# VI. ALGEBRA

## 1. OPERACIJE

Def.: Dvomestna operacija je preslikava $f:AxB \rightarrow C$
n-mestna operacija je preslikava $f:A_1xA_2x...xA_n \rightarrow C$

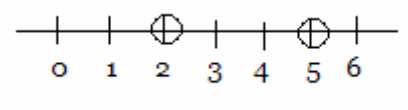
Večinoma se bomo ukvarjali z notranjimi dvomestnimi operacijami $f:AxA \rightarrow A$

Zgled: seštevanje v N √
odštevanje v N //
odštevanje v Z √
množenje v N √
deljenje v N,Q,R // (Q,R: preglavice dela deljenje z 0)

Def.: Algebrska struktura je urejena n-terka
(A, B, C, ..., +, *, □, ..., R, S, T, ..., e, s, 0, ...)
množice operacije relacije posebni elementi

Def.: Grupoid je algebrska struktura, kjer je A neprazna množica
(A,*)
*: AxA →A dvomestna notranja operacija

Zgled: (N,d): N={0,1,2,...}
d:NxN→N




d(m,n) = |m-n|

d(5,d(3,2)) ≠ d(d(5,3),2)
4=d(5,1) d(2,2)=0

d ni asociativna
(N,min) min:NxN→N min(m,n)={m≤n: m, sicer n
min(5,min(3,2))=min(min(5,3),2)

### PODAJANJE OPERACIJ:

- tabelarično
- algoritmično
- opisno
- generično

tabelarični opis, majhna množica je pogoj

| * | a | b | c |
|---|---|---|---|
| a | c | b | a |
| b | b | a | c |
| c | c | c | b |

b*c=c
Cayleyjeva tabelica

opisno: največji skupni delitelj
gcd(m,n) ... največji skupni delitelj števil m in n
gcd: $N^+ x N^+ \rightarrow N^+$
$N=\{1,2,3,4,...\}$

$d=gcd(m,n) \Leftrightarrow d|m \wedge d|n \wedge \forall k:(k|m \wedge k|n \Rightarrow k|d)$ $[k \leq d]$

algoritmično ...

```
gcd(m,n) {
    dokler (n≠0) {
        t ← m mod n
        m ← n
        n ← t
        }
    rezultat ← m
}
```

generični opis
na enakostraničnem trikotniku definiramo "dve" operaciji
R... rotacija trikotnika za 120°
Z... zrcaljenje preko navpične osi
E... pusti trikotnik na miru
R◦R◦R=E=Z◦Z=E◦E
Z◦R=R◦R◦Z
E◦X=X◦E=X (za poljuben X)

Vsa gibanja trikotnika so:

| | E | R | R◦R | Z | R◦Z | R◦R◦Z |
|---|---|---|---|---|---|---|
| E | E | R | R◦R | Z | R◦Z | R◦R◦Z |
| R | R | R◦R | E | Z◦R | Z◦R | Z |
| R◦R | R◦R | E | R | Z◦R | Z | R◦Z |
| Z | Z | Z◦R | R◦Z | E | R◦R | R |
| R◦Z | R◦Z | Z | R◦R◦Z | R | E | R◦R |
| R◦R◦Z | R◦R◦Z | R◦Z | Z◦R | R◦R | R | E |

R◦Z◦R◦R◦Z
R◦Z◦Z◦R
R◦E◦R=R◦R

## 2. KOMPOZITUM MNOŽIC, TRDNE MNOŽICE, GENERATORJI

Def.: Naj bo (A,*) grupoid in B,C⊆A
$B*C = \{ b*c \mid b \in B \wedge c \in C \}$
Def.: Naj bo (A,*) grupoid. B⊆A je trdna (zaprta za operacijo *), če je B*B⊆B.

Zgled: (R,+) Q,Z,N so trdne množice
[10,∞), (0,∞)
"večkratniki števila 3"

"števila z manj kot sedmimi mesti za decimalno piko"
2 3 7 1 5 8 6 0 0 0 ...√
3 1 2 5 8 9 3 3 4 5 ... //

Izrek: Presek trdnih množic je trdna množica-
B, C trdni, potem je B∩C trdna
$B_i$ i∈I trdne množice, potem je ∩[i∈I]$B_i$ trden.

Dokaz:
Naj bosta B in C trdni množici
(B∩C)*(B∩C) ⊆ B*B ⊆ B
(B∩C)*(B∩C) ⊆ C*C ⊆ C
B, C trdna
Torej
(B∩C)*(B∩C) ⊆ B∩C zato je B∩C trdna.

Znova naj bo (A,*) grupoid. C⊆A
<C> je najmanjša trdna množica, ki vsebuje C.
- C⊆<C>
- <C> je trdna
- če D trdna in C⊆D, potem <C>⊆D
- <<C>> = <C>

Trditev:
<C> je presek vseh trdnih množic, ki vsebujejo C.
Če je <C>=A pravimo, da C porodi (generira) množico A.
Tudi: množica C je množica generatorjev A-ja.

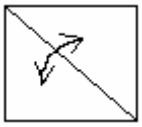
Zgled: (Z,+) <{7,-10}> = Z
<{7,10}> ≠ Z ( = vsebuje vsa naravna števila od 100 naprej, [DN])
<{-15,10}> ≠ Z

## 3. LASTNOSTI OPERACIJ

Naj bo (A,*) grupoid

Def.: * je komutativna, če za ∀a,b∈A velja a*b=b*a

Komentar: Cayleyjeva tabelica komutativne operacije je simetrična glede na diagonalo



Def.: Grupoid s komutativno operacijo imenujemo Abelov grupoid

Def.: Operacija * je asociativna, če za ∀a,b,c∈A velja:
(a*b)*c=a*(b*c)=a*b*c

Če je operacija * asociativna, lahko definiramo potence.

Velja: $a^1 = a$

$a^{n+1} = a^n * a \quad n \geq 1$

## LASTNOSTI POTENC:

$a^n * a^m = a^{n+m}$, $(a^n)^m = a^{n*m} \quad n,m \geq 1$.

Def.: Grupoid v katerem je operacija asociativna imenujemo polgrupa.

Def.: Polgrupa $(A,*)$ je ciklična, če obstaja $g \in A$ za katerega je $\langle\{g\}\rangle = A$

Komentar: $\langle\{g\}\rangle = \{ g, g^2, g^3, g^4, g^5, \ldots \}$
g je generator A in A je sestavljen natančno iz potenc g-ja

Zgled: $N^+ = \{1,2,3,\ldots\}$
$(N^+,+)$

$\langle\{1\}\rangle = N^+$
1, 1+1, 1+1+1, 1+1+1+1, ....

Zgled: $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 5 & 7 & 2 & 1 & 2 & 4 & 3 \end{pmatrix}$

$f^2 = f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 7 & 2 & 2 & 4 & 6 & 4 & 7 & 5 \end{pmatrix}$

$f^3 = f^2 \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 2 & 4 & 4 & 7 & 1 & 7 & 2 & 2 \end{pmatrix}$

DN: $f^4, f^5, f^6, f^7, f^8, f^9 = f^3$
$f^{10} = f^4$
$f^{11} = f^5$

## 4. POSEBNI ELEMENTI

Def.: $e \in A$ je enota v grupoidu $(A,*)$, če za $\forall a \in A$ velja:
$e*a = a*e = a$

Zgled: $(Z,+)$ 0 je enota
$(R,*)$ 1 je enota
$(PB,\cup)$ Ø je enota

Def.: Polgrupa z enoto je monoid.

Komentar: Z enoto e lahko razširimo definicijo potence
$a^0 = e$

Izrek: V grupoidu obstaja največ ena enota.

Dokaz:
Recimo, da sta $e_1$ in $e_2$ enoti, $e_1 = e_1 * e_2 = e_2$
ker je $e_2$ enota ker je $e_1$ enota

Kako spoznamo enoto v Cayleyjevi tabeli?

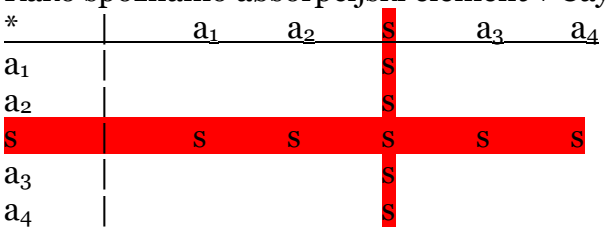

Def.: s∈A je absorpcijski element v grupoidu (A,*) če za ∀a∈A: a*s=s*a=s

Zgled: (Z,*) 0 je absorpcijski element
(N⁺, min) 1 je abssorpcijski element min(1,a)=1
(PB,∩) Ø je absorpcijski element

Izrek: V grupoidu obstaja kvečjemu en absorpcijski element.

Dokaz:
Recimo, da sta $s_1$ in $s_2$ absorpcijska elementa
$s_1 = s_1 * s_2 = s_2$
ker je $s_1$ absorpcijski element $s_2$ absorpcijski

Kako spoznamo absorpcijski element v Cayleyjevi tabeli?



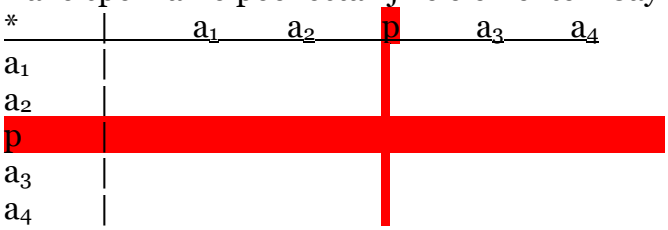

Def.: Element a iz grupoida (A,*) je poenostavljiv, če za ∀b,c∈A držita implikaciji:
a*b=a*c ⇒ b=c
b*a=c*a ⇒ b=c

Poenostavljiv element ... lahko ga "krajšamo"

Zgled: (Z,+)
3+a=3+b ⇒ a=b 3 je poenostavljiv
(Z,*)
2*a=2*b ⇒ a=b 2 je poenostavljiv
(N,min)
min(5,n) = min(5,m) ≠> m = n
5 ni poenostavljiv
(PB,∩)
{a,b}∩{a,c}={a,b}∩{a} ≠> {a,c} = {a}
(Z,*)
0*m = 0*n ≠> m = n

Trditev: enota je poenostavljiva, absorpcijski element pa ne.

Kako spoznamo poenostavljive elemente v Cayleyjevi tabeli?




Def.: Element a v grupoidu (A,+) z enoto e je obrnljiv natanko tedaj, ko obstaja a'∈A, za katerega velja a*a' = a'*a = e

Elementu a' pravimo tudi obrat, inverz, obratni element, inverzni element k/od elementu/a a.

Izrek: V monoidu (A,+) z enoto e ima vsak element a največ en obrat a'.

Dokaz:

Denimo, da sta a' in a'' oba obrata k a.
a' = a' * e = a' * (a*a'') = (a' * a) * a'' = e * a'' = a''
(asociativnost) □

Izrek: V monoidu so obrnljivi elementi tudi poenostavljivi.

Dokaz (skica):

a*b = a*c
a'*a*b = a'*a*c (v monoidu velja asociativnost)
e*b = e*c
b = c (obrnljivi elementi so poenostavljivi)

Def.: Če je (A,*) monoid, v katerem so vsi elementi obrnljivi, mu pravimo grupa.