ALGEBRSKE STRUKTURE z 1 OPERACIJO.

Binarna operacija na množici A: $f: A \times A \to A$, f preslikava.

Če notranja. Par (A, f) je grupoid.

$f((x,y))$ zapišemo kot $x \cdot y$ in (A, f) pišemo kot $(A, \cdot)$.

Lahko zahtevamo dodatne lastnosti operaciji

asociativnost:

$\forall a,b,c \in A: (a \cdot b) \cdot c = a \cdot (b \cdot c) \Rightarrow (A, \cdot)$ je polgrupa ali asociativen grupoid.

Primer: naj bo A množica predstavljivih števil v računalniku. Naj bo $\cdot$ množenje. Za recimo IEEE754 32bitna floate, torej v splošnem, operacija ni asociativna, torej je $(A, \cdot)$ grupoid, a ne polgrupa.

enota:

enota je element $e \in A \ni: \forall a \in A: a \cdot e = e \cdot a = a$

Polgrupi z enoto pravimo monoid.

Primeri: 1.) Let $\mathcal{Y}$ množica vseh končnih (abstraktnih) grafov.

↳ izomorfni grafi so si v tej množici enaki.

operacija naj bo $\square$ — kartezični produkt grafov.

$(\mathcal{Y}, \square)$ je monoid.

- notranjost ✓
- asociativnost ✓
  - ↳ $\forall g,h,k \in \mathcal{Y}: (g \square h) \square k \cong g \square (h \square k)$
- enota ✓
  - ↳ $\exists K_1 \in \mathcal{Y}\ \forall g \in \mathcal{Y}: K_1 \square g \cong g \square K_1 \cong g$

2.) Množica $\mathbb{R}_0^+ = \{ x \in \mathbb{R} ; x \geq 0 \}$

Operacija $\max : \mathbb{R}_0^{+2} \longrightarrow \mathbb{R}_0^+$

$$(x,y) \longmapsto \begin{cases} x ; & x > y \\ y ; & \text{drugače} \end{cases}$$

$(\mathbb{R}_0^+, \max)$ je monoid:

- notranjost ✓
- asociativnost ✓

$\forall a,b,c \in \mathbb{R}_0^+ :$ $(a(\max)b)(\max)c = a(\max)(b(\max)c) =$

$\max\{a,b,c\} = \max\{a,b,c\}$

- enota ✓

$\exists\, 0 \in \mathbb{R}_0^+ \; \forall a \in \mathbb{R}_0^+ :$ $0(\max)a = a(\max)0 = a$

3.) X naj bo poljubna množica s končno elementi.

$X = \{x_1, \dots, x_n\}$, elementi so „simboli".

X^* naj bo množica vseh končnih besed nad X,

kjer je beseda zaporedje simbolov iz X.

λ naj bo prazna beseda, beseda dolžine 0, $\lambda \in X^*$.

$X^* = \{ \lambda, x_1, x_2, \dots, x_n, x_1x_1, x_1x_2, \dots x_1x_n, x_2x_1, \dots \}$

V X^* vpeljimo concat operacijo $\cdot$.

$(x_1x_2x_3) \cdot (x_8x_{14}) = (x_1x_2x_3x_8x_{14})$

$\in X^* \quad \in X^* \quad \in X^*$

$(X^*, \cdot)$ je monoid.

- notranjost ✓

· asociativnost ✓

· enota λ ✓

<u>obstoj inverzov:</u>

Monoidu, v katerem so vsi elementi obrnljivi, pravimo grupa.

$$\forall a \in A \ \exists \ b \in A \ \ni: \ ab = ba = e$$

Če je a v monoidu obrnljiv, ima enolićen inverz. Dokazali pri LA.

Posledično lahko vpeljemo oznako a^{-1} za inverz a.

Kar se tiče oznak, ob · pišemo inverze a^{-1} in jim pravimo multiplikativni inverzi, ob + pa jih označimo z $-a$ in jim pravimo aditivni.

<u>Izrek:</u> Če sta a in b v monoidu obrnljiva, je obrnljiv tudi njun produkt in velja

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

<u>Dokaz:</u> $(a \cdot b)(b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot e \cdot a^{-1} =$

$= a \cdot a^{-1} = e$

$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} e b = e$$

(*)

$$\Rightarrow (a \cdot b)(b^{-1} a^{-1}) = (b^{-1} a^{-1})(ab) = e$$

$$\Rightarrow ab = (b^{-1} a^{-1})^{-1}$$

POSLEDICA: Če so $a_1, \dots, a_k$ obrnljivi elementi monoida, je $(a_1 a_2 \cdots a_k)$ obrnljiv element monoida in velja:

$(a_1 \cdots a_k)^{-1} = a_k^{-1} \cdots a_1^{-1}$.

Potaz z indukcijo:

Baza: $k=2$ ✓ (*) , $k=1$ ✓

Korak: Predp: $(a_1 \cdots a_k)^{-1} = a_k^{-1} \cdots a_1^{-1}$

$$a_1 \cdots a_k a_{k+1} = \left((a_1 \cdots a_k) a_{k+1}\right)^{-1} =$$

$$= a_{k+1}^{-1} (a_1 \cdots a_k)^{-1} \overset{I.P.}{=} a_{k+1}^{-1} a_k^{-1} \cdots a_1^{-1} \quad ✓$$

Definicija potenc elementov:

Let $(A, \cdot)$ monoid, $n \in \mathbb{N}_0$:

$$a^0 = e$$
$$a^n = a \cdot a^{n-1}, \quad n \geq 1$$

Enaki velja $a^n a^m = a^{n+m}$ $\quad (a^n)^m = a^{nm}$

$$(a^{-1})^n = \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{n\text{-krat}} = \underbrace{(a \cdots a)^{-1}}_{n\text{-krat}} = (a^n)^{-1}$$

Torej, če je $a \in A$ obrnljiv, velja $(a^n)^{-1} = (a^{-1})^n$.

Primer: $\mathbb{Z}_m = \{0 .. (m-1)\}$

operacija $+_m$: $\forall x, y \in \mathbb{Z}_m : x +_m y := (x+y) \,\%\, m$

$(\mathbb{Z}_m, +_m)$ je grupa.

. notr ✓ . asoc ✓ . enota ✓ . inverzi ✓

operacija $\cdot_m$: $\forall x, y \in \mathbb{Z}_m : x \cdot_m y := (x \cdot y) \,\%\, m$

$(\mathbb{Z}_m, \cdot_m)$ je monoid

. notr ✓ . asoc ✓ . enota ✓ . inverzi ne vedo

$(\mathbb{Z}_p^*, \cdot_p)$ je grupa, če je p praštevilo. (vsi neničelni elementi so obr.)

Izrek: $k \in \mathbb{Z}_n$ je obrnljiv v $(\mathbb{Z}_n, \cdot_n) \Leftrightarrow \underbrace{k \perp n}$

k je tuje n,
$\gcd(k,n) = 1$

$x \equiv y \pmod m$ in $x' \equiv y' \pmod m$
(x, y sta kongruentni po m)

$\Rightarrow$ $x +_m x' \equiv y +_m y' \pmod m$ in
$x \cdot_m x' \equiv y \cdot_m y' \pmod m$

↳ dokažimo:

$x = km + p$ $\quad x' = k'm + p'$
$y = lm + p$ $\quad y' = l'm + p'$

$xx' = (km + p)(k'm + p') = kk'mm + kmp' + k'mp + pp' = sm + pp'$

$yy' = (lm + p)(l'm + p') = ll'mm + lp'm + pl'm + pp' = tm + pp'$

[GRUPE IN PODGRUPE]

Def.:
Let $(A, \cdot)$ poljuben grupoid. Če $\forall a,b \in A: ab = ba \Rightarrow$
$(A, \cdot)$ je komutativen.

Opz.: Grupa je abelova $\Leftrightarrow$ grupa je komutativna.

Primeri grup: · $(\mathbb{Z}_m, +_m)$, $m \in \mathbb{N}$

· $(\mathbb{Z}_p, \cdot_p)$, p praštevilo

· G graf: $\mathrm{Aut}\, G = \{\alpha;\ \alpha \text{ je avt } G\}$

bijekcija $VG \to VG$;
$uv \in EG \Leftrightarrow \alpha u\, \alpha v \in EG$

zaprtost ✓
inverz: α^{-1} ✓
enota: id ✓
asoc.: ✓

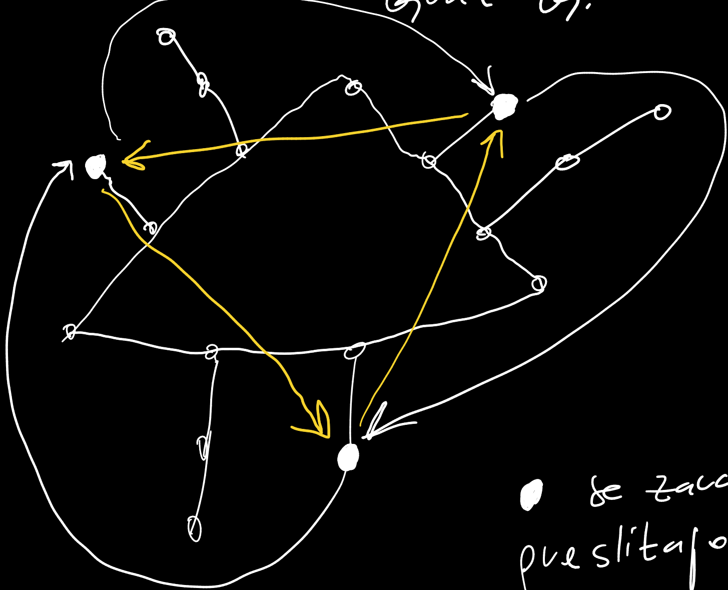
← Če za operacijo vzamemo komponiranje preslikav, je $(\mathrm{Aut}\, G, \circ)$ grupa.

$$(\mathrm{Aut}\, K_n, \circ) \cong \mathrm{Sym}(\{1..n\})$$

↳ polna simetrična grupa v vse možne permutacije
$\varphi: \{1..n\} \to \{1..n\}$, φ bijekcija
oper: $\circ$, običajno komponiranje preslikav.

Primer:

Graf G:



oglejmo si vozlišča •.

avt slika vozlišča stopnje k v vozlišča stopnje k.

• se zaradi stopenj sosedov lahko preslikajo zgolj med seboj

poleg id imamo le dva avt:  in 

$(\mathrm{Aut}\, G, \circ) \cong (\mathbb{Z}_3, +_3)$.

Primer: $A = \{1, 3, 7, 9\}$

operacija: $\cdot_{10}$

$\cdot_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

→ CAYLEY-jeva grupa

$(\{1,3,7,9\}, \cdot_{10})$ je grupa, kot je razvidno iz tabele:

- asoc ✓
- enota ✓
- notr ✓
- inverz ✓

Izrek: Če je G grupa, $a, b, c \in G$, potem velja

(i) $ab = ac \Rightarrow b = c$

(ii) $ba = ca \Rightarrow b = c$

---

zadnjo uro nisem pisal. slike zapiskov: S21fe/20240509_11*