

LINEARNA ALGEBRA 2020/21
11. VAJE: 14. 12. 2019

1. Naj bosta

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 7 & 8 & 6 & 3 & 5 & 4 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 8 & 7 & 4 \end{pmatrix} \in S_8$$

permutaciji.

Zapiši π, σ kot produkt disjunktnih ciklov.

Izračunaj red α in β .

2. Pokaži, da S_3 ni komutativna.
3. Naj bo G grupa in $g \in G$. Pokaži, da je $f: (\mathbb{Z}, +) \rightarrow G, f(n) = g^n$ homomorfizem grup.
4. Pokaži, da je $f: (\mathbb{R}, +) \rightarrow (\mathbb{R}^+, *), f(x) = e^x$ homomorfizem grup. Ali je tudi izomorfizem?
5. Naj bosta $1_G, 1_H$ enoti grup G, H , naj bo $f: G \rightarrow H$ homomorfizem. Pokaži, da je f injektiven natanko tedaj, ko iz $f(g) = 1_H$ sledi $g = 1_G$.
6. Naj bo $f: G \rightarrow H$ homomorfizem. Pokaži, da red elementa $g \in G$ deli red elementa $f(g) \in H$.
7. Določi red elementa $k \in \mathbb{Z}_n$. Kdaj obstaja kak netrivialen homomorfizem iz $(\mathbb{Z}_n, +)$ v $(\mathbb{Z}_m, +)$?
8. Pokaži, da je $\mathbb{Z}_2 \times \mathbb{Z}_3$ izomorfna $\mathbb{Z}_6$. Pokaži, da $\mathbb{Z}_9$ ni izomorfna $\mathbb{Z}_3 \times \mathbb{Z}_3$.
9. Naj bo $(R, +, \cdot)$ (asociativen) kolobar pokaži, da je $r0 = 0r = 0$ za vsak $r \in R$.
Dokaži: če je $1 = 0$, potem je $R = \{0\}$.

1. Naj bosta

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 7 & 8 & 6 & 3 & 5 & 4 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 8 & 7 & 4 \end{pmatrix} \in S_8$$

permutaciji.

Zapiši π, σ kot produkt disjunktnih ciklov.

Izračunaj red ~~π~~ in ~~σ~~ .

S_n = množica bijekcij iz $\{1, 2, 3, \dots, n\}$ v $\{1, 2, 3, \dots, n\}$.
operacija: kompozicija preslikav.

$$f = \begin{pmatrix} 1 & 2 & \dots & j & \dots & n \\ x_1 & x_2 & \dots & x_j & \dots & x_n \end{pmatrix} \in S_n$$

$f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$
vsak element iz $\{1, \dots, n\}$ se pojavi natanko enkrat.

$$f(i) = x_i$$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 7 & 8 & 6 & 3 & 5 & 4 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 8 & 7 & 4 \end{pmatrix} \in S_8$$

...

$$\pi \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 7 & 2 & 6 & 3 & 4 & 5 & 8 \end{pmatrix}$$

$$\pi \sigma(1) = \pi(2) = 1, \pi \sigma(2) = \pi(3) = 7, \pi \sigma(3) = \pi(1) = 2$$

$$\pi \sigma(4) = \pi(5) = 6, \dots$$

Cikli

$\alpha = (x_1, x_2, x_3, \dots, x_k)$ — noben x_i se ne ponovi

• $\alpha(x_i) = x_{i+1}$, $\alpha(x_k) = x_1$, $\alpha(y) = y$, če $y \notin \{x_1, x_2, \dots, x_k\}$

• zapis ni evkliden $(x_1, x_2, \dots, x_k) = (x_2, x_3, \dots, x_k, x_1) = (x_k, x_1, x_2, \dots, x_{k-1})$

• zapis je evkliden, če na prvo mesto postavimo najmanjše število.



- Vsako permutacijo lahko zapisemo (do vrstnega reda ciklov) enolično kot produkt disjunktih ciklov.

↓
cikla $\alpha = (x_1, \dots, x_k)$, $\beta = (y_1, \dots, y_l)$ sta disjunktna, če je $\{x_1, \dots, x_k\} \cap \{y_1, \dots, y_l\} = \emptyset$

- disjunktne cikli komutirajo — ($\alpha\beta = \beta\alpha$)

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 7 & 8 & 6 & 3 & 5 & 4 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 8 & 7 & 4 \end{pmatrix}$$

$$\pi = (1, 2)(3, 7, 5, 6)(4, 8)$$

$$\sigma = (1, 2, 3)(4, 5, 6, 8)(7) = (1, 2, 3)(4, 5, 6, 8)$$

↘ cikle dolžine 1 lahko spustimo

- Če cikla nista disjunktna, njunemu produktu pripadno neke zapis z disjunktini cikli npr.

$$(1, 2, 3)(2, 3, 5) = (1, 2)(3, 5)$$

$$(1, 2, 3)(2, 3, 5)[1] = (1, 2, 3)[1] = 2$$

$$(1, 2, 3)(2, 3, 5)[2] = (1, 2, 3)[3] = 1$$

- red elementa je najmanjši (če obstaja) $n \in \mathbb{N}$, da je $g^n = 1$

- red cikla dolžine k je enak k

$$\pi = (x_1, \dots, x_k)$$

$$\pi^i(x_i) = x_{i+j} \quad \left(\begin{array}{l} \text{Uporabimo zapis} \\ x_{i+j} = x_{i+j-k} \text{ če je } i+j > k \end{array} \right)$$

$$x_i \neq x_{i+j} \quad j < k$$

$$x_i = x_{i+k} \quad \checkmark$$

$$\pi^k = \text{id}$$

če je n red g , $m \in \mathbb{N}$, da je $g^m = 1$, potem $n \mid m$.

Predpostavimo $m > n$

(Če je $m = n$, potem $n \mid m$ če je očitno, je to v resnici z minimalnostjo n)

$$\text{potem je } g^{m-n} = 1$$

$$(1) \quad m-n = k \Rightarrow m = 2n$$

$$(2) \quad (m-n) > n$$

$$(3) \quad (m-n) < n \Rightarrow \text{z minimalnostjo}$$

Pozor! Če je $m = kn$ za $k \in \mathbb{N}$.

- $\pi = (x_1 \dots x_k)(y_1 \dots y_l) \dots$ produkt disjunktih ciklov z dolžinami $k_1, \dots, k_r$

$$\text{red } \pi = \text{lcm}(k_1, \dots, k_r)$$

nej. ko $k = \text{red } \pi$

$$\pi^k = (x_1 \dots x_k)^k (y_1 \dots y_l)^k \dots$$

$(x_1 \dots x_k)^k = \text{id} \Rightarrow k_1 \mid k$ podobno $k_j \mid k \quad j=1, \dots, r$ $k = \text{lcm}(k_1, \dots, k_r)$ je najmanjši, ki ustreza tem pogojem. Velja tudi $\pi^{\text{lcm}(k_1, \dots, k_r)} = \text{id}$.

S_3 ni komutativna!

Vse grupe moči ≤ 6 so komutativne!

$$(12)(13) = (132)$$

$$(13)(12) = (123)$$

Nasli smo $\alpha, \beta \in S_3$ $\alpha\beta \neq \beta\alpha$.

G, H grupi

$f: G \rightarrow H$ je homomorfizem

$$\forall g_1, g_2 \in G \quad \underbrace{f(g_1 g_2)}_{\text{operacija v } G} = \underbrace{f(g_1) \cdot f(g_2)}_{\text{operacija v } H}$$

3. Naj bo G grupa in $g \in G$. Pokaži, da je $f: (\mathbb{Z}, +) \rightarrow G, f(n) = g^n$ homomorfizem grup.

4. Pokaži, da je $f: (\mathbb{R}, +) \rightarrow (\mathbb{R}^+, \cdot), f(x) = e^x$ homomorfizem grup. Ali je tudi izomorfizem?

$$3. f(n) = g^n = \underbrace{g \cdot g \cdots g}_n$$

$$f(n+m) = g^{n+m} = \underbrace{g \cdots g}_{n+m} = \underbrace{(g \cdots g)}_n \underbrace{(g \cdots g)}_m = g^n \cdot g^m = f(n) \cdot f(m)$$

$$4. e^{x+y} = e^x \cdot e^y \quad (e^x > 0 \quad \forall x \in \mathbb{R})$$

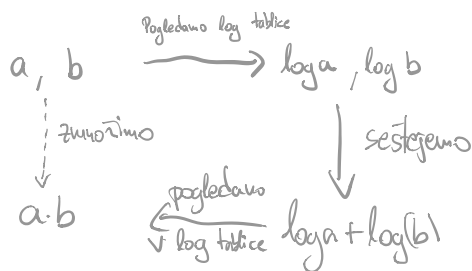
pozitivna realna števila
 $(\mathbb{R}^+, \cdot)$
 1
 inverz a je $\frac{1}{a}$

Isomorfizem je bijektivni homomorfizem

$$f(x) = e^x \quad \text{tudi inverz } \ln(x) \quad \ln(xy) = \ln(x) + \ln(y)$$

Trivna: Uporabo logaritmskih tablic

ljude raje sestevamo kot množimo.



5. Naj bosta $1_G, 1_H$ enoti grup G, H , naj bo $f: G \rightarrow H$ homomorfizem. Pokaži, da je f injektiven natanko tedaj, ko iz $f(g) = 1_H$ sledi $g = 1_G$.
6. Naj bo $f: G \rightarrow H$ homomorfizem. Pokaži, da red elementa $g \in G$ deli red elementa $f(g) \in H$.

Lema če je $f: G \rightarrow H$ homomorfizem, potem je $f(1_G) = 1_H$ in $f(g)^{-1} = f(g^{-1})$

$$f(1_G) = f(1_G 1_G) = f(1_G) f(1_G) \quad / : f(1_G)^{-1}$$

$$1_H = f(1_G)$$

$$f(g) \cdot f(g^{-1}) = f(g g^{-1}) = f(1_G) = 1_H \stackrel{\text{def. inverza}}{\Rightarrow} f(g^{-1}) = f(g)^{-1}$$

$$\parallel$$

$$f(g^{-1}) \cdot f(g)$$

5. Za splošne preslikava f je injektivna, če iz $f(x) = f(y)$ sledi $x = y$
 $\Rightarrow$

Naj bo f injektiven homomorfizem, potem iz $f(g) = f(1_G) = 1_H$ sledi $g = 1_G$

$\Leftarrow$ Predpostavimo, da iz $f(g) = 1_H$ sledi $g = 1_G$

Naj bo $f(g) = f(h)$, potem je $f(g) \cdot f(h^{-1}) = 1_H$ $f(g h^{-1}) = 1_H \stackrel{\text{predpostavba}}{\Rightarrow} g h^{-1} = 1_G$
 $\downarrow$
 $g = h$

Pokazali smo iz $f(g) = f(h)$ sledi $g = h$. (injektivnost)

6. Naj bo n red elementa g .
 Želimo pokazati $f(g)^n = 1_H$
 $f(g)^n = f(g^n) = f(1_G) = 1_H$.

$\bar{c}$ je n red g , $m \in \mathbb{N}$, da
 je $g^m = 1$, potem $n \mid m$.
 (Če je $m = n$, potem $n \mid m$ če je $0 \leq m < n$
 je to v resnici z minimálností n)
 Predpostavimo $m > n$
 potem je $g^{m-n} = 1$
 ① $m - n = n \Rightarrow m = 2n$
 ② $(m - n) > n$
 ③ $(m - n) < n \Rightarrow$ z minimálností
 Potem je v obeh $m = 2n$ za $2 \in \mathbb{N}$.

7. Določi red elementa $k \in \mathbb{Z}_n$. Kdaj obstaja kak netrivialen homomorfizem iz $(\mathbb{Z}_n, +)$
 v $(\mathbb{Z}_m, +)$?

8. Pokaži, da je $\mathbb{Z}_2 \times \mathbb{Z}_3$ izomorfna $\mathbb{Z}_6$. Pokaži, da $\mathbb{Z}_9$ ni izomorfna $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Elemente $\mathbb{Z}_n$ označujemo enako kot elemente $\{0, \dots, n-1\} \subseteq \mathbb{Z}$, v mislih imamo, da je
 operacija drugačna. Uporabili bomo oznako $k_1 + k_2 \equiv k_3$ če enakovrednost velja v $\mathbb{Z}_n$.

Uporabili bomo tudi oznako $n \cdot k = \overbrace{k + \dots + k}^{n \text{ krat}}$
 $n \in \mathbb{Z}$ $k \in \mathbb{Z}_n$

• Red elementa $1 \in \mathbb{Z}_n$ ima red n ($n \cdot 1 \equiv 0$, $k \cdot 1 \equiv k \neq 1$ za $k < n$)

• Za vsak element $r \in \mathbb{Z}_n$ je $n \cdot r \equiv 0$.

7. Za vsak homomorfizem $f: \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ je $f(k) = f(\underbrace{1+1+\dots+1}_k) = k f(1)$.

f je netrivialen $\Leftrightarrow f(1) \neq 0 \in \mathbb{Z}_m$

$0 = f(0) = f(n \cdot 1) = n \cdot f(1) \Rightarrow n \cdot f(1) \equiv 0$ in $m \cdot f(1) \equiv 0$ (tudi $\gcd(n, m) f(1) = 0$)

Če je $\gcd(n, m) = 1$ (n, m sta tuja) $\Rightarrow f(1) \equiv 0 \Rightarrow f$ je trivialen

če $\gcd(n, m) = k$, potem $f(1) = \frac{m}{k}$ določa homomorfizem.
 $\mathbb{N} \{1, 2, \dots, m-k\}$

8. Naj bo $f: \mathbb{Z}_3 \times \mathbb{Z}_3 \rightarrow \mathbb{Z}_9$ homomorfizem. Potem, obstaja $(u, v) \in \mathbb{Z}_3 \times \mathbb{Z}_3$, da je $f(u, v) = 1 \in \mathbb{Z}_9$
 $1 \in \mathbb{Z}_9$ ima red 9, (u, v) ima red 3 ali 1 $\mathbb{Z}_{3,1} \rightarrow \mathbb{Z}_9$ torej homomorfizem ne obstaja