let G ciklična grupa. $a \in G$

$$G \cong \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\} \quad n \text{ je red } |a|.$$

ali je $(\mathbb{Z}_9, +)$ ciklična. če je, poišči vse $a \in \mathbb{Z}_9$, da je $\mathbb{Z}_9 \cong \langle a \rangle$. tak a je 1.

$1^2 = 2$
$1^3 = 3$
$1^4 = 4$
$\vdots$
$1^9 = 0$

red $1 = 9$

$\mathbb{Z}_9$ je ciklična,
$\langle 1 \rangle = \mathbb{Z}_9$

$2^2 = 4$
$2^3 = 6$
$2^4 = 8$
$2^5 = 1$
$2^6 = 3$
$2^7 = 5$
$2^8 = 7$
$2^9 = 0$

$3: \ 3, 6, 0$

...

$\langle 2 \rangle = G$
$\langle 3 \rangle \neq G$
$\langle 4 \rangle = G$
$\langle 5 \rangle = G$
$\langle 6 \rangle \neq G$
$\langle 7 \rangle = G$
$\langle 8 \rangle = G$
$\langle 0 \rangle \neq G$

velja: $\langle n \rangle = \mathbb{Z}_k \Leftrightarrow \gcd(n, k) = 1$

N

<u>Vsaka podgrupa ciklične grupe je ciklična.</u>

let G ciklična, $H \leq G$ <u>H ciklična $\Leftrightarrow \exists h \in H \ni: \langle h \rangle = H$</u>

(trivialni)
vsaka grupa ima vsaj podgrupi $\{e\}$ in G. Do
predpostavki sta ti dve ciklični.

Prava podgrupa je podgrupa, ki ni trivialna.

let H prava podgrupa.
$\exists h \in H \ni: h \neq e$

let a osnovni element G: $\langle a \rangle = G$.

ker so vsi elementi G a^t, je tudi $h = a^t$ za nek t. tudi h^{-1} mora biti v H. $h^{-1} = a^{-t}$

a ni v H, sicer bi bil $H = G$ in s tem neprava podgrupa. So pa v H neke potence a. naj bo a^m najmanjša potenca a, ki je v H.

$$\underline{\langle a^m \rangle = H}$$

let b poljuben $\in H$.
ker je $b \in G$, je $\underline{b = (a^m)^r}$.

vemo $m < t$, če $m = t$ je $b = a^t$.

PDDRAA $b \neq (a^m)^i$

$$t = m \cdot i + q, \quad 0 < q < m$$

ker t ni deljiv z m.

$$b = a^t = a^{mi+q} = a^{mi} a^q$$

$$b^{-1} = a^{-t} = a^{-mi-q} = (a^{mi} a^q)^{-1} = (a^m)^{-i} a^{-q}$$

vemo: $a^{mi} \in H$
$\Rightarrow a^{-mi} \in H$

$$\underbrace{a^{mi+q}}_{b \in H} \cdot \overbrace{a^{-mi}}^{\in H} = a^q \in H \quad \times,$$

$q < m$, toda m je najmanjši $a^m \in H$.

nts. ideja: nek matematični dokaz z RAA napiši drugače -- tako, da najdeš protislovje s čim drugim. za katere resnične trditve lahko dokažeš, da ne držijo, ko si v nekem RAA okolju? A lahko falsificiraš poljubno mat. trditev?

ja, lahko. Dokažeš namreč true = false, torej polgrupa true.txt = polgrupa false.txt
i think...

N

let L_n množica vseh lihih permutacij.

Ali je L_n grupa za kompozicijo?

Ne. Operacija ni notranja, saj je $\pi_1 \circ \pi_2$ soda.
liha liha

N

Pokaži: za vsako permutacijsko grupo so bodisi vse permutacije sode bodisi je sodih enako tot lihih.

$G \leq S_n$.

$id \in G$, id soda

case $\forall \pi \in G: \pi$ soda ✓

case (sicer): $\exists \pi \in G \ni: \pi$ liha ✓

f bijektivna $\quad f: G \to G$

$f(\sigma) \mapsto \sigma\pi$

injekcija: $\sigma_1, \sigma_2, f\sigma_1 \neq f\sigma_2 \Rightarrow \sigma_1 \neq \sigma_2$ ✓

pravilo krajšanja

$\pi^{-1}\backslash \quad \pi\sigma_1 \neq \pi\sigma_2$

$\sigma_1 \neq \sigma_2$

surjekcija: $\forall \sigma \in G \; \exists \sigma' \ni: f\sigma' = \sigma$

$f\sigma' \overset{?}{=} \sigma$

$\pi\sigma' = \sigma$

$\sigma' = \pi^{-1}\sigma$ ✓

□

N

$(\mathbb{R},+) \cong (\mathbb{R}^+,\cdot)$

iščemo bijektivni hmf oz. imf.

$\hookrightarrow f(a +_1 b) = f(a) +_2 f(b)$

$$e^{a+b} = e^a \cdot e^b$$

$$\ln(ab) = \ln a + \ln b$$

ln je bijekcija ✓

inj: strogo naraščajoča

surj: inverz

N

$(\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}, +)$ je grupa.

$\hookrightarrow$ seštevanje po komponentah

$(\mathbb{Z}_2 \times \mathbb{Z}_3, +) \approx (\mathbb{Z}_6, +)$

$\mathbb{Z}_2 = \{0,1\}$ $\quad \mathbb{Z}_3 = \{0,1,2\}$ $\quad \mathbb{Z}_6 = \{\underset{1}{0}, \underset{6}{1}, \underset{3}{2}, \underset{2}{3}, \underset{3}{4}, \underset{6}{5}\}$

redi:

$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{ \overset{1}{(0,0)}, \overset{3}{(0,1)}, \overset{3}{(0,2)}, \overset{2}{(1,0)}, \overset{6}{(1,1)}, \overset{6}{(1,2)} \}$

Če obstaja tak imf, velja $f((0,0)) = 0$

imf ohrani red.

imf:

0	(0,0)
1	(1,1)
2	(0,2)
3	(1,0)
4	(0,1)
5	(1,2)

N

Dokaži: $(\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}, +) \approx (\mathbb{Z}_{n_1 n_2}, +) \Leftrightarrow \gcd(n_1, n_2) = 1$

$(\Rightarrow)$: predp.: $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \approx \mathbb{Z}_{n_1 n_2}$
v obeh obstaja element reda $n_1 n_2$, saj je $\mathbb{Z}_{n_1 n_2}$ ciklična in se red ohranja. Zato v $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ obstaja (x,y) reda $n_1 n_2$.

$\mathrm{red}(x) = r_x \leq n_1 \quad r_x \mid n_1$
$\mathrm{red}(y) = r_y \leq n_2 \quad r_y \mid n_2 \quad \Rightarrow r_x, r_y \mid n_1 n_2$

$r_x, r_y \mid \mathrm{lcm}(n_1, n_2)$

$\mathrm{red}((x,y)) = \mathrm{lcm}(r_x, r_y) \leq \mathrm{lcm}(n_1, n_2) = \frac{n_1 n_2}{\gcd(n_1, n_2)}$

$\mathrm{red}((x,y)) = n_1 n_2$

$ab = \mathrm{lcm}(a,b)\gcd(a,b)$
$\mathrm{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$

$n_1 n_2 \leq \frac{n_1 n_2}{\gcd(n_1, n_2)}$
$\Rightarrow \gcd(n_1, n_2) = 1$

$(\Leftarrow)$: $\gcd(n_1, n_2) = 1$:predpostavka
n_1, n_2 tuji $\Rightarrow \exists\, a \in \mathbb{Z}_{n_1} \ni: \langle a \rangle = \mathbb{Z}_{n_1}$
$\exists\, b \in \mathbb{Z}_{n_2} \ni: \langle b \rangle = \mathbb{Z}_{n_2}$
$\Rightarrow$ $\mathrm{red}\ a = n_1$, $\mathrm{red}\ b = n_2$ $\Rightarrow \mathrm{red}(ab) = \mathrm{lcm}(a,b) = n_1 n_2$

z ab lahko generiramo
$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} = \langle ab \rangle$

$\Rightarrow |\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}| = n_1 n_2$

$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \cong \mathbb{Z}_{n_1 n_2}$

N

S_3 a) poišči vse podgrupe $\forall a,b \in H : a^{-1} b \in H$

b) poišči vse edinke

$S_3 = \{ id, (12), (13), (2\ 3), (1\ 3\ 2), (1 2 3) \}$

moč podgrupe mora deliti moč grupe: možne moči:

6, 1, 3, 2

S_3 id

vse sode

$\{ id, (123), (132) \}$

podgrupa ne bodisi le sode bodisi lihih toliko ~~tot~~ sodih.

$\{ id, (12) \}, \{ id, (1 3) \}, \{ id, (2\ 3) \},$

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

ne, ker ni zaprta: $(132)(132) = (123)$

zaprtost: $(1 2\ 3)(1\ 3\ 2) = id$

$(132)(1 2\ 3) = id$

Grupa je edinka, ko je $\forall a \in G : aH = Ha = H = aHa^{-1}$

$\{ id, (1,2) \} \triangleright G$?

$(2\ 3)(1\ 2)(2\ 3)^{-1} = (2\ 3)(12)(2\ 3) = (2\ 3)(1\ 2\ 3) = (1\ 3) \notin \{ id, (1,2) \}$

ni edinka

$\{ id, (1,3) \}$ ... ni edinka

$\{ id, (2,3) \}$ ... ni edinka

$\{ id, (1,2,3) \} = A_3$, $x \in S_3$

soda

$\underline{x} \ \underline{\pi} \ \underline{x}^{-1} \in \underline{A_3}$

enaki parnosti

$x \pi x^{-1}$ soda $\in A^3$

JE EDINKA ✓

N

H je množica permutacij $\{\pi \in S_4 \ ; \ \pi(4) = 4\} = H$

↳ fiksna točka

$\underline{H \leq S_4}$

$\forall a,b \in H: \ a^{-1}b \in H$

$a(4) = 4$
$a^{-1}(4) = 4$
$b(4) = 4$
$b^{-1}(4) = 4$

in $(a^{-1}b)(4) = 4$

✓ torej je podgrupa.

H edinka?

$H = \{id, (12), (13), (23), (123), (132)\}$

↳ $\forall a \in S_4: \ aHa^{-1} = H$

protiprimer $a = (1\ 4)$:

$(14)(13)(14)^{-1} = (14)(13)(14) = (14)(4\ 3\ 1) =$

$= (3\ 4) \notin H$, torej

ni edinka

Kaj so levi odseki S_4 po H?

$\forall a \in H: \ aH = H$

$\forall a \in H: \ aH = \{a, a(12), a(13), a(2\ 3), a(132), a(1\ 2\ 3)\}$

recimo $a = (1\ 4)$:

$(14)H = \{(14), (124), (134), (14)(23), (1234),$
$(1\ 3\ 2\ 4)\}$

to so vse preslikave, ki slikajo 4 v 1.

$(24)H \ldots$ vse, ki ... 4 v 2

$(34)H \ldots$ 4 v 3

Naši levi odseki so torej H, $(14)H$, $(24)H$, $(34)H$