DS 2 VAJE 10

1. $GL(\mathbb{R}, 2)$

$$H = \left\{ \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix};\ \varphi \in \mathbb{R} \right\}$$

DOKAŽI, DA JE $H \leq GL(\mathbb{R}, 2)$.

OPERACIJA NOTRANJA:

$$\begin{bmatrix} \cos\varphi_1 & -\sin\varphi_1 \\ \sin\varphi_1 & \cos\varphi_1 \end{bmatrix} \cdot \begin{bmatrix} \cos\varphi_2 & -\sin\varphi_2 \\ \sin\varphi_2 & \cos\varphi_2 \end{bmatrix} =$$

$$= \begin{bmatrix} \cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 & -\cos\varphi_1\sin\varphi_2 - \sin\varphi_1\cos\varphi_2 \\ \sin\varphi_1\cos\varphi_2 + \cos\varphi_1\sin\varphi_2 & -\sin\varphi_1\sin\varphi_2 + \cos\varphi_1\cos\varphi_2 \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\varphi_1+\varphi_2) & -\sin(\varphi_1+\varphi_2) \\ \sin(\varphi_1+\varphi_2) & \cos(\varphi_1+\varphi_2) \end{bmatrix} \in H$$

$$\begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix}^{-1} = \frac{1}{\underbrace{\cos^2\varphi + \sin^2\varphi}_{=1}} \begin{bmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{bmatrix}$$

$$= \begin{bmatrix} \cos(-\varphi) & -\sin(-\varphi) \\ \sin(-\varphi) & \cos(-\varphi) \end{bmatrix} \in H$$

$\Rightarrow$ H JE PODGRUPA

2. V S_7:

a) KAKŠEN JE RED EL. $(1\,2\,3\,4)$?

RED: NAJMANJŠI x, DA

$$(1234)^x = id$$

$$red((1234)) = 4$$

b) $red((1\,3\,2)(5\,7)) =$

$$(132)(57)\,(132)(57) = (123)(5)(7)$$

$$red((132)) = 3$$

$$red((57)) = 2$$

$$red((132)(57)) = lcm(3,2) = 6$$

c) POIŠČI EL. REDA 12.

$$(1234)(567)$$

d) $Z(S_7) = ?$

$$Z(S_7) = \{ id \}$$

ČE $\pi \neq id$: $\quad \pi = \begin{pmatrix} \dots & x & \dots \\ & \downarrow & \\ & y & \end{pmatrix}$ $\quad x \neq y$

$z \neq x, y$

$$\pi' = \begin{pmatrix} 1 & 2 & \dots & x & \dots & y & z & \dots & 7 \\ 1 & 2 & \dots & x & \dots & z & y & \dots & 7 \end{pmatrix} = (y\,z)$$

$$\pi' \pi = \begin{pmatrix} \dots & x & \dots \\ & y & \end{pmatrix}$$

$$\pi \pi' = \begin{pmatrix} \dots & x & \dots \\ & z & \end{pmatrix}$$

$$\Rightarrow \pi' \pi \neq \pi \pi' \Rightarrow \pi \notin Z(S_7)$$

3. S_4: POIŠČI NAJMANJŠO PODGRUPO, KI VSEBUJE $(1\,2)(3\,4)$ IN $(1\,4)$.

H:
- $id \in H$ $\quad 1$
- $\big((1\,2)(3\,4)\big)^{-1} \in H$, $\quad (1\,4)^{-1} \in H$

  $= (1\,2)(3\,4)$ $\quad 2$ $\qquad\qquad$ $= (4\,1) = (1\,4)$ $\quad 3$
- $(1\,2)(3\,4) \cdot (1\,4) = (1\,2\,4\,3) \in H$ $\quad 4$

$\Rightarrow (1342) \in H$ (INVERZ) 5

- $(1243)\cdot(1243) = (14)(23) \in H$ 6
- $(1243)^3 = (1243) \in H$
- $(14)\cdot(14)(23) = (23) \in H$ 7
- $(23)\cdot(12)(34) = (2431)\cdot(1243)$
- $(1243)\cdot(23) = (13)(42) \in H$ 8

...

$$H = \{id, (14), (23), (14)(23), (1243), (1342), (12)(34)\}$$

PODGRUPA

H GENERIRANA Z $(12)(34)$ IN (14).

4.

- NAJ V G VELJA $a^6 = b^3 = e$, $a^5 b^2 = b^2 a^5$. POKAŽI, DA a IN b KOMUTIRATA $(ab = ba)$

$$a^5 \cdot b^2 = b^2 \cdot a^5 \quad / \cdot a$$

$$a^5 b^2 \cdot a = b^2 \cdot a^6$$

$a \rightarrow \quad a^5 b^2 a = b^2$

$b \rightarrow \quad b^2 a = a b^2 \quad \leftarrow b$

$b^3 a b = b a b^3$

$a b = b a \quad \checkmark$

- NAJ V G VELJA, DA JE VSAK EL. ENAK INVERZU. DOKAŽI, DA G ABELOVA.

$\rightarrow x \quad x y \overset{?}{=} y x \qquad \forall x, y \in G$

$x^2 y \overset{?}{=} x y x$

$y \overset{?}{=} x y x$

$\vdots$

$\leftarrow x \cdot y$

$(x \cdot y) \cdot (x \cdot y) \overset{?}{=} y (x \cdot x) y$

$e \overset{?}{=} y \cdot e \cdot y$

$e = e \quad \checkmark$

5. $G = (\mathbb{Z}_n, +)$, $x \in G$, $x \neq 0$.

- KAKŠEN JE RED x? MOČ NAJMANJŠE PODGRUPE, KI VSEBUJE x?

$x + x + x + x \ldots + x = 0 \pmod{n}$

$k \cdot x = 0 \pmod{n}$

$kx = l \cdot n \qquad l, k \in \mathbb{Z}^+$

(RECIMO $k \cdot 55 = l \cdot 100$)

$k \dfrac{x}{\gcd(x,n)} = l \dfrac{n}{\gcd(x,n)}$

($k \cdot 11 = l \cdot 20$
$= l \cdot 2^2 \cdot 5$)

TUJI

$\Rightarrow \dfrac{n}{\gcd(x,n)}$ DELI k

NAJMANJŠI TAK

$\Rightarrow k = \dfrac{n}{\gcd(x,n)} \qquad \left(l = \dfrac{x}{\gcd(x,n)} \right)$

($k = 20$)

red(x)

$H = \{0, x, 2x, 3x, \ldots, (\text{red}(x) - 1) \cdot x\}$

PODGRUPA GENERIRANA Z x

JE PODGRUPA

$|H| = \text{red}(x) = \dfrac{x}{\gcd(x,n)}$

• ČE $y \in \mathbb{Z}_n$, $y \neq 0$ IN NAJ $\gcd(x,y)$ DELI n.

NAJMANJŠA PODGRUPA GEN. Z x IN y?

VSI ELEMENTI, KI JIH GEN. x IN y OBLIKE:

$$k \cdot x + l \cdot y \pmod n$$

$$k \cdot x + l \cdot y = d$$

DIOFANSKA ENAČBA

NAJMANJŠI TAK d JE $\gcd(x,y)$

$$\Rightarrow H = \{0, \gcd(x,y), 2 \cdot \gcd(x,y), \ldots, \ldots, n - \gcd(x,y)\}$$

6. $\mathbb{Z}_n^*$ MNOŽICA VSEH OBRNLJIVIH EL.

$(\mathbb{Z}_n, \cdot)$

DOKAŽI, DA $(\mathbb{Z}_n^*, \cdot)$ GRUPA.

- ČE $x \in \mathbb{Z}_n^*$ ALI JE $x^{-1} \in \mathbb{Z}_n^*$?

  (x^{-1}) JE OBRNLJIV $(x^{-1})^{-1} = x$

- $(x \cdot y)$ OBRNLJIV?

$$(x \cdot y)^{-1} = y^{-1} x^{-1} \quad \checkmark$$

$\Rightarrow$ JE GRUPA

7. $G = (\mathbb{Z}_{81}^*, \cdot)$

$|G| = ?$

$$|G| = \varphi(81) = 81 \cdot \left(1 - \frac{1}{3}\right) = 54$$

EULERJEVA FUNKCIJA $\quad 81 = 3^4$

$x \in (\mathbb{Z}_{81}, \cdot)$ JE OBRNLJIV $\Longleftrightarrow$ x TUJ 81

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \left(1 - \frac{1}{p_l}\right)$$

$$n = p_1^{k_1} \cdot \ldots \, p_l^{k_l}$$

$$17 \in \left(\mathbb{Z}_{81}^{*}, \cdot\right)$$

17^{-1}

$$17 \cdot x \equiv 1 \pmod{81}$$

$$17x + 81 \cdot k = 1$$

RAZŠIRJEN EVKLIDOV ALG. (REA):

r_i	q_i	s_i	t_i
	81	1	0
4	17	0	1
1	13	1	-4
3	4	-1	5
	1	4	$\boxed{-19}$

$$x \equiv -19 \pmod{81}$$
$$\equiv 62$$

$$17^{-1} = 62$$

8.

$$G = (\mathbb{Z}_{72}^*, \cdot)$$

$|G| = ?$ $\qquad$ $53^{-1} = ?$

$$|G| = \varphi(72) = 72 \cdot \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{2}\right) =$$

$$\boxed{72 = 2^3 \cdot 3^2} \quad = 72 \cdot \frac{2}{3} \cdot \frac{1}{2} = 24$$

$53^{-1} = ?$

	72	1	0
1	53	0	1
2	19	1	-1
1	15	-2	3
3	4	3	-4
1	3	-11	15
	1	+14	$\boxed{-19}$

$$53^{-1} = -19 \pmod{72}$$

$$= 53$$