Grupoid

- $(A,*)$ je trdna

Polgrupa

- $(G,*)$ je trdna
- $*$ asociativna operacija

Monoid (polgrupa z enoto)

- $(G,*)$ je trdna
- $*$ asociativna operacija
- ima enoto e za operacijo $*$

Grupa

- $(G,*)$ je trdna
- $*$ asociativna operacija
- ima enoto e za operacijo $*$
- vsak element je obrnljiv

- Cayleyjeva tabela:
  - v vsakem stolpcu in vrstici element nastopi le enkrat
  - vrstica in stolpec, ki se ujemata z začetno vrstico in stolpcem $\Rightarrow$ enota
  - vse pojavitve enote so simetrične na diagonalo
  - začetni element, različen od enote, se ne more pojaviti na diagonali v pripadajočem stolpcu ali vrstici
  - inverz elementa je koordinata stolpca, v katerem se v pripadajoči vrstici pojavi enota

Lastnosti

$(A,*)$ je trdna, če velja $A * A \to A$, operacija $*$ je zaprta

$(A,*)$ je grupoid in $A_1, A_2, \ldots$ trdne množice, potem je $\bigcap_{i=1}^{\infty} A_i$ tr

Komutativnost : $a * b = b * a$
Lastnosti : komutativen = Abelov
Posledica : vrstni red elementov ni pomemben
Cayleyjeva tabela : simetrično glede na diagonalo

Asociativnost : $(a * b) * c = a * (b * c)$
Posledica : opuščamo lahko oklepaje
Dokaz : Zamenjamo a in c ter preverimo, če dobimo isto

Enota (nevtralni element) $e \in G$: ($\approx$ 1 za množenje)

$\forall a \in G, a * e = e * a = a$

$e * a = a$ ... leva enota (Cayleyjeva tabela : vrstica enote enaka začetni vrstici)

$a * e = a$ ... desna enota (Cayleyjeva tabela : stolpec enote enak začetnemu stolpcu)

Lastnosti :

- v grupoidu obstaja največ ena enota, če obstajata leva in desna enota, sta enaki
- lahko pa ima grupoid več levih enot in nobene desne ter obratno

Absorpcijski element $s \in G$: (≈ 0 za množenje)
$\forall a \in G, a * s = e * s = s$
Lastnosti : v grupoidu obstaja največ en absorpcijski elemen
Cayleyjeva tabela : vrstica in stolpec z absorpcijskim elemer
le ta element

Obrnljiv element : (enota vedno obrnljiv element $e * e = e$)

$a' * a = a * a' = e$

$a' * a = e$ … levi inverz

$a * a' = e$ … desni inverz

Pogoj : element a grupoida $(A,*)$ je obrnljiv, če ima enoto

Posledice :

- če ima element monoida levi in desni inverz, sta enaka
- v monoidu :
  - ima vsak element kvečjemu en inverz
  - obrnljivi elementi tvorijo trdno podmnožico : $(a * b)' = b' * a'$
- vsak poenostavljiv element grupoida ima največ en obnljiv element

Poenostavljivost (krajšanje) :
$\forall a, b \in A : ((a * b = a * c \Rightarrow b = c) \wedge (b * a = c * a \Rightarrow b = c))$
V monoidu je vsak obrnljiv element poenostavljiv (ga lahk
bodisi z leve ali z desne.
Cayleyjeva tabela : vsi elementi v pripadajoči vrstici(leva) i
stolpcu(desna) so med seboj različna

Identpotenti so tisti elementi a, za katere velja $a * a = a$,

kjer je $(G,*)$ grupoida.

V grupi je edini identpotentni element enota.

V grupoidu $(G,*)$, kjer velja identpotentnost, komutativnost, asociativnost

velja : $a * b = a \Leftrightarrow b = b$ (polmreža)

Cikličnost :

Polgrupa $(A,*)$ je ciklična, če obstaja generator $g \in A : \langle g \rangle = A$.

$A = \{g, g^2, g^3, \ldots\}$

Posledica : ciklične polgrupe so komutativne; če je grupa praštevilske

moči, je ciklična

Generator :

$\langle g \rangle \equiv \langle \{g\} \rangle$

$(A,*)$ je polgrupa, $g \in A : \langle g \rangle = A$

$\exists g \in A, \forall a \in A, \exists n \in N^+ : a = g^n$

Podgrupe

$\emptyset \neq B \subseteq A$ določa podgrupo $(B,*)$ grupe $(A,*)$, ko velja :

$\forall a, b \in B : a' * b \in B$

◦ B trdna množica v končni grupi $(A,*)$ $\Rightarrow$ $(B,*)$ podgrupa grupe $(A,*)$

◦ $|aB| = |B| = |Ba|$

◦ $(B,*)$ podgrupa grupe $(A,*)$ $\Rightarrow$ $b \in B \sim bB = B$

◦ $R \subseteq A \times A$

$aRb \Leftrightarrow aB = bB$

- $[a] = aB$

- $aRb \sim a' * b \in B$

Opombe

Kaj je tretja potenca števila 2?

$(Z,+)$ $2 + 2 + 2 = 6$

$(Z,\cdot)$ $2 \cdot 2 \cdot 2 = 8$

Vrsta preslikave
$f : N \rightarrow 2N$
$f(n) = 2n$
injekcija : $f(m) = f(n) \Rightarrow 2m = 2n \Rightarrow m = n$
surjekcija : m sod $\Rightarrow m = 2n$; $n \in N \Rightarrow m = f(n)$

Morfizmi

Homomorfizem je preslikava grupoida $(A,\circ)$ v grupoid $(B,*)$, če velja :

$\forall a,b \in A : h(a \circ b) = h(a) * h(b)$.

Kompozitum homomorfizmov je spet homomorfizem.

Izomorfizem je bijektivni homomorfizem.
Lastnosti : Izomorfni strukturi sta enaki, gre le za drugačno c
elementov in poimenovanje operacij.

Surjektivni homomorfizem (epimorfizem) :

- funkcija ohranja asociativnost, komutativnost, identpoten
- enota v $(B,*)$ je slika enote v $(A,\circ)$
- obratni element v $(B,*)$ je slika obratnega elementa v $(A,\circ$

Produkt algebrajskih struktur

$(A,\circ)$, $(B,*)$ sta grupoida, kjer je produkt $A \times B$, ohranja lastnosti :

$(a_1,a_2) \cdot (b_1,b_2) = (a_1 \circ a_2, b_1 * b_2)$

Kongurenčne relacije

$(A,\circ)$ je grupoid in in R ekvivalenčna relacija. R je kongure
velja : $(aRb) \wedge (cRd) \Rightarrow (a \circ c) R (c \circ d)$.

Ekvivalenčna relacija $\Leftrightarrow$ razbitje množice
- refleksivnost $(\forall a : aRa)$
- simetričnost $(\forall a,b : aRb \Rightarrow bRa)$
- tranzitivnost $(\forall a,b : aRc \wedge cRb \Rightarrow aRb)$

Preslikave množic

- $f : A \longrightarrow B$ je surjekcija, če slike elementov množice A ses
  množico B. Množica A se preslika na množico B.
- $f : A \longrightarrow B$ je injekcija, če se vsaka dva različna elementa
  preslikata v različna elementa množice B
  (funkcijske vrednosti se ne ponavljajo)
- $f : A \longrightarrow B$ je bijekcija, če je hkrati surjektivna in injektivn

- $A \geq B \equiv \exists A' \subseteq A : A' \sim B \equiv \exists f : A \rightarrow B$, f surjekcija
- $A \hbar B \equiv (\exists A' \subseteq A : A' \sim B) \wedge (\neg\exists B' \subseteq B : B' \sim A)$
- $A \square B \equiv (\neg\exists A' \subseteq A : A' \sim B) \wedge (\exists B' \subseteq B : B' \sim A)$
- $A \sim B \equiv (\exists A' \subseteq A : A' \sim B) \wedge (\exists B' \subseteq B : B' \sim A) \equiv$
  $\equiv \exists f : A \rightarrow B$, f bijekcija

Moč množic

- $\circ$ $A \subset B$, če je A neskončna, je tudi B neskončna
- $\circ$ $f : A \longrightarrow B$ je injektivna in povsod definirana, A neskončna
  B neskončna množica
- $\circ$ množica vseh realnih števil na $(0,1)$ ni števno neskončna
- $\circ$ vsaka neskončna množica vsebuje števno neskončno podm
- $\circ$ če je A neskončna in B števna $\Rightarrow A \cup B \sim A$
- $\circ$ $A \square PA$
- $\circ$ $(0,1) \sim [0,1] \sim (0,1) \times (0,1) \sim PN$
- $\circ$ $(0,1) \sim (a,b) \quad f(x) = a + (b-a)x$
- $\circ$ $(0,1) \sim R^+ \quad f(x) = \dfrac{x}{1-x}$
- $\circ$ $(0,1) \sim R \quad f(x) = \dfrac{1-2x}{x(1-x)}$

Cantorjeva diagonalna konstrukcija

$f : N \longrightarrow (0,1)$ surjekcija? NE
$f(0), f(1), f(2), \ldots$ množica $(0,1)$
$f(0) = 0.c_{01}c_{02}c_{03}\ldots$
$f(1) = 0.c_{11}c_{12}c_{13}\ldots$
$c_{ij} \in \{0,1,\ldots,9\}$

$x = 0.d_1d_2\ldots$

$$d_i = \begin{matrix} 1, \text{če } c_{ij} \neq 1 \\ 2, \text{če } c_{ij} = 1 \end{matrix}$$

$0{,}111 \leq x \leq 0{,}222 \Rightarrow x \in (0,1)$
$x\ (d_i)$ se razlikuje od $f(i^{-1})$ v i - ti (c_{ii}) decimalki $\Rightarrow x \neq f(i)$
$\Rightarrow x$ ne nastopa v zaporedju $f(0), f(1), \ldots \Rightarrow f$ ni surjekcija