

פתרון תרגיל 4 – אלגברה מופשטת

1. מצאו את קבוצה המנה G/H של החבורות G לגבי תת החבורות H .

1.1. $H = 5Z, G = Z$

פתרון:

$$G/H = \{gH \mid g \in G\} = \{0+5Z, 1+5Z, 2+5Z, 3+5Z, 4+5Z\} = \{[0],[1],[2],[3],[4],[5]\} = Z_5$$

1.2. $H = \{0\} \times R, G = (R^2, +)$

פתרון:

$$\begin{aligned} G/H &= \{gH \mid g \in G\} = \{(a,b) + \{0\} \times R \mid (a,b) \in R^2\} = \{(a,b) + (0,x) \mid x \in R\} \mid (a,b) \in R^2\} \\ &= \{(a,x+b) \mid x \in R\} \mid (a,b) \in R^2\} = \{(a,y) \mid y \in R\} \mid (a,b) \in R^2\} = \{(a,y) \mid y \in R\} \mid a \in R \} \end{aligned}$$

נשים לב: זוהי בדיוק קבוצת הישרים המקבילים לציר ה y .

1.3. $H = \{(t,4t) \mid t \in R\}, G = (R^2, +)$

פתרון:

$$\begin{aligned} G/H &= \{gH \mid g \in G\} = \{(a,b) + H \mid (a,b) \in R^2\} = \{(a,b) + (t,4t) \mid t \in R\} \mid (a,b) \in R^2\} \\ \text{נשים לב} &= \{(a+t, b+4t) \mid t \in R\} \mid (a,b) \in R^2\} = \{(x, b+4(x-a)) \mid l \in R\} \mid (a,b) \in R^2\} \\ &= \{(x, 4x+b-4a) \mid l \in R\} \mid (a,b) \in R^2\} = \{(x, 4x+c) \mid x \in R\} \mid c \in R \} \end{aligned}$$

לב: זוהי בדיוק קבוצת הישרים המקבילים בעלי שיפוע 4.

1.4. $H = \langle 11 \rangle, G = U_{30}$

פתרון:

נשים לב: $U_{30} = \{1,7,11,13,17,19,23,27\}$ ו $H = \{1,11\}$

לפי משפט לגרנז',

$$[G:H] = \frac{|G|}{|H|} = \frac{8}{2} = 4$$

הקוסטים השמאליים:

$$1H = \{1,11\}, 7H = \{7,17\}, 13H = \{13,23\}, 19H = \{19,29\}$$

הם ארבעה קוסטים שונים זה מזה.

לכן,

$$G/H = \{\{1,11\}, \{7,17\}, \{13,23\}, \{19,29\}\}$$

(שימו לב, איחוד כל הקוסטים השמאליים, אכן שווה ל G).

1.5. $(C^* = C \setminus \{0\}, \cdot)$ (כאשר) $H = \{z \in C \mid \|z\|=1\}$, $G = (C^*, \cdot)$.
פתרון:

$$\begin{aligned} G/H &= \{xH \mid x \in C^*\} = \{x\{z \in C \mid \|z\|=1\} \mid x \in C^*\} = \{\{xz \in C \mid \|z\|=1\} \mid x \in C^*\} \\ &= \{\{y \in C \mid \|y\|=\|x\|\} \mid x \in C^*\} = \{\{y \in C \mid \|y\|=\|x\|\} \mid x \in R_+\} \end{aligned}$$

נשים לב: זוהי קבוצת כל המעגלים סביב ראשית הצירים.

2. הוכיחו את הטענות הבאות.

2.1. תהי G חבורה, $H, K \leq G$, תתי חבורות מסדר m, n בהתאמה כך ש $(m, n) = 1$.
אזי $H \cap K = \{e\}$.
הוכחה:

$$H \cap K \leq H, K$$

לכן, לפי משפט לגרנז',

$$\begin{aligned} |H \cap K| \mid |H| = m \quad , \quad |H \cap K| \mid |K| = n \\ \Rightarrow |H \cap K| \mid (m, n) = 1 \\ \Rightarrow |H \cap K| = 1 \\ \Rightarrow H \cap K = \{e\} \end{aligned}$$

2.2. אם G חבורה אבלית ו $a, b \in G$ איברים מסדר m, n בהתאמה כך ש $(m, n) = 1$,
אזי $o(ab) = mn$.

הוכחה: (למעשה הוכחנו זאת בתרגיל הקודם. נוכיח זאת שוב באמצעות סעיף 2.1)

$$(ab)^{mn} = a^{mn} b^{mn} = (a^m)^n (b^n)^m = e^n e^m = e$$

לכן: מ"ל מינמליות. יהא $t \in N$ כך ש $(ab)^t = e$. אזי,

$$(ab)^t = e \Rightarrow a^t b^t = e \Rightarrow a^t = b^{-t} \Rightarrow a^t \in \langle a \rangle \cap \langle b \rangle$$

אבל, $\langle a \rangle$ חבורה מסדר m ו $\langle b \rangle$ חבורה מסדר n ו $(m, n) = 1$. לכן, לפי הסעיף הקודם, $\langle a \rangle \cap \langle b \rangle = \{e\}$.

לכן, $o(a) = m \mid t$ ו $a^t = e$.

בדומה, $o(b) = n \mid t$, לכן $b^t = a^{-t} = e$.

בסה"כ $[m, n] = mn \mid t$. לכן, $mn \leq t$. מש"ל.

2.3. יהיו m, n מספרים טבעיים. אזי, $Z_m \times Z_n \cong Z_{mn}$ אם ורק אם $(m, n) = 1$.

הוכחה:

(\Rightarrow) נניח כי $(m,n)=1$ ונוכיח כי $Z_m \times Z_n$ ציקלית. מכיוון ש $|Z_m \times Z_n| = mn$ נקבל כי $Z_m \times Z_n \cong Z_{mn}$ ממשפט המיזוג של חבורות ציקליות. נשים לב, האיבר $(1,0) \in Z_m \times Z_n$ הוא איבר מסדר m . בדומה, האיבר $(0,1) \in Z_m \times Z_n$ הוא איבר מסדר n . מכיוון ש $(m,n)=1$ והחבורה $Z_m \times Z_n$ אבלית, נובע מהסעיף הקודם, כי $o((1,1)) = o((1,0)) + o((0,1)) = mn$. לכן $\langle (1,1) \rangle = Z_m \times Z_n$ ציקלית מסדר mn כדרוש. (\Leftarrow) נתון כי $Z_m \times Z_n \cong Z_{mn}$. בפרט, $Z_m \times Z_n$ ציקלית וקיים איבר $(a,b) \in Z_m \times Z_n$ מסדר $o((a,b)) = mn$. נניח בשלילה כי $(m,n) \neq 1$. אזי, $d := \text{lcm}(m,n) < mn$, $d(a,b) = (da, db) = (0,0)$ מתקיים $d(a,b) = (da, db) = (0,0)$ מכיוון ש $m|d, n|d$. לכן, $o((a,b)) = d < mn$. סתירה.

3. ענו על הסעיפים הבאים.

3.1. תהי G חבורה כך ש $|G| < 60$, קיים $a \in G$ מסדר 5 ו $S_3 \leq G$. מצאו את הסדר של G .

פתרון: קיים $a \in G$ מסדר 5. לכן, לפי מסקנה ממשפט לגרנז', $5| |G|$. בנוסף, מכיוון ש $S_3 \leq G$ ת"ח מסדר 6, $6| |G|$. מכיוון ש $(5,6)=1$, $30 = 5 \cdot 6 = |G|$. אבל, $|G| < 60$, לכן $|G| = 30$.

3.2. תהי G חבורה לא אבלית מסדר 2^t עבור $t \in \mathbb{N}$ כלשהו. הוכיחו כי קיימת ב- G תת חבורה ציקלית מסדר 4.

הוכחה: לפי משפט לגרנז' כל איבר ב G הוא מסדר 2^k עבור k כלשהו (התלוי באיבר). אם כל האיברים ב G הם מסדר 2 לכל היותר, לפי תרגיל משיעורי בית קודמים, החבורה G אבלית, בסתירה לנתון. לכן קיים ב G איבר a מסדר 2^k עבור $k \geq 2$ כלשהו.

נגדיר $n = 2^{k-2}$ ונתבונן ב $b = 2^a$. עבורו:

$$o(b) = o(a^n) = \frac{o(a)}{(o(a), n)} = \frac{2^k}{(2^k, 2^{k-2})} = \frac{2^k}{2^{k-2}} = 4$$

ציקלית מסדר זה.

4. ענו על הסעיפים הבאים:

4.1. חשבו $197^{81} \pmod{34}$.
פתרון:

$197 \equiv 27 \pmod{34}$ לכן $197^{81} \equiv 27^{81} \pmod{34}$.
 $(27, 34) = 1$, לכן, $27 \in U_{34}$ ולפי משפט אוילר: $27^{\varphi(34)} \equiv 1 \pmod{34}$.
 נחשב, $\varphi(34) = \varphi(2)\varphi(17) = 1 \cdot 16 = 16$, לכן, $27^{16} \equiv 1 \pmod{34}$.
 $197^{81} \equiv 27^{81} \pmod{34} \equiv 27^{16 \cdot 5 + 1} \pmod{34} = (27^{16})^5 \cdot 27 \pmod{34} \equiv 1 \cdot 27 \pmod{34} \equiv 27 \pmod{34}$

4.2. מצאו את שתי הספרות האחרונות של $20087853^{199} + 876$.
 פתרון: נחשב, $20087853^{199} \pmod{100} = 53^{199} \pmod{100}$.
 $(53, 100) = 1$, לכן, $53 \in U_{100}$ ולפי משפט אוילר: $53^{\varphi(100)} \equiv 1 \pmod{100}$.

נחשב, $\varphi(100) = 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 40$, לכן, $53^{40} \equiv 1 \pmod{100}$.
 $53^{199} \equiv 53^{40 \cdot 5 - 1} \pmod{100} \equiv (53^{40})^5 \cdot 53^{-1} \pmod{100} \equiv 1 \cdot 53^{-1} \pmod{100} \equiv 53^{-1} \pmod{100}$
 נשים לב, מכיוון ש $53 \in U_{100}$, $53^{-1} \pmod{100}$ מוגדר היטב.
 נמצא את $53^{-1} \pmod{100}$ באמצעות אלגוריתם אוקלידס המוכלל.

$$(100, 53) = (53, 47) = (47, 6) = (6, 5) = 1$$

$100 = 1 \cdot 53 + 47$	$53 = 1 \cdot 47 + 6$	$47 = 7 \cdot 6 + 5$	$6 = 1 \cdot 5 + 1$
$47 = 100 - 1 \cdot 53$	$6 = 53 - 1 \cdot 47$	$5 = 47 - 7 \cdot 6$	$1 = 6 - 1 \cdot 5$
	$6 = 53 - 1 \cdot (100 - 1 \cdot 53)$	$5 = (100 - 1 \cdot 53) - 7 \cdot (-1 \cdot 100 + 2 \cdot 53)$	$1 = (-1 \cdot 100 + 2 \cdot 53) - 1 \cdot (8 \cdot 100 - 15 \cdot 53)$
	$6 = -1 \cdot 100 + 2 \cdot 53$	$5 = 8 \cdot 100 - 15 \cdot 53$	$1 = -9 \cdot 100 + 17 \cdot 53$

לכן,

$$17 \cdot 53 - 9 \cdot 100 = 1 \Rightarrow 17 \cdot 53 \equiv 1 \pmod{100} \Rightarrow 53^{-1} \equiv 17 \pmod{100}$$

בסה"כ, $20087853^{199} \pmod{100} \equiv 17 \pmod{100}$
 $(20087853^{199} + 876) \pmod{100} = 17 + 76 \pmod{100} = 93 \pmod{100}$
 לכן, שתי הספרות האחרונות של המספר הנתון הן, 93.

5. הוכיחו את המסקנה הבאה ממשפט לגרנז': תהי G חבורה סופית, ויהיו $K \leq H \leq G$.
 ת"ח. אזי $[G : K] = [G : H][H : K]$.

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 . שימו לב שבמקרה זה, זו אינה מסקנה ממשפט לגרנז', אלא הכללה שלו.

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 מתקדמים. 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 $\bigcup_{i=1}^n g_i H = G$ נקבל שקיים

$$g = g_i h \quad 1 \leq i \leq n \quad h \in H \quad \text{ש-} g = g_i h$$

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-

$$g = g_i h \in g_i h_j K$$

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 $g_{i_1} = g_{i_2}, h_{j_1} = h_{j_2}$.

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- $h_{j_1}^{-1} g_{i_1}^{-1} g_{i_2} h_{j_2} \in H$. 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, $g_{i_2} h_{j_2} = (g_{i_1} h_{j_1})^{-1} g_{i_2} h_{j_2} \in K$ ואנו

גם יודעים מהשלב האחרון ש- $g_{i_1}^{-1}g_{i_2} = e$ (כאשר e איבר היחידה) ומכאן

נקבל ש- $h_{j_2} \in h_{j_1}K$ ומכיון ש- $\bigcup_{j=1}^m h_jK = H$ והאיחוד הוא זר

נקבל שבהכרח $h_{j_1} = h_{j_2}$ וסיימנו את ההוכחה.

בהצלחה! ☺