

## פתרון תרגיל 5 מבוא לתורת החבורות תשע"ט

**שאלה 1.** תהי  $G$  חבורה, ותהי  $N \triangleleft G$ .

א. תהי  $H \leq G$ . הוכיחו כי  $N \cap H \triangleleft H$ .

ב. הוכיחו כי  $Z(N) \triangleleft G$ . שימו לב כי שברור ש- $N \triangleleft Z(N)$ , אבל כאן צריך להראות נורמליות בתוך  $G$ .

פתרון. א. אנחנו כבר יודעים שחיתוך תת-חבורות הוא תת-חבורה. יהי  $x \in N \cap H$  וצריך להוכיח כי לכל  $h \in H$  מתקיים כי  $h^{-1}xh \in N \cap H$ . אם  $x, h \in H$ , אז מפני ש- $H$  סגורה להופכי ולמכפלה ברור כי  $h^{-1}xh \in H$ . נתון כי  $N \triangleleft G$ , ולכן לכל  $g \in G$  מתקיים  $g^{-1}xg \in N$ , ובפרט אם  $g \in H$ . לכן  $h^{-1}xh \in N \cap H$ , כדרוש.

ב. מפני ש- $Z(N) \leq N$  וגם  $N \leq G$ , אז ברור ש- $Z(N) \leq G$ . נותר להראות נורמליות. כלומר צריך להראות שלכל  $g \in G$  מתקיים  $gZ(N)g^{-1} \subseteq Z(N)$ . יהי  $x \in gZ(N)g^{-1}$ . לכן קיים  $z \in Z(N)$  כך ש- $x = gzg^{-1}$ . צריך להראות כי לכל  $n \in N$  מתקיים  $nx = xn$ , כי לפי הגדרת  $Z(N)$ , לכל  $n \in N$  מתקיים  $nz = zn$ . מפני ש- $N$  נורמלית ב- $G$ , אז לכל  $g \in G$  מתקיים כי  $gzg^{-1} \in N$  וגם  $gng^{-1} \in N$ . נסתכל על המשוואה  $ngzg^{-1} = gzg^{-1}n$  ונכפול אותה מימין ב- $g^{-1}$  ומשמאל ב- $g^{-1}$  ונקבל  $g^{-1}ngz = zg^{-1}ng$ . אבל  $g^{-1}ng = n'$  עבור איזשהו  $n' \in N$ . לכן המשוואה שקולה למשוואה  $n'z = zn'$ , והיא מתקיימת כי  $z \in Z(N)$ .

**שאלה 2.** נתבונן בחבורה  $G = \mathbb{Q}/\mathbb{Z}$ .

א. הוכיחו שהסדר של כל איבר ב- $G$  הוא סופי, אבל שישנם איברים בחבורה מסדר גדול כרצוננו.

ב. הראו כי תת-החבורה  $H = \langle \frac{2}{5} + \mathbb{Z}, \frac{3}{14} + \mathbb{Z} \rangle$  (שנוצרת על ידי המחלקות של  $\frac{2}{5}$  ו- $\frac{3}{14}$ ) היא ציקלית. מצאו את האינדקס  $[G : H]$ .

פתרון. א. איבר היחידה בחבורה  $G$  הוא המחלקה  $0 + \mathbb{Z}$ . לכן יש למצוא לכל  $x \in G$  מספר טבעי  $n \in \mathbb{N}$  כך שנקבל  $n \cdot x + \mathbb{Z} = \mathbb{Z}$ . שימו לב כי החבורה חיבורית ולכן למציאת הסדר "העלאה בחזקה" היא כפל ב- $n$ .

כל איבר בחבורה אפשר לרשום בצורה  $x = \frac{a}{b} + \mathbb{Z}$  עבור  $a \in \mathbb{Z}, b \in \mathbb{N}$ . מכאן ניתן לראות כי  $b \cdot (\frac{a}{b} + \mathbb{Z}) = a + \mathbb{Z} = \mathbb{Z}$ . לכן  $x$  הוא לכל היותר מסדר (סופי)  $b$ . נניח כי  $\frac{a}{b}$  הוא שבר מצומצם, ולכן הסדר של  $x$  במקרה זה הוא בדיוק  $b$ . סדרת השברים  $\{\frac{1}{n}\}_{n \in \mathbb{N}}$  מתאימה לסדרה של איברים ב- $G$  שסדרם עולה ממש.

ב. יש להוכיח שקיים  $q \in \mathbb{Q}$  כך שמתקיים  $\langle \frac{2}{5} + \mathbb{Z}, \frac{3}{14} + \mathbb{Z} \rangle = \langle q + \mathbb{Z} \rangle$ . נראה שאפשר לבחור את  $q = \frac{1}{70}$ . בשביל להראות הכלה דו-כיוונית, מספיק להראות הכלה של היוצרים. נשים לב כי  $\frac{1}{70} = 7 \cdot \frac{2}{5} - 13 \cdot \frac{3}{14}$ , ולכן  $\langle \frac{1}{70} + \mathbb{Z} \rangle \subseteq \langle \frac{2}{5} + \mathbb{Z}, \frac{3}{14} + \mathbb{Z} \rangle$ . מצד שני  $\frac{2}{5} = 28 \cdot \frac{1}{70}$ ,  $\frac{3}{14} = 15 \cdot \frac{1}{70}$ , ולכן  $\langle \frac{1}{70} + \mathbb{Z} \rangle = \langle \frac{2}{5} + \mathbb{Z}, \frac{3}{14} + \mathbb{Z} \rangle$ . סדר תת-החבורה  $H$  הוא 70 ואילו  $G$  היא אינסופית, ולכן האינדקס שלה היא אינסופי לפי משפט לגראנז'. בנוגע לאינדקס, אפשר להראות גם שלכל שני מספרים ראשוניים  $p_1 \neq p_2$  שונים שאינם מחלקים את 70 יתקיים כי  $p_1 + H \neq p_2 + H$  ולכן ישנן אינסוף מחלקות שמאליות שונות.

**שאלה 3.** תהינה  $G, H$  חבורות ויהי  $f : G \rightarrow H$  הומומורפיזם. הוכיחו:  $f$  חח"ע אם ורק אם  $\ker f = \{e_G\}$ .

פתרון. לכיוון הראשון, נניח שההומומורפיזם  $f$  חח"ע.  $f$  הומומורפיזם ולכן  $f(e_G) = e_H$ .  $f$  חח"ע ולכן  $e_G$  היחיד שהולך לאיבר  $e_H$ , ולכן  $\ker f = \{e_G\}$ .  
 לכיוון השני, נניח שמתקיים:  $\ker f = \{e_G\}$ . נניח שעבור  $g_1, g_2$  מתקיים  $f(g_1) = f(g_2)$ , ונרצה להראות שגם  $g_1 = g_2$ . אם כן,  $f(g_1) f(g_2)^{-1} = e_H$  ומכיוון שזהו הומומורפיזם מתקיים:  $f(g_1 g_2^{-1}) = e_H$ . לכן  $g_1 g_2^{-1} \in \ker f$  ומהנתון נקבל:  $g_1 g_2^{-1} = e_G$ , ולכן  $g_1 = g_2$ . לכן  $f$  אכן חח"ע.

**שאלה 4.** תהי  $G$  חבורה. נגדיר  $f : G \rightarrow G$  ע"י:  $f(g) = g^2$ .

1. הוכיחו שהפונקציה  $f$  היא הומומורפיזם אם ורק אם  $G$  אבלית.
2. נניח שהחבורה  $G$  אבלית וסופית. הוכיחו שהפונקציה  $f$  היא איזומורפיזם אם ורק אם הסדר של  $G$  הוא אי-זוגי.

פתרון. ב. לכיוון הראשון, נניח שהחבורה אבלית. יהיו  $g, h \in G$ . כעת:  $f(gh) = (gh)^2 = ghgh = g^2 h^2 = f(g) f(h)$ .  
 נניח ש:  $f$  הומומורפיזם. יהיו  $g, h \in G$ . כעת:  $f(gh) = (gh)^2 = ghgh$  וגם  $f(gh) = f(g) f(h) = g^2 h^2$ . כלומר  $ghgh = g^2 h^2$ . נצמצם ונקבל:  $gh = hg$  כלומר  $G$  אבלית.

ב. לכיוון הראשון, נניח שהחבורה מסדר אי-זוגי. מכיוון שהפונקציה היא הומומורפיזם (לפי הסעיף הראשון) והחבורה סופית, מספיק להראות שהפונקציה חח"ע. לשם כך יש להסביר מדוע הגרעין הוא טריוויאלי. נניח בשלילה שקיים  $g \in \ker f$  המקיים  $g \neq e_G$ . מהגדרת הפונקציה,  $e_G = f(g) = g^2$ , ולכן הסדר של  $g$  הוא 2. הסדר של  $g$  מחלק את הסדר של החבורה ולכן הסדר של החבורה הוא זוגי וסתירה.

לכיוון השני, נניח שהפונקציה היא איזומורפיזם. נניח בשלילה שהסדר של החבורה הוא זוגי, לכן יש איבר מסדר 2 (ראינו בתרגול) ולכן  $f$  לא חח"ע (האיבר הזה ואיבר היחידה שניהם בגרעין) וסתירה.

**שאלה 5.** עבור כל אחת מן ההעתקות הבאות קבעו והוכיחו האם היא הומומורפיזם, מונומורפיזם, אפימורפיזם או איזומורפיזם.

א.  $f : \mathbb{C}^* \rightarrow \mathbb{C}^*$  המוגדרת לפי  $f(x) = x^{-3}$ .

ב.  $f_x : G \rightarrow G$  המוגדרת לפי  $f_x(g) = xgx^{-1}$  כאשר  $G$  חבורה ו- $x \in G$  איבר.

ג.  $f : \mathbb{Z} \rightarrow \mathbb{Z}_n \times \mathbb{Z}_n$  המוגדרת לפי  $f(k) = ([k], [k])$ .

פתרון. א. הפונקציה היא אפימורפיזם, אבל לא מונומורפיזם. למשל  $f(1) = f(e^{\frac{2\pi i}{3}}) = 1$ .

ב. הפונקציה הזו היא איזומורפיזם. סוג כזה של איזומורפיזם נקרא אוטומורפיזם פנימי. נראה שאכן מדובר בהומומורפיזם:

$$f_x(gh) = xghx^{-1} = xgx^{-1}xhx^{-1} = f_x(g)f_x(h)$$

כדי לראות ש- $f_x$  הוא חח"ע נשים לב שאם  $xgx^{-1} = e$ , אז  $g = x^{-1}ex = e$  ולכן  $g = e$ . כדי להראות ש- $f_x$  הוא על, יהי  $h \in G$ . נבחר בתור המקור שלו את  $x^{-1}hx$ , ואכן  $f_x(x^{-1}hx) = h$ .

ג. פונקציה זו היא אכן הומומורפיזם. עם זאת, היא לא אפימורפיזם (אלא אם  $n = 1$  ואז זה דבילי. לזוג  $([0], [1])$  למשל אין מקור) ולא מונומורפיזם (למשל  $f(k) = f(k+n)$ ).