$\mathrm{red}(i_1\, i_2\, i_3 \dots i_k) = k$ cikel dolžine k

$\sigma \in S_n$

$\sigma = \gamma_1 \cdots \gamma_k$ produkt k ciklov

$r = \mathrm{lcm}(m_1, m_2, m_3, \dots m_k) = \mathrm{red}(\sigma)$

↳ dolžine ciklov

N

Poišči podgrupo z 2 in 3 elementi v S_3.

vse možne permutacije 3 elementov.

$\{id, (1,2)\}$

$\{id, (1\,2\,3), (3\,2\,1)\}$

$id * (1\;2\;3) = (1\;2\;3)$

$id * id = id$

$(1\;2\;3) * (1\;2\;3) = (1\;3\;2)$

N

Pokaži, da je množica preslikav $\mathbb{N} \to \mathbb{N}$ monoid za kompozicijo in da ima

$f(n) = \begin{cases} 1, & n=1 \\ n-1; & n \geq 2 \end{cases}$ desni inverz, ne pa levega.

monoid: asociativnost, zaprtost, grupoid

kompozicija je zaprta in asociativna

enota: $e(n) = n$ $\}$ id

protiprimer, da to ni grupa (nima inverza):

$f(n) = \begin{cases} 1, & n=1 \\ n-1, & n \geq 2 \end{cases}$ ima desni, ne pa levi inverz.

$f \circ f^{-1} = e$

$f^{-1} \circ f = e$

↳ ✗

$f^{-1}(n) = n+1$

levi inverz ne obstaja, ker se v 1 slikata tako 1 kot 2.

alternativno navedimo dva desna inverza, torej levi ne obstaja. — ni bijektivna.

drugi desni inverz je

$$f_2^{-1}(n) = \begin{cases} 1; & n=1 \\ n+1; & \text{drugače} \end{cases}$$

N

let $(M, \circ)$ monoid

Pokaži, da je množica vseh obrnljivih elementov v M podmonoid, ki je tudi grupa.

$M^* = \{m \in M; \exists m^{-1}\}$

M^* zaprt za operacijo:

$a, b \in M^*$.

dokazujemo $a \circ b \in M^*$, dokazujemo $\exists (a \circ b)^{-1}$

$\exists a^{-1}, b^{-1}$

Po izreku $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ → $\exists b^{-1}, a^{-1}$

za monoid moramo imeti enoto.

za enoto velja $e \circ e = e$.

↳ torej e je obrnljiva, torej e je v M^*.

grupa?:

Vsak $m \in M^*$ mora biti obrnljiv. Je, po definiciji.

torej je $(M^*, \circ)$ grupa

N

$(G, \circ)$ je grupa. Pokaži, da je

$C(G) = \{ s \in G;\ g \circ s = s \circ g \quad \forall g \in G \}$

podgrupa.

$a, b \in C(G) \Rightarrow a \circ b^{-1} \in C(G)$ → izrek od včeraj.

DOKAZ:

$x, y \in C(G) \Rightarrow x \circ y^{-1} \in C(G)$

$g \circ (x \circ y^{-1}) = (g \circ x) \circ y^{-1} =$

$= (x \circ g) \circ y^{-1} = x \circ (g \circ y^{-1}) =$

$= x \circ (y^{-1} \circ g) = (x \circ y^{-1}) \circ g$

velja:
- asociativnost
- $g \circ x = x \circ g$
- $g \circ y = y \circ g$

$y^{-1} \circ g \circ y = y^{-1} \circ y \circ g$

$y^{-1} \circ g \circ y \cancel{\circ y^{-1}} = \cancel{y^{-1} \circ y} \circ g \circ y^{-1}$

$y^{-1} \circ g = g \circ y^{-1}$

N

Prepričaj se, da so naslednje preslikave homomorfizmi! izomorfizmi?

a) $f: (\mathbb{C} \setminus \{0\}, \cdot) \longrightarrow (\mathbb{R} \setminus \{0\}, \cdot)$

$f(z) = |z|$

Preveriti je treba, da je $f(zw) = f(z) f(w)$

$|zw| = |z||w|$

ni injektivna, ker $f(1) = f(-1) = 1 \Rightarrow$ ni izomorfizem je homomorfizem, ker $|zw|=|z||w|$ velja.

b) $f:(\mathbb{R},+)\to((0,\infty),\cdot)$

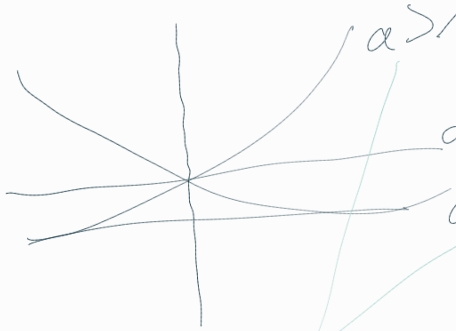
$f(x)=a^x \quad a>0$

$f(x)f(y)=f(x+y)=a^x a^y = a^{x+y}$ ✓

je homomorfizem.

je izomorfizem, razen za $a\neq 1$, ko ni.

za $a\neq 1$,



N

b) $(G,\circ)$ grupa $\quad f: G\to G$

$f(x)=x\circ x$

G komutativna $\Leftrightarrow f$ homomorfizem

Dokaz $\Rightarrow$:

vemo: $x\circ y = y\circ x$ $\qquad$ dokazujemo G komutativna

$f(x\circ y)=f(x)\circ f(y)$

$x\circ y\circ x\circ y = x\circ x\circ y\circ y =$

$= x\circ y\circ x\circ y$ ✓

Dokaz $\Leftarrow$:

vemo: G homomorfizem $\qquad$ dokazujemo $x\circ y=y\circ x$

$f(x\circ y)=f(x)\circ f(y)=$ $\qquad$ grupa ima inverze!

$= x^{-1} \circ | \ x \circ y \circ x \circ y = x \circ x \circ y \circ y \quad | \circ y^{-1}$

$= \cancel{x^{-1} \circ x} \circ y \circ x \circ \cancel{y \circ y^{-1}} = \cancel{x^{-1} \circ x} \circ x \circ y \circ \cancel{y \circ y^{-1}}$

$y \circ x = x \circ y$

N

homomorfizem $f: G \to H$ pokaži, da red elementa $f(g)$ deli $\text{red}(g)$

<namig>

namig: $g^m = 1 \iff \text{red}\, g \mid m$

$g^m = 1 \qquad \text{red}\, g = n$

hočemo $m|n$.

$m = qn + r$

$r = 0$

$g^{qn+r} = 1 = (g^n)^q \quad g^r = 1$

$1 \cdot g^r = 1$

$r = 0$

$\text{red}(\ell)$

$\downarrow$

tak $n \neq 0$, da

$\ell^n = e$ enota

Dokaz $\Leftarrow \quad \underbrace{\text{red}\, g}_{n} \mid m \qquad g^m = 1$

$m = qn \qquad g^{qn} = 1$

$(g^n)^q = 1 = 1^q = 1$

</namig>

$f(g)^n = 1 = f(g) f(g) \cdots f(g) = f(g^n)$

homomorfizmi

$f(1) = 1$ ZENOTA!

↳ homomorfizem ohranja enoto.

N
Def: KOLOBAR: $(M, +, \cdot)$
↳ dve operaciji:

pogoji za kolobar:

- $(M, +)$ abelova grupa (komut. grupa)
- $(M, \cdot)$ polgrupa
- velja distributivnost

če imamo enoto v $(M, \cdot)$, je „kolobar z enoto"
če je komutativna $(M, \cdot)$, je „komutativen kolobar"

$a \oplus b = a + b + 1$ $\quad a, b \in \mathbb{R}$.
$a \otimes b = a + b + ab$

a je $(\mathbb{R}, \oplus, \otimes)$ kolobar?

- a je $(\mathbb{R}, \oplus)$ abelova grupa?

asociativnost:

$(a \oplus b) \oplus c = a \oplus (b \oplus c)$

$(a + b + 1) + (a + b + 1) + c + 1 = \dots$

da, zaradi asoc. +.

komutativnost

da, zaradi komutativnosti + v $\mathbb{R}$

enota:

-1.

inverz:

$a^{-1} = -a - 2$

$(\mathbb{R}, \otimes)$ je polgrupa (dokazali začetič)

asoc ✓
kom ✓
enota 0

$a \neq 1: a^{-1} = -\frac{a}{1+a}$

distributivnost: $(a \oplus b) \otimes c$