ALGEBRSKE STRUKTURE

Uvod: M naj bo neprazna množica

Operacija na M pove, kako iz dveh elementov M dobimo nov element M.

Recimo: če $a, b \in M$, tedaj $a \circ b$ je nov element M.

Formalna definicija: ↪ kartezični produkt: urejeni pari.

Operacija na M je funkcija $M \times M \to M$

$(a, b) \to \underbrace{\circ(a, b)}_{a \circ b}$

Na isti množici imamo lahko več operacij. Začnimo jih tako, da uvedemo pojem grupoida: Grupoid je (množica, izbrana operacija).

$(M, \circ)$ $M \neq \{\}$

↪ $M \times M \to M$

Še posebej nas zanimajo operacije z lepimi lastnostmi:

↳ asociativnost, komutativnost, enota, inverz

Grupoid, katerega $\circ$ ima vse te lastnosti, je ABELOVA GRUPA.

Asociativnost: $\circ$ je asoc. $\Leftrightarrow \forall a, b, c \in M: (a \circ b) \circ c = a \circ (b \circ c)$

- Grupoidi z asoc. vel. se reče POLGRUPA.
- Smisel asociativnosti: Vrednost izraza ni odvisna od razloženitve '(,)'.

Tedaj skladnja dopušča pisanje brez oklepajev: $a \circ b \circ c \circ d$.

Komutativnost: $\circ$ je kom. $\Leftrightarrow \forall a, b \in M: a \circ b = b \circ a$

- Grupoidom s kom. vel. se reče KOMUTATIVNI GRUPOID
- Smisel komutativnosti: Predpostavka: Smo v POLGRUPI.

Vrednost izraza ni odvisna od vrstnega reda faktorjev.

PRIMERI: use operacije

I. asoc. in kom.: $(\mathbb{N}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{N}, +)$ – številske operacije

II. asoc., a ne kom.: • množenje matrik $(M_n(\mathbb{R}), \cdot)$

matrike $n \times n$ elementi | množenje

III. kom., a ne asoc.:

• Jordanski produkt matrik:
$A \circ B = \frac{1}{2}(AB + BA)$

IV. niti kom. niti asoc.

• vektorski produkt v $\mathbb{R}^3$
$(\mathbb{R}^3, \times)$

• PRIMER: M je neprazna
F = vse funkcije $M \to M$
$\circ$ = kompozitum dveh funkcij
IZKAŽE SE, DA:
– $(F, \circ)$ je vedno polgrupa.
Če ima M vsaj 3 elemente,
– $(F, \circ)$ ni komutativna

DOKAZ ASOCIATIVNOSTI:
Def. kompozituma: $(f \circ g)(x) = f(g(x))$

$(f \circ g) \circ h \overset{?}{=} f \circ (g \circ h)$

$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$

$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$

Enote: Naj bo $(M, \circ)$ grupoid. Element $e \in M$ je enota, če $\forall a \in M : a \circ e = a \wedge e \circ a = a$.

če velja le eno izmed takih izrazov konjunkcije: leva enota, desna enota; tedaj ni enota.

Da je e enota, mora biti leva enota in desna enota.

PRIMERI:
$(\mathbb{R}, +)$: enota je 0.
$(\mathbb{N}, \cdot)$: enota je 1.
$(\mathbb{N}, +)$: ni enote. $0 \notin \mathbb{N}$.
$(M_n(\mathbb{R}), \cdot)$: enota je I_n.

TRDITEV: Vsak grupoid ima največ eno enoto. Dve enoti v istem grupoidu sta enaki. Če več vsaka leva enota je enaka vsaki desni enoti.

DOKAZ: let e leva enota : $e \circ a = a$ $\forall a$
let f desna enota : $b \circ f = b$ $\forall b$

$e \circ f = f$
$e \circ f = e$

Ker je vsaka leva enota enaka vsaki desni enoti, sta poljubni dve enoti enaki.

Enota je ena sama, če obstaja.
Obenem je edina leva in edina desna enota.

ŠE EN PRIMER: Lahko se zgodi, da $\exists$ poljubno različnih levih, a nobene desne enote.

$\circ$ je množenje matrik.

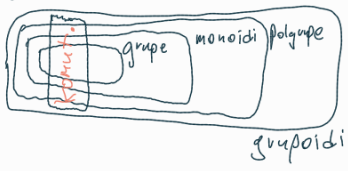
to je grupoid (celo polgrupa):

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} ac & ad \\ 0 & 0 \end{bmatrix}$$

Vsi elementi oblike $\begin{bmatrix} 1 & x \\ 0 & 0 \end{bmatrix}$ so leve enote.

Iz dejstva da je več (celo neskončno) levih enot, sledi dejstvo, da ni desnih enot.

POLGRUPI Z ENOTO REČEMO MONOID.



Inverzi: Let $(M, \circ)$ monoid z enoto e.

Inverz elementa $a \in M$: $b \in M$ t.: $\underbrace{a \circ b = e}_{\text{desni inverz}}$ $\wedge$ $\underbrace{b \circ a = e}_{\text{levi inverz}}$.

Inverz a je tak element, ki je tako levi kot tudi desni inverz a.

Obstoj inverza: Ne vselej, recimo v $(M_n(\mathbb{R}), \cdot)$.

Inverz je vedno enoličen.

TRDITEV: Vsak element monoida ima kvečjemu en inverz.
Vsak levi inverz je enak vsakemu desnemu.

Let b levi inverz a. $b \circ a = e$

Let c desni inverz a. $a \circ c = e$

$$b \circ e = b = b \circ (a \circ c) =$$
$$= (b \circ a) \circ c = e \circ c = c.$$

Če obstaja, je inverz en sam, in to je edini levi in edini desni inverz.

OZNAKA za inverz elementa a: a^{-1}

PRIMERI: Kaj je inverz a v $(\mathbb{Z}, +)$? $-a$.

a v $(\mathbb{Z}, \cdot)$? inverz 1 je 1
-1 -1
ostali nimajo inverza.

a v $(\mathbb{Q} \setminus \{0\}, \cdot)$? $1/a$

Če ni drugega, imamo lahko več levih inverzov.

PRIMER: M := vse funkcije $\mathbb{N} \to \mathbb{N}$

o := kompozitum funkcij.

$f \in M$ ima levi inverz, to je f injektivna.
$f \in M$ ima desni inverz, to je f surjektivna.
$f \in M$ ima inverz, to je f bijektivna.

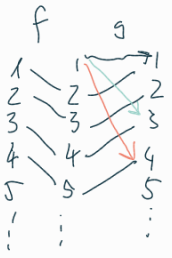
PRIMER: $f(n) = n+1$ je injektivna, a ne surjektivna

Poišči vse leve inverze f!

$g(x) = \begin{cases} x-1 ; & x > 1 \\ \text{kakršnakoli} ; & x = 1 \end{cases}$ → enico lahko slikamo v kakršnokoli.

$(g \circ f) = id$

$g = f^{-1}$.



PRIMER: V $(M_n(\mathbb{R}), \cdot)$ je vsak levi inverz tudi desni inverz. To je res tudi za fle na končni množici. V splošnem to ni res.

Definicija: GRUPA je tak monoid, v katerem ima vsak element inverz.

Daljše: GRUPA je taka neprazna množica G skupaj z operacijo $\circ$, ki zadošča asociativnosti, obstaja enota in za vsak element obstaja njegov inverz.

Definicija: GRUPI s komutativno operacijo večkrat ABELOVA GRUPA

Primeri abelovih grup: $(\mathbb{Z}, +)$, $(\mathbb{Q} - \{0\}, \cdot)$, $(M_n(\mathbb{R}), +)$, $(\mathbb{R}^n, +)$

Primeri ne-abelovih grup:

PRIMER: M := vse obrnljive matrike s fiksnim številom stolpcev

o := množenje matrik

PRIMER: S := neprazna končna množica

M := vse bijektivne funkcije $S \to S$

o := kompozitum funkcij

„permutacije"

[PODSTRUKTURE]

• Podgrupoid | Let $(M, \circ)$ grupoid. Rečemo, da je Neprazna

- podpolgrupa
- podmonoid
- podgrupa

podmnožica M. Tako se zgodi, da za $a, b \in N$ ne velja $a \circ b \in N$.

Primer: $M = \mathbb{Z}$ $\circ = +$ N = liha števila. liho + liho = sodo.

Pravimo, da je podmnožica $N \subseteq M$ zaprta za $\circ$, če za $\forall a, b \in N$ velja $a \circ b \in N$.

Primer: soda števila v $\mathbb{Z}$ za seštevanje.

Takemu N, kjer je $N \subseteq M$ zaprta za $\circ$, pravimo podgrupoid.

Podgrupoidu privedimo operacijo $a \circ_N b = a \circ b$. tako je $(N, \circ_N)$ grupoid.