

אלגברה מופשטת – פתרון 3

שאלה 1

- א. הוכיחו שבחבורת הסימטריה S_n כל שני מחזורים זרים מתחלפים זה עם זה.
- בניח 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 $\tau = (i_1 i_2 \dots i_r)(i_{r+1} i_{r+2} \dots i_{r+l})$, $\sigma = (i_{r+1} i_{r+2} \dots i_{r+l})(i_1 i_2 \dots i_r)$ 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 נקודת שבת של τ וגם של σ . מכאן $\tau = \sigma$ והמחזורים הזרים מתחלפים.
- ב. הוכיחו שהמחזורים $(12345) \in S_6, (13524)$ מתחלפים, על אף שאינם זרים. קל לראות שמתקיים $(12345)(13524) = (14253) = (13524)(12345)$.
- ג. רשמו את לוח הכפל של החבורה S_3 ומצאו את הסדר של כל איבר.
- ד. בחבורה S_8 מצאו איברים מסדר 4, 7, 12, 15, 19, 20. אם אין איבר מסדר מסויים, הסבירו מדוע.
- אין $o(1234) = 4, o(1234567) = 7, o((123)(4567)) = 12, o((123)(45678)) = 15$
- 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 באורך 4. אבל שני מחזורים זרים, אחד באורך 4 ואחד באורך 5, דורשים שימוש ב-9 מספרים שונים, ואין 9 מספרים שונים ב- S_8 .

שאלה 2

- א. הוכיחו ש- $\langle (12)(34), (13)(24) \rangle \leq S_4 = U_8$ איזומורפית ל- U_8 .
- V הנ"ל נקראית "חבורת קליין" ומורכבת מ-4 איברים: $V = \{id, (12)(34), (13)(24), (14)(23)\}$
- $f: V \rightarrow U_8$: $f(id) = 1, f((12)(34)) = 3, f((13)(24)) = 5, f((14)(23)) = 7$
- (ויש לבדוק שזהו אכן איזומורפיזם).
- שימו לב, שהחבורות איזומורפיות ל- $\mathbb{Z}_2 \times \mathbb{Z}_2$.
- ב. רשמו את איברי תת החבורה של S_6 הנוצרת על ידי שני האיברים $(145)(263), (15)(36)$.
- האיברים הם: $\{id, (145)(263), (15)(36), (154)(236), (26)(45), (14)(23)\}$
- שימו לב שהחבורה הזאת איזומורפית ל- D_3 (מדוע?).

שאלה 3

- א. תנו דוגמא לחבורה סופית G ותת-חבורה H המראות שההתאמה $Hx \rightarrow xH$ אינה בהכרח מוגדרת היטב.
 ב. תנו דוגמא לחבורה (אינסופית) שיש לה תת קבוצה סגורה ביחס לפעולה, שאיננה תת חבורה.

פתרון

(א) ראשית – שימו לב: העתקה f היא מוגדרת היטב אם כשמתקיים $a=b$ אז $f(a)=f(b)$. נקח את החבורה הדיהדרלית $G = D_3 = \langle \sigma, \tau \rangle$ ואת תת החבורה שלה H הנוצרת ע"י τ (השיקוף), ז"א $H = \{1, \tau\}$. נסמן את ההתאמה $xH \mapsto Hx$.

ב- f . נכתוב את המחלקות השמאלית והימנית של σ ביחס ל- H .
 $\sigma H = \{\sigma, \sigma\tau\}$, $H\sigma = \{\sigma, \tau\sigma\}$. לכן $f(\sigma H) = H\sigma$.
 עתה, נשים לב ש- $\sigma H = \{\sigma\tau, \sigma\tau^2\} = \{\sigma\tau, \sigma\} = \sigma H$ מצד שני,
 $f(\sigma\tau H) = H\sigma\tau = \{\sigma, \tau\sigma\tau\} \neq H\sigma = f(\sigma H)$ ז"א ש- f אינה מוגדרת היטב.

(ב) ניקח את $G = (\mathbb{Z}, +)$ ואת $H = (\mathbb{N}, +)$.

$H \subset G$ ו- H סגורה ביחס לחיבור, אך H איננה חבורה ולכן H אינה תת חבורה של G .

שאלה 4

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

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

ב. $G = \mathbb{R}^2, H = \{(t, 3t) \mid t \in \mathbb{R}\}$

ג. $G = X_1 \times X_2, H = X_1 \times \{e\}$ (X_1, X_2 חבורות)

ד. $G = U_{20}, H = \langle 11 \rangle$.

פתרון

(א) המחלקות הן $\{12\mathbb{Z}, 12\mathbb{Z} + 4, 12\mathbb{Z} + 8\}$

(ב) המחלקות הן:

$$\{(t, 3t) + (a, b) : (a, b) \in \mathbb{R}\} = \{(a+t, b+3t) : a, b \in \mathbb{R}\} = \{(x, y) : y = 3x + b - 3a, a, b \in \mathbb{R}\}$$

משמע, אלה הם ישרים עם שיפוע 3.

(ג) המחלקות הן: $\{(X_1 \times \{e\}) \cdot (a, b) : a \in X_1, b \in X_2\} = \{X_1 a \times \{b\}\} = \{X_1 \times \{b\} : b \in X_2\}$

ולכן קבוצת המחלקות איזומורפית ל- X_2 (ועל כך בהמשך הקורס).

(ד) $U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$ ו- $\langle 11 \rangle = \{1, 11\}$. לכן יש 4 מחלקות:
 $\langle 11 \rangle, 3\langle 11 \rangle = \{3, 13\}, 7\langle 11 \rangle = \{7, 17\}, 9\langle 11 \rangle = \{9, 19\}$

שאלה 5

רשמו את הקוסטים הימניים והשמאליים של תת החבורות
 $H = \langle (12) \rangle$, $K = \langle (1 2 3) \rangle$ בחבורה S_3 .

פתרון

עבור K מתקיים שהקוסטים הימניים שווים לשמאליים ויש רק שני קוסטים (יכולתם לגלות זאת ידנית, אבל כעת אתם כבר יודעים את הנימוקים המשוכללים יותר המערבים תתי חבורות נורמליות). לכן המחלקות (הימניות, לדוגמא) הן: $K, (12)K$.

לגבי H נרשום רק את הימניים (מצאו באופן דומה גם את השמאליים):
 $H, (123)H, (132)H$. וודאו שהפעם הקוסטים הימניים אינם מתלכדים עם הקוסטים השמאליים.

שאלה 6

הוכיחו את המסקנה הבאה ממשפט לגרנג': תהי G חבורה סופית, ויהי

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

[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

$[H$

פתרון

יש להפעיל את משפט לגרנג' 3 פעמים. 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

$$[G : K] = [G : H][H : K]$$

פתרון תרגיל אתגר

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

שנית, בניח 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

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

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

מהשוויון $g_i h_j K = g_{i_2} h_{j_2} K$ נקבל ש $g_i h_j K = (g_{i_1} h_{j_1})^{-1} g_{i_2} h_{j_2} \in K$ מכיון ש

$K \leq H$ נקבל ש $h_{j_1}^{-1} g_{i_1}^{-1} g_{i_2} h_{j_2} \in H$. מכיון 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 $i_1 \neq i_2$

מתקיים ש g_{i_1}, g_{i_2} שייכים לקוסטים שונים. כעת,

$g_{i_1}^{-1} g_{i_2} = e$ מהשלב האחרון ש $h_{j_1}^{-1} g_{i_1}^{-1} g_{i_2} h_{j_2} = (g_{i_1} h_{j_1})^{-1} g_{i_2} h_{j_2} \in K$

(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.

שאלה 7

השתמשו במשפט אוילר ו:

א. מצאו את שתי הספרות האחרונות של 1959^{1999}

ב. מצאו שתי ספרות אחרונות של $8073767^{1999} + 2011$

ג. הוכיחו שלכל שני טבעיים $n > 1$ ו $a > 1$ מתקיים $n \mid \phi(a^n - 1)$ (כאשר ϕ היא

פונקציית אוילר).

פתרון

(א) למעשה יש לחשב את הביטוי $1959^{1999} \pmod{100}$ או $59^{1999} \pmod{100}$. ניעזר

במשפט אוילר 2. $\phi(100) = 40$ ולכן $59^{40} \equiv 1 \pmod{100}$. כמו כן מתקיים:

$$1999 = 40 \cdot 49 + 39 \text{ ולכן}$$

$$59^{1999} = (59^{40})^{49} \cdot 59^{39} \equiv 1 \cdot 59^{39} \pmod{100} \equiv 59^{-1} \cdot 59^{40} \equiv 59^{-1} \pmod{100}$$

את ההופכי של 59 מודולו 100. זאת אומרת, עלינו לפתור את המשוואה $59x \equiv 1 \pmod{100}$. ניתן לנחש ש- $x = 39$ ולכן הספרה האחרונה של המספר היא 39.

דרך נוספת למצוא את ההופכי:

נשים לב שמתקיים $59x \equiv 1 \pmod{100}$ אמ"מ קיים $k \in \mathbb{Z}$ כך ש- $59x + 100k = 1$. כעת נשתמש באלגוריתם אוקלידס עם חישוב מקדמים על מנת למצוא את x .

$$\begin{aligned} (100, 59) &= (59, 41) = (41, 18) = (18, 5) = \\ &= (5, 3) = (3, 2) = (2, 1) = 1 \end{aligned}$$

$$1 = 39 \cdot 59 + (-23) \cdot 100 \text{ ומהצבה לאחור נקבל: } x = 39$$

(ב) צריך למצוא את 2 הספרות האחרונות של $8073767^{1999} + 2011$ כלומר לחשב את $8073767^{1999} + 2011 \pmod{100}$ כלומר את $67^{1999} + 11 \pmod{100}$. נמצא את $67^{1999} \pmod{100}$: נחשב כי $\varphi(100) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$ ונקבל לפי משפט אוילר ש- $67^{1999} \equiv 67^{40 \cdot 50 - 1} \equiv (67^{40})^{50} \cdot 67^{-1} \equiv 67^{-1} \pmod{100}$. כלומר מחפשים מספר $x \in \mathbb{Z}$ כך ש- $67x \equiv 1 \pmod{100}$ כלומר $67x - 1 \mid 100$ כלומר צ"ל $x \in \mathbb{Z}, y \in \mathbb{Z}$ כך ש- $67x + 100y = 1$ כלומר $100y = 67x - 1$ בעצם צריכים לבטא את ה-gcd של 67, 100 כצירוף לינארי של 67, 100. באמצעות אלגוריתם אוקלידס המורחב נמצא כי $x = 3, y = 2$ כלומר ההופכי של 67 ב- U_{100} הוא 3. לסיכום נקבל כי $8073767^{1999} + 2011 \pmod{100} \equiv 67^{-1} + 11 \equiv 3 + 11 \equiv 14 \pmod{100}$ כלומר שתי הספרות האחרונות של המספר הן 14.

(ג) תחילה נשים לב שעבור $n = 1$ הטענה ברורה שכן 1 מחלק כל מספר שלם. לכן ניתן להניח ש- $a, n > 1$. במצב זה מתקיים $a < a^n - 1$. כמו כן $(a, a^n - 1) = 1$ אפשר לראות זאת ע"י מציאת צירוף לינארי מינימלי של $a, a^n - 1$ שנותן את 1 או פשוט מהעובדה שכל גורם ראשוני שמחלק את a יחלק גם את a^n ולכן בודאות לא יחלק את $a^n - 1$. מכאן נובע ש- $a \in U_{a^n - 1}$. עפ"י תוצאה של משפט לגרנז' סדר

איבר מחלק את סדר החבורה. לכן $o(a) \mid \phi(a^n - 1)$. נראה ש $o(a) = n$ ונסיק
הדרוש. נשים לב ש $a^n = 1 \pmod{a^n - 1}$. כמו כן לכל $1 \leq i < n - 1$ מתקיים
 $1 < a^i < a^n - 1$ ולכן לכל $1 \leq i < n - 1$ $a^i \not\equiv 1 \pmod{a^n - 1}$. מכאן $o(a) = n$.

דוגמא (השלמה) לקבוצה של מני
 $\mathbb{A} = [GL_2(\mathbb{R}) : GL_2(\mathbb{Q})]$. מכיוון ש- $GL_2(\mathbb{R}) = \cup x \cdot GL_2(\mathbb{Q})$ איחוד זר על כל
הקוסטים. כל קוסט הוא מעוצמה \mathbb{A}_0 ולכן יש בדיוק \mathbb{A} קוסטים כאלה.