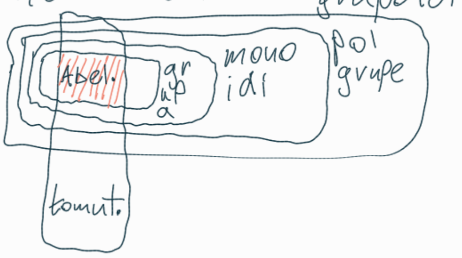
Ponovitev:



Podstrukture. let $(M,\circ)$ grupoid.

Podmnožica $N \subseteq M$ je zaprta za $\circ$ (= podgrupoid) če za vsak $a,b \in N$ velja $a \circ b \in N$, lahko tudi na N definiramo $\circ_N$ s predpisom $a \circ_N b = a \circ b$

Rečemo, da N podeduje operacijo iz M.

↳ lahko le, kadar je zaprt.

Če je $\circ$ asociativna, je tudi $\circ_N$ asociativna.
Če je $\circ$ komutativna, je tudi $\circ_N$ komutativna.
Če $\exists$ enota v $(M,\circ)$, ni rečeno, da $\exists$ enota v $(N, \circ_N)$.
Prav tako se obstoj inverza ne podeduje.

Def.: Če je $(M,\circ)$ polgrupa (asociativen grupoid) in $N \subseteq M$, pravimo, da je N podpolgrupa, če je zaprta za $\circ$.

ki se ne deduje.

Def: Če $(M,\circ)$ monoid (polgrupa z enoto) in $N \subseteq M$, je N podmonoid, če:

- je zaprt za $\circ$
- vsebuje enoto iz $(M,\circ)$.

PRAV TISTO! Če ima enoto, ni dovolj, mora biti ista.

Primer: $(\mathbb{N}, \cdot)$ je monoid. Soda števila so podpolgrupa (zaprta za množenje), niso pa podmonoid, saj ne vsebujejo enice (enote).

Primer: $\mathbb{N} \times \mathbb{N}$ je monoid za $(a,b)\circ(c,d) = (ac, bd)$.

enota je $(1,1)$.

$\mathbb{N} \times 0$ je podpolgrupa v $(\mathbb{N} \times \mathbb{N}, \circ)$. Ima enoto $(1,0)$, vendar, ker $(1,0) \neq (1,1)$, to ni podmonoid.

Def: Če je $(M, \circ)$ grupa in $N \subseteq M$, pravimo, da je N podgrupa $\iff$
- je zaprta za $\circ$
- vsebuje isto enoto kot $(M, \circ)$
- vsebuje inverz vsakega svojega elementa, inverzi so po enoličnosti enaki inverzom iz $(M, \circ)$.

Primeri: $\underbrace{GL_n}_{\text{grupa vseh obrnljivih } n \times n \text{ matrik.}}$ • Podgrupa $\underbrace{SL_n}_{\text{vse } n\times n \text{ matrike z } \det = 1}$.

$\hookrightarrow \det I = 1$

$\hookrightarrow \det$ je multiplikativna

$\hookrightarrow \det A = 1 \iff \det A^{-1} = 1$

• Podgrupa O_n — vse $n \times n$ matrike A, ki zadoščajo $A^T A = I$ (ortogonalne matrike).

$\hookrightarrow A, B \in O_n \overset{?}{\Rightarrow} AB \in O_n$

$$(AB)^T AB \overset{?}{=} I$$

$$B^T \underbrace{A^T A}_{I} B = B^T I B \overset{\checkmark}{=} I.$$

$\hookrightarrow I^T I = I$

$\hookrightarrow A \in O_n \overset{?}{\Rightarrow} A^{-1} \in O_n$

$$(A^{-1})^T A^{-1} \overset{?}{=} I$$

ker $A^T A = I$, sledi

$$A^T = A^{-1}$$

$$\Downarrow$$

$$(A^{-1})^T A^{-1} = (A^T)^T A^{-1} \stackrel{!}{=}$$

$$A A^{-1} \stackrel{\checkmark}{=} I$$

Primer: $\underbrace{SO_n}_{\text{specialna ortogonalna grupa}} := O_n \cap \underbrace{SL_n}_{\text{specialna linearna grupa}}$

Pokažemo lahko celo bolj splošno; da je presek dveh podgrup spet podgrupa.

TRDITEV: (Kako te tri lastnosti združimo v eno lastnost, s čimer skrajšamo preverjanje, da je nekaj podgrupa?)

Let $(M, \circ)$ grupa in $N \subseteq M$ je podgrupa $\Leftrightarrow$

(*) $\forall a, b \in N : a \circ b^{-1} \in N$ zdb: $a, b \in N \Rightarrow a \circ b^{-1} \in N$

Dokaz $\Rightarrow$: let N podgrupa v $(M, \circ)$.

vzemimo $a, b \in N$. Upoštevamo $b \in N \Rightarrow b^{-1} \in N$ iz definicije podgrupe. $a, b^{-1} \in N \Rightarrow a \circ b^{-1} \in N$ iz definicije podgrupe.

$\Leftarrow$: let $\forall a, b \in N : a \circ b^{-1} \in N$

preverimo lastnosti 1, 2, 3 iz def. podgrupe:

N je neprazna (itak mora vsebovati enoto).

lastnost 2.) $N \neq \emptyset \Rightarrow a \in N$.

$$a, a \in N \stackrel{(*)}{\Rightarrow} \underbrace{a \circ a^{-1}}_{\text{enota}} \in N \Rightarrow e_{\text{enota}} \in N$$

lastnost 3.) $a \in N \Rightarrow a, e \in N \Rightarrow \underbrace{e \circ a^{-1}}_{a^{-1}} \stackrel{*}{\in} N \Rightarrow a^{-1} \in N$

lastnost 1.) $a, b \in N \Rightarrow a, b^{-1} \in N \Rightarrow a \stackrel{*}{\circ} (b^{-1})^{-1} \in N \Rightarrow a \circ b \in N$

Opomba: V Abelovih grupah pogosto označimo operacijo označine s +.

Tedaj $a+b^{-1}=a-b$ (oznaka).

Podgrupa Abelove grupe je zaprta za odštevanje.

Opomba: V končnih grupah se da lastnost (*) še bolj poenostaviti. Tam zadošča le preveriti zaprtost za $\circ$.
[note to self: poglej]

~~~~~~~~ ODMOR ~~~~~~~~

HOMOMORFIZMI

To so preslikave, ki ohranjajo strukturo.

Let $(M_1, \circ_1)$, $(M_2, \circ_2)$ dva grupoida.

Preslikava $f: M_1 \longrightarrow M_2$ je homomorfizem, če
$\forall a,b \in M_1 : (f(a \circ_1 b) = f(a) \circ_2 f(b))$ (*)

Enaka definicija v polgrupah.

Pri monoidih zahtevamo še $f(e_1)=e_2$

Primer: $f: \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$
$a \longrightarrow (a, 0)$

operacija$_1$: množenje
operacija$_2$: $(a,b)\circ(c,d) = (ac, bd)$

ta preslikava zadošča (*),
ker $f(a\cdot b) = (a\cdot b, 0) = (a,0)\circ(b,0) = f(a)\circ f(b)$
ta f ne slika enote v enoto:
$f(1) = (1,0) \neq (1,1)$
↳ enota v $\mathbb{N}\times\mathbb{N}$.

Pri grupah zahtevamo še, da se inverzi slikajo v inverze
↳ $f(a^{-1}) = f(a)^{-1}$

Izkaže se, da ohranjanje enote in inverzov pri grupnih homomorfizmih že sledi iz (*).
~~~~~~~~

Trditev: naj bosta $(M_1, \circ_1)$ in $(M_2, \circ_2)$ grupi.
naj bo $f: M_1 \to M_2$ preslikava, ki zadošča (*). Trdimo, da slika enoto v enoto in inverze v inverze.

Dokaz: let e_1 enota za $(M_1, \circ_1)$
e_2 enota za $(M_2, \circ_2)$

Dokažimo, da je $f(e_1) = e_2$.

Sledi iz: $f(e_1) = f(e_1 \circ_1 e_1) \xRightarrow{(*)} f(e_1) \circ_2 f(e_1)$

ker je e_2 enota,
$f(e_1) \circ_2 f(e_1) = f(e_1) \circ_2 e_2$

$$\Downarrow$$

$$\underbrace{f(e_1)^{-1} \circ_2 f(e_1)}_{e_2} \circ_2 e_2 = \underbrace{f(e_1)^{-1} \circ_2 f(e_1)}_{e_2} \circ_2 f(e_1)$$

$$e_2 \circ e_2 = e_2 \circ f(e_1)$$

Dokažimo še ohranjanje inverzov:

b je inverz za $a \xRightarrow{(*)} f(b)$ je inverz $f(a)$

$\Downarrow$ $a \circ_1 b = e_1 \Rightarrow f(a) \circ_2 f(b) \overset{(*)}{=} f(a \circ_1 b) = f(e_1) = e_2$

$b \circ_1 a = e_1 \Rightarrow f(b) \circ_2 f(a) \overset{(*)}{=} f(b \circ_1 a) = f(e_1) = e_2$

Primeri Homomorfizmov:

- Determinanta: $M_n(\mathbb{R}) \to \mathbb{R}$. operaciji $\cdot \to \cdot$

  ker $\det(AB) = \det A \det B$, je det homomorfizem.

- S_n so vse permutacije $\{1, 2, \dots, n\}$.

  vsaki permutaciji σ iz S_n priredimo permutacijsko matriko $P_\sigma \in M_n(\mathbb{R})$.

In to tabole:

v $\begin{bmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix}$ navedimo s σ permutacijo stolpcev:

$e_1 \; e_2 \; e_{n-1} \; e_n$

$$P_\sigma := [\vec{e}_{\sigma(1)} \; \vec{e}_{\sigma(2)} \cdots \vec{e}_{\sigma(n-1)} \; \vec{e}_{\sigma(n)}]$$

Imamo preslikavo:

$$\left.\begin{array}{l} S_n \to M_n(\mathbb{R}) \\ \sigma \to P_\sigma \end{array}\right\}$$ Trdimo, da je to homomorfizem

Radi bi dokazali, da je

$$P_{\sigma \circ \tau} = P_\sigma P_\tau \quad \text{za vse } \sigma, \tau \in S_n$$

↳ operacija na matrikah je $\times$

↳ operacija na preslikavah je kompozitum

$P_\sigma e_1 = e_{\sigma(1)}$ (= prvi stolpec P_σ)

$P_\sigma e_n = e_{\sigma(n)}$ (= zadnji stolpec P_σ)

povzetek: $P_\sigma e_i = e_{\sigma(i)} \quad \forall i$

Če i zamenjamo s $\tau(i)$, dobimo

$$P_\sigma e_{\tau(i)} = e_{\sigma(\tau(i))} = e_{(\sigma \circ \tau)(i)}$$

$$\boxed{P_\sigma P_\tau} = P_\sigma [e_{\tau(1)} \cdots e_{\tau(n)}]$$

$$= [P_\sigma e_{\tau(1)} \cdots P_\sigma e_{\tau(n)}] = [e_{(\sigma\circ\tau)(1)} \cdots e_{(\sigma\circ\tau)(n)}] =$$

$$\boxed{= P_{\sigma\circ\tau}}$$

$\Rightarrow$ preslikava je res homomorfizem

TRDITEV: kompozitum dveh homomorfizmov je homomorfizem.

$$
\begin{tikzcd}
(M_1, \circ_1) \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & (M_2, \circ_2) \arrow[r, "g"] & (M_3, \circ_3)
\end{tikzcd}
$$

homomorfizem

$$(g\circ f)(a \circ_1 b) \overset{\text{hmf}}{=} g(f(a\circ_1 b)) \overset{\text{hmf}}{=} g(f(a) \circ_2 f(b)) \overset{\text{hmf}}{=}$$

$$\overset{\text{hmf}}{=} g(f(a)) \circ_3 g(f(b)) \overset{\text{hmf}}{=} (g\circ f)(a) \circ_3 (g\circ f)(b)$$

Primer:

$$
\begin{tikzcd}
S_n \arrow[r, "\sigma"] \arrow[rr, bend right, "\mathrm{sgn}"'] & M_n(\mathbb{R}) \arrow[r, "\det"] & \mathbb{R}
\end{tikzcd}
$$

$\hookrightarrow \quad \mathrm{sgn}(\sigma) = \det A$

Preslikava sgn je homomorfizem, ker je kompozitum dveh homomorfizmov.

Def.: Izomorfizem je preslikava, ki je bijektivna in je homomorfizem.

Dve grupi sta izomorfni, če med njima obstaja izomorfizem.

S stališča algebre sta v abstraktnem smislu enaki, saj je izomorfizem samo preimenovanje elementov.