje se u njima javljaju, kao elemenata skupa G.

Interpretacija I klase zakona Z nazivamo modelom klase zakona Z ako je svaki zakon $z \in Z$ tačna formula pri toj interpretaciji. Prema tome, univerzalna algebra $\mathcal{G}$ je model klase zakona Z ako u njoj važe svi zakoni iz te klase.

Na primer : svaka grupa je model za klasu zakona Z gde je

II def. $Z = \{x.(y.z) = (x.y).z \ , \ x.e = x \ , \ x.x' = e\}$ .

. se interpretira kao operacija grupe , $()'$ kao nalženje inverznog elementa , e kao jedinični element grupe, a x,y,z kao elementi grupe.

### 2. Primitivne klase univerzalnih algebri.

Pojam jednakotipnost algebri suviše je opšt da bi mogao da razdvoji razne klase algebarskih struktura. Na primer nije svaka univerzalna algebra s jednom binarnom , jednom unarnom i jednom nularnom operacijom grupa mada je jednakotipna s grupama. Medju ovakvim algebrama grupe karakteriše to što za njih važe zakoni : $x.(y.z) = (x.y).z$ , $x.e = x$ , $x.x = e$ .

Ako je data klasa algebarskih zakona Z tada sve jednakotipne univerzalne algebre u kojima važe svi zakoni iz Z čine primitivnu klasu univerzalnih algebri. Nju takodje označavamo istim slovom

Z kao i klasu zakona koja je odredjuje.
Na primer grupe čine primitivnu klasu algebri.
Abelove grupe čine užu primitivnu klasu , jer za njih važi dopunski zakon $x.y = y.x$ . Još užu primitivnu klasu čine grupe za koje važi zakon $x^2 = e$.

Prsteni, asocijativni prsteni, asocijativno-komutativni prsteni, Lee-evi prsteni takodje su primitivne klase univerzalnih algebri.

Čitavu klasu medju sobom jednakotipnih univerzalnih algebri takodje možemo smatrati primitivnom klasom i to za prazan skup zakona . S druge strane klasa zakona Z može biti takva da je njena posledica zakon $x = y$ . Tada se odgovarajuća primitivna klasa sastoji iz jedne jedine algebre koja ima samo jedan element.

Svaka primitivna klasa univerzalnih algebri zajedno sa svakom svojom algebrom sadrži sve njene podalgebre i sve njene homomorfne slike.

3. Posledica klase zakona.

Neka je Z izvesna klasa univerzalnih algebarskih zakona. Neka $u[v]$ označava da je term v podterm za term u , i neka je $u[w]$ term koji se dobija iz $u[v]$ kad se term v zameni termom w. Terme $u[v]$ i $u[w]$ nazivamo susednim ako zakon $v = w$ pripada klasi Z. Takodje kažemo da je svaki term susedan samome sebi.
Ako je $u, u_1, u_2, \ldots, u_n, v$ niz terma takvih da su u i $u_1$, $u_1$ i $u_2$, $\ldots, u_n$ i v susedni termi tada kažemo da je zakon $u = v$ sintaktička posledica klase zakona Z i pišemo $Z \vdash u = v$.
Smatramo i $Z \vdash u = u$ .

Sintaktičku posledicu klase zakona Z možemo definisati i na sledeći način :

Skup svih posledica klase zakona Z, u oznaci Con(Z) (od Consequence = posledica) je minimalni skup za koji je :

1. $Z \subseteq Con(Z)$
2. $u = u \in Con(Z)$
3. $u = v \in Con(Z) \Rightarrow v = u \in Con(Z)$
   $u = v$ , $v = w \in Con(Z) \Rightarrow u = w \in Con(Z)$
4. Ako $u = v \in Con(Z)$ onda i $\overline{u} = \overline{v} \in Con(Z)$
   gde su $\overline{u}$ i $\overline{v}$ termi koji se dobijaju iz terma u i v kada se promenljive koje u njima učestvuju zamene nekim termima (pravila supstitucije).
5. Ako je f operacijski simbol dužine n koji se pojavljuje u zakonima iz Z i ako
   $u_1 = v_1, u_2 = v_2, \ldots, u_n = v_n \in Con(Z)$
   onda $f(u_1, u_2, \ldots, u_n) = f(v_1, v_2, \ldots v_n) \in Con(Z)$

Kažemo da je zakon z sintaktička posledica klase zakona Z : $Z \vdash z$ ako z pripada ovako definisanom skupu Con(Z).
Neposredno se proverava da su sve ove definicije ekvivalentne.

Ako definišemo formalnu teoriju čije su aksiome Z i x = x, a pravila izvodjenja su u skladu sa 3.,4.,i 5. dobijamo teoriju čiji je skup teorema Con(Z).

Kažemo da je zakon z semantička posledica klase zakona Z ako je svaki model za Z istovremeno i model za z. To se označava sa

$$Z \models z$$

Očigledno važi : ako $Z \vdash z$ onda $Z \models z$ .

Primeri:

1) Neka je klasa zakona $Z = \{x.x = x\}$
   Tada Con(Z) sadrži , naprimer, sledeće zakone :
   $(x.x).(x.x) = x.x$
   $(x.x).(y.y) = x.y$
2) Posledica asocijativnog zakona (tj. $Z = \{x(yz) = (xy)z\}$ ) je uopšteni asocijativni zakon.
3) Ako je $Z = \{x(yz) = (xy)z\ ,\ x.e = x\ ,\ x.x' = e\}$ tada
   $e.x = x\ ,\ x'.x = e\ ,\ x'' = x\ ,\ (xy)' = y'x' \in Con(Z)$

Dokaz :

Dokažimo prvo da važi zakon kancelacije :

$ax = bx$

$a = ae = a(xx') = (ax)x' = (bx)x' = b(xx') = be = b$

tj. $ax = bx \Rightarrow a = b$

Tada je :

$(ex)x' = e(xx') = ee = e = xx' \Rightarrow ex = x \in Con(Z)$

$(x'x)x' = x'(xx') = x'e = x'.\ ex' \Rightarrow x'x = e \in Con(Z)$

$\left.\begin{matrix} x''x' = e \\ xx' = e \end{matrix}\right\}\ x''x' = xx' \Rightarrow x'' = x \in Con(Z)$

$\left.\begin{matrix} (xy).(xy) = e \\ (y'x').(xy) = e \end{matrix}\right\} \Rightarrow (xy).(xy) = (y'x')xy \Rightarrow (xy)' = y'x' \in Con(Z)$

Važe sledeća tvrdjenja :

1) Grupoid s jednim elementom zadovoljava svaki algebarski zakon.
2) Svaki konačan grupoid ima netrivijalne zakone.
3) Svi konačni grupoidi reda n imaju zajedničke zakone.
4) Ne postoji zakon koji zadovoljavaju svi konačni grupoidi.
5) Postoji beskonačan (prebrojiv) grupoid koji ne zadovoljava nijedan zakon.

Navedimo dokaze tvrdjenja pod 3) , 4) , i 5) .

Dokaz tvrdjenja 3.

Dokazaćemo da postoji bar jedan algebarski zakon

$$u(x,y) = v(x,y)$$

(gde su u i v različiti termi , čije su sve promenljive x i y i operacijski simbol . ), koji zadovoljava svaki grupoid , koji ima tačno n elemenata ( n-dati prirodan broj) .

Dokaz.

U skup $G = \{g_1, g_2, \ldots, g_n\}$ može se na $n^{n^2}$ načina uvesti operacija $* : G \times G \to G$, tj. može ima $n^{n^2}$ grupoida $\mathcal{G}_i = (G, *_i)$ $(i = 1,2,\ldots,n^{n^2})$.

Obrazujemo klasu $K_o$ svih terma, u koje ulaze promenljive x,y i operacijski simbol . .

$$K_o = \{ x.y \ , \ y.x \ , \ x.(y.y) \ , \ y.(x.x) \ , \ \ldots \}$$

Nije teško uvideti da je klasa $K_o$ beskonačna.

Uzmimo sada grupoid $\mathcal{G}_1$ . Promenljive x i y interpretirajmo nekim parom elemenata iz G, a operacijski simbol . sa $*_1$ . Svaki term iz $K_o$ dobije pri toj interpretaciji odredjenu vrednost iz G. Iz konačnosti grupoida G i beskonačnosti klase $K_o$ sledi da postoji beskonačna klasa $K_1$ , u kojoj termi imaju istu vrednost. Sada uzmimo drugi par elemenata iz G i klasu $K_1$ itd. Kada iscrpimo sve parove iz G dolazimo do klase $K_{n^2}$ . Za grupoid $\mathcal{G}_2$ ponovimo opisani postupak uzimajući za polaznu klasu $K_{n^2}$ , ...,itd.

Konačno se dobije klasa $K_{n^{n^2}+2} = K$ . $(n^{n^2} . n^2 = n^{n^2+2})$ sa osobinom : Ma kako interpretirali promenljive x i y elementima iz G i operacijski simbol . elementima iz skupa $\{*_1, *_2, \ldots, *_{n^{n^2}}\}$ termi u K imaju jednake vrednosti. Ako su u(x,y) , v(x,y) bilo koja dva terma iz K onda očevidno je

$$u(x,y) = v(x,y)$$

traženi algebarski zakon.

Daćemo ideju dokaza za 4.

4. je ekvivalentna sa :

Za svaki netrivijalan zakon postoji konačan grupoid koji ne zadovoljava taj zakon .

Neka je zakon $x.y = y.(x.x)$.

Obrazovaćemo konačan grupoid koji ne zadovoljava taj zakon. Polazimo od skupa $\{a,b\}$ .

Polazeći od a i b i operacijskog simbola . kao i simbola ( i ) obrazujmo sve reči koje imaju najviše tri slova . To su reči :

a,b,(a.a),(a.b),(b.a),(b.b).(a.(a.a)),(b.(a.a)),(a.(a.b)), (b.(a.b)),(a.(b.a)),(b.(b.a)),(a.(b.b)),(b.(b.b)),((a.a).a), ((a.a).b),((a.b).a),((a.b).b),((b.a).a),((b.a).b),((b.b).a), ((b.b).b).

Elementi grupoida koji obrazujemo su navedene reči i simbol $\infty$.
Operaciju . definišemo na ovaj način

$$u.v = (u.v) \quad \text{ako je } (u.v) \text{ jedna od navedenih reči}$$
$$= \infty \quad \text{inače}$$

Takodje $\infty.v = u.\infty = \infty.\infty = \infty$
Dobijeni grupoid ne zadovoljava navedeni zakon, jer ako umesto x i y redom stavimo a i b dobijamo :

$$a . b = (a.b)$$
$$b.(a.a) = (b.(a.a))$$

odnosno $a.b \neq b.(a.a)$ jer su (a.b) i (b.(a.a)) različiti elementi .

Dokaz tvrdjenja 5.

Obrazujmo skup W svih terma u koje ulaze slova a i b, operacijski simbol . - dužine dva, kao i pomićni simboli ( i ) .
Skup W je minimalan skup koji zadovoljava uslove :
1) $a,b \in W$
2) $u,v \in W \Rightarrow (u.v) \in W$
Na primer

$$(a.a) , (b.(b.a)) , (((a.a).b).(a.b))$$

su elementi skupa W.
U skupu W uvodimo operaciju o na sledeći način :

$$u \circ v \overset{def}{=} (u . v)$$

Tako $a \circ b = (a . b)$ , $a \circ (a \circ b) = (a . (a . b))$.
Taj grupoid $\mathcal{W} = (W , o)$ je primer grupoida reči ( umesto $\{a,b\}$ mogli smo uzeti i bilo koji neprazan skup) .
Grupoid reči ne zadovoljava nikakav netrivijalan zakon (odnosno zakon različiti od zakona t = t , t je term).
Na primer, zakon $x \circ y = y \circ x$ nije zadovoljen jer uzimajući umesto x i y redom a i b imamo $a \circ b \neq b \circ a$ jer $a \circ b = (a.b)$ i $b \circ a = (b.a)$ a reči (a.b) i (b.a) su različite.

# VIŠEOPERACIJSKE GRUPE

Za algebru $\mathcal{G}$ kažemo da je višeoperacijska grupa, ili $\Omega$-grupa, ukoliko ima skupovni deo $G$, binarnu operaciju $+$ i skup $\Omega$ drugih operacija skupa $G$ i ako su pritom ispunjeni uslovi:

1) $(G,+)$ je grupa sa neutralnim elementom 0 (ova grupa nemora biti komutativna)

2) Ako operacija $w$ pripada skupu $\Omega$ i ako je $d(w) = n$ $(n \geqslant 1)$ tada je $w(0,0,\ldots,0) = 0$ .(*)

Jasno je da se višeoperacijska grupa svodi na običnu grupu ukoliko je $\Omega = \emptyset$, a na prsten ako je grupa $(G,+)$ komutativna i skup $\Omega$ se sastoji od samo jedne operacije i to binarne koja je sa operacijom $+$ vezana odgovarajućim distributivnim zakonima.

Svaka pod-algebra neke višeoperacijske grupe je takodje višeoperacijska grupa.

Takodje, dokazuje se kao za algebre, da je presek svih $\Omega$-podgrupa $\Omega$-grupe $G$ opet $\Omega$-podgrupa ( koja sadrži 0).

Svaka homomorfna slika $\Omega$-grupe $G$ je sama $\Omega$-grupa (označimo je sa $G'$).

Stvarno, ako je $\Omega$-grupa $G$ homomorfizmom $f$ preslikana na istotipnu univerzalnu algebru $G'$ tada je $f$ homomorfizam i za grupu $(G +)$ pa je zato algebra $G'$ i sama grupa u odnosu na odgovarajuću operaciju $+'$ (nulu ove grupe obeležimo sa $0'$ ). Dalje, pošto je $f$ homomorfizam, i $f(0) = 0'$ to za svaku operaciju $w' \in \Omega'$ važi zbog (*), $w'(0',0',\ldots,0') = 0'$ pa je grupa $G'$ stvarno $\Omega$-grupa.

Ideal višeoperacijske grupe čemo definisati analogno definiciji ideala prstena.

Definicija 1.

Kažemo da je ideal višeoperacijske grupe $G$ neprazan podskup skupa $G$ koji zadovoljava uslove :

1) $(I,+)$ je normalna podgrupa grupe $(G,+)$

2) Za svaku operaciju $w \in \Omega$ dužine $n$, i za sve $n$-torke $i_1, i_2, .., i_n$ iz $I$, i $x_1, x_2, \ldots, x_n$ iz $G$, važi :

$w( i_1 + x_1, i_2 + x_2, \ldots, i_n + x_n) - w(x_1, x_2, \ldots, x_n) \in I$ .

Ovako definisan ideal se poklapa sa normalnom podgrupom kod grupa jer tamo uslov 2) odpada.

Kod prstena se ovako uveden pojam ideala poklapa sa pojmom ideāla.

Uslov 2) u definiciji 1. se može zameniti sledećim uslovom :

$2')$ "Za svaku operaciju $w \in \Omega$ dužine $n$, i za svaku $n$-torku $x_1, .., x_n$ iz $G$ i svaki $i$ iz $I$ važi :

$w(x_1, x_2, \ldots, x_{k-1}, x_k + i, x_{k+1}, \ldots, x_n) - w(x_1, x_2, \ldots, x_n) \in I$ $(k=1,2,\ldots)$

Lako se dokazuje ekvivalentnost ove dve definicije.

Iz definicije ideala sledi da je svaki ideal I $\Omega$-grupe ustvari jedna $\Omega$-podgrupa te grupe. Stvarno, (I,+) je, zbog uslova 1), podgrupa grupe (G,+). Dalje, za svaku operaciju $w \in \Omega$ dužine n i svaku n-torku $i_1,i_2,\ldots,i_n$ iz I, pri $x_1=x_2=\ldots=x_n=0$, je, zbog (*) $w(i_1,i_2,\ldots,i_n) \in I$ i time je dokazano da je ideal I stvarno $\Omega$-grupa.

Višeoperacijsku grupu nazivamo prostom ako nema drugih ideala osim one podgrupe čiji je jedini element 0.

Lako se proverava da je presek svih ideala $\Omega$ grupe opet ideal.

Definicija 2.

Relaciju kongruencije po modulu ideala , kod višeoperacijske grupe, uvedemo na sledeći način: $x \equiv y \pmod I \iff x - y \in I$

Lako se dokazuje da ovako uvedena relacije je relacija ekvivalencije . Sada možemo govoriti o razbijanju $\Omega$-grupe na klase u odnosu na relaciju $\equiv \bmod I$ (tj. o razlganju $\Omega$grupe po idealu I) i pritom čemo to shvatati kao razlaganje grupe (G,+) po normalnoj pod grupi I.

(za neku relaciju ekvivalencije $\sim$ kažemo da je kongruencija $\Omega$-grupe ako je saglasna sa operacijom + i sa svakom operacijom $w \in \Omega$ , tj. ako je : $x_1 \sim y_1$ i $x_2 \sim y_2$ tada $x_1 + x_2 \sim y_1 + y_2$ i $x_1 \sim y_1, x_2 \sim y_2, \ldots, x_n \sim y_n$ tada $w(x_1,\ldots,x_n) \sim w(y_1,\ldots,y_n)$ .

Formulišimo i dokažimo stav o kongruencijam višeoperacijskih grupa :

Stav 1.

1) Ako je I ideal višeoperacijske grupe G onda je relacija $\equiv \bmod I$ kongruencija.
2) Ako je neka relacija $\sim$ kongruencija višeoperacijske grupe G onda ta višeoperacijska grupa ima bar jedan ideal I takav da je $\sim \; = \; \equiv \bmod I$.

Dokaz.

1) Već smo rekli da je relacija $\equiv \bmod I$ relacija ekvivalencije

Dokažimo još da je saglasna sa operacijom + i svim operacijama skupa $\Omega$. Pošto je (I,+) normalna podgrupa grupe (G,+) to je relacija $\equiv \bmod I$ saglasana sa operacijom + (to je dokazano prilikom dokazivanja ove teoreme za grupe).

Neka je w ma koja operacija iz skupa $\Omega$ dužine n. Treba još dokazati da važi :

$x_1 \equiv y_1 \pmod I$, $x_2 \equiv y_2 \pmod I$,..., $x_n \equiv y_n \pmod I$

$w(x_1,x_2,\ldots,x_n) \equiv w(y_1,y_2,\ldots,y_n) \pmod I$

Leva strana ove implikacije može da se napiše u obliku:

$x_1 - y_1 \in I$, $x_2 - y_2 \in I$,..., $x_n - y_n \in I$ tj. postoje elementi $i_1,\ldots,i_n \in I$

takvi da je :

$x_1 = y_1 + i_1$, $x_2 = y_2 + i_2$, ..., $x_n = y_n + i_n$ a to znači da je $w(x_1,x_2,...,x_n) = w(y_1 + i_1, y_2 + i_2, ..., y_n + i_n) \in w(y_1,y_2,...,y_n) + I$ odnsno $w(x_1,x_2,..,x_n) - w(y_1,y_2,..,y_n) \in I$ a ovo upravo nam daje $w(x_1,x_2,...,x_n) \equiv w(y_1,y_2,...y_n) \pmod I$ i time smo dokazali da je $\equiv \bmod I$ kongruencija.

2) Neka je relacija $\sim$ kongruencija $\Omega$-grupe G. Definišimo skup I ovako : $I \overset{def}{=} \{x \mid x \in G \text{ i } x \sim 0\}$ i dokažimo najpre da je I ideal $\Omega$-grupe G.

Prilikom dokazivanja odgovarajučeg stava za grupe, dokazali smo da je (I,+) normalna podgrupa grupe (G,+). Dokažimo da je zadovoljena i karakteristika 2) iz definicije ideala.

Neka je w ma koja operacija skupa $\Omega$ i neka je $d(w) = n$ $(n \geq 1)$. Ako je $i_1,i_2,...,i_n \in I$, a $x_1,x_2,...,x_n$ su ma koji elementi iz G, onda je : $i_1 \sim 0$, $i_2 \sim 0$, $i_3 \sim 0$, ..., $i_n \sim 0$ (1)

$$x_1 \sim x_1,\ x_2 \sim x_2, ..., x_n \sim x_n \qquad (2)$$

pa pošto je $\sim$ kongruencija, iz (1) i (2) sledi :

$i_1 + x_1 \sim x_1$, $i_2 + x_2 \sim x_2$, ..., $i_n + x_n \sim x_n$ i odavde, iz istog razloga, imamo $w(i_1 + x_1, i_2 + x_2, ..., i_n + x_n) \sim w(x_1,x_2,...,x_n)$ (3)

No, pošto je $-w(x_1,x_2,...,x_n) \sim -w(x_1,x_2,...,x_n)$ to odavde i iz (3) dobijamo : $w(i_1 + x_1, i_2 + x_2, .., i_n + x_n) - w(x_1,x_2,...,x_n) \sim 0$, tj. $w(i_1 + x_1, i_2 + x_2, ..., i_n + x_n) - w(x_1,x_2,...x_n) \in I$

Ovim smo dokazali da je I ideal. Dokažimo još da je $\sim = \equiv \bmod I$.

a) $x \sim y$ i $-y \sim -y \Rightarrow$ ... $0$ $x - y \in I \Rightarrow \sim \subseteq \equiv \bmod I$

b) $x \equiv y \pmod I \Rightarrow x - y \in I \Rightarrow x - y \sim 0 \Rightarrow x - y \sim 0$ i $y \sim y \Rightarrow$

$x \sim y \Rightarrow \equiv \bmod I \subseteq \sim$

a odavde sledi da $\sim = \equiv \bmod I$ .

Razlaganje $\Omega$-grupe G po kongruenciji ideala I, odnosno po idealu I, čemo označavati sa G/I.

Očevidno je da je ideal I nula ove $\Omega$-grupe G/I.

U $\Omega$-grupi G/A se definiše operacija $\oplus$ na sledeći način :

$(I + x_1) \oplus (I + x_2) = I + (x_1 + x_2)$ i $(I + x)^{-1} = (I + x^{-1})$

$\mathbb{W}(I + x_1, I + x_2, ..., I + x_n) = I + w(x_1,x_2,...,x_n)$ za svako $\mathbb{W}$ iz $\Omega$, gde su $\oplus$ i $\mathbb{W}$ operacije u G/I koje odgovaraju operacijama + i w u G.

Koristeći ranije dokazan stav o vezi izmedju homomorfizama i kongruencija univerzalne algebre kao i predhodni stav o vezi kongruencija $\Omega$grupe i nekog ideala, zaključujemo da važi sledeći stav :

Stav 2.

1) Neka je I ideal $\Omega$-grupe G i neka je G/I odgovarajuča količnička $\Omega$-grupa. Tada je $\Omega$-grupa G/I homomorfna slika $\Omega$-grupe G.

(jedan homomorfizam je tzv. prirodni homomorfizam : f : f(x) = Ix
2) Ako je $\Omega$-grupa G' homomorfna slika $\Omega$-grupe G tada $\Omega$-grupa G ima bar jedan ideal I takav da su $\Omega$-grupe G/I i G' medjusobom izomorfne.

Stav 3.

1) Neka je G proizvoljna $\Omega$-grupa, I njen ideal, a G'= G/I odgovarajuća količnička $\Omega$-grupa . Neka je B' proizvoljna $\Omega$-podgrupa $\Omega$-grupe G', a B potpun skup njenih originala u $\mathfrak{G}$ pri prirodnom homomorfizmu f : G$\to$G' tj. B je skup svih elemenata iz G koji leže u kosetima od kojih je načinjena $\Omega$ podgrupa B'. Tada je B $\Omega$-podgrupa u G.

2) Ako je data proizvoljna $\Omega$-grupa G, pri čemu B sadrži ideal iz G, tada je njena slika B'pri prirodnom homomorfizmu f: G$\to$G' jedna $\Omega$-podgrupa u G' i pritom je B potpun skup njenih originala.

Dokaz.

1) Dokažimo da iz x,y$\in$ B sledi x + y$\in$ B .
No, iz x,y$\in$B sledi I + x, I + y$\in$B'pa je I + (x+y) = (I+x)$\oplus$(I+y) - element iz B' te i x+y je iz B. Dalje, iz pretpostavke I-x = -(I+x)$\in$ B' sledi da i -x$\in$B kada x$\in$B. Prema formulaciji zadatka, u B se nalazi i neutralni element $\Theta$ u odnosu na operaciju +.
Za operaciju w$\in\Omega$, dužine n, n elemenata iz B u oznaci $x_1,..,x_n$ zbog toga što važi da je I + x$\in$B'i I + x = x + I (i=1,2,...,n) sledi : $I+W(x_1,x_2,...,x_n) = w((I + x_1),(I + x_2),...,(I + x_n))\in B'$ pa je $w(x_1,x_2,...,x_n) \in B$.
Dakle dokazali smo da je B $\Omega$ grupa.

2) Zaista, prirodni homomorfizam f : G$\to$G' inducira homomorfizam kojim se B$\in$ G preslikava na B'$\subset$G'. Na osnovu ranije dokazanog stava, B'je $\Omega$ podgrupa u G'. Dalje, iz L$\in$ B sledi da se svaki element koji je u nekom kosetu iz B', nalazi u B pa je zato B potpun skup originala $\Omega$ grupe B'.

## SLOBODNE UNIVERZALNE ALGEBRE . STRUKTURNE JEDNAKOSTI.

Upoznaćemo jedan metod kojim se mogu opisati (a u nekim slučajevima i konstruisati) sve univerzalne algebre koje zadovoljavaju odredjenu klasu algebarskih zakona.

Navodimo prethodno jedan primer.

Neka je klasa algebarskih zakona sledeći skup:

$$Z = \{(x.x) = x,\ (x.y) = (y.x),\ (x.(y.z)) = ((x.y).z)\}$$

Obrazovaćemo tzv. slobodan grupoid generisan slobodnim generatornim elementima a i b koji zadovoljava sve zakone iz Z.

Postupak koji ćemo ovde izložiti analogan je postupku koji se primenjuje u opštem skučaju.

1) Obrazujemo grupoid reči koji smo razmatrali u prethodnoj tački. Skupovni deo tog grupoida je :

$$W = \{a, b, (a.b), (b.a), (a.a), (a.(b.(a.b))), \ldots\}$$

tj. skup terma obrazovanih pomoću slova a i b i operacijskog simbola . dužine dva.

U skupu W uvodimo operaciju $\theta$ dužine dva na sledeći način :

$$u, v \in W \quad u \,\theta\, v \overset{def}{=} (u.v)$$

Znači , za dve reči u i v iz skupa W rezultat je reč (u.v).

Na primer za reči (a.b) i (a.a) imamo $(a.b)\theta(a.a) = ((a.b).(a.a))$

Grupoid reči je onda $\mathcal{W} = (W, \theta)$.

Taj grupoid ne zadovoljava nikakav zakon sem (trivijalnog) zakona u = u.

U grupoidu $\mathcal{W}$ definišemo relaciju $\sim$ (zvačemo je "kongruencija po modulu klase zakona Z" i označavati $\equiv \pmod{Z}$) na sledeći način :

Za dve reči u i v reći ćemo da su ekvivalentne (pišemo $u \sim v$) ako se od reči u može preći na reč v konačnom primenom zakona Z.

Ta relacija je relacija ekvivalencije skupa W.

Dokažimo da su zadovoljeni uslovi koji definišu relaciju ekvivalencije :

a) Refleksivnost. $u \sim u$ je ispunjeno (broj primena zakona je nula)

b) Simetričnost. Ako je $u \sim v$ onda je $v \sim u$. Ovo neposredno sledi iz reverzibilnosti procesa primene zakona Z.

c) Tranzitivnost. $u \sim v$ i $v \sim w$ povlači $u \sim w$. Zaista, od u možemo preći na v konačnom primenom zakona Z, na isti način od v na w, što znači da smo od u na w prešli konačnom primenom zakona Z.

Uvedena relacija $\sim$ je i kongruencija za $\mathcal{W}$. Zaista, neka je $u_1 \sim v_1$ i $u_2 \sim v_2$. Treba dokazati da je $u_1 \theta u_2 \sim v_1 \theta v_2$ tj. $(u_1.u_2) \sim (v_1.v_2)$.

Kako je $u_1 \sim v_1$ to od reči $(u_1.u_2)$ možemo preći na reč $(v_1.u_2)$ konačnom primenom zakona Z, pa je $(u_1.u_2) \sim (v_1.u_2)$ (1)
Iz pretpostavke $u_2 \sim v_2$ analogno sledi $(v_1.u_2) \sim (v_1.v_2)$ (2)
Na osnovu tranzitivnosti iz (1) i (2) sledi tvrdjenje.
U našem primeru sve reči koje sadrže samo a ekvivalentne su reči a , a one koje sadrže samo b ekvivalentne su sa b. Ako neka reč sadrži i slova a i slova b onda je primenom drugog i trećeg zakona možemo svesti na ekvivalentnu reč, kod koje prvo dolaze a-ovi pa onda b-ovi. Zbog prvog i trećeg zakona ova je reč ekvivalentna sa (a.b).
Iz svega sledi da je skup-količnik $W/_{\sim} = \{Ca, Cb, Ca.b\}$.
Dokažimo da su klase Ca,Cb,Ca.b, različite. Zbog jednakoslovnosti zakona Z prelaskom od reči u na njoj ekvivalentnu reč v skup slova koja ulaze u reč u ostaje nepromenjen. Stoga su klase Ca,Cb,Ca.b zaista različite.
Količnik grupoid $W/_{\sim}$ nazivamo slobodan grupoid klase Z nad skupom $\Gamma$ ($\Gamma = \{a,b\}$)
Njegova Cayley-va tablica je :

| $\ominus$ | Ca | Cb | Ca.b |
|---|---|---|---|
| Ca | Ca | Ca.b | Ca.b |
| Cb | Ca.b | Cb | Ca.b |
| Ca.b | Ca.b | Ca.b | Ca.b |

(*)

Dobijeni grupoid zadovoljava zakone Z.
Zaista, neka su Cu,Cv,Cw, neki elementi tog grupoida. Tada :
$Cu \ominus Cu = Cu.u = Cu$
$Cu \ominus Cv = Cu.v = Cv.u = Cv \ominus Cu$
$(Cu \ominus Cv) \ominus Cw = C((u.v).w) = C(u.(v.w) = Cu \ominus (Cv \ominus Cw)$
jer su reči u i (u.u), (u.v) i (v.u), (u.(v.w)) i((u.v).w) ekvivalentne (u paru).
Da su klase Ca,Cb,Ca.b medju sobom različite možemo zaključiti i na sledeći način :
Pretpostavimo da ne znamo da su Ca,Cb,Ca.b tri različite klase i da smo obrazovali tablicu (*) koristeći definiciju
$Cu \ominus Cv \overset{df}{=} Cu.v$
Dobijena tablica nas inspiriše da uvedemo sledeći grupoid :

| * | 1 | 2 | 3 |
|---|---|---|---|
| 1 | 1 | 3 | 3 |
| 2 | 3 | 2 | 3 |
| 3 | 3 | 3 | 3 |

(Ta druga tablica je obrazovana pomoću prve "zamenjivanjem Ca,Cb,Ca.b redom sa 1,2,3").

<u>Tvrdimo da su klase Ca,Cb,Ca.b različite ukoliko dobijeni grupoid zadovoljava zakone Z.</u>

Inače, u ovom slučaju, neposredno proveravamo da taj grupoid zaista zadovoljava zakone Z.

Pretpostavimo na primer Ca = Cb.

U tom slučaju postoji izvestan niz $a\, u_1 u_2 \ldots u_n\, b$ čiji je prvi član a, poslednji b, takav da se na idući član prelazi jednom primenom izvesnog zakona Z. Pretpostavimo da se u tom nizu a i b zamene sa 1 i 2. Tako se dolazi do izvesnog niza $1\, \bar{u}_1\, \bar{u}_2 \ldots \bar{u}_n\, 2$. Ako još . interpretiramo kao $*$, onda pošto grupoid $(\{1,2,3\}, *)$ zadovoljava zakone Z, dobijamo $1 = \bar{u}_1$, $\bar{u}_1 = \bar{u}_2, \ldots, \bar{u}_n = 2$ što je kontradikcija.

Slično pretpostavka Ca = Ca.b dovodi do 1 = 3, a pretpostavka Cb = Ca.b , do 2 = 3.

Navedeni postupak utvrdjivanja različitosti elemenata slobodne strukture pomoću pomoćne ("Šifrirane") strukture je vrlo opšti i biće i dalje korišćen. Elemente pomoćne strukture zovemo u daljem kanonski predstavnici.

Prelazimo na opšti slučaj.

Neka je data klasa Z zakona, neka je $\Gamma = \{\delta_i / \ i \in I\}$ skup slobodnih generatornih elemenata, zatim $A = \{a_k / \ k \in K\}$ skup konstanti (shvatamo ih kao nularne operacije), koje učestvuju u zakonima Z. Neka je dalje $\Omega = \{w_j / \ j \in J\}$ skup svih operacijskih slova, koja ulaze u zakone Z.

1) Uočavamo skup $\Gamma \cup A = G$. Taj skup zovemo polazni alfabet.

2) Definišemo skup W na sledeći način :

   a) $\delta_i (i \in I)$ i $a_k (k \in K)$ su u skupu W.

   b) Ako su $t_1, t_2, \ldots, t_n \in W$, $w \in \Omega$ operacijsko slovo dužine n, onda je $w(t_1, t_2, \ldots, t_n) \in W$

   c) Elementi skupa W su samo one reči koje su odredjene uslovima a i b .

U skupu W definišemo operacije na sledeći način.

   a) Svaku konstantu $a_k \in W$ uzimamo za nularnu operaciju skupa W.

   b) Operacijskom simbolu $w \in \Omega$ dužine n ($n \geq 1$) dodeljujemo operaciju $\mathfrak{w}$ iste dužine , definisanu pomoću $\mathfrak{w}(t_1, t_2, \ldots t_n) \overset{def}{=} w(t_1, t_2, \ldots, t_n)$, gde su $t_1, t_2, \ldots, t_n \in W$.

Dobijena algebra reči $\mathcal{W}$ ne zadovoljava nikakav algebarski zakon sem trivijalnog t = t, gde je t neki term. Primetimo da zakoni Z do sada nisu imali skoro nikakvu ulogu. U vezi sa tim zakonima uvodimo jednu relaciju ekvivalencije skupa W, koja je, u stvari, kongruencija algebre $\mathcal{W}$.

Definicija 1.

Reč $t_2$ je ekvivalentna sa reči $t_1$ (pišemo $t_1 \sim t_2$) ako se reč $t_1$ može dobiti iz $t_2$ konačnom primenom zakona Z što znači da postoji niz $t_1 t' t'' \ldots t^n t_2$, tako da se od jednog člana prelazi na sledeći jednom primenom samo jednog zakona. Pri tome uzimamo da je $t_1 \sim t_1$. Uvedena relacija je relacija ekvivalencij što se neposredno proverava (kao u prethodnom primeru). Dokažimo da je ona i kongruencija algebre $\mathcal{W}$. Neka je $w \in \Omega$ bilo koje operacijsko slovo dužine n . Odgovarajuća operacija u $\mathcal{W}$ je $\mathfrak{W}$ (takodje dužine n).

Neka je $u_\nu \sim v_\nu$ ($\nu = 1,2,\ldots,n$) i dokažimo da je

$$\mathfrak{W}(u_1,u_2,\ldots,u_n) \sim \mathfrak{W}(v_1,v_2,\ldots,v_n), \text{ tj.}$$

$$w(u_1,u_2,\ldots,u_n) \sim w(v_1,v_2,\ldots,v_n) \qquad (*)$$

Kako se od reči u prelazi na v konačnom primenom zakona Z to isto važi i za reči $w(u_1,u_2,\ldots,u_n)$ i $w(v_1,v_2,\ldots,v_n)$, pa je

$$w(u_1,u_2,\ldots,u_n) \sim w(v_1,u_2,\ldots,u_n) \qquad (1)$$

slično nalazimo

$$w(v_1,u_2,\ldots,u_n) \sim w(v_1,v_2,\ldots,u_n) \qquad (2)$$

$$\ldots\ldots\ldots \qquad \ldots$$

$$w(v_1,v_2,\ldots,u_n) \sim w(v_1,v_2,\ldots,v_n) \qquad (n)$$

Iz (1),(2),...,(n) na osnovu tranzitivnosti relacije $\sim$ sledi (*) što je trebalo dokazati.

Količničku strukturu $\mathcal{W}/\sim$ zovemo <u>slobodna univerzalna algebra klase Z nad skupom $\Gamma$ slobodnih generatornih elemenata.</u> Tako nazivamo i svaku njoj izomorfnu strukturu.

Inače, elementi količničke strukture su klase Ct ($t \in W$), a operacije su :

a) Ca - nularne operacije

b) Svakoj operaciji w, odnosno $\mathfrak{W}$, odgovara operacija $\Theta$

$$\Theta(Ct_1,Ct_2,\ldots,Ct_n) = C\mathfrak{W}(t_1,t_2,\ldots,t_n) \text{ tj.}$$

$$\Theta(Ct_1,Ct_2,\ldots,Ct_n) = C_{w(t_1,t_2,\ldots,t_n)}$$

Dokažimo da algebra $\mathcal{W}/\sim$ zadodoljava zakone Z.

Neka je $t_1 = t_2$ (**) proizvoljan zakon iz Z.

Neka su $x,\ldots,a,\ldots,w,\ldots$ redom promenljive, konstante i operacijska slova koja učestvuju u pomenutom zakonu. Terme $t_1$ i $t_2$ označimo $t_1\{x,\ldots a,\ldots w,\ldots\}$ , $t_2\{x,\ldots a,\ldots w,\ldots\}$

Treba dokazati de je

$$t_1\{Ct,\ldots Ca,\ldots \Theta,\ldots\} = t_2\{Ct,\ldots Ca,\ldots \Theta,\ldots\}$$

što je s obzirom na definicju operacija u $\mathcal{W}/\sim$ ekvivalentno sa

$$C_{t_1}\{t,\ldots a,\ldots w,\ldots\} = C_{t_2}\{t,\ldots a,\ldots w,\ldots\} \quad (***)$$

gde su t,... proizvoljne reči iz W.

Kako je $t_1\{t,\ldots a,\ldots w,\ldots\} \sim t_2\{t,\ldots a,\ldots w,\ldots\}$ (od $t_1$ se prelazi na $t_2$ jednom primenom zakona (**) tj. zaista važi (***) , što je i trebalo dokazati.

U primeru koji smo na početku naveli utvrdili smo efektivno koji su elementi slobodnog grupoida. Odnosno u tom slučaju za relaciju $\sim$ (ekvivalentnost reči) imamo određen algoritam pomoću koga se za bilo koje dve reči u i v može utvrditi da li $u \sim v$ ili $u \not\sim v$ .

Jedan takav algoritam izlazi iz činjenice :

$u \sim v \Leftrightarrow$ skup slova reči u = skup slova reči v

Međutim u opštem slučaju za relaciju $\sim$ ne može se naći odgovarajući algoritam. Može se navesti primer relacije $\sim$ za koju ne postoji nikakav algoritam "prepoznavanja ekvivalentnosti reči". Problem postojanja navedenog algoritma zove se problem reči. Inače slobodna univerzalna algebra obrazovana na izloženi način egzistira (u matematičkom smislu ).

Primetimo da skup $\Gamma$ može biti prazan, ali skup $\Gamma \cup A = G$ (polazni alfabet) ne može biti prazan. Ilustrujmo to na primeru.

Neka je skup zakona Z sledeći skup

$Z = \{(1.1)=1,\ (1.2)=2,\ (2.1)=2,\ (2.2)=1\}$

Zatim

$\Gamma \neq \emptyset$ , $G = \Gamma \cup A = \{1,2\} = A$.

Rezultat je struktura čiji je skupovni deo $\{C_1, C_2\}$ i koja ima sledeće operacije : $\Theta$ dužine 2, i nularne operacije $C_1, C_2$.

Cayleyeva tablica operacije $\Theta$ je

| $\Theta$ | $C_1$ | $C_2$ |
|---|---|---|
| $C_1$ | $C_1$ | $C_2$ |
| $C_2$ | $C_2$ | $C_1$ |

Pošto i izomorfnu strukturu uzimamo kao slobodnu možemo i sledeće zaključiti :

Rezultat je struktura koja se dobija od grupoida $(\{1,2\}, *)$

| $*$ | 1 | 2 |
|---|---|---|
| 1 | 1 | 2 |
| 2 | 2 | 1 |

uzimanjem svih njegovih elemenata za nularne operacije.

U stvari i u opštem slučaju , ako je $\mathcal{A}$ bilo koja univerzalna algebra onda je algebarska struktura $\mathcal{B}$ , dobijena iz nje uzimanjem svih elemenata algebre $\mathcal{A}$ za nularne operacije, slobodna. Naravno, strukture $\mathcal{A}$ i $\mathcal{B}$ zadovoljavaju iste zakone.

Primeri slobodnih univerzalnih algebri.

1) Slobodna semi-grupa.

Neka je $\Gamma$ izvestan neprazan skup i neka klasa Z sadrži jedino asocijativni zakon : $(x.(y.z)) = ((x.y).z)$.
Odgovarajuću slobodnu algebru zovemo slobodna semigrupa nad skupom $\Gamma$.
U ovom slučaju skup W je odredjen uslovima :
$\Gamma \subseteq W$ , $u,v \in W \Rightarrow (u.v) \in W$.
Operacija $\Theta$ je definisana pomoću : $u,v \in W$ , $u \Theta v \overset{def}{=} (u.v)$.
Pošto uopšteni asocijativni zakon je posledica asocijativnog zakona to su svake dve reči sa istim slovima u istom redu medju sobom ekvivalentne. Na primer, ako $a,b,c,d \in \Gamma$ onda je reč $((a.b).((c.d).a))$ ekvivalentna reči $((a.((b.).d)).a)$. Svaka reč iz W je ekvivalentna sa izvesnom reči oblika $(\ldots((u_1.u_2).u_3)\ldots u_n)$ gde $n = 1,2,\ldots$ i gde $u_i \in \Gamma$.
Ove reči (tzv. proizvodi $\prod_{i=1}^{n} u_i$ ) označavamo, dogovorno $u_1u_2u_3\ldots u_n$
Na primer, reč $(((a.b).c).a)$ ima oznaku abca.
Reč $u_1u_2\ldots u_n$ zovemo kanonski predstavnik(svoje klase.
Elementi slobodne semigrupe su klase tih predstavnika $C_{u_1u_2\ldots u_n}$
Očigledno, prema opštoj definiciji $\Theta$ , imamo,

$$C_{u_1u_2\ldots u_n} \Theta C_{v_1v_2\ldots v_m} = C_{u_1u_2\ldots u_nv_1v_2\ldots v_m}.$$

Pitanje je koji su (različiti) elementi slobodne semigrupe, odnosno da li svaka klasa ima tačno jednog kanonskog predstavnika.
Dakle, da li :

$$C_{u_1u_2\ldots u_n} = C_{v_1v_2\ldots v_m} \qquad u_1u_2\ldots u_n = v_1v_2\ldots v_n .$$

Odgovor je potvrdan što se zaključuje iz činjenice : pomoćni grupoid G čiji su elementi reči $u_1u_2\ldots u_n$ , a operacija $\ast$ :

(1) $u_1u_2\ldots u_n \ast v_1v_2\ldots v_m = u_1u_2\ldots u_nv_1v_2\ldots v_m$

zadovoljava asocijativni zakon.
Taj grupoid je izomorfan sa dobijenom slobodnom semigrupom.
Iz toga razloga često se slobodna semigrupa $\mathcal{S}$ nad $\Gamma$ definiše na sledeći način.
Skupovni deo semigrupe $\mathcal{S}$ čine sve reči dužine 1,2,3,... nad alfabetom $\Gamma$. Operacija te semigrupe je definisana jednakošću (1) - tzv. konkatenacija (dopisivanje).

2)Slobodna grupa.

Neka je $\Gamma$ izvestan skup i neka se Z sastoji iz zakona : $(x.(y.z)) = ((x.y).z), (x.e) = x, (x,x') = e$

gde su : . - operacijski simbol dužine 2, ′- operacijski simbol dužine 1, e - konstanta.

Slobodna univerzalna algebra klase Z nad skupom $\Gamma$ zove se slobodna grupa nad $\Gamma$.

Skup W je u ovom slučaju odredjen uslovima :

1. $e \in W$ , $\Gamma \subseteq W$
2. $u,v \in W \quad (u.v) \in W$ , $u' \in W$ .

Struktura $\mathcal{W}$ ima operacije 0, :

$$u\ 0\ v = (u.v) \ , \quad u^0 = u'$$

i operaciju dužine 0 - element e.

Sledeći zakoni su posledice zakona Z :

$(e.x) = x$ , $(x'.x) = e$ , $x'' = x$ , $(x.y)' = y'.x'$.

Označimo sa $\Gamma'$ skup svih reči $\delta'$ gde $\delta \in \Gamma$ , a sa $u_1u_2u_3...u_n$ reč $(...((u_1.u_2).u_3)....,u_n)$.

Svaka reč iz W ekvivalentna je ( u odnosu na zakone Z ) sa nekom reči oblika $u_1u_2...u_n$ gde $u_i \in \Gamma \cup \Gamma' \cup \{e\}$

Pretpostavimo da za neko i, $u_i$ i $u_{i+1}$ su redom $\delta$ i $\delta'$ gde je $\delta$ izvestan element iz $\Gamma$ ,

Reč $u_1u_2...u_n$ ekvivalentna je sa reči $u_1u_2...u_{i-1}u_{i+2}...u_n$ . Isto važi i ukoliko su $u_i$ i $u_{i+1}$ redom $\delta'$ i $\delta$. Za reč $u_1u_2...u_{i-1}u_{i+2}...u_n$ kažemo da je dobijena iz reči $u_1u_2...u_n$ jednim skraćivanjem ( u stvari primenjeni su zakoni $(x'.x) = e$ , $(x.x') = e$ , $(x.e) = x$ , kao i asocijativni zakon ).

Označimo sa $S(u_1u_2...u_n)$ reč dobijenu iz reči $u_1u_2...u_n$ posle izvršenih svih skraćivanja ( koja su obavljena izvesnim redosledom - na primer "s leva na desno ".)

Primeri :

$S(baa'b'b'cc') = S(bb'b'cc') = S(b'cc') = b'$ .

$S(c'b'a'abc) = S(c'b'bc) = S(c'c) = e$ .

$S(aaa'bacc'cc) = abacc$ .

Reči $S(u_1u_2...u_n)$ nazovimo kanonski predstavnici.

U te reči dolazi reč e kao i svaka reč oblika

$$v_1v_2...v_k \quad (v_i \in \Gamma \cup \Gamma')$$

gde $v_i$ i $v_{i+1}$ nisu oblika $\delta$ i $\delta'$ ili $\delta'$ i $\delta$ za neko $\delta \in \Gamma$ .

Elementi količničke strukture $\mathcal{W}/\sim$ - odnosno slobodne grupe su klase ekvivalencije i u svakoj od tih klasa nalazi se bar po jedna reč koja je kanonski predstavnik .

Operacije te strukture su :

$\theta$ : $C_{u_1u_2\ldots u_n}\ \theta\ C_{v_1v_2\ldots v_k} = C_{S(u_1u_2\ldots u_nv_1v_2\ldots v_k)}$

$\theta$ : $(C_{u_1u_2\ldots u_n})^{-1} = C_{u_n'u_{n-1}'\ldots u_2'u_1'}$

($u_1u_2\ldots u_n, v_1v_2\ldots v_k$ su kanonski predstavnici ; ovde $u_i'$ je $\delta'$ ili $\delta$ prema tome da li je $u_i = \delta$ ili $u_i = \delta'$ )

$C_e$ - nularna operacija.

Pitanje je da li svaka klasa sadrži tačno po jedan kanonski predstavnik, odnosno da li važi :

(*) $C_{u_1u_2\ldots u_n} = C_{v_1v_2\ldots v_m} \iff u_1u_2\ldots u_n = v_1v_2\ldots v_m$

gde su $u_1u_2\ldots u_n$ , $v_1v_2\ldots v_m$ kanonski predstavnici.

Odgovor je potvrdan i to se zaključuje na sličan način kao kod semigrupa .

Uočimo skup K svih kanonskih predstavnika i u tom skupu definišimo operaciju $*$ na sledeći način :

$u_1u_2\ldots u_n * v_1v_2\ldots v_m \overset{def}{=} S(u_1u_2\ldots u_nv_1v_2\ldots v_m)$

Operaciju dužine 1 , u oznaci $^{-1}$ , uvodimo pomoću jednakosti :

$(u_1u_2\ldots u_n)^{-1} \overset{def}{=} u_n'u_{n-1}'\ldots u_1'$

($u_i'$ je $\delta'$ ili $\delta$ gde $\delta \in \Gamma$ , prema tome da li je $u_i = \delta'$ ili $u_i = \delta$ ).

Reč e je , po definiciji , nularna operacija skupa K.

Struktura $\mathcal{K} = (K, *, ^{-1}, e)$ je, što se može neposredno dokazati, grupa.

Grupa $\mathcal{K}$ je izomorfna sa količničkom strukturom $\mathcal{W}/\sim$ .

Grupa $\mathcal{K}$ je, prema tome, slobodna grupa nad skupom $\Gamma$ .

Napomenimo da je $\mathcal{K}$ sa jednim elementom ako je $\Gamma = \emptyset$ i da je ona beskonačna ciklična grupa ukoliko $\Gamma$ ima tačno jedan element.

Ako je $\Gamma = \{a,b\}$ onda su izvesni elementi grupe $\mathcal{K}$ sledeći :

a , e , aababbba'a', a'a'a'bbbaaaa ...

3) Neka skup zakona Z ima elemente :

$(x.(y.z)) = ((x.y).z)$

$(x.e) = x$

$(x.x') = e$

$(\alpha.\beta) = (\beta.\alpha)$

$(\alpha.\alpha) = e$

$(\beta.\beta) = e$

(e , $\alpha$, $\beta$ - konstante, . - operacisjki simbol dužine 2 i ' - operacijski simbol dužine 1 ).

Neka je $\Gamma = \emptyset$ . Tada polazni alfabet ima elemente $e,\alpha,\beta$, a skup W je odredjen na sledeći način :

(1) $e,\alpha,\beta \in W$ (2) $u,v \in W \Rightarrow (u.v) \in W$ , $u' \in W$.

Svakareč je ekvivalentna sa jednom od reči $e, \alpha, \beta, (\alpha.\beta)$ .

Te reči su kanonski predstavnici.

Operacije ◎ i ◎ imaju tablice :

| ◎ | $C_e$ | $C_\alpha$ | $C_\beta$ | $C_{(\alpha.\beta)}$ |
|---|---|---|---|---|
| $C_e$ | $C_e$ | $C_\alpha$ | $C_\beta$ | $C_{(\alpha.\beta)}$ |
| $C_\alpha$ | $C_\alpha$ | $C_e$ | $C_{(\alpha.\beta)}$ | $C_\beta$ |
| $C_\beta$ | $C_\beta$ | $C_{(\alpha.\beta)}$ | $C_e$ | $C_\alpha$ |
| $C_{(\alpha.\beta)}$ | $C_{(\alpha.\beta)}$ | $C_\beta$ | $C_\alpha$ | $C_e$ |

| | ◎ |
|---|---|
| $C_e$ | $C_e$ |
| $C_\alpha$ | $C_\alpha$ |
| $C_\beta$ | $C_\beta$ |
| $C_{(\alpha.\beta)}$ | $C_{(\alpha.\beta)}$ |

Klase $C_e$ , $C_\alpha$ , $C_\beta$ su nularne operacije.

Dobijene klase su različite jer skup $\{e, \alpha, \beta, (\alpha.\beta)\}$ u odnosu na operacije

| $\times$ | $e$ | $\alpha$ | $\beta$ | $(\alpha.\beta)$ |
|---|---|---|---|---|
| $e$ | $e$ | $\alpha$ | $\beta$ | $(\alpha.\beta)$ |
| $\alpha$ | $\alpha$ | $e$ | $(\alpha.\beta)$ | $\beta$ |
| $\beta$ | $\beta$ | $(\alpha.\beta)$ | $e$ | $\alpha$ |
| $(\alpha.\beta)$ | $(\alpha.\beta)$ | $\beta$ | $\alpha$ | $e$ |

| | $-1$ |
|---|---|
| $e$ | $e$ |
| $\alpha$ | $\alpha$ |
| $\beta$ | $\beta$ |
| $(\alpha.\beta)$ | $(\alpha.\beta)$ |

čini strukturu koja zadovoljava date zakone. Tablicom $\times$ je definisana grupa - ona je izomorfna sa poznatom Kleinovom četvornom grupom permutacija (1) , (12)(34) , (13)(24) , (14)(23) .

Krajnji rezultat je struktura $\mathcal{H}$ čiji su elementi $C_e$ , $C_\alpha$ , $C_\beta$ , $C_{(\alpha\beta)}$ i operacije ◎, ◎, $C_e$, $C_\alpha$ , $C_\beta$ , $C_{(\alpha.\beta)}$. Označimo sa $\mathcal{G}$ strukturu koja ima iste elemente i čije su operacije ◎, ◎ $C_e$. Ta struktura je grupa. Kažemo da ta grupa ima <u>strukturne jednakosti</u>

$$(\alpha.\beta) = (\beta.\alpha) \ , \ (\alpha.\alpha) = e \ , \ (\beta.\beta) = e.$$

<u>Strukturne jednakosti.</u>

Pretpostavimo da je klasa zakona Z unija dve klase zakona $Z_1$ i $Z_2$. Neka klasa $Z_2$ u svojim zakonima ne sadrži nijednu promenljivu već samo neke konstante. Neka, dalje, nijedna od tih konstanti ne ulazi u zakone $Z_1$. Označimo sa $A_1$ i $A_2$ skupove svih konstanti koje ulaze u zakone $Z_1$ odnosno $Z_2$.

Neka je $\mathcal{A}$ slobodna univerzalna algebra klase Z nad skupom $\Gamma = \emptyset$ . Za tu algebru je polazni alfabet $A_1 \cup A_2$.

Označimo sa $\mathcal{B}$ univerzalnu algebru koja ima iste elemente kao algebra $\mathcal{A}$ i iste operacije dužina 1,2,...kao ta algebra, ali čije su nularne operacije jedino $C_a$ gde je $a \in A_1 \setminus A_2$.

<u>Za algebru $\mathcal{B}$ kažemo da je univerzalna algebra klase Z sa klasom strukturnih jednakosti $Z_2$ .</u>

Navodimo primere. U tim primerima koristićemo izvesne uobičajne dogovore označavanja reči, kao na primer : reč $((u.u).u)$ označavamo $u^3$ , reč e označavamo $u^0$ u slučaju grupe .

Primer 1.

Konstruisati semi grupu koja ima strukturne jednakosti

$$a^2 = a \ , \quad ab = ba \ , \quad ac = ca \ , \quad bc = c \quad (Z_2)$$

Primetimo da je u ovom skučaju $Z_1 = \{x(yz) = (xy)z\}$ .

Skup W reči je $W = \{a, a^2, \ldots, ab, ba, \ldots, abc, bc, ca, \ldots\}$ .

S obzirom na jednakosti $Z_2$ svaku reč iz W možemo svesti na oblik

$a^{\alpha} c^{\gamma} b^{\beta}$ ( $\alpha \in \{0,1\}$ , $\beta, \gamma \in \{0,1,2,\ldots\}$ )

(pri tome ne može biti $\alpha = \beta = \gamma = 0$ ) jer sve a-ove možemo staviti na početak, a svaki b koji se nadje ispred c nestaje. Na taj način smo izdvojili kanonske predstavnike i opisali sve klase.

Proizvod dve klase je :

$$C_{a^{\alpha_1} b^{\beta_1} c^{\gamma_1}} \circledcirc C_{a^{\alpha_2} b^{\beta_2} c^{\gamma_2}} = \begin{cases} C_{a^{(\alpha_1+\alpha_2)'} c^{\gamma_1+\gamma_2} b^{\beta_2}} & \text{za } \gamma_2 > 0 \\ C_{a^{(\alpha_1+\alpha_2)'} c^{\gamma_1} b^{\beta_1+\beta_2}} & \text{za } \gamma_2 = 0 \end{cases}$$

gde $(\alpha_1 + \alpha_2)'$ znači svodjenje mod 2.

Količnička struktura je $W/\sim \; = \{ C_{a^{\alpha} c^{\gamma} b^{\beta}} / \; \alpha \in \{0,1\}, \; \beta, \gamma \in \{0,1,2,\ldots\}, \circledcirc \}$.

Primer 2.

Konstruisati grupu sa strukturnim jednakostima :

$$i^4 = 1 \ , \quad j^4 = 1 \ , \quad i^2 = j^2 \ , \quad i.j.i = j \ .$$

Klase su $C_1$ , $C_i$ , $C_j$ , $C_{i^{-1}}$, $C_{j^{-1}}$, $C_{j^{-1}i^{-1}}$, $C_{i^2}$ .

Uvodeći za ij , $i^{-1}$ , $j^{-1}$ , $j^{-1}i^{-1}$, $i^2$ redom oznake k, -i, -j , -k , -l , dobijemo klase :

$$C_1 \ , \ C_i \ , \ C_j \ , \ C_k \ , \ C_{-i} \ , \ C_{-j} \ , \ C_{-k} \ , \ C_{-l} \ ,$$

kojima odgovara sledeća Cayleyeva tablica :

| $\circledcirc$ | $C_1$ | $C_{-1}$ | $C_{-i}$ | $C_i$ | $C_{-j}$ | $C_j$ | $C_{-k}$ | $C_k$ |
|---|---|---|---|---|---|---|---|---|
| $C_1$ | $C_1$ | $C_{-1}$ | $C_{-i}$ | $C_i$ | $C_{-j}$ | $C_j$ | $C_{-k}$ | $C_k$ |
| $C_{-1}$ | $C_{-1}$ | $C_1$ | $C_i$ | $C_{-i}$ | $C_j$ | $C_{-j}$ | $C_k$ | $C_{-k}$ |
| $C_{-i}$ | $C_{-i}$ | $C_i$ | $C_{-1}$ | $C_1$ | $C_k$ | $C_{-k}$ | $C_{-j}$ | $C_j$ |
| $C_i$ | $C_i$ | $C_{-i}$ | $C_1$ | $C_{-1}$ | $C_{-k}$ | $C_k$ | $C_j$ | $C_{-j}$ |
| $C_{-j}$ | $C_{-j}$ | $C_j$ | $C_{-k}$ | $C_k$ | $C_{-1}$ | $C_1$ | $C_i$ | $C_{-i}$ |
| $C_j$ | $C_j$ | $C_{-j}$ | $C_k$ | $C_{-k}$ | $C_1$ | $C_{-1}$ | $C_{-i}$ | $C_i$ |
| $C_{-k}$ | $C_{-k}$ | $C_k$ | $C_j$ | $C_{-j}$ | $C_{-i}$ | $C_i$ | $C_{-1}$ | $C_1$ |
| $C_k$ | $C_k$ | $C_{-k}$ | $C_{-j}$ | $C_j$ | $C_i$ | $C_{-i}$ | $C_1$ | $C_{-1}$ |

Dobijena grupa zove se grupa Kvaterniona.

Primer 3.

Konstruisati grupu čije su strukturne jednakosti :

$$a^3 = e \ , \quad b^2 = e \ , \quad ba = a^2 b \ .$$

Skup količnik je

$$W/\sim \; = \{C_a, \; C_{a^2}, C_e \ , C_b \ , C_{ab}, C_{a^2 b}\}$$

Dobijena grupa, (tzv, grupa $S_3$) ima sledeću multiplikacionu tablicu :

| | $C_e$ | $C_a$ | $C_{a^2}$ | $C_b$ | $C_{ab}$ | $C_{a^2b}$ |
|---|---|---|---|---|---|---|
| $C_e$ | $C_e$ | $C_a$ | $C_{a^2}$ | $C_b$ | $C_{ab}$ | $C_{a^2b}$ |
| $C_a$ | $C_a$ | $C_{a^2}$ | $C_e$ | $C_{ab}$ | $C_{a^2b}$ | $C_b$ |
| $C_{a^2}$ | $C_{a^2}$ | $C_e$ | $C_a$ | $C_{a^2b}$ | $C_b$ | $C_{ab}$ |
| $C_b$ | $C_b$ | $C_{a^2b}$ | $C_{ab}$ | $C_e$ | $C_{a^2}$ | $C_a$ |
| $C_{ab}$ | $C_{ab}$ | $C_b$ | $C_{a^2b}$ | $C_a$ | $C_e$ | $C_{a^2}$ |
| $C_{a^2b}$ | $C_{a^2b}$ | $C_{ab}$ | $C_b$ | $C_{a^2}$ | $C_a$ | $C_e$ |

Primer 4.

Konstruisati grupoid sa strukturnim jednakostima :

$$a_i a_j = b_{ij} \qquad (i,j = 1,2,\ldots,n)$$
$$0.a_i = 0 = a_i.0$$
$$0.b_{ij} = 0 = b_{ij} . 0$$
$$a_i.b_{jk} = 0 = b_{jk}.a_i$$
$$b_{jk}.b_{il} = 0$$

Skup količnik je $\mathcal{U}/_{\lambda} = \{C_0 ; C_{a_i} , C_{b_{ij}} / i,j = 1,2,\ldots,n\}$.

Pravila "množenja" u ovom primeru neposredno se dobiju iz strukturnih jednakosti.

Napomenimo da je dobijeni grupoid semigrupa. Zaista , ako je bar jedan element trojke $(x,y,z)$ $C_{b_{ij}}$ ili nula, asocijativni zakon se svodi na $0 = 0$ . Ako su sva tri elementa oblika $C_{a_i}$ rezlutat je opet $0 = 0$ .

Očigledno je da je <u>svaka univerzalna algebra neke klase $Z_1$ izvesna univerzalna algebra iste klase sa nekom klasom strukturnih jednakosti $Z_2$</u>.