

תרגיל:

$$\underbrace{\sigma \cdot (a_1 \dots a_k)}_{T_1} \cdot \sigma^{-1} = \underbrace{(\sigma(a_1) \dots \sigma(a_k))}_{T_2}$$

הוכיחו כי  
 $\sigma \in S_n$

הוכחה:

יהי  $1 \leq y \leq n$ .

נניח ש- $y = \sigma(a_i)$  לא בטוחו  $i$ . 1 מקרה

$$T_2(y) = \sigma(a_{i+1})$$

$$T_1(y) = (\sigma(a_1 \dots a_k) \sigma^{-1})y = \sigma(a_1 \dots a_k)(\sigma^{-1}(y)) = \\ = \sigma(a_1 \dots a_k)(a_i) = \sigma(a_{i+1})$$

נניח ש- $y \neq \sigma(a_i)$  לכל  $i$ . 2 מקרה ואם כן,  $T_2(y) = y$  ו- $T_1(y) = y$  גם כן.

חבורת אילר

$(\mathbb{Z}_n, +)$  חבורת אילר

$(\mathbb{Z}_n, \cdot)$  חבורת אילר

$$U_n = U((\mathbb{Z}_n, \cdot)) = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$$

דוגמה:

$$n=4$$

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$$U_4 = \{1, 3\}$$

$U_n$  היא תבורה ביחס לפעל מוזעלו  $n$ .

טענה:

$$U_n = \{m \mid 1 \leq m < n, \text{ (m, n) = 1}\}$$

טלומי מ-1  
זויים

דוגמה: 1 2 3 4 5 6 7 8 9 10 11 12 13 14

$$U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

$$U_{12} = \{1, 5, 7, 11\}$$

13 דוגמה:

$$5 \cdot 7 = 35 \equiv 11 \pmod{12}$$

$U_{12} \cong$

הזכרה:

סוקרטי אוליו

$$\varphi(n) = |U_n|$$

$$\varphi(p_1^{t_1} \dots p_k^{t_k}) = \underline{n} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right)$$

$$\varphi(12) = \varphi(2^2 \cdot 3) = 12 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$$

תת-תבורה של תבורה  $G$  היא תת-קבורה

$G$  תבורה,  $S \subseteq G$  תת-קבורה. הקצוה שקולו:

א.  $\langle S \rangle =$  תת-תבורה הקטנה ביותר של  $G$  שמכילה את  $S$

$$\langle S \rangle = \bigcap_{S \subseteq H \leq G} H$$

ב.

ג.  $\langle S \rangle =$  ס המכפול סה הגדלים והסדנים האפשריים  
ל איסויים ו- $S$  וההיסכיים שלהם.

הנחיה

$$\langle S \rangle = \langle a \rangle$$

$$S = \{a\}$$

$$S = \{(1,1)\}$$

$$\langle (1,1) \rangle = \{(n,n) \mid n \in \mathbb{Z}\}$$

$$G = \mathbb{Z} \times \mathbb{Z}$$

הנחיה

$$S = \{(1\ 2), (3\ 4)\} \subseteq G, \quad G = S_4$$

$$\langle S \rangle = \{\text{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$

הנחיה

$$H = \langle 15, 20 \rangle, \quad G = \mathbb{Z}$$

$$H = \{15n + 20m \mid n, m \in \mathbb{Z}\}$$

$$H = 5\mathbb{Z} \quad \text{לכ"ן}$$

$$5\mathbb{Z} = \langle 5 \rangle \subseteq H \quad \text{כי } 5 = 20 + (-15) \text{ ו } 5 \in H \quad \square$$

$$\langle 15, 20 \rangle \subseteq 5\mathbb{Z} \quad \text{כי } 15, 20 \in 5\mathbb{Z} \quad \square$$

למה - סיבול

חבורה  $G$  פועלת על קבוצה  $X$ .  $x \in X$  נקראת

$$\text{orb}(x) = \{g \cdot x \mid g \in G\} \subseteq X$$

$$\text{stab}_G(x) = \{g \in G \mid g \cdot x = x\} \leq G$$

$$|\text{orb}(x)| = [G : \text{stab}_G(x)] = \frac{|G|}{|\text{stab}_G(x)|} \quad \text{למה - סיבול}$$

הנחיה

על  $S_3$  פועלת חבורת סימון של שלושה אותיות  $x_1, x_2, x_3$  על האותיות  $a, b, c$

$$\text{orb}(x_1, x_2 + x_1, x_3) = \{x_1, x_2 + x_1, x_3, x_1, x_2 + x_3, x_2, x_3 + x_1, x_3\}$$

$$\text{stab}_{S_3}(x_1, x_2, x_3) = \{\text{id}, (2\ 3)\}$$

$$|\text{orb}| = 3,$$

$$|\text{stab}| = 2$$

$$3 \cdot 2 = 6 = |S_3|$$

מסקנה:

$$|\text{orb}(x)| \mid |G|$$

$$\begin{aligned} \text{orb}(x) &= \text{conj}(x) && \text{בפעולה ההדדית,} \\ \text{stab}_G(x) &= C_G(x) = \{g \in G \mid gx = xg\} \end{aligned}$$

טענה:

$$|G| = p^n \text{ לזושהו } n \in \mathbb{N} \iff G \text{ חבורת } p\text{-סופית}$$

הוכחה:

$\Rightarrow$  לגוראנץ', כי מסדרו של איבר מחלק את סדר החבורה.

$\Leftarrow$  משפט קולי - אם  $G$  סופית,  $p \mid |G|$  יש ב- $G$  איבר מסדר  $p$ .  
ראשון

נ"ח בשלילה ש- $|G| = p^n \cdot m$  עם  $m$  שאינו מתחלק ב- $p$ .

ניקח ראשון  $m$  ומשפט קולי יש ב- $G$  איבר מסדר  $q$ , הסתירה.  
 $\downarrow$   
 $q \neq p$

משפט קולי:

אם  $G$  חבורה סופית ו- $p \mid |G|$ , יש ב- $G$  איבר מסדר  $p$ .

$$1, a, \dots, a^{p-1}$$

לגזור פעולה על  $\mathbb{Z}_p$   $X = \{(g_0, \dots, g_{p-1}) \mid g_i \in G, g_0 \dots g_{p-1} = e\}$   $\curvearrowright$   $p$

$$k * (g_0, \dots, g_{p-1}) = (g_k, g_{k+1}, \dots, g_{k-1})$$

הקבוצה של  $n$  מסלול יטל זהיו  $1$  או  $p$ . (ממלכות מסלול  $n$  "3")

ממלכות  $n$   $|X| = |G|^{p-1}$ , כי כל בחירה של  $g_1, \dots, g_{p-1}$  יש  $g_p = e$  יחיד שמלכ את.

$$|X| = |\text{Fix}_G(X)| + \sum_{\substack{\text{מסלול} \\ \text{גודל } p}} |\text{מסלול}|$$

*ממלכות  $p$  -  $p$  ממלכות  $p$  -  $p$*

$\Leftarrow$  כמוהו נקודת השלם ממלכות  $p$ .

נקודת שלם =  $(g, \dots, g)$  מאכלהו  $g \in G$   $g^p = e$ .

יש נקודת שלם שהיא  $(e, e, \dots, e) \Leftarrow$  יש  $\forall p$  נקודת שלם, ובפרט אבר מסדר  $p$ .