מבנים אלגבריים

תרגיל בית 4*
פתרונות

1. תנו דוגמא נגדית לטענות השגויות הבאות:

- תהי G חבורה מסדר זוגי. אם $x^3 = y^3$ אז $x = y$.
- תהי G חבורה מסדר n. יש ב־G איבר מסדר n.
- כל חבורה אבלית מסדר 9 היא ציקלית.

פתרון כדלהלן:

- נביט בחבורה D_3, שהיא חבורה מסדר זוגי ($|D_3| = 6$). נסמן כאן את הסיבוב ב־$120°$ נגד כיוון השעון על ידי σ, ואת השיקוף על אחד מצירי השיקוף על ידי τ. ניקח $x = \sigma$ ו־$y = id$. מתקיים $x^3 = \sigma^3 = id = id^3 = y^3$ אבל $x \neq y$.
- נביט שוב בחבורה D_3. זו חבורה מסדר 6, אבל בחינה של כל איבריה מראה שיש בה איברים מסדרים 1, 2 ו־3 בלבד. למעשה, כל חבורה לא ציקלית תקיים הנדרש כאן.
- נביט בחבורה $\mathbb{Z}_3 \times \mathbb{Z}_3$, עם פעולת החיבור רכיב־רכיב. זו חבורה מסדר 9. יהי (x, y) איבר בחבורה. מתקיים

$$3 \cdot (x, y) = (x, y) + (x, y) + (x, y) = (3x, 3y) = (0, 0)$$

מצאנו, אפוא, כי הסדר של כל איבר של החבורה מחלק את 3, ובפרט אין איבר מסדר 9. נסיק מכאן כי אין לחבורה יוצר, ומשכך היא איננה ציקלית. ■

2. תהי G חבורה, ותהי I קבוצת אינדקסים, לתת־חבורות של G: לכל $i \in I$, $H_i \leq G$ (I לא בהכרח סופית). הראו כי $\bigcap_{i \in I} H_i \leq G$.

פתרון נסמן $H = \bigcap_{i \in I} H_i \leq G$. נשתמש בקריטריון המקוצר לתת־חבורות. ראשית נראה כי H לא ריקה: לכל $i \in I$, מתקיים $e_G \in H_i$, כי $H_i \leq G$. לכן איבר זה נמצא בחיתוך של כולם, או: $e_G \in H$, ו־H לא ריקה. נראה כעת סגירות לכפל בהופכי. יהיו $g, h \in H$ ונראה שאכן $gh^{-1} \in H$. נתון כי $g, h \in H$. לפי הגדרת H כחיתוך, נסיק כי לכל $i \in I$ מתקיים $g, h \in H_i$. בפרט, החבורה H_i סגורה לכפל בהופכי, ולכן $gh^{-1} \in H_i$. טענה זו נכונה לכל $i \in I$, ולכן נכונה גם בחיתוך של כולן, H. מצאנו כי $gh^{-1} \in H$. בכך הושלם השימוש בקריטריון המקוצר לתת־חבורות, ואכן $H \leq G$. ■

* להגשה עד ג' בטבת (25 דצמ')

3. תהי G חבורה סופית, ו־H תת־קבוצה לא ריקה של G הסגורה לכפל[1]. הוכיחו כי H תת־חבורה של G.

רמז השתמשו בקריטריון **הארוך** לתת־חבורות.[2]

פתרון כבר נתון כי H היא תת־קבוצה לא ריקה וסגורה לכפל. נותר רק להראות כי היא סגורה להיפוך. יהי $g \in H$ נתון. נביט בקבוצת החזקות הטבעיות של g, $A = \{h \in G | \exists n, h = g^n\}$. קבוצה זו מוכלת כמובן ב־H, כי זהו כפל סופי של איברים ב־H. בנוסף, קבוצה זו סופית, כי היא תת־קבוצה של קבוצה סופית. לכן קיימים $n_1 \neq n_2$ כך ש־$g^{n_1} = g^{n_2}$, לפי עקרון שובך היונים. נסמן $n = |n_1 - n_2| > 0$. אזי $g^n = 1$. נכפיל משוואה זו ב־g^{-1} בצד ימין, ונקבל $g^{-1} = g^{n-1} \in A$.[3] אם כן, ההופכי של g נמצא בקבוצה הנ"ל, ובפרט ב־H. מצאנו כאן כי H סגורה להיפוך איברים, והשלמנו את תנאי הקריטריון הארוך לתת־חבורות. ■

4. נניח $a \in H \leq G$[4]. הוכיחו כי הסדר של האיבר a בחבורה G שווה לסדרו בחבורה H.

פתרון נביט ב־$\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$. זו תת־חבורה של H, ולכן גם תת־חבורה של G. למעשה, $\langle a \rangle \subseteq H \cap G$, ולכן לא יכול להיות שקיים n_G כך שב־G $a^{n_G} = 1$ אבל לא ב־H או להיפך. מכאן עולה כי כל הפתרונות של המשוואה $a^n = 1$ הם זהים, בין אם נעבוד ב־H או ב־G. בפרט הפתרון החיובי־ממש הנמוך ביותר הוא זהה. בנוסחא:

$$o_G(a) = \min\{n \in \mathbb{N} : a^n = e_G\} \overset{e_G = e_H}{=} \min\{n \in \mathbb{N} : a^n = e_H\} = o_H(g)$$

■

5. תהיינה $(G, \bullet), (H, *)$ חבורות (לא קשורות זו לזו). נגדיר את **המכפלה הקרטזית** של החבורות G ו־H להיות החבורה $G \times H$ עם הפעולה $\odot$ כדלהלן:

$$\forall g_1, g_2 \in G, \forall h_1, h_2 \in H, \quad (g_1, h_1) \odot (g_2, h_2) = (g_1 \bullet g_2, h_1 * h_2)$$

הוכיחו כי זו אכן חבורה.

הערה 0.1 אנו צפויים לשוב ולהשתמש פעמים רבות במושג זה במהלך הקורס. בכל פעם שנדבר על החבורה $G \times H$ אנו נתכוון לפעולה הזו.

פתרון לפי הגדרת חבורה, עלינו לבדוק התכונות הבאות: הפעולה מוגדרת, אסוציטיבית, קיים איבר יחידה, וכל האיברים הפיכים.

---

[1] לכל $h_1, h_2 \in H$ מתקיים $h_1 h_2 \in H$/

[2] הקריטריון הארוך לתת־חבורות הוא כדלהלן: תהי H תת־קבוצה לא ריקה של החבורה G. אזי H היא תת־חבורה של G א.ס.ס.

(א) $\forall h_1, h_2 \in H, h_1 h_2 \in H$.

(ב) $\forall h \in H, h^{-1} \in H$.

[3] ההנחה כי $g^{n-1} \in A$ נובעת מכך ש־$n - 1$ הוא טבעי. אבל אם $n = 1$, זה לא נכון. צריך לנמק מקרה זה אחרת: נניח כי $g^1 = 1$. אזי $g^{-1} = g^1 \in A$. ההמשך נשאר כשהיה.

[4] דהיינו G חבורה, H תת־חבורה של G, ו־a איבר של H.

- מוגדרות: יהיו $(g_1,h_1),(g_2,h_2)\in G\times H$ נתונים. אזי

$$(g_1,h_1)\odot(g_2,h_2)=(g_1\bullet g_2,h_1*h_2)$$

ולפי הגדרת הפעולות בחבורות הנתונות בשאלה, הפעולה מוגדרת.

- אסוציטיביות: יהיו $(g_1,h_1),(g_2,h_2),(g_3,h_3)\in G\times H$.

$$\begin{aligned}\Big[(g_1,h_1)\odot(g_2,h_2)\Big]\odot(g_3,h_3)&=(g_1\bullet g_2,h_1*h_2)\odot(g_3,h_3)\\&=([g_1\bullet g_2]\bullet g_3,[h_1*h_2]*h_3)\\&=(g_1\bullet[g_2\bullet g_3],h_1*[h_2*h_3])\\&=(g_1,h_1)\odot(g_2\bullet g_2,h_2*h_3)\\&=(g_1,h_1)\odot\Big[(g_2,h_2)\odot(g_3,h_3)\Big]\end{aligned}$$

- איבר יחידה: האיבר הוא (e_G,e_H). ואכן, לכל $(g,h)\in G\times H$ מתקיים

$$(g,h)\odot(e_G,e_H)=(g\bullet e_G,h*e_H)=(g,h)$$

הכפל בכיוון השני דומה.

- האיברים הפיכים: ניקח $(g,h)\in G\times H$ איבר כללי של החבורה. אזי ההופכי לו הוא $\left(g^{-1},h^{-1}\right)\in G\times H$ (פעולת ההופכי מוגדרת כאן בתוך החבורות G ו־H). נראה זאת:

$$\left(g^{-1},h^{-1}\right)\odot(g,h)=\left(g^{-1}\bullet g,h^{-1}*h\right)=(e_G,e_H)$$

הכפל בכיוון השני דומה.

לסיכום, עברנו על כל תכונות של חבורה, והראנו כי החבורה $G\times H$ מקיימת אותן, אחת לאחת. אם כן, זו חבורה, כנדרש. ■

6. תהי $G=\langle g\rangle$ חבורה ציקלית מסדר 12, ונסמן $H_1=\left\langle g^3\right\rangle$, $H_2=\left\langle g^4\right\rangle$. חשבו את האינדקסים של התת־חבורות האלו ב־G, ורשמו את כל הקוסטים השמאליים שלהן.

פתרון נתחיל ב־H_1. לפי לגרנז', $[G:H_1]=\frac{|G|}{|H|}=\frac{12}{4}=3$. יש לנו שלושה קוסטים שמאליים. לצורך חישוב הקוסטים, נתחיל ברישום של איברי התת־חבורה $H_1=\left\{g^3,g^6,g^9,e\right\}$. כמובן, זהו אחד הקוסטים. נבחר בכל שלב איבר אחר של G שלא רשמנו לפני כן, ונמשיך עד שלא יוותרו איברים שלא נרשמו, ונקבל את מספר הקוסטים הנדרש.

$$\begin{aligned}eH_1&=H_1=\left\{g^3,g^6,g^9,e\right\}\\gH_1&=\left\{g,g^4,g^7,g^{10}\right\}\\g^2H_1&=\left\{g^2,g^5,g^8,g^{11}\right\}\end{aligned}$$

כעת, נעבוד באופן דומה על $H_2 = \{e, g^4, g^8\}$. האינדקס הוא $[G: H_2] = \frac{12}{3} = 4$. ארבעת הקוסטים הם:

$$\begin{aligned} eH_2 &= H_2 = \{e, g^4, g^8\} \\ gH_2 &= \{g, g^5, g^9\} \\ g^2H_2 &= \{g^2, g^6, g^{10}\} \\ g^3H_2 &= \{g^3, g^7, g^{11}\} \end{aligned}$$

לסיום, נזכיר כי על ידי ההומומורפיזם $g^k \mapsto k + 12\mathbb{Z}$ ניתן למצוא איזומורפיזם $G \cong \mathbb{Z}/12\mathbb{Z} = \mathbb{Z}_{12}$, וניתן לחשוב מחדש על כל החישובים בהתאם לאיזומורפיזם זה. ■

תזכורת (משפט אוילר) יהי $a \in \mathbb{Z}$ ויהי $n \in \mathbb{N}$. אם $(a, n) = 1$ אז

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

תזכורת (משפט פרמה הקטן) יהי $a \in \mathbb{Z}$ ויהי p מספר ראשוני. אם $p \nmid a$ אז

$$a^{p-1} \equiv 1 \pmod{p}$$

7. חשבו: $6^{48} \bmod 11$.

פתרון ראשית נזכיר כי $6^{-1} \equiv 2 \pmod{11}$[5]. לפי משפט פרמה הקטן, לכל $a \in \mathbb{Z} \setminus p\mathbb{Z}$, מתקיים $a^{11-1} = a^{10} \equiv 1 \pmod{11}$. לכן

$$6^{48} = 6^{-2} \cdot 6^{50} \equiv 2^2 \cdot \left(6^{10}\right)^5 \equiv 4 \cdot (1)^5 = 4 \pmod{11}$$

לסיכום, $6^{48} \equiv 4 \pmod{11}$. ■

8. הוכיחו: $n^5 \equiv n \pmod{30}$.

פתרון מכיוון ש־30 הוא מספר פריק, די להראות את קיום הטענה עבור גורמיו, מרוכזים לפי ראשוני. זאת אומרת שדי להוכיח $n^5 \equiv n \pmod{p}$ כאשר $p = 2, 3, 5$. אנו נעבוד עם המשפט פרמה הקטן. המשפט קובע כי עבור p ראשוני, $n^p \equiv n \pmod{p}$. לפיכך

$$\begin{aligned} n^5 = n^2 \cdot n^2 \cdot n &\equiv n^3 = n^2 \cdot n \equiv n^2 \equiv n \pmod{2} \\ n^5 = n^3 \cdot n^2 &\equiv n^3 \equiv n \pmod{3} \\ n^5 &\equiv n \pmod{5} \end{aligned}$$

מכאן נובע כי עבור $p = 2, 3, 5$ מתקיים $p \mid n^5 - n$, ולכן גם עבור $\operatorname{lcm}(2, 3, 5) = 30$ מתקיים $30 \mid n^5 - n$, או $n^5 \equiv n \pmod{30}$. ■

בהצלחה!

[5] לפי אוקלידס הפוך עם 6 ו־11 מקבלים $11 \cdot 1 - 2 \cdot 6 = (11 - 6) - 6 = 5 - 6 = 1$, בדקו! ניתן לגלות גם בניסוי וטעיה, אחרי שהגענו למסקנה שאכן $6 \in U_{11}$.