

## אלגברה מופשטת – פתרון תרגיל 3

### שאלה 1

פתרו את המשוואה  $(123)^2 x = (12)(132)^{-1}$ .

פתרון

$$\begin{aligned}(132)^{-1} &= (312) \\ (12)(132)^{-1} &= (12)(312) = (32) \\ (123)^2 &= (123)(123) = (132) \\ \Rightarrow (132)x &= (32) \\ (132)^{-1} &= (312) \\ x &= (312)(32) = (21)\end{aligned}$$

מש"ל

### שאלה 2

א. הוכיחו שבחבורת הסימטריה  $S_n$  כל שני מחזורים זרים מתחלפים זה עם זה.

פתרון

נניח שקיימים טבעיים  $r, l$  ו- $i_1, i_2, \dots, i_r, i_{r+1}, i_{r+2}, \dots, i_{r+l}$  איברים שונים בין 1 ל- $n$ . נתבונן בתמורות  $\sigma = (i_{r+1} i_{r+2} \dots i_{r+l})(i_1 i_2 \dots i_r)$  ו- $\tau = (i_1 i_2 \dots i_r)(i_{r+1} i_{r+2} \dots i_{r+l})$ . קל לראות שאם  $1 \leq k \leq r-1$  או  $r+1 \leq k \leq r+l-1$  אז  $\tau(i_k) = \sigma(i_k) = i_{k+1}$  וכך  $\tau(i_r) = \sigma(i_r) = i_1$ ,  $\tau(i_{r+l}) = \sigma(i_{r+l}) = i_{r+1}$  הוא נקודת שבת של  $\tau$  וגם של  $\sigma$ . מכאן  $\tau = \sigma$  והמחזורים הזרים מתחלפים.  
מש"ל

ב. הוכיחו שאם  $\alpha, \beta$  הם מחזורים זרים, אזי  $ord(\alpha\beta) = lcm(ord(\alpha), ord(\beta))$ .

פתרון

נסמן  $ord(\alpha) = n, ord(\beta) = m$ ,  $k = lcm(ord(\alpha), ord(\beta))$ . תחילה נשים לב שמתקיים  $(\alpha\beta)^k = \alpha^k \beta^k = id$  (מדוע?) ולכן  $ord(\alpha\beta) \leq k$ . נוכיח את אי-השוויון ההפוך. נניח שמתקיים  $(\alpha\beta)^t = id$ , אזי  $\alpha^t \beta^t = id$  ולכן  $\alpha^t = \beta^t = id$  (מדוע?) ומכאן  $n|t \wedge m|t$ . לכן, לפי הגדרת  $lcm$  נקבל  $k \leq t$ .

מש"ל

ג. בחבורה  $S_8$  מצאו איברים מסדר 4, 7, 12, 15, 19, 20. אם אין איבר מסדר

מסויים, הסבירו מדוע.

פתרון

$o(1234) = 4$ ,  $o(1234567) = 7$ ,  $o((123)(4567)) = 12$ ,  $o((123)(45678)) = 15$   
איבר מסדר 19, שכן 19 הינו מספר ראשוני שאינו מחלק את סדר החבורה.  
אין איבר מסדר 20. הסבר: נניח שיש לנו איבר מסדר 20. ניתן לכתוב אותו  
כמכפלה של מחזורים זרים. על מנת שה-  $lcm$  של הסדרים יהיה 20, חייב  
להופיע בפירוק מחזור באורך 5 (כי צריך כפולה של 5, ו-10 הוא גדול מדי).  
בנוסף, צריך שיהיה מחזור מאורך 4. אבל שני מחזורים זרים, אחד מאורך 4  
ואחד מאורך 5, דורשים שימוש ב-9 מספרים שונים, ואין 9 מספרים שונים ב-  
 $S_8$ .

מש"ל

ד. הוכיחו שהמחזורים  $(12345), (13524) \in S_6$  מתחלפים, על אף שאינם זרים.

פתרון

קל לראות שמתקיים  $(12345)(13524) = (14253) = (13524)(12345)$ .

מש"ל

ה. תהי  $H = \langle (14), (13) \rangle$  תת חבורה של  $S_4$ . רשמו את לוח הכפל שלה ואז

הוכיחו שהיא איזומורפית ל- $S_3$ . כתבו את האיזומורפיזם בצורה מפורשת.

פתרון

איברי החבורה הם:  $H = \{id, (14), (13), (34), (134), (143)\}$ . מלוח הכפל

(שאותו לא נציג כאן) ניתן לראות את האיזומורפיזם המפורש  $\varphi: H \rightarrow S_3$ ,

$$id \mapsto id$$

$$(14) \mapsto (12)$$

$$(13) \mapsto (13)$$

$$(34) \mapsto (23)$$

$$(134) \mapsto (132)$$

$$(143) \mapsto (123)$$

והוא:

מש"ל

### שאלה 3

א. הוכיחו שחבורת קליין, כלומר תת חבורה של  $S_4$  המוגדרת על-ידי

$$U_8, V = K_4 = \langle (12)(34), (13)(24) \rangle$$

### פתרון

החבורה הנתונה מורכבת מארבעה איברים:

$$V = \{id, (12)(34), (13)(24), (14)(23)\}$$

$$f: V \rightarrow U_8$$

$$f(id) = 1, f((12)(34)) = 3, f((13)(24)) = 5, f((14)(23)) = 7$$

שזהו אכן איזומורפיזם.

שימו לב, שהחבורות  $V, U_8$  שתיהן איזומורפיות ל- $\mathbb{Z}_2 \times \mathbb{Z}_2$  (מדוע לא ל- $\mathbb{Z}_4$ ?).  
מש"ל

**ב.** רשמו את איברי תת החבורה של  $S_6$  הנוצרת על ידי שני האיברים

$$(145)(263), (15)(36)$$

### פתרון

$$\{id, (145)(263), (15)(36), (154)(236), (26)(45), (14)(23)\}$$

מש"ל

## שאלה 4

תארו את הקוסטים השמאליים והימניים של חבורה  $G$  לגבי ת"ח  $H$ :

$$; G = 4\mathbb{Z}, H = 12\mathbb{Z} \quad \text{א.}$$

### פתרון

החבורה אבלית ולכן המחלקות הימניות שוות לשמאליות. המחלקות הן

$$\{12\mathbb{Z}, 12\mathbb{Z} + 4, 12\mathbb{Z} + 8\}$$

$$; G = S_3, H = \langle (13) \rangle \quad \text{ב.}$$

### פתרון

המחלקות השמאליות הן:

$$H = (13)H$$

$$(12)H = (132)H = \{(12), (132)\}$$

$$(23)H = (123)H = \{(23), (123)\}$$

המחלקות הימניות הן:

$$H = H(13)$$

$$H(12) = H(123) = \{(12), (123)\}$$

$$H(23) = H(132) = \{(23), (132)\}$$

$$; G = S_3, H = \langle (123) \rangle \quad \text{ג.}$$

### פתרון

כאן המחלקות הימניות שוות למחלקות שמאליות (שימו לב שכאשר נשתפשף במושג של "תת חבורה נורמלית" נדע שזה מה שקורה כאן גם ללא בדיקה טכנית ישירה).  
נרשום את המחלקות השמאליות:

$$H = (123)H = (132)H$$

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

$$. G = U_{30}, H = \langle 13 \rangle \quad \text{ד.}$$

### פתרון

ידוע לנו כי  $|U_{30}| = \varphi(30) = 8$ , ואפשר לחשב כי  $U_{30} = \{1, 7, 11, 13, 17, 19, 23, 29\}$ . תת-החבורה  $H$  היא  $\langle 13 \rangle = \{1, 13, 19, 7\}$ . לפי משפט לגראנז' נקבל כי יש רק שתי מחלקות:  
 $\langle 13 \rangle = \{1, 13, 19, 7\}$ , ושוב שימו לב כי החבורה אבלית, ולכן המחלקות השמאליות שוות לימניות.

מש"ל

## שאלה 5

הוכיחו את המסקנה הבאה ממשפט לגרנז': תהי  $G$  חבורה סופית, ויהיו

$$. [G : K] = [G : H][H : K] \quad \text{ת"ח. } K \leq H \leq G$$

[תרגיל אתגר: הוכיחו את אותה תוצאה כאשר מניחים רק ש- $K$  תת חבורה מאינדקס סופי ב- $G$ . כלומר, מבלי להניח ש- $G$  סופית, ומבלי להניח סופיות

של  $H$ .]

### פתרון

יש להפעיל את משפט לגרנז' 3 פעמים.  $[G:K] \cdot |K| = |G|$  וגם  $[G:H] \cdot |H| = |G|$  ולכן  $[G:K] \cdot |K| = [G:H] \cdot |H|$ . בפעם השלישית נקבל  $[H:K] \cdot |K| = |H|$ . נציב במשוואה הקודמת ונקבל ש-  $[G:K] \cdot |K| = [G:H] \cdot [H:K] \cdot |K|$ . מכאן  $[G:K] = [G:H] \cdot [H:K]$ .

### פתרון תרגיל אתגר

- כאן מובא הפתרון הקומבינטורי של השאלה, שכן בשלב זה עוד לא היו לנו כלים מתקדים. אך שימו לב שבהרצאה מאוחרת יותר, הוכחתם שוב את הטענה הזאת, והפעם באמצעות שיקולים קצת יותר אלגנטיים.

ראשית, נסו להוכיח שאם  $[G:K]$  סופי אז גם אינדקסים  $[H:K]$  ו-  $[G:H]$  סופיים.

שנית, נניח ש  $\bigcup_{i=1}^n g_i H = G$  וגם  $\bigcup_{j=1}^m h_j K = H$  (שני האיחודים זרים) כלומר ש-

$[G:H] = n$  ו-  $[H:K] = m$ . כדי להוכיח הדרוש מ"ל ש-  $\bigcup_{i=1}^n \bigcup_{j=1}^m g_i h_j K = G$  ושזהו

איחוד זר כי אז נקבל ש  $[G:K] = mn$ . נוכיח תחילה את השוויון. ברור שאגף שמאל מוכל בימין ולכן נראה רק את ההכלה ההפוכה. יהי  $g \in G$  אזי מהשוויון

$$\bigcup_{i=1}^n g_i H = G \text{ נקבל שקיים } 1 \leq i \leq n \text{ ו- } h \in H \text{ כך ש- } g = g_i h.$$

כעת  $h \in H$  ומתקיים  $\bigcup_{j=1}^m h_j K = H$  ולכן קיים  $1 \leq j \leq m$  כך ש  $h \in h_j K$ . נקבל ש-

$$g = g_i h \in g_i h_j K \text{ ומזה נובעת ההכלה הדרושה.}$$

נוכיח כעת שהאיחוד זר (זה החלק היותר קשה). כזכור, כל שני קוסטים הם או מתלכדים או זרים. נניח ש-  $g_i h_j K = g_{i_2} h_{j_2} K$  ונראה שבהכרח  $h_{j_1} = h_{j_2}$ ,  $g_{i_1} = g_{i_2}$ .

מהשוויון  $g_i h_j K = g_{i_2} h_{j_2} K$  נקבל ש-  $g_i h_j K = (g_{i_2} h_{j_2})^{-1} g_i h_j K \in K$ . מכיוון ש-

$K \leq H$  נקבל ש-  $h_{j_1}^{-1} g_{i_2}^{-1} g_i h_{j_2} \in H$ . מכיוון ש-  $h_{j_1}, h_{j_2} \in H$  נסיק (איר?) ש-

$g_{i_1}^{-1} g_{i_2} \in H$ . אך מכך נובע ש-  $g_{i_2} \in g_{i_1} H$  לכן בהכרח  $g_{i_1} = g_{i_2}$  שכן עבור  $i_1 \neq i_2$

האברים  $g_{i_1}, g_{i_2}$  שייכים לקוסטים שונים. כעת,

$h_{j_1}^{-1} g_{i_1}^{-1} g_{i_2} h_{j_2} = (g_{i_1} h_{j_1})^{-1} g_{i_2} h_{j_2} \in K$  ואנו גם יודעים מהשלב האחרון ש-  
 $g_{i_1}^{-1} g_{i_2} = e$  (כאשר  $e$  איבר היחידה) ומכאן  $h_{j_1}^{-1} g_{i_1}^{-1} g_{i_2} h_{j_2} = h_{j_1}^{-1} h_{j_2} \in K$ . נקבל  
 ש-  $h_{j_2} \in h_{j_1} K$  ומכיון ש-  $\bigcup_{j=1}^m h_j K = H$  והאיחוד הוא זר נקבל שבהכרח  $h_{j_1} = h_{j_2}$ .  
 וסיימנו את ההוכחה.

מש"ל

## שאלה 6

**א.** מצאו את שתי הספרות האחרונות של  $5353^{202}$ .

**ב.** מצאו את  $5773^{862} + 2013 \pmod{80}$ .

### פתרון

**א.** יש לחשב את הביטוי  $5353^{202} \pmod{100}$  ששווה לביטוי  $53^{202} \pmod{100}$ .

מתקיים  $\varphi(100) = 40$  ולכן לפי משפט אוילר  $53^{40} \equiv 1 \pmod{100}$ . לכן,

שתי  $53^2 = 2709$ ,  $53^{202} = 53^{40 \cdot 5 + 2} = (53^{40})^5 \cdot 53^2 \equiv 53^2 \pmod{100}$

הספרות האחרונות הן 09.

**ב.** נשים לב כי  $2000 \equiv 0 \pmod{80}$  וגם כי  $5773 = 72 \cdot 80 + 13 \equiv 13 \pmod{80}$ . לכן

צריך לחשב את הביטוי  $13^{862} + 13 \pmod{80}$ . מפני ש-  $\varphi(80) = 32$ , לפי

משפט אוילר נקבל כי  $13^{32} \equiv 1 \pmod{80}$ . לכן

$13^{862} = 13^{26 \cdot 32 + 30} = 13^{30} \pmod{80}$  לכן מפני ש-

$13^{30} = 13^{32} \cdot 13^{-2} = 13^{-2} \pmod{80}$ , נרצה למצוא הופכי של 13 בחבורה  $U_{80}$ .

ישנו פתרון למשוואה  $13x \equiv 1 \pmod{80}$  אם ורק אם קיים  $k \in \mathbb{Z}$  כך ש-

$80k + 59x = 1$ . נשתמש באלגוריתם אוקלידס כדי למצוא את  $x$ , כלומר

למצוא ביטוי של  $\gcd(80, 13)$  כצירוף לינארי של 13 ושל 80:

$(80, 13) = (13, 2) = (2, 1) = 1$   
 $80 = 6 \cdot 13 + 2$        $13 = 6 \cdot 2 + 1$

$$1 = 13 - 6 \cdot 2 = -6 \cdot 80 + 37 \cdot 13$$

מתקיים  $x = 37$ . כלומר  $1 = 13 - 6 \cdot 2 = -6 \cdot 80 + 37 \cdot 13$

$$.5773^{862} + 2013 \equiv 9 + 13 \equiv 22 \pmod{80} \text{ ולכן } 13^{-2} \equiv 37^2 \equiv 9 \pmod{80}$$

מש"ל