$(S, \cdot)$, $\cdot$ binarna operacija na S

$\mathbb{Z}$ z operacijama $+$ in $\cdot$
$A \subseteq \mathbb{Z}$ je zaprta za $\cdot$, če $a, b \in A \Rightarrow a \cdot b \in A$

soda števila so zaprta za $+$ in $\cdot$
negativna cela števila so zaprta za $+$, ne pa za $\cdot$
liha števila so zaprta za $\cdot$, ne pa za $+$
$\{1, -1\}$ je -||-
$\mathbb{Z} \setminus \{0\}$ je -||-

Naj bo $|S| = n$. Koliko je binarnih operacij na S?

$|S \times S| = |S|^2$

$\underbrace{|S| \cdot \ldots \cdot |S|}_{|S|^2} = |S|^{|S|^2}$

$\cdot$ je asociativna, če velja:
$\forall a, b, c \in S : (a \cdot b) \cdot c = a \cdot (b \cdot c)$

Pokaži, da za asociativno operacijo $\cdot$ rezultat $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ ni odvisen od postavitve oklepajev.

$(a_1 \cdot a_2) \cdot (a_3 \cdot a_4) = a_1 \cdot (a_2 \cdot (a_3 \cdot a_4)) = a_1 \cdot ((a_2 \cdot a_3) \cdot a_4)$

Uporabimo indukcijo.

Za $n \leq 4$ smo dokazali.

Predpostavimo, da drži za $3 \leq k < n$, za $n \geq 4$.

Poglejmo zadnjo uporabo operacije.

$(a_1 \cdots a_\ell) \cdot (a_{\ell+1} \cdots a_n)$, $1 \leq \ell \leq n-1$

$\ell = 1$: Po I.P. velja $a_1 (a_2 (\cdots (a_{n-1} a_n)))$

$\ell \geq 2$: $\overset{\text{I.P.}}{(a_1 \cdots a_\ell) \cdot (a_{\ell+1} (a_{\ell+2} (\cdots (a_{n-1} a_n))))} \overset{\text{I.P.}}{=}$

$= \underbrace{(a_1 (a_2 (\cdots (a_{\ell-1} a_\ell))))}_{a} \cdot \underbrace{(a_{\ell+1} (\cdots (a_n)))}_{c} \overset{\text{asoc.}}{=}$

$= a_1 \cdot (\underbrace{b \cdot c}_{b}) \overset{\text{I.P.}}{=} a_1 \cdot (a_2 \cdot (a_3 \cdot (\cdots (a_n))))$

Polgrupa $(S, \cdot)$, kjer je $\cdot$ asociativna na S.

Monoid je polgrupa z enoto: $\forall s \in S: 1 \cdot s = s \cdot 1 = s$

No je monoid, ki ni grupa.

Naj bo $(S, \cdot)$ monoid in $s \in S$. Element $t \in S$ je levi oziroma desni inverz od s, če velja $t \cdot s = 1$ oziroma $s \cdot t = 1$.

Če je ℓ levi inverz od s in r desni inverz od s, potem je $\ell = r$.

$$l = l \cdot 1 = l \cdot (s \cdot r) = (l \cdot s) \cdot r = 1 \cdot r = r$$

Če ima s inverz, potem je inverz en sam.

Naj bo S končen monoid in ima $s \in S$ levi inverz. Dokaži, da je potem S obrnljiv.

Po predpostavki velja $t \cdot s = 1$ za vsak $t \in S$.

$1, s, s^2, s^3, \ldots$

V tem zaporedju so ponavljanja.

$s^n = s^{n+m}$, kjer je $m \geq 1$

$t^2 \cdot s^2 = (t \cdot t) \cdot (s \cdot s) = t \cdot (ts) \cdot s = t \cdot s$
$t^3 \cdot s^3 = t \cdot t^2 s^2 \cdot s = t \cdot s$

$\Rightarrow \forall n : t^n s^n = 1$

$1 = t^n \cdot s^n = t^n \cdot s^{n+m} = t^n s^n \cdot s^m = 1 \cdot s^m = s^m$

$1 = s \cdot \underbrace{s^{m-1}}_{\text{desni inverz}} = \underbrace{s^{m-1}}_{\text{levi inverz}} \cdot s$

$\Rightarrow s$ ima levi in desni inverz in $t = s^{m-1}$

Navedite primer monoida S in elementa $s \in S$, ki ima levi inverz, nima pa desnega. Navedi vsaj dva različna leva inverza.

Označimo s $\mathcal{F}(X)$ množico vseh preslikav iz X v X. To je monoid z operacijo kompozituma.

$\mathcal{F}(\mathbb{N})$

Obrljivi elementi $Sim(\mathbb{N})$ so bijekcije / permutacije.

$f(n) = 2n$ je injektivna, ampak ni surjektivna

Definirajmo $g : \mathbb{N} \to \mathbb{N}$ s predpisom:

$g_1(2n) = n$
$g_1(2n+1) = 1$ ali $g_2(2n+1) = 2n+1$
za $n \in \mathbb{N}$

$\Rightarrow \forall n \in \mathbb{N} : g(f(n)) = n$
$\Rightarrow g \circ f = id$
$\Rightarrow g$ je levi inverz za f

$\Rightarrow g_1$ in g_2 sta leva inverza

$\Rightarrow f$ nima desnega inverza

Naj bo $(S, \cdot)$ monoid. Ali sta $x, y \in S$ obrnljiva, če je obrnljiv xyx oziroma če je obrnljiv xy?

a) xyx obrnljiv
$\Rightarrow z \cdot xyx = xyx \cdot z = 1$

$\Rightarrow$ Inverz od x je $zxy = yxz$.

x, y obrnljiva
$\Rightarrow$ xy je obrnljiv in velja $(xy)^{-1} = y^{-1}x^{-1}$

x obrnljiv
$\Rightarrow$ x^{-1} je obrnljiv in $(x^{-1})^{-1} = x$

$y = 1 \cdot y \cdot 1 = x^{-1}xyxx^{-1}$

$\Rightarrow$ y obrnljiv kot produkt obrnljivih elementov

b) xy obrnljiv

Iz prejšnje naloge:
$g_1 \circ f = id$

g_1 in f nista obrnljivi, id pa je.
Torej ne velja.